(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ

(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ

(11) **1-0040151**

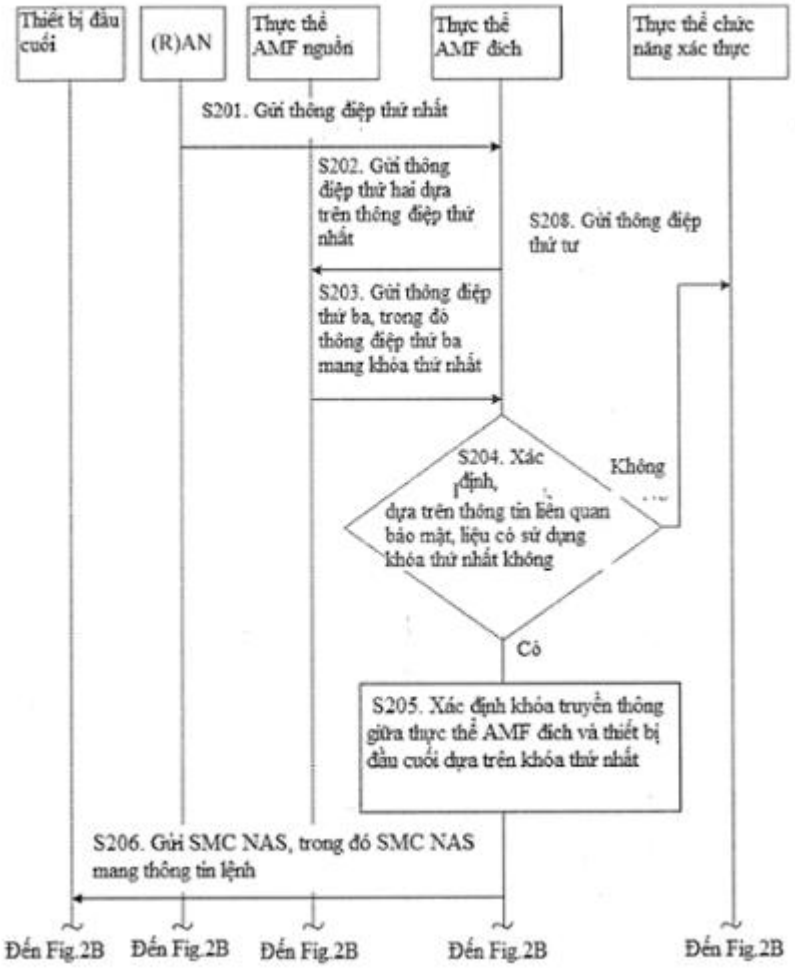
(51)[19] **H04W 12/04**

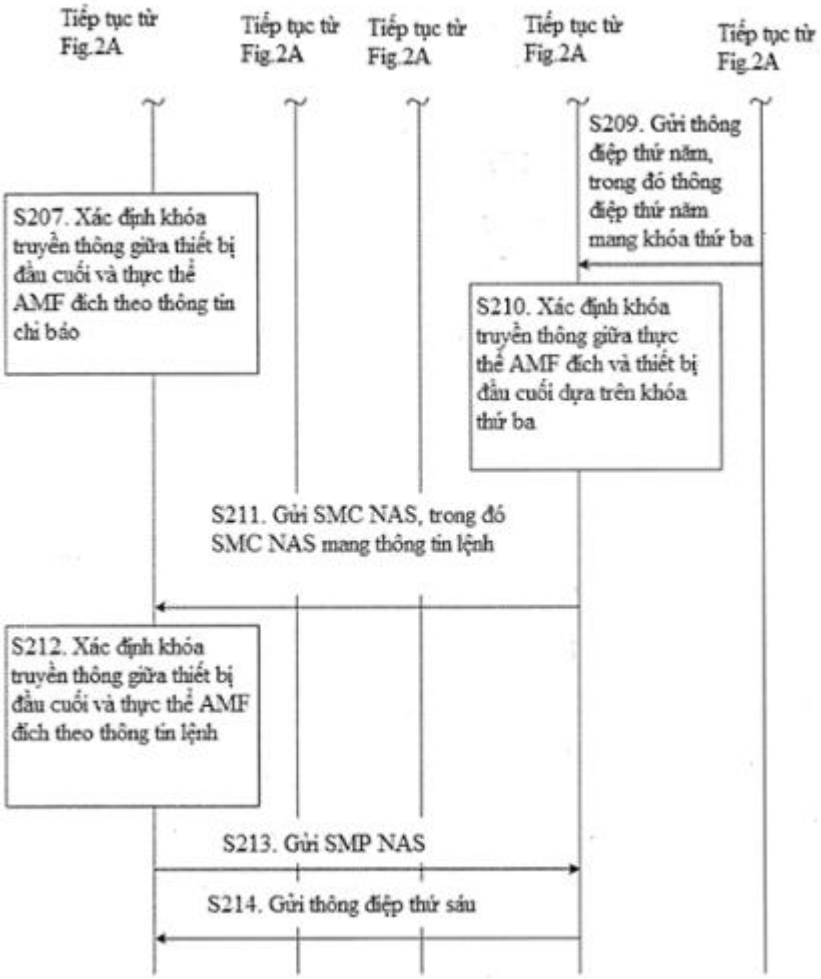
(13) **B**

(21) 1-2019-06436
(22) 04/05/2017
(86) PCT/CN2017/083072 04/05/2017
(87) WO2018/201398 08/11/2018
(45) 25/06/2024 435
(43) 30/01/2020 382A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District Shenzhen, Guangdong 518129, China
(72) CHEN, Jing (CN); PAN, Kai (CN); LI, He (CN).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ THU THẬP KHÓA, PHƯƠNG PHÁP XỬ LÝ BẢO MẬT KHI DI CHUYỂN THIẾT BỊ ĐẦU CUỐI VÀ THIẾT BỊ TRUYỀN THÔNG

(57) Sáng chế đề xuất phương pháp và thiết bị thu thập khóa, thiết bị đầu cuối, vật lưu trữ máy tính đọc được, phương pháp xử lý bảo mật khi di chuyển thiết bị đầu cuối và hệ thống truyền thông. Phương pháp thu thập khóa bao gồm các bước: nhận, bởi thực thể chức năng quản lý di động và truy nhập (access and mobility management function, AMF) đích, thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối; gửi, bởi thực thể AMF đích, thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm bộ nhận dạng (Identifier, ID) của thiết bị đầu cuối; nhận, bởi thực thể AMF đích, thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba mang khóa thứ nhất; xác định, bởi thực thể AMF đích, dựa trên thông tin liên quan đến bảo mật, liệu có sử dụng khóa thứ nhất hay không; và khi thực thể AMF đích xác định sử dụng khóa thứ nhất, xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất.


Thiết bị đầu cuối
(R)AN
Thực thể AMF nguồn
Thực thể AMF đích
Thực thể chức năng xác thực
S201. Gửi thông điệp thứ nhất
S202. Gửi thông điệp thứ hai dựa trên thông điệp thứ nhất
S208. Gửi thông điệp thứ tư
S203. Gửi thông điệp thứ ba, trong đó thông điệp thứ ba mang khóa thứ nhất
S204. Xác định, dựa trên thông tin liên quan bảo mật, liệu có sử dụng khóa thứ nhất không
Không
Có
S205. Xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất
S206. Gửi SMC NAS, trong đó SMC NAS mang thông tin lệnh
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B


Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
S209. Gửi thông điệp thứ năm, trong đó thông điệp thứ năm mang khóa thứ ba
S207. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo
S210. Xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba
S211. Gửi SMC NAS, trong đó SMC NAS mang thông tin lệnh
S212. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin lệnh
S213. Gửi SMP NAS
S214. Gửi thông điệp thứ sáu

Lĩnh vực kỹ thuật của sáng chế

Sáng chế đề cập đến các công nghệ truyền thông, và cụ thể là, đến phương pháp và thiết bị thu thập khóa, thiết bị đầu cuối, vật lưu trữ máy tính đọc được, phương pháp xử lý bảo mật khi di chuyển thiết bị đầu cuối và hệ thống truyền thông.

Tình trạng kỹ thuật của sáng chế

Với sự phát triển của các công nghệ truyền thông, việc bảo mật truyền thông thu hút sự chú ý ngày càng tăng. Hiện tại, bảo mật truyền thông thường được đảm bảo thông qua bảo vệ mật mã hóa và bảo vệ tính toàn vẹn.

Trong hệ thống tiến hóa dài hạn (Long Term Evolution, LTE), điểm kết thúc của tầng không truy nhập (Non Access Stratum, NAS) là thực thể quản trị di động (Mobility Management Entity, MME), và chủ yếu chịu trách nhiệm quản lý di động, quản lý kênh mang, xác thực người dùng, lựa chọn cổng nối phục vụ (Serving Gateway, S-GW), lựa chọn cổng nối mạng dữ liệu gói (Packet Data Network Gateway, P-GW), và tương tự. Trong LTE, nếu MME mà được truy nhập bởi thiết bị người dùng (User Equipment, UE) thay đổi do vị trí của UE thay đổi (ở đây, vị trí của UE ở trạng thái không hoạt động thay đổi), thì MME nguồn cần gửi ngữ cảnh bảo mật của UE đến MME đích, và sau đó khóa truyền thông giữa MME nguồn và UE được sử dụng giữa MME đích và UE.

Trong hệ thống truyền thông di động thế hệ thứ 5 (5th Generation mobile communications, 5G), thực thể chức năng quản lý di động và truy nhập (Access and Mobility Management Function, AMF) là điểm kết thúc của NAS, và chịu trách nhiệm chính để đăng ký, kết nối, quản lý di động, xác thực thông tin thuê bao, và tương tự của UE. Khi thực thể AMF mà được truy nhập bởi UE thay đổi do vị trí của UE thay đổi (ở đây, vị trí của UE ở trạng thái không hoạt động thay đổi), thì thực thể AMF nguồn cần gửi ngữ cảnh bảo mật của UE được lưu

trữ trong thực thể AMF nguồn đến thực thể AMF đích, sao cho UE và thực thể AMF đích có thể tiếp tục truyền thông.

Có thể biết rằng việc truyền ngữ cảnh bảo mật từ một thực thể này sang thực thể khác tồn tại trong cả LTE lẫn mạng thế hệ tiếp theo, và khóa giữa thực thể đích và UE giống như khóa giữa thực thể nguồn và UE. Điều này có thể gây ra nguy cơ bảo mật.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất các phương pháp và các thiết bị thu thập khóa, và các hệ thống truyền thông, để cải thiện bảo mật mạng.

Theo khía cạnh thứ nhất, phương án thực hiện sáng chế đề xuất phương pháp thu thập khóa, phương pháp được thực hiện bởi thực thể AMF đích, và phương pháp bao gồm các bước:

nhận, bởi thực thể AMF đích, thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối;

gửi, bởi thực thể AMF đích, thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm ID của thiết bị đầu cuối;

nhận, bởi thực thể AMF đích, thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai, thông điệp thứ ba mang khóa thứ nhất, và khóa thứ nhất thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối; và

xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa thứ nhất.

Trong phương pháp thu thập khóa nêu trên, thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật bằng cách sử dụng khóa trung gian được gửi bởi thực thể AMF nguồn. Khóa trung gian thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối, và do

vậy thực thể AMF đích không thể biết khóa truyền thông được sử dụng giữa thực thể AMF nguồn và thiết bị đầu cuối. Theo cách này, việc cô lập khóa đạt được giữa thực thể AMF đích và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Theo thiết kế khả thi, phương pháp còn bao gồm các bước: gửi, bởi thực thể AMF đích, lệnh chế độ bảo mật (Security Mode Command, SMC) NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối.

Một cách tùy chọn thông tin liên quan đến bảo mật bao gồm: chính sách được tiền tạo cấu hình, trong đó chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực; hoặc thông tin cô lập khóa của thực thể AMF đích, trong đó thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF đích được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn; hoặc trạng thái bảo mật của thực thể AMF nguồn, trong đó trạng thái bảo mật được sử dụng để chỉ báo liệu thực thể AMF nguồn có bảo mật hay không.

Ngoài ra, việc xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa thứ nhất bao gồm: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu

cuối dựa trên khóa thứ nhất; hoặc khi thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất.

Một cách tùy chọn, việc thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa được nhận từ thực thể AMF nguồn bao gồm: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định, bởi thực thể AMF đích, để sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, xác định, bởi thực thể AMF đích, để sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định, bởi thực thể AMF đích, để sử dụng khóa được nhận từ thực thể AMF nguồn.

Một cách tùy chọn, việc xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất bao gồm các bước: sử dụng, bởi thực thể AMF đích, khóa thứ nhất làm khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối; hoặc dẫn xuất, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất và số ngẫu nhiên của thiết bị đầu cuối; hoặc dẫn xuất, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích; hoặc dẫn xuất, bởi thực thể AMF đích, khóa thứ hai bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất và khóa thứ hai; hoặc dẫn xuất, bởi thực thể AMF đích, khóa thứ hai bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu

cuối, dẫn xuất khóa thứ ba dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ hai và khóa thứ ba.

Theo thiết kế khả thi, khóa thứ nhất thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi, khóa thứ nhất thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

Theo thiết kế khả thi, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là khóa phiên chủ (Master Session Key, MSK), hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên khóa mật mã (Cipher Key, CK) và khóa toàn vẹn (Integrity Key, IK).

Theo khía cạnh thứ hai, phương án thực hiện sáng chế đề xuất phương pháp thu thập khóa, phương pháp được thực hiện bởi thực thể AMF đích, và phương pháp bao gồm các bước:

nhận, bởi thực thể AMF đích, thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối;

gửi, bởi thực thể AMF đích, thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm bộ nhận dạng (Identifier, ID) của thiết bị đầu cuối;

nhận, bởi thực thể AMF đích, thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai;

gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông điệp thứ ba, trong đó thông điệp thứ tư được sử dụng để yêu cầu khóa, và thông điệp thứ tư bao gồm ID của thiết bị đầu cuối;

nhận, bởi thực thể AMF đích, thông điệp thứ năm từ thực thể chức năng xác thực, trong đó thông điệp thứ năm mang khóa thứ nhất, và khóa thứ nhất thu

được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối; và

xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất.

Trong phương pháp thu thập khóa nêu trên, thực thể AMF đích trực tiếp yêu cầu khóa mới từ thực thể chức năng xác thực để xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Theo thiết kế khả thi, phương pháp còn bao gồm các bước: gửi, bởi thực thể AMF đích, SMC NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Theo thiết kế khả thi, việc gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực bao gồm: gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông tin liên quan đến bảo mật; hoặc khi thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa được nhận từ thực thể AMF nguồn, gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực.

Một cách tùy chọn thông tin liên quan đến bảo mật bao gồm: chính sách được tiền tạo cấu hình, trong đó chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực; hoặc thông tin cô lập khóa của thực thể AMF đích, trong đó thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF đích được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn; hoặc trạng thái bảo mật của thực thể AMF nguồn, trong đó trạng thái bảo mật được sử dụng để chỉ báo liệu thực thể AMF nguồn có bảo mật hay không.

Ngoài ra, việc gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể

chức năng xác thực dựa trên thông tin liên quan đến bảo mật bao gồm: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực, gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn, gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn không bảo mật, gửi, bởi thực thể AMF đích, thông điệp thứ tư đến thực thể chức năng xác thực.

Một cách tùy chọn việc thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa được nhận từ thực thể AMF nguồn bao gồm: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực, xác định, bởi thực thể AMF đích, không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn, xác định, bởi thực thể AMF đích, không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn không bảo mật, xác định, bởi thực thể AMF đích, không sử dụng khóa được nhận từ thực thể AMF nguồn.

Theo thiết kế khả thi, việc xác định, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất bao gồm: sử dụng, bởi thực thể AMF đích, khóa thứ nhất làm khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối; hoặc dẫn xuất, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên

khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích; hoặc dẫn xuất, bởi thực thể AMF đích, khóa thứ hai bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất và khóa thứ hai; hoặc dẫn xuất, bởi thực thể AMF đích, khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất và số ngẫu nhiên của thiết bị đầu cuối; or dẫn xuất, bởi thực thể AMF đích, khóa thứ hai bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ ba dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ hai và khóa thứ ba.

Theo thiết kế khả thi, khóa thứ nhất thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi, khóa thứ nhất thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn thông điệp thứ nhất bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là MSK mở rộng (Extended MSK, EMSK), hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Theo khía cạnh thứ ba, phương án thực hiện sáng chế đề xuất phương pháp thu thập khóa, phương pháp được thực hiện bởi thiết bị đầu cuối, và phương pháp bao gồm các bước:

nhận, bởi thiết bị đầu cuối, SMC NAS được gửi bởi thực thể AMF đích, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, hoặc thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối

để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực; và

xác định, bởi thiết bị đầu cuối, khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo.

Trong phương pháp thu thập khóa nêu trên, thiết bị đầu cuối dẫn xuất khóa tương ứng theo SMC NAS được gửi bởi thực thể AMF đích, sao cho khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích được cô lập khỏi khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Theo thiết kế khả thi thứ nhất, việc xác định, bởi thiết bị đầu cuối, khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo bao gồm: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và sử dụng khóa thứ nhất làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và việc sử dụng khóa thứ hai làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Theo thiết kế khả thi thứ hai, SMC NAS còn mang số ngẫu nhiên của thực thể AMF đích. Việc xác định, bởi thiết bị đầu cuối, khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo bao gồm: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa

truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ hai và số ngẫu nhiên của thực thể AMF đích.

Theo thiết kế khả thi thứ ba, SMC NAS còn mang số ngẫu nhiên của thiết bị đầu cuối. Việc xác định, bởi thiết bị đầu cuối, khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo bao gồm: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất và số ngẫu nhiên của thiết bị đầu cuối; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ hai và số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi thứ tư, SMC NAS còn mang số ngẫu nhiên của thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF đích. Việc xác định, bởi thiết bị đầu cuối, khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo bao gồm: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ ba bằng cách sử dụng thuật toán trao

đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất và khóa thứ ba; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ hai và khóa thứ ba.

Theo thiết kế khả thi thứ năm, SMC NAS còn mang số ngẫu nhiên của thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF đích. Việc xác định, bởi thiết bị đầu cuối, khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo bao gồm: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ tư dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ ba bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba và khóa thứ tư; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ năm dựa trên khóa thứ hai và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ ba bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu

cuối và thực thể AMF đích dựa trên khóa thứ ba và khóa thứ năm.

Một cách tùy chọn, việc dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn bao gồm: dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối; hoặc dẫn xuất, bởi thiết bị đầu cuối, khóa thứ nhất dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tùy chọn, việc dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực bao gồm: dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối; hoặc dẫn xuất, bởi thiết bị đầu cuối, khóa thứ hai dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn, SMC NAS còn mang số ngẫu nhiên của thực thể chức năng xác thực.

Theo thiết kế khả thi, trước khi nhận, bởi thiết bị đầu cuối, SMC NAS được gửi bởi thực thể AMF đích, phương pháp còn bao gồm: gửi, bởi thiết bị đầu cuối, thông điệp thứ nhất đến nút mạng truy nhập (access network, AN), trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối; hoặc gửi, bởi thiết bị đầu cuối, thông điệp thứ nhất đến thực thể AMF đích, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối.

Một cách tùy chọn, thông điệp thứ nhất mang số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi, khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK. Khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Theo khía cạnh thứ tư, phương án thực hiện sáng chế đề xuất phương pháp thu thập khóa, phương pháp được thực hiện bởi thực thể chức năng xác thực, và phương pháp bao gồm các bước:

nhận, bởi thực thể chức năng xác thực, thông điệp thứ nhất được gửi bởi thực thể AMF, trong đó thông điệp thứ nhất được sử dụng để yêu cầu khóa, và thông điệp thứ nhất bao gồm ID của thiết bị đầu cuối;

dẫn xuất, bởi thực thể chức năng xác thực, khóa thứ nhất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối; và

gửi, bởi thực thể chức năng xác thực, thông điệp thứ hai đến thực thể AMF, trong đó thông điệp thứ hai mang khóa thứ nhất.

Trong phương pháp thu thập khóa nêu trên, thực thể chức năng xác thực đề xuất khóa mới cho thực thể AMF, sao cho thực thể AMF xác định khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa mới được tạo bởi thực thể chức năng xác thực. Theo cách này, việc cô lập khóa đạt đến giữa các thực thể AMF khác nhau, nhờ đó tránh nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Theo thiết kế khả thi, việc dẫn xuất, bởi thực thể chức năng xác thực, khóa thứ nhất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối bao gồm: dẫn xuất, bởi thực thể chức năng xác thực, khóa thứ nhất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn thông điệp thứ nhất còn bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi, việc dẫn xuất, bởi thực thể chức năng xác thực, khóa thứ nhất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối bao gồm: dẫn xuất, bởi thực thể chức năng xác thực, khóa thứ nhất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Theo khía cạnh thứ năm, để triển khai phương pháp xử lý tối ưu hóa mạng di động nêu trên theo khía cạnh thứ nhất, phương án thực hiện sáng chế đề xuất thiết bị thu thập khóa, và thiết bị có chức năng triển khai phương pháp thu thập khóa nêu trên. Chức năng có thể được triển khai bởi phần cứng, hoặc có thể được triển khai bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều mô đun tương ứng với chức năng nêu trên.

Theo triển khai khả thi của khía cạnh thứ năm, thiết bị bao gồm các môđun hoặc khối chức năng, được tạo cấu hình để triển khai phương pháp thu thập khóa bất kỳ theo khía cạnh thứ nhất.

Theo khía cạnh thứ sáu, phương án thực hiện sáng chế đề xuất thực thể AMF, và cấu trúc của thực thể AMF có thể bao gồm bộ xử lý và bộ thu phát. Bộ xử lý được tạo cấu hình để hỗ trợ thực thể AMF khi thực hiện các chức năng tương ứng trong phương pháp thu thập khóa bất kỳ theo khía cạnh thứ nhất. Bộ thu phát được tạo cấu hình để hỗ trợ truyền thông giữa thực thể AMF và thiết bị mạng khác, và có thể là, chẳng hạn, môđun tần số vô tuyến hoặc môđun băng gốc tương ứng. Thực thể AMF có thể còn bao gồm bộ nhớ. Bộ nhớ được tạo cấu hình để được ghép nối với bộ xử lý, và lưu trữ lệnh chương trình và dữ liệu được yêu cầu bởi thực thể AMF để thực hiện phương pháp thu thập khóa nêu trên.

Theo khía cạnh thứ bảy, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bởi thực thể AMF đích nêu trên. Vật lưu trữ máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh thứ nhất.

Theo khía cạnh thứ tám, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính, bao gồm lệnh. Khi chương trình máy tính được thực hiện bởi máy tính, lệnh cho phép máy tính có thể thực hiện các chức năng được thực hiện bởi thực thể AMF đích ở phương pháp nêu trên.

Theo khía cạnh thứ chín, để triển khai phương pháp thu thập khóa nêu trên theo khía cạnh thứ hai, phương án thực hiện sáng chế đề xuất thiết bị thu thập khóa, và thiết bị có chức năng triển khai phương pháp thu thập khóa nêu trên. Chức năng có thể được triển khai bởi phần cứng, hoặc có thể được triển khai

bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều mô đun tương ứng với chức năng nêu trên.

Theo triển khai khả thi của khía cạnh thứ chín, thiết bị bao gồm các môđun hoặc khối chức năng, được tạo cấu hình để triển khai phương pháp thu thập khóa bất kỳ theo khía cạnh thứ hai.

Theo khía cạnh thứ mười, phương án thực hiện sáng chế đề xuất thực thể AMF, và cấu trúc của thực thể AMF có thể bao gồm bộ xử lý và bộ thu phát. Bộ xử lý được tạo cấu hình để hỗ trợ thực thể AMF khi thực hiện các chức năng tương ứng trong phương pháp thu thập khóa bất kỳ theo khía cạnh thứ hai. Bộ thu phát được tạo cấu hình để hỗ trợ truyền thông giữa thực thể AMF và thiết bị mạng khác, và có thể là, chẳng hạn, môđun tần số vô tuyến hoặc môđun băng gốc tương ứng. Thực thể AMF có thể còn bao gồm bộ nhớ. Bộ nhớ được tạo cấu hình để được ghép nối với bộ xử lý, và lưu trữ lệnh chương trình và dữ liệu được yêu cầu bởi thực thể AMF để thực hiện phương pháp thu thập khóa nêu trên.

Theo khía cạnh thứ mười một, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bởi thực thể AMF đích nêu trên. Vật lưu trữ máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh thứ hai.

Theo khía cạnh thứ mười hai, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính, bao gồm lệnh. Khi chương trình máy tính được thực hiện bởi máy tính, lệnh cho phép máy tính có thể thực hiện các chức năng được thực hiện bởi thực thể AMF đích ở phương pháp nêu trên.

Theo khía cạnh thứ mười ba, để triển khai phương pháp thu thập khóa nêu trên theo khía cạnh thứ ba, phương án thực hiện sáng chế đề xuất thiết bị thu thập khóa, và thiết bị có chức năng triển khai phương pháp thu thập khóa nêu trên. Chức năng có thể được triển khai bởi phần cứng, hoặc có thể được triển khai bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều mô đun tương ứng với chức năng nêu trên.

Theo triển khai khả thi của khía cạnh thứ mười ba, thiết bị bao gồm các môđun hoặc khối chức năng, được tạo cấu hình để triển khai phương pháp thu

thập khóa bất kỳ theo khía cạnh thứ ba.

Theo khía cạnh thứ mười bốn, phương án thực hiện sáng chế đề xuất thiết bị đầu cuối, và cấu trúc của thiết bị đầu cuối có thể bao gồm bộ xử lý và bộ thu phát. Bộ xử lý được tạo cấu hình để hỗ trợ thiết bị đầu cuối khi thực hiện các chức năng tương ứng trong phương pháp thu thập khóa bất kỳ theo khía cạnh thứ ba. Bộ thu phát được tạo cấu hình để hỗ trợ truyền thông giữa thiết bị đầu cuối và thiết bị mạng khác, và có thể là, chẳng hạn, môđun tần số vô tuyến hoặc môđun băng gốc tương ứng. Thiết bị đầu cuối có thể còn bao gồm bộ nhớ. Bộ nhớ được tạo cấu hình để được ghép nối với bộ xử lý, và lưu trữ lệnh chương trình và dữ liệu được yêu cầu bởi thiết bị đầu cuối để thực hiện phương pháp thu thập khóa nêu trên.

Theo khía cạnh thứ mười năm, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bởi thiết bị đầu cuối nêu trên. Vật lưu trữ máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh thứ ba.

Theo khía cạnh thứ mười sáu, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính, bao gồm lệnh. Khi chương trình máy tính được thực hiện bởi máy tính, lệnh cho phép máy tính có thể thực hiện các chức năng được thực hiện bởi thiết bị đầu cuối ở phương pháp nêu trên.

Theo khía cạnh thứ mười bảy, để triển khai phương pháp thu thập khóa nêu trên theo khía cạnh thứ tư, phương án thực hiện sáng chế đề xuất thiết bị thu thập khóa, và thiết bị có chức năng triển khai phương pháp thu thập khóa nêu trên. Chức năng có thể được triển khai bởi phần cứng, hoặc có thể được triển khai bởi phần cứng thực thi phần mềm tương ứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều mô đun tương ứng với chức năng nêu trên.

Theo triển khai khả thi của khía cạnh thứ mười bảy, thiết bị bao gồm các môđun hoặc khối chức năng, được tạo cấu hình để triển khai phương pháp thu thập khóa bất kỳ theo khía cạnh thứ ba.

Theo khía cạnh thứ mười tám, phương án thực hiện sáng chế đề xuất thực thể chức năng xác thực, và cấu trúc của thực thể chức năng xác thực có thể bao gồm bộ xử lý và bộ thu phát. Bộ xử lý được tạo cấu hình để hỗ trợ thực thể

chức năng xác thực khi thực hiện các chức năng tương ứng trong phương pháp thu thập khóa bất kỳ theo khía cạnh thứ tư. Bộ thu phát được tạo cấu hình để hỗ trợ truyền thông giữa thực thể chức năng xác thực và thiết bị mạng khác, và có thể là, chẳng hạn, môđun tần số vô tuyến hoặc môđun băng gốc tương ứng. Thực thể chức năng xác thực có thể còn bao gồm bộ nhớ. Bộ nhớ được tạo cấu hình để được ghép nối với bộ xử lý, và lưu trữ lệnh chương trình và dữ liệu được yêu cầu bởi thực thể chức năng xác thực để thực hiện phương pháp thu thập khóa nêu trên.

Theo khía cạnh thứ mười chín, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính, được tạo cấu hình để lưu trữ lệnh phần mềm máy tính được sử dụng bởi thực thể chức năng xác thực. Vật lưu trữ máy tính bao gồm chương trình được thiết kế để thực hiện khía cạnh thứ tư.

Theo khía cạnh thứ hai mươi, phương án thực hiện sáng chế đề xuất sản phẩm chương trình máy tính, bao gồm lệnh. Khi chương trình máy tính được thực hiện bởi máy tính, lệnh cho phép máy tính có thể thực hiện các chức năng được thực hiện bởi thực thể chức năng xác thực ở phương pháp nêu trên.

Theo khía cạnh thứ hai mươi mốt, phương án thực hiện sáng chế đề xuất hệ thống truyền thông, bao gồm thiết bị đầu cuối có thiết bị thu thập khóa theo khía cạnh thứ mười ba, thực thể AMF đích có thiết bị thu thập khóa theo khía cạnh thứ năm hoặc khía cạnh thứ chín, thực thể chức năng xác thực có thiết bị thu thập khóa theo khía cạnh thứ mười bảy, và thực thể AMF nguồn.

Theo khía cạnh thứ hai mươi hai, phương án thực hiện sáng chế đề xuất hệ thống truyền thông, bao gồm thiết bị đầu cuối theo khía cạnh thứ mười bốn, thực thể AMF đích theo khía cạnh thứ sáu hoặc khía cạnh thứ mười, thực thể chức năng xác thực theo khía cạnh thứ mười tám, và thực thể AMF nguồn.

So với giải pháp kỹ thuật đã biết, trong các phương pháp, các thiết bị, và các hệ thống theo các phương án thực hiện sáng chế, thực thể AMF đích xác định, bằng cách sử dụng khóa trung gian được gửi bởi thực thể AMF nguồn, khóa truyền thông được sử dụng giữa thực thể AMF đích và thiết bị đầu cuối, hoặc thực thể AMF đích yêu cầu khóa mới từ thực thể chức năng xác thực để xác định khóa truyền thông được sử dụng giữa thực thể AMF đích và thiết bị

đầu cuối, và ra lệnh thiết bị đầu cuối dẫn xuất khóa tương ứng. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật mạng.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ kiến trúc của kịch bản ứng dụng theo phương án thực hiện sáng chế;

Fig.2A và Fig.2B là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế;

Fig.3 là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế;

Fig.4A và Fig.4B là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế;

Fig.5 là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế;

Fig.6 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế;

Fig.7 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế;

Fig.8 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế;

Fig.9 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế;

Fig.10 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế;

Fig.11 là sơ đồ cấu trúc của thực thể AMF theo phương án thực hiện sáng chế;

Fig.12 là sơ đồ cấu trúc của thực thể AMF theo phương án thực hiện sáng chế;

Fig.13 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng

chế;

Fig.14 là sơ đồ cấu trúc của thực thể chức năng xác thực theo phương án thực hiện sáng chế; và

Fig.15 là sơ đồ cấu trúc của thực thể AMF theo phương án thực hiện sáng chế.

Mô tả chi tiết sáng chế

Các giải pháp kỹ thuật theo các phương án thực hiện sáng chế áp dụng được cho mạng di động. Mạng di động theo các phương án thực hiện sáng chế là tổ hợp của các loại phần tử mạng di động khác nhau, các mạng truyền, và các hệ thống phụ quản lý mạng. Các loại phần tử mạng di động khác nhau có các chức năng khác nhau, chẳng hạn trạm cơ sở (base station, BS), bộ điều khiển, và mạng lõi (Core Network, CN). Mạng truyền được sử dụng để kết nối với phần tử mạng di động, và hệ thống phụ quản lý mạng được sử dụng để quản lý phần tử mạng di động và mạng truyền.

Thiết bị đầu cuối theo các phương án thực hiện sáng chế có thể là điện thoại thông minh, máy tính tablet, máy tính bảng, UE, hoặc tương tự, hoặc có thể là thiết bị đầu cuối Internet vạn vật (Internet of Things, IoT) chẳng hạn máy đo nước thông minh. Mạng di động và thiết bị đầu cuối được liên kết bằng cách sử dụng giao diện không dây, và các công nghệ không dây có thể được sử dụng bởi giao diện không dây. Theo các phương án thực hiện sáng chế, công nghệ không dây có thể được sử dụng bởi giao diện không dây bao gồm công nghệ 4G, hoặc có thể là 5G hiện đang được nghiên cứu hoặc thậm chí công nghệ truyền thông di động khác được nghiên cứu tiếp theo.

Theo các phương án thực hiện sáng chế, hệ thống dự án hợp tác thế hệ thứ ba (3rd Generation Partnership Project, 3GPP) được thể hiện trên Fig.1 được sử dụng làm ví dụ để mô tả kịch bản ứng dụng của sáng chế. Fig.1 là sơ đồ kiến trúc của kịch bản ứng dụng theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.1, các khối chức năng lôgic trong kiến trúc hệ thống chủ yếu bao gồm:

(1) Mạng truy nhập vô tuyến ((Radio) Access Network, (R)AN): (R)AN để

xuất tài nguyên mạng để truy nhập thiết bị đầu cuối.

(2) Thực thể AMF: Thực thể AMF chủ yếu chịu trách nhiệm cho điểm kết thúc của mặt phẳng điều khiển RAN, điểm kết thúc của báo hiệu không truy nhập, quản lý di động, nghe lén hợp pháp, ủy quyền/xác thực truy nhập, và tương tự.

(3) Thực thể chức năng quản lý phiên (Session Management Function, SMF): Thực thể SMF chịu trách nhiệm chính quản lý phiên, gán và quản lý địa chỉ giao thức Internet (Internet Protocol, IP) của thiết bị đầu cuối, chọn chức năng mặt phẳng người dùng quản lý được, điểm kết thúc của giao diện chức năng tính cước và điều khiển chính sách, thông báo dữ liệu liên kết xuống, và tương tự.

(4) Thực thể chức năng mặt phẳng người dùng (User Plane Function, UPF): Thực thể UPF chịu trách nhiệm chính cho quản lý phiên và kênh mang, gán địa chỉ IP, và tương tự.

(5) Thực thể chức năng máy chủ xác thực (Authentication Server Function, AUSF): Thực thể AUSF chịu trách nhiệm chính cho xác thực người dùng, và tương tự. Thực thể chức năng xử lý và kho lưu trữ ủy nhiệm xác thực (Authentication Credential Repository and Processing Function, ARPF): Thực thể ARPF chịu trách nhiệm chính lưu trữ trạng thái tin cậy bảo mật dài hạn của thiết bị đầu cuối.

(6) Mạng dữ liệu (Data Network, DN): DN là mạng truyền dữ liệu, chẳng hạn mạng Internet.

(7) Thực thể chức năng điều khiển chính sách (Policy Control Function, PCF): Thực thể chức năng bao gồm chức năng quyết định điều khiển chính sách, và chịu trách nhiệm chính tạo chính sách cho mạng.

Nên lưu ý rằng, do cấu trúc 5G không được xác định, kiến trúc theo các phương án thực hiện sáng chế chỉ được sử dụng làm ví dụ để mô tả các giải pháp theo sáng chế. Chẳng hạn, kiến trúc hệ thống có thể còn bao gồm thực thể chức năng neo bảo mật (Security Anchor Function, SEAF) (chịu trách nhiệm chính cho chức năng liên quan đến neo bảo mật mạng), và thực thể SEAF có thể là phần tử mạng độc lập trong kiến trúc hệ thống, hoặc có thể là phần tử

mạng được tích hợp với thực thể mạng hiện tại. Chẳng hạn, thực thể SEAF được tích hợp với thực thể quản lý di động và truy nhập, hoặc có thể được tích hợp với phần tử mạng khác. Do vậy, kiến trúc trong kịch bản ứng dụng nêu trên sẽ không nhằm giới hạn sáng chế.

Theo các phương án thực hiện sau của sáng chế, phần tử mạng được định nghĩa ở mức cao hơn được sử dụng, và được gọi là thực thể chức năng xác thực để biểu diễn thực thể được sử dụng để xác thực chức năng máy chủ, chẳng hạn, AUSF, ARPF, hoặc SEAF. Thực thể chức năng xác thực có thể là phần tử mạng được khai triển trong CN, hoặc có thể là máy chủ ứng dụng nằm ngoài CN, hoặc có thể là chức năng của phần tử mạng hiện tại (chẳng hạn, môđun chức năng bên trong thực thể AUSF hoặc thực thể AMF), hoặc có thể là phần tử mạng tách riêng khác trong tương lai.

Phương pháp thu thập khóa theo các phương án thực hiện sáng chế có thể được áp dụng cho kịch bản truyền thông 5G, hoặc có thể được áp dụng cho kịch bản truyền thông 4G. Khi phương pháp thu thập khóa được sử dụng trong kịch bản 4G, mối quan hệ phần tử mạng tương ứng là: AMF và SMF trong 5G được thay thế bằng MME trong 4G, UPF trong 5G được thay thế bằng S-GW và P-GW trong 4G, và AUSF và ARPF trong 5G được thay thế bằng máy chủ thuê bao tại gia (Home Subscriber Server, HSS) trong 4G.

Phần sau mô tả chi tiết các giải pháp kỹ thuật của sáng chế bằng cách sử dụng các phương án thực hiện cụ thể. Các giải pháp kỹ thuật của sáng chế chủ yếu được áp dụng cho kịch bản chuyển vùng trong đó vị trí của thiết bị đầu cuối ở trạng thái không hoạt động thay đổi. Trong kịch bản này, ngữ cảnh bảo mật của thiết bị đầu cuối có thể được truyền từ một thực thể sang thực thể khác, và khóa giữa thực thể đích và thiết bị đầu cuối giống như khóa giữa thực thể nguồn và thiết bị đầu cuối. Điều này có thể đặt ra nguy cơ bảo mật. Chẳng hạn, khi khóa bị rò, nhà khai thức không thể biết liệu khóa có bị rò rỉ từ thực thể nguồn hoặc thực thể đích, và do vậy các trách nhiệm không thể được phân chia hiệu quả; hoặc nếu một trong thực thể nguồn và thực thể đích bị tấn công, thực thể còn lại cũng bị ảnh hưởng. Do vậy, khi ngữ cảnh bảo mật của thiết bị đầu cuối được truyền từ một thực thể sang thực thể khác, cách thức thực hiện việc

cô lập khóa trở thành vấn đề cấp thiết cần được giải quyết.

Do vậy, các phương án thực hiện sáng chế đề xuất các phương pháp thu thập khóa và các thiết bị, và các hệ thống truyền thông, để cải thiện bảo mật mạng. Các phương án thực hiện cụ thể sau có thể được kết hợp lẫn nhau, và các khái niệm hoặc các quá trình giống nhau hoặc tương tự có thể không được mô tả lặp lại theo một số phương án thực hiện.

Fig.2A và Fig.2B là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế. Các chi tiết như sau:

S201. Thực thể AMF đích nhận thông điệp thứ nhất.

Thông điệp thứ nhất có thể được sử dụng để yêu cầu đăng ký thiết bị đầu cuối, và thông điệp thứ nhất có thể là thông điệp yêu cầu đăng ký.

Trong ví dụ, khi vị trí của thiết bị đầu cuối ở trạng thái không hoạt động thay đổi, thiết bị đầu cuối gửi yêu cầu đăng ký đến (R)AN, và (R)AN lựa chọn thực thể AMF đích cho thiết bị đầu cuối theo yêu cầu đăng ký của thiết bị đầu cuối, và gửi yêu cầu đăng ký của thiết bị đầu cuối đến thực thể AMF đích.

Trong ví dụ khác, (R)AN dò thấy rằng vị trí của thiết bị đầu cuối thay đổi, lựa chọn thực thể AMF đích cho thiết bị đầu cuối dựa trên vị trí hiện tại của thiết bị đầu cuối, và gửi yêu cầu đăng ký đến thực thể AMF đích.

Trong ví dụ khác nữa, (R)AN dò thấy rằng vị trí của thiết bị đầu cuối thay đổi, lựa chọn thực thể AMF đích cho thiết bị đầu cuối dựa trên vị trí hiện tại của thiết bị đầu cuối, và thông báo thiết bị đầu cuối về thực thể AMF đích được chọn, và thiết bị đầu cuối gửi yêu cầu đăng ký đến thực thể AMF đích.

Trong hình vẽ đi kèm (Fig.2A và Fig.2B) tương ứng với phương án thực hiện, ví dụ trong đó (R)AN gửi thông điệp thứ nhất đến thực thể AMF đích được sử dụng để mô tả.

S202. Thực thể AMF đích gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất.

Thông điệp thứ hai có thể được sử dụng để yêu cầu ngữ cảnh bảo mật của thiết bị đầu cuối, và có thể là, chẳng hạn, thông điệp yêu cầu thông tin.

Ngoài ra, thông điệp thứ hai có thể bao gồm ID của thiết bị đầu cuối, chẳng hạn, danh tính người dùng lâu dài hoặc danh tính tạm thời chẳng hạn danh tính

thuê bao di động quốc tế (International Mobile Subscriber Identity, IMSI) hoặc danh tính UE tạm thời duy nhất toàn cục (Globally Unique Temporary UE Identity, GUTI), sao cho thực thể AMF nguồn gửi ngữ cảnh bảo mật tương ứng với ID của thiết bị đầu cuối đến thực thể AMF đích.

S203. Thực thể AMF đích nhận thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba mang khóa thứ nhất.

Thông điệp thứ ba có thể được sử dụng để đáp ứng thông điệp thứ hai, và thông điệp thứ ba có thể được sử dụng để gửi ngữ cảnh bảo mật của thiết bị đầu cuối đến thực thể AMF đích. Chẳng hạn, thông điệp thứ ba là thông điệp đáp ứng thông tin.

Khóa thứ nhất (được gọi là K_{oAMF}' dưới đây) được mang trong thông điệp thứ ba có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa (được gọi là khóa thứ hai dưới đây và được đánh dấu là K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Ngoài ra, khóa thứ nhất có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối, hoặc có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

Khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối. Cụ thể là, khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối có thể là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK. IK và CK có thể được dẫn xuất bởi AUSF hoặc ARPF dựa trên khóa cố định K.

Nên lưu ý rằng khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối là khóa được sử dụng để truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối. Chẳng hạn, thiết bị đầu cuối sử dụng khóa truyền thông để thực hiện xử lý bảo vệ mật mã hóa hoặc xử lý bảo vệ tính toàn vẹn trên dữ liệu hoặc báo hiệu sẽ được gửi bởi thiết bị đầu cuối đến thực thể AMF nguồn, và sau đó gửi dữ liệu hoặc báo hiệu được xử lý đến thực thể AMF nguồn. Các ý nghĩa về

các khóa truyền thông trong bản mô tả là giống nhau, và các chi tiết không được mô tả.

Trong ví dụ, thực thể AMF nguồn có thể dẫn xuất K_{oAMF}' bằng cách sử dụng chức năng dẫn xuất khóa (Key Derivation Function, KDF) dựa trên K_{oAMF}. Theo cách này, bảo mật ngược của khóa có thể được triển khai, cụ thể là, thực thể AMF đích không thể dẫn xuất khóa được sử dụng bởi thực thể AMF nguồn. Chẳng hạn, nếu thực thể AMF nguồn không thể xác định liệu thực thể AMF đích có bảo mật hay không, AMF nguồn có thể sử dụng cách thức này thay cho việc trực tiếp gửi khóa được sử dụng giữa thực thể AMF nguồn và thiết bị đầu cuối đến thực thể AMF đích.

Trong ví dụ khác, khóa thứ nhất có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối. Nói theo cách khác, thực thể AMF nguồn có thể dẫn xuất K_{oAMF}' bằng cách sử dụng KDF dựa trên K_{oAMF} và số ngẫu nhiên của thiết bị đầu cuối.

Số ngẫu nhiên của thiết bị đầu cuối được mang trong thông điệp yêu cầu đăng ký được gửi bởi thiết bị đầu cuối đến (R)AN, và sau đó (R)AN gửi, đến thực thể AMF đích, thông điệp thứ nhất mang số ngẫu nhiên của thiết bị đầu cuối; hoặc số ngẫu nhiên của thiết bị đầu cuối được mang khi thiết bị đầu cuối gửi thông điệp yêu cầu đăng ký của thiết bị đầu cuối đến thực thể AMF đích. Then thực thể AMF đích gửi, đến thực thể AMF nguồn, thông điệp thứ hai mang số ngẫu nhiên của thiết bị đầu cuối, và thực thể AMF nguồn sử dụng số ngẫu nhiên của thiết bị đầu cuối làm tham số đầu vào khi dẫn xuất khóa thứ nhất (K_{oAMF}').

Trong ví dụ khác nữa, khóa thứ nhất thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn. Cụ thể là, thực thể AMF nguồn có thể dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên K_{oAMF} và số ngẫu nhiên của thực thể AMF nguồn. Do khả năng tạo số ngẫu nhiên bởi thiết bị đầu cuối có thể kém hơn khả năng của phía mạng, tức là, tính ngẫu nhiên không đủ mạnh, thực thể AMF nguồn sử dụng số ngẫu nhiên của thực thể

AMF nguồn làm tham số đầu vào khi dẫn xuất khóa thứ nhất (K_{oAMF} '), để tăng cường hiệu ứng cô lập khóa.

Trong trường hợp này, thông điệp thứ ba mà được gửi bởi thực thể AMF nguồn và được nhận bởi thực thể AMF đích ở bước S203 có thể còn mang số ngẫu nhiên của thực thể AMF nguồn.

S204. Thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, liệu có sử dụng khóa thứ nhất hay không.

Nếu khóa thứ nhất sẽ được sử dụng, các bước từ S205 đến S207 được thực hiện; nếu khóa thứ nhất không được sử dụng, các bước từ S208 đến S212 được thực hiện.

Thông tin liên quan đến bảo mật có thể bao gồm ít nhất một trong trong chính sách được tiền tạo cấu hình, thông tin cô lập khóa của thực thể AMF đích, và trạng thái bảo mật của thực thể AMF nguồn.

Chính sách được tiền tạo cấu hình được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực.

Thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF đích được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn. Chẳng hạn, khi thực thể AMF đích có thể dẫn xuất khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bằng cách sử dụng khóa được tạo bởi thực thể AMF nguồn, khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn. Khi thực thể AMF đích không thể dẫn xuất khóa giữa thực thể AMF nguồn và thiết bị đầu cuối dựa trên khóa được tạo bởi thực thể AMF nguồn, và thực thể AMF nguồn không thể dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối, khóa của thực thể AMF đích hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn.

Trạng thái bảo mật của thực thể AMF nguồn được sử dụng để chỉ báo liệu thực thể AMF nguồn có bảo mật hay không. Liệu thực thể AMF nguồn có bảo mật hay không có thể là liệu vị trí của thực thể AMF nguồn có bảo mật hay không, liệu thực thể AMF nguồn và thực thể AMF đích có trong cùng miền mạng hay không, liệu thực thể AMF nguồn có đáng tin cậy không, hoặc tương

tự. Chẳng hạn, nếu vị trí của thực thể AMF nguồn có bảo mật hay không, thực thể AMF nguồn có bảo mật hay không, và nếu vị trí của thực thể AMF nguồn không bảo mật, thực thể AMF nguồn không bảo mật; hoặc nếu thực thể AMF nguồn và thực thể AMF đích trong cùng miền mạng, thực thể AMF nguồn có bảo mật hay không, và nếu thực thể AMF nguồn và thực thể AMF đích không trong cùng miền mạng, thực thể AMF nguồn không bảo mật; hoặc nếu thực thể AMF nguồn có đáng tin cậy không, thực thể AMF nguồn có bảo mật hay không, và nếu thực thể AMF nguồn không đáng tin, thực thể AMF nguồn không bảo mật.

Chẳng hạn, bước S204 có thể được triển khai theo các cách sau:

khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, thực thể AMF đích xác định để sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc

khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa của thực thể AMF đích được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, thực thể AMF đích xác định để sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc

khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, thực thể AMF đích xác định để sử dụng khóa được nhận từ thực thể AMF nguồn.

Chẳng hạn, bước S204 có thể được triển khai theo cách khác theo các cách sau:

khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực, thực thể AMF đích xác định không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc

khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa của thực thể AMF đích được sử dụng để chỉ

báo rằng khóa của thực thể AMF đích hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn, thực thể AMF đích xác định không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc

khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn không bảo mật, thực thể AMF đích xác định không sử dụng khóa được nhận từ thực thể AMF nguồn.

Dĩ nhiên, nội dung được bao gồm trong thông tin liên quan đến bảo mật có thể được sử dụng cùng nhau. Chẳng hạn, khi thông tin liên quan đến bảo mật bao gồm chính sách được tiền tạo cấu hình và trạng thái bảo mật của thực thể AMF nguồn, liệu có sử dụng khóa thứ nhất hay không được xác định dựa trên trạng thái bảo mật của thực thể AMF nguồn. Trong ví dụ khác, khi thông tin liên quan đến bảo mật bao gồm thông tin cô lập khóa của thực thể AMF đích và trạng thái bảo mật của thực thể AMF nguồn, nếu thông tin cô lập khóa của thực thể AMF đích chỉ báo rằng khóa của thực thể AMF đích hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn, và trạng thái bảo mật của thực thể AMF nguồn chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, được xác định không sử dụng khóa thứ nhất. Các chi tiết không được mô tả.

S205. Thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất.

S206. Thực thể AMF đích gửi SMC NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo.

Thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối, chẳng hạn, ra lệnh thiết bị đầu cuối dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ hai (K_{oAMF}).

Trong ví dụ, do khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, khi khóa thứ nhất (K_{oAMF}') được dẫn xuất dựa trên khóa truyền thông giữa thực thể AMF

nguồn và thiết bị đầu cuối, thông tin chỉ báo có thể được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối, hoặc được sử dụng để chỉ báo để dẫn xuất khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối dựa trên khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối và sau đó dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối; hoặc khi khóa thứ nhất (K_{oAMF}') được dẫn xuất dựa trên khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối.

S207. Thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo.

S208. Thực thể AMF đích gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Thông điệp thứ tư có thể được sử dụng cho yêu cầu khóa, và có thể là, chẳng hạn, thông điệp yêu cầu khóa, và thông điệp thứ tư có thể mang ID của thiết bị đầu cuối, sao cho thực thể chức năng xác thực thu được, dựa trên ID của thiết bị đầu cuối, khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối (có thể được gọi là khóa thứ tư và được đánh dấu là K_{AUF}).

Khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Chẳng hạn, sau khi thực hiện xác thực thuê bao trên thiết bị đầu cuối, thực thể chức năng xác thực có thể tạo hai khóa (giả sử rằng hai khóa này là khóa A và khóa B), và khóa A được giữ trong thực thể chức năng xác thực. Trong trường hợp này, khóa A có thể được sử dụng làm K_{AUF}, và khóa B được gửi đến phần tử mạng khác (chẳng hạn, AMF/MME).

Trong trường hợp khả thi, giao thức xác thực mở rộng (Extensible Authentication Protocol, EAP) được sử dụng trong quá trình xác thực. Do hai khóa: EMSK và MSK được tạo sau khi hoàn thành xác thực EAP, EMSK có

thể được xem là khóa A, MSK được xem là khóa B, và EMSK được chia sẻ (không được gửi) giữa thực thể chức năng xác thực và thiết bị đầu cuối, và MSK được gửi đến phần tử mạng khác chẳng hạn AMF nguồn. Trong trường hợp này, K_{AUF} có thể là EMSK, và sau đó MSK có thể được xem là K_{oAMF}. Nếu thực thể AMF đích không sử dụng khóa trung gian được dẫn xuất bằng cách sử dụng K_{oAMF}, thực thể AMF đích yêu cầu khóa từ thực thể chức năng xác thực. Nói theo cách khác, khóa mới được dẫn xuất bằng cách sử dụng K_{AUF} được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và AMF nguồn không biết khóa mới được dẫn xuất.

Trong trường hợp khả thi khác, nếu giao thức hệ thống gói tiến hóa (Evolved Packet System, EPS) được sử dụng trong quá trình xác thực, K_{AUF} có thể là khóa được tạo bằng cách sử dụng CK và IK. Cả CK và IK được tạo bằng cách sử dụng khóa cố định K. Chẳng hạn, trong LTE, CK và IK có thể được tạo bằng cách sử dụng khóa cố định K, và sau đó K_{ASME} được tạo bằng cách sử dụng CK và IK. Theo phương án thực hiện, hai khóa K_{ASME} có thể được tạo bằng cách sử dụng CK và IK. Một khóa giống như K_{ASME} trong mạng 4G được chuyển phát đến MME, và khóa còn lại được lưu trữ trong thực thể chức năng xác thực dưới dạng K_{AUF}.

Chẳng hạn, thông điệp thứ ba có thể mang địa chỉ của thực thể chức năng xác thực, và thực thể AMF đích có thể gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên địa chỉ của thực thể chức năng xác thực, hoặc thực thể AMF đích có thể chọn thực thể chức năng xác thực dựa trên ID của thiết bị đầu cuối, và sau đó gửi thông điệp thứ tư đến thực thể chức năng xác thực.

S209. Thực thể AMF đích nhận thông điệp thứ năm được gửi bởi thực thể chức năng xác thực, trong đó thông điệp thứ năm mang khóa thứ ba.

Thông điệp thứ năm có thể được sử dụng để đáp ứng thông điệp thứ tư, và có thể là, chẳng hạn, thông điệp đáp ứng khóa.

Khóa thứ ba (được gọi là K_{AUF}' dưới đây) có thể thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Theo triển khai tùy chọn thứ nhất, thực thể chức năng xác thực có thể dẫn

xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa thứ tư (K_{AUF}).

Theo triển khai tùy chọn thứ hai, khóa thứ ba thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối. Cụ thể là, thực thể chức năng xác thực có thể dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa thứ tư (K_{AUF}) và số ngẫu nhiên của thiết bị đầu cuối.

Số ngẫu nhiên của thiết bị đầu cuối có thể được mang khi thiết bị đầu cuối gửi thông điệp yêu cầu đăng ký đến (R)AN, và sau đó (R)AN gửi, đến thực thể AMF đích, thông điệp thứ nhất mang số ngẫu nhiên của thiết bị đầu cuối; hoặc số ngẫu nhiên của thiết bị đầu cuối có thể được mang khi thiết bị đầu cuối gửi thông điệp yêu cầu đăng ký của thiết bị đầu cuối đến thực thể AMF đích. Sau đó thực thể AMF đích gửi, đến thực thể chức năng xác thực, thông điệp thứ tư mang số ngẫu nhiên của thiết bị đầu cuối, và thực thể chức năng xác thực sử dụng số ngẫu nhiên của thiết bị đầu cuối làm tham số đầu vào khi dẫn xuất khóa thứ ba (K_{AUF}').

Theo triển khai tùy chọn thứ ba, khóa thứ ba thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực. Cụ thể là, thực thể chức năng xác thực có thể dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa thứ tư (K_{AUF}) và số ngẫu nhiên của thực thể chức năng xác thực. Do khả năng tạo số ngẫu nhiên bởi thiết bị đầu cuối có thể kém hơn khả năng của phía mạng, tức là, tính ngẫu nhiên không đủ mạnh, thực thể chức năng xác thực sử dụng số ngẫu nhiên của thực thể chức năng xác thực làm tham số đầu vào khi dẫn xuất khóa thứ ba (K_{AUF}').

S210. Thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba.

S211. Thực thể AMF đích gửi SMC NAS đến thiết bị đầu cuối.

SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức

năng xác thực và thiết bị đầu cuối.

Một cách tùy chọn SMC NAS còn bao gồm ID tập khóa, và ID tập khóa giống như KSI_ASME trong LTE, và được sử dụng để chỉ báo khóa gốc được sử dụng bởi thiết bị đầu cuối để dẫn xuất. ID tập khóa có thể có cùng định dạng với KSI_AMSE.

S212. Thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo chỉ báo thông tin chỉ báo.

Một cách tùy chọn phương pháp có thể còn bao gồm các bước sau:

S213. Thiết bị đầu cuối gửi thông điệp hoàn thành chế độ bảo mật (Security Mode Complete, SMP) NAS đến thực thể AMF đích.

S214. Thực thể AMF đích gửi thông điệp thứ sáu đến thiết bị đầu cuối.

Thông điệp thứ sáu có thể được sử dụng để thông báo thiết bị đầu cuối rằng việc đăng ký của thiết bị đầu cuối được chấp nhận, và có thể là, chẳng hạn, thông điệp chấp nhận đăng ký.

Ở phương pháp thu thập khóa theo phương án thực hiện, thực thể AMF đích xác định động liệu có sử dụng khóa trung gian được gửi bởi thực thể AMF nguồn để xác định khóa truyền thông được sử dụng giữa thực thể AMF đích và thiết bị đầu cuối, hoặc yêu cầu khóa mới từ thực thể chức năng xác thực để xác định khóa truyền thông được sử dụng giữa thực thể AMF đích và thiết bị đầu cuối, và ra lệnh thiết bị đầu cuối để dẫn xuất khóa tương ứng. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật mạng.

Một cách tùy chọn theo kịch bản triển khai thứ nhất của phương án thực hiện nêu trên, S205 đến S207 có thể được triển khai cụ thể theo các cách sau:

Cách thức 1: Trong quá trình triển khai cụ thể của bước S205, thực thể AMF đích sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối.

Trường hợp 1: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất

(K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, và sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Trường hợp 2: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, và sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Trong trường hợp này, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối.

Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn, và sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Trong trường hợp này, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thực thể AMF nguồn.

Nên lưu ý rằng, trong trường hợp 3, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối. Trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối được sử dụng chỉ bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 2: Trong quá trình triển khai cụ thể của S205, thực thể AMF đích

dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối. Ngoài ra, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 1: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 2: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối. Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối. Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 3: Trong quá trình triển khai cụ thể của S205, thực thể AMF đích

dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích. Ngoài ra, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thực thể AMF đích.

Trường hợp 1: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích.

Trường hợp 2: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích. Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Ngoài ra, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 3: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích.

Nên lưu ý rằng, trong trường hợp 3, ở bước S206, SMC NAS được gửi bởi

thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối. Trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối được sử dụng chỉ bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 4: Trong quá trình triển khai cụ thể của S205, thực thể AMF đích dẫn xuất khóa (có thể được gọi là khóa thứ sáu và được đánh dấu làm K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}).

Ngoài ra, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 1: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 2: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết

bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 5: Trong quá trình triển khai cụ thể của S205, thực thể AMF đích dẫn xuất khóa thứ năm (được gọi là K_{nAMF}' dưới đây) dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ năm (K_{nAMF}') và khóa thứ sáu (K_{DH}).

Ngoài ra, ở bước S206, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 1: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu

nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ năm (K_{nAMF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 2: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ năm (K_{nAMF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ nhất (K_{oAMF}') được dẫn xuất bởi thực thể AMF nguồn dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tương ứng, ở bước S207, thiết bị đầu cuối dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ năm (K_{nAMF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong

trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Chẳng hạn, thuật toán trao đổi khóa có thể là thuật toán trao đổi khóa Diffie-Hellman, có thể được gọi tắt là thuật toán trao đổi khóa DH. Nguyên lý triển khai cụ thể của thuật toán trao đổi khóa DH nhất quán với nguyên lý trong công nghệ đã biết, và các chi tiết không được mô tả ở đây.

Một cách tùy chọn, theo kịch bản triển khai thứ hai của phương án thực hiện nêu trên, các bước từ S210 đến S212 có thể được triển khai cụ thể theo các cách sau:

Cách thức 1: Trong quá trình triển khai cụ thể của S210, thực thể AMF đích sử dụng khóa thứ ba (K_{AUF}') làm khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối.

Trường hợp 1: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực, và sử dụng khóa thứ ba (K_{AUF}') as khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Trường hợp 2: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối, và sử dụng khóa thứ ba (K_{AUF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Trong trường hợp này, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối.

Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực, và sử dụng khóa thứ ba (K_{AUF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Trong trường hợp này, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thực thể chức năng xác thực.

Nên lưu ý rằng, trong trường hợp 3, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối. Trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối được sử dụng chỉ bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 2: Trong quá trình triển khai cụ thể của S210, thực thể AMF đích dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối. Ngoài ra, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 1: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 2: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba

(K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối. Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối. Trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 3: Trong quá trình triển khai cụ thể của S210, thực thể AMF đích dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích. Ngoài ra, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thực thể AMF đích.

Trường hợp 1: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích.

Trường hợp 2: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích. Có thể hiểu rằng, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Ngoài ra, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 3: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích.

Nên lưu ý rằng, trong trường hợp 3, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối có thể còn mang số ngẫu nhiên của thiết bị đầu cuối. Trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối được sử dụng chỉ bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 4: Trong quá trình triển khai cụ thể của bước S210, thực thể AMF đích dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}).

Ngoài ra, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 1: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng

xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 2: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba

(K_{AUF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Cách thức 5: Trong quá trình triển khai cụ thể của S210, thực thể AMF đích dẫn xuất khóa (có thể được gọi là khóa thứ bảy và được đánh dấu làm K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ bảy (K_{nAUF}') và khóa thứ sáu (K_{DH}).

Ngoài ra, ở bước S211, SMC NAS được gửi bởi thực thể AMF đích đến thiết bị đầu cuối còn mang số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối.

Trường hợp 1: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ bảy (K_{nAUF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 2: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác

thực và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ bảy (K_{nAUF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Trường hợp 3: Khóa thứ ba (K_{AUF}') được dẫn xuất bởi thực thể chức năng xác thực dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tương ứng, ở bước S212, thiết bị đầu cuối dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể AMF nguồn, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ bảy (K_{nAUF}') và khóa thứ sáu (K_{DH}). Một cách tương tự, trong trường hợp này, số ngẫu nhiên của thiết bị đầu cuối có thể còn được sử dụng bởi thiết bị đầu cuối để dò thấy phát lại, để ngăn ngừa tấn công phát lại.

Nên lưu ý rằng phương án thực hiện không giới hạn lên KDF được sử dụng trong các triển khai nêu trên.

Fig.3 là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế. Ở phương pháp thu thập khóa theo phương án thực hiện, thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa trung gian được gửi bởi thực thể AMF nguồn, và ra lệnh thiết bị đầu cuối dẫn xuất khóa tương ứng. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn. Đối với bước giống hệt hoặc tương tự và danh từ liên quan, tham khảo các phần mô tả của phương án thực hiện nêu trên trên Fig.2A và Fig.2B.

Các chi tiết không được mô tả lại theo phương án thực hiện.

Như được thể hiện trên Fig.3, phương pháp thu thập khóa theo phương án thực hiện bao gồm các bước sau.

S301. Thực thể AMF đích nhận thông điệp thứ nhất.

Thông điệp thứ nhất có thể được sử dụng để yêu cầu đăng ký thiết bị đầu cuối, và có thể là, chẳng hạn, thông điệp yêu cầu đăng ký. Trên Fig.3, ví dụ trong đó (R)AN gửi thông điệp thứ nhất đến thực thể AMF đích được sử dụng để mô tả.

S302. Thực thể AMF đích gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất.

Thông điệp thứ hai có thể được sử dụng để yêu cầu ngữ cảnh bảo mật của thiết bị đầu cuối từ thực thể AMF nguồn, thông điệp thứ hai có thể là thông điệp yêu cầu thông tin, và thông điệp thứ hai bao gồm ID của thiết bị đầu cuối.

S303. Thực thể AMF nguồn dẫn xuất khóa thứ nhất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối.

Một cách tùy chọn thực thể AMF nguồn có thể dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối. Để biết chi tiết tham khảo các phần mô tả liên quan của phương án thực hiện được thể hiện trên Fig.2A và Fig.2B.

Chẳng hạn, thực thể AMF nguồn có thể dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Trong ví dụ khác, thực thể AMF nguồn có thể dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

S304. Thực thể AMF đích nhận thông điệp thứ ba từ thực thể AMF nguồn.

Thông điệp thứ ba có thể được sử dụng để đáp ứng thông điệp thứ hai. Chẳng hạn, ngữ cảnh bảo mật của thiết bị đầu cuối được gửi đến thực thể AMF đích bằng cách sử dụng thông điệp thứ ba. Thông điệp thứ ba có thể là thông điệp đáp ứng thông tin. Thông điệp thứ ba mang khóa thứ nhất (K_{oAMF}'). Để hiểu khóa thứ nhất, tham khảo các phần mô tả liên quan của phương án thực

hiện được thể hiện trên Fig.2A và Fig.2B.

S305. Thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa thứ nhất.

Theo trường hợp khả thi, khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}').

Theo trường hợp khả thi khác, khi thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa được nhận từ thực thể AMF nguồn, thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất.

Đối với triển khai trong đó thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa được nhận từ thực thể AMF nguồn, tham khảo các phần mô tả liên quan của S204 theo phương án thực hiện được thể hiện trên Fig.2A và Fig.2B.

Đối với triển khai trong đó thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}'), tham khảo các phần mô tả liên quan của bước S205. Các chi tiết không được mô tả lại.

S306. Thực thể AMF đích gửi SMC NAS đến thiết bị đầu cuối.

Như được mô tả theo phương án thực hiện nêu trên được thể hiện trên Fig.2A và Fig.2B, SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{oAMF}) giữa thực thể

AMF nguồn và thiết bị đầu cuối.

S307. Thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo.

Đối với bước S307, tham khảo triển khai liên quan của S207. Các chi tiết không được mô tả lại.

Một cách tùy chọn phương pháp còn bao gồm các bước S308 và S309 sau:

S308. Thiết bị đầu cuối gửi NAS SMP đến thực thể AMF đích.

S309. Thực thể AMF đích gửi thông điệp thứ sáu đến thiết bị đầu cuối.

Thông điệp thứ sáu được sử dụng để thông báo thiết bị đầu cuối rằng việc đăng ký của thiết bị đầu cuối được chấp nhận, và thông điệp thứ sáu có thể là thông điệp chấp nhận đăng ký.

Ở phương pháp thu thập khóa theo phương án thực hiện, thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật bằng cách sử dụng khóa trung gian được gửi bởi thực thể AMF nguồn. Khóa trung gian thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối, và do vậy thực thể AMF đích không thể nhận biết khóa truyền thông được sử dụng giữa thực thể AMF nguồn và thiết bị đầu cuối. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Fig.4A và Fig.4B là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế. Ở phương pháp thu thập khóa theo phương án thực hiện, thực thể AMF đích yêu cầu khóa mới từ thực thể chức năng xác thực để xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối, và ra lệnh thiết bị đầu cuối dẫn xuất khóa tương ứng. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn. Đối với bước tương tự hoặc giống hệt và danh từ liên quan, tham khảo các phần mô tả của phương án thực hiện nêu trên trên Fig.2A và Fig.2B. Các chi tiết không được mô tả lại theo phương án thực hiện.

Như được thể hiện trên Fig.4A và Fig.4B, phương pháp thu thập khóa theo

phương án thực hiện bao gồm các bước sau.

S401. Thực thể AMF đích nhận thông điệp thứ nhất.

Thông điệp thứ nhất có thể được sử dụng để yêu cầu đăng ký thiết bị đầu cuối, và thông điệp thứ nhất có thể là thông điệp yêu cầu đăng ký. Trong các hình vẽ đi kèm tương ứng với phương án thực hiện, ví dụ trong đó (R)AN gửi thông điệp thứ nhất đến thực thể AMF đích được sử dụng để mô tả.

S402. Thực thể AMF đích gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất.

Thông điệp thứ hai có thể được sử dụng để yêu cầu ngữ cảnh bảo mật của thiết bị đầu cuối từ thực thể AMF nguồn, thông điệp thứ hai có thể là thông điệp yêu cầu thông tin, và thông điệp thứ hai có thể bao gồm ID của thiết bị đầu cuối.

S403. Thực thể AMF nguồn dẫn xuất khóa thứ nhất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối.

Đối với khóa giữa thực thể AMF nguồn và thiết bị đầu cuối, tham khảo các phần mô tả liên quan của bước 203. Các chi tiết không được mô tả lại.

S404. Thực thể AMF đích nhận thông điệp thứ ba từ thực thể AMF nguồn.

Thông điệp thứ ba có thể mang khóa thứ nhất. Thông điệp thứ ba có thể được sử dụng để đáp ứng thông điệp thứ hai. Chẳng hạn, ngữ cảnh bảo mật của thiết bị đầu cuối được gửi đến thực thể AMF đích bằng cách sử dụng thông điệp thứ ba. Thông điệp thứ ba có thể là thông điệp đáp ứng thông tin, và thông điệp thứ ba mang khóa thứ nhất.

S405. Thực thể AMF đích gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông điệp thứ ba.

Thông điệp thứ tư được sử dụng để yêu cầu khóa, thông điệp thứ tư có thể là thông điệp yêu cầu khóa, và thông điệp thứ tư bao gồm ID của thiết bị đầu cuối.

Thông điệp thứ ba có thể mang địa chỉ của thực thể chức năng xác thực, và thực thể AMF đích có thể gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên địa chỉ. Rõ ràng là, thông điệp thứ ba có thể chỉ được sử dụng để kích hoạt thực thể AMF đích để gửi thông điệp thứ tư, và điều này không bị

giới hạn.

Việc gửi thông điệp thứ tư đến thực thể chức năng xác thực ở bước S405 có thể được triển khai theo cách thức sau:

Cách thức 1: Thực thể AMF đích gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông tin liên quan đến bảo mật.

Để biết thông tin liên quan đến bảo mật, tham khảo các phần mô tả liên quan của phương án thực hiện được thể hiện trên Fig.2A và Fig.2B. Các chi tiết không được mô tả lại.

Trong ví dụ, khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực, thực thể AMF đích gửi thông điệp thứ tư to thực thể chức năng xác thực.

Trong ví dụ khác, khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, thực thể AMF đích gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Trong ví dụ khác nữa, khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn không bảo mật, thực thể AMF đích gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Cách thức 2: Khi thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa được nhận từ thực thể AMF nguồn, thực thể AMF đích gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Đối với triển khai trong đó thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa được nhận từ thực thể AMF nguồn, tham khảo các phần mô tả liên quan của S204 theo phương án thực hiện được thể hiện trên Fig.2A và Fig.2B.

Nên lưu ý rằng gửi thông điệp thứ tư đến thực thể chức năng xác thực ở bước S405 có thể được thay thế bằng cách thức 1 hoặc cách thức 2.

Rõ ràng là, nội dung được bao gồm trong thông tin liên quan đến bảo mật

có thể được sử dụng cùng nhau. Để biết chi tiết, tham khảo các phần mô tả liên quan của bước S204.

S406. Thực thể chức năng xác thực dẫn xuất khóa thứ ba dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Đối với khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối, tham khảo các phần mô tả liên quan của S208. Các chi tiết không được mô tả lại.

Một cách tùy chọn thực thể chức năng xác thực có thể dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối. Để biết chi tiết tham khảo các phần mô tả liên quan của phương án thực hiện được thể hiện trên Fig.2A và Fig.2B.

Một cách tùy chọn thực thể chức năng xác thực có thể dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối. Ngoài ra, thông điệp thứ tư còn bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn thực thể chức năng xác thực có thể dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

S407. Thực thể AMF đích nhận thông điệp thứ năm từ thực thể chức năng xác thực.

Thông điệp thứ năm được sử dụng để đáp ứng thông điệp thứ tư, thông điệp thứ năm có thể là thông điệp đáp ứng khóa, và thông điệp thứ năm mang khóa thứ ba (K_{AUF}').

S408. Thực thể AMF đích xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba.

S409. Thực thể AMF đích gửi SMC NAS đến thiết bị đầu cuối.

Như được mô tả theo phương án thực hiện nêu trên được thể hiện trên Fig.2A và Fig.2B, SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa

thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

S410. Thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo.

Một cách tùy chọn phương pháp còn bao gồm các bước S411 và S412 sau:

S411. Thiết bị đầu cuối gửi NAS SMP đến thực thể AMF đích.

S412. Thực thể AMF đích gửi thông điệp thứ sáu đến thiết bị đầu cuối.

Thông điệp thứ sáu có thể được sử dụng để thông báo thiết bị đầu cuối rằng việc đăng ký của thiết bị đầu cuối được chấp nhận, và có thể là, chẳng hạn, thông điệp chấp nhận đăng ký.

Ở phương pháp thu thập khóa theo phương án thực hiện, thực thể AMF đích trực tiếp yêu cầu khóa mới từ thực thể chức năng xác thực để xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối. Theo cách này, việc cô lập khóa đạt đến giữa thực thể AMF đích và thực thể AMF nguồn, nhờ đó tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Fig.5 là lưu đồ của phương pháp thu thập khóa theo phương án thực hiện sáng chế. Phương pháp thu thập khóa theo phương án thực hiện được thực hiện bởi thiết bị đầu cuối, tức là, phương pháp được sử dụng bởi thiết bị đầu cuối để thu được khóa. Ở phương pháp thu thập khóa theo phương án thực hiện, thiết bị đầu cuối dẫn xuất khóa tương ứng theo SMC NAS được gửi bởi thực thể AMF đích, sao cho khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích được cô lập khỏi khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF nguồn. Đối với bước tương tự hoặc giống hệt và danh từ liên quan, tham khảo các phần mô tả của phương án thực hiện nêu trên trên Fig.2A và Fig.2B. Các chi tiết không được mô tả lại theo phương án thực hiện.

Như được thể hiện trên Fig.5, phương pháp thu thập khóa theo phương án thực hiện bao gồm các bước sau.

S501. Thiết bị đầu cuối nhận SMC NAS được gửi bởi thực thể AMF đích.

SMC NAS có thể mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị

đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, hoặc thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Đối với khóa truyền thông, thông tin chỉ báo, và tham số tương tự, tham khảo các phần mô tả liên quan của phương án thực hiện được thể hiện trên Fig.2A và Fig.2B. Các chi tiết không được mô tả lại.

S502. Thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo SMC NAS.

Khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, đối với quá trình triển khai trong đó thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích, tham khảo các phần mô tả của bước S207 theo phương án thực hiện nêu trên trên Fig.2A và Fig.2B. Các chi tiết không được mô tả lại ở đây.

Khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, đối với quá trình triển khai trong đó thiết bị đầu cuối xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích, tham khảo các phần mô tả của bước S212 theo phương án thực hiện nêu trên trên Fig.2A và Fig.2B. Các chi tiết không được mô tả lại ở đây.

Một cách tùy chọn, trước bước S501, phương pháp còn bao gồm bước sau:

S503. Thiết bị đầu cuối gửi thông điệp thứ nhất đến thực thể AMF đích.

Thông điệp thứ nhất có thể được sử dụng để yêu cầu đăng ký thiết bị đầu cuối, và thông điệp thứ nhất có thể là thông điệp yêu cầu đăng ký.

Trong ví dụ của sáng chế, thiết bị đầu cuối có thể còn gửi thông điệp thứ nhất đến (R)AN, và (R)AN lựa chọn thực thể AMF đích cho thiết bị đầu cuối dựa trên thông điệp thứ nhất, chẳng hạn, có thể lựa chọn thực thể AMF đích dựa trên ID của thiết bị đầu cuối được mang trong thông điệp thứ nhất, hoặc có thể lựa chọn thực thể AMF đích dựa trên loại truy nhập vô tuyến (Radio Access

Type, RAT) hoặc thông tin hỗ trợ lựa chọn lát mạng (Network Slice Selection Assistance information, NSSAI) trong thông điệp thứ nhất, và gửi thông điệp thứ nhất đến thực thể AMF đích.

Ngoài ra, sau bước S503, phương pháp có thể còn bao gồm các bước sau:

S504. Thực thể AMF đích gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất.

Thông điệp thứ hai có thể được sử dụng để yêu cầu ngữ cảnh bảo mật của thiết bị đầu cuối từ thực thể AMF nguồn, thông điệp thứ hai có thể là thông điệp yêu cầu thông tin, và thông điệp thứ hai bao gồm ID của thiết bị đầu cuối.

S505. Thực thể AMF nguồn dẫn xuất khóa thứ nhất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối.

S506. Thực thể AMF nguồn gửi thông điệp thứ ba đến thực thể AMF đích.

Thông điệp thứ ba có thể được sử dụng để đáp ứng thông điệp thứ hai, thông điệp thứ ba có thể được sử dụng để gửi ngữ cảnh bảo mật của thiết bị đầu cuối đến thực thể AMF đích, và thông điệp thứ ba có thể là thông điệp đáp ứng thông tin. Như được mô tả theo phương án thực hiện nêu trên được thể hiện trên Fig.2A và Fig.2B, thông điệp thứ ba mang khóa thứ nhất (K_{oAMF}').

S507. Thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, liệu có sử dụng khóa thứ nhất hay không.

Chẳng hạn, nếu thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa thứ nhất, thông tin chỉ báo được mang trong SMC NAS được gửi bởi thực thể AMF đích và được nhận bởi thiết bị đầu cuối ở bước S501 được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn.

Chẳng hạn, nếu thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa thứ nhất, thông tin chỉ báo được mang trong SMC NAS được gửi bởi thực thể AMF đích và được nhận bởi thiết bị đầu cuối ở bước S501 được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Một cách tùy chọn, phương pháp có thể còn bao gồm các bước sau:

S508. Thiết bị đầu cuối gửi NAS SMP đến thực thể AMF đích.

S509. Thiết bị đầu cuối nhận thông điệp thứ sáu từ thực thể AMF đích.

Thông điệp thứ sáu được sử dụng để thông báo thiết bị đầu cuối rằng việc đăng ký của thiết bị đầu cuối được chấp nhận, và thông điệp thứ sáu có thể là thông điệp chấp nhận đăng ký.

Ở phương pháp thu thập khóa theo phương án thực hiện, thiết bị đầu cuối dẫn xuất khóa tương ứng theo SMC NAS được gửi bởi thực thể AMF đích, sao cho khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích được cô lập khỏi khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF nguồn. Điều này có thể tránh hiệu quả nguy cơ bảo mật theo giải pháp kỹ thuật đã biết và cải thiện bảo mật truyền thông.

Dựa trên ý tưởng giống như ý tưởng của phương pháp nêu trên theo các phương án thực hiện, các phương án thực hiệ sáng chế còn đề xuất các thiết bị thu thập khóa. Các thiết bị có thể được triển khai bằng cách sử dụng phần mềm, phần cứng, hoặc tổ hợp của phần mềm và phần cứng, và có thể được tạo cấu hình để triển khai phương pháp thu thập khóa theo phương pháp nêu trên các phương án thực hiện. Một phần thiết bị tương ứng với phương pháp nêu trên, và nội dung tương ứng và hiệu quả kỹ thuật của bộ phận thiết bị giống như của phương pháp nêu trên và không được mô tả lại ở đây.

Fig.6 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.6, thiết bị có thể được triển khai dưới dạng một phần hoặc tất cả thực thể AMF đích bằng cách sử dụng phần mềm, phần cứng, hoặc tổ hợp của phần mềm và phần cứng. Thiết bị có thể bao gồm môđun nhận 61, môđun gửi 62, và môđun xác định 63.

Môđun nhận 61 được tạo cấu hình để nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối.

Môđun gửi 62 được tạo cấu hình để gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm ID của thiết bị đầu cuối.

Môđun nhận 61 còn được tạo cấu hình để nhận thông điệp thứ ba từ thực

thể AMF nguồn, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai, thông điệp thứ ba mang khóa thứ nhất (K_{oAMF}'), và khóa thứ nhất thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Môđun xác định 63 được tạo cấu hình để xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa thứ nhất (K_{oAMF}').

Chẳng hạn, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Chẳng hạn, thông tin liên quan đến bảo mật có thể bao gồm: chính sách được tiền tạo cấu hình, trong đó chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực; hoặc thông tin cô lập khóa của thực thể AMF đích, trong đó thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF đích được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn; hoặc trạng thái bảo mật của thực thể AMF nguồn, trong đó trạng thái bảo mật được sử dụng để chỉ báo liệu thực thể AMF nguồn có bảo mật hay không.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ

nhất (K_{oAMF}'); hoặc khi thực thể AMF đích xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}').

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể còn được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, xác định sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định sử dụng khóa được nhận từ thực thể AMF nguồn.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể sử dụng khóa thứ nhất (K_{oAMF}') dưới dạng khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}).

Một cách tùy chọn trong ứng dụng thực, môđun xác định 63 có thể dẫn xuất

khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF đích, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ sáu (K_{DH}) và khóa thứ năm (K_{nAMF}').

Trong ứng dụng thực, khóa thứ nhất (K_{oAMF}') có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

Trong ứng dụng thực, khóa thứ nhất (K_{oAMF}') có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

Trong ứng dụng thực, thông điệp thứ nhất có thể bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun gửi 62 có thể còn được tạo cấu hình để gửi SMC NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích bằng cách sử dụng khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Thiết bị thu thập khóa theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể AMF đích ở phương án thực hiện phương pháp được thể hiện trên Fig.2A và Fig.2B hoặc Fig.3. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.7 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.7, thiết bị có thể được triển khai dưới dạng một phần hoặc tất cả thực thể AMF đích bằng cách sử dụng phần mềm, phần cứng, hoặc tổ hợp của phần mềm và phần cứng. Thiết bị có thể bao gồm môđun nhận 71, môđun gửi 72, và môđun xác định 73.

Môđun nhận 71 được tạo cấu hình để nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối.

Môđun gửi 72 được tạo cấu hình để gửi thông điệp thứ hai đến thực thể

AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm ID của thiết bị đầu cuối. Môđun nhận 71 còn được tạo cấu hình để nhận thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai.

Môđun gửi 72 còn được tạo cấu hình để gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông điệp thứ ba, trong đó thông điệp thứ tư được sử dụng để yêu cầu khóa, và thông điệp thứ tư bao gồm ID của thiết bị đầu cuối.

Môđun nhận 71 còn được tạo cấu hình để nhận thông điệp thứ năm từ thực thể chức năng xác thực, trong đó thông điệp thứ năm mang khóa thứ ba (K_{AUF}'), và khóa thứ ba (K_{AUF}') thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Môđun xác định 73 được tạo cấu hình để xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}').

Chẳng hạn, khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Chẳng hạn, môđun gửi 72 có thể được tạo cấu hình cụ thể để: gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông tin liên quan đến bảo mật; hoặc khi môđun xác định 73 xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa được nhận từ thực thể AMF nguồn, gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Trong ứng dụng thực, thông tin liên quan đến bảo mật có thể cụ thể bao gồm: chính sách được tiền tạo cấu hình, trong đó chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực; hoặc thông tin cô lập khóa của thực thể AMF đích, trong đó thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF đích được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn; hoặc trạng thái bảo mật của thực thể AMF nguồn, trong đó trạng thái bảo mật được sử dụng để chỉ báo liệu

thực thể AMF nguồn có bảo mật hay không.

Một cách tùy chọn trong ứng dụng thực, môđun gửi 72 có thể được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực, gửi thông điệp thứ tư đến thực thể chức năng xác thực; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn, gửi thông điệp thứ tư đến thực thể chức năng xác thực; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn không bảo mật, gửi thông điệp thứ tư to thực thể chức năng xác thực.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 73 có thể còn được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF đích và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF đích không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, xác định không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định không sử dụng khóa được nhận từ thực thể AMF nguồn.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 73 có thể sử dụng khóa thứ ba (K_{AUF}') as khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 73 có thể dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 73 có thể dẫn xuất

khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 73 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}).

Một cách tùy chọn trong ứng dụng thực, môđun xác định 73 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, và dẫn xuất khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ sáu (K_{DH}) và khóa thứ bảy (K_{nAUF}').

Một cách tùy chọn khóa thứ ba (K_{AUF}') thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn khóa thứ ba (K_{AUF}') thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn thông điệp thứ nhất bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun gửi 72 có thể còn được tạo cấu hình để gửi SMC NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Thiết bị thu thập khóa theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể AMF đích ở phương án thực hiện phương pháp được thể hiện trên Fig.2A và Fig.2B hoặc Fig.4A và Fig.4B. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương

án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.8 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.8, thiết bị có thể được triển khai dưới dạng một phần hoặc tất cả thiết bị đầu cuối bằng cách sử dụng phần mềm, phần cứng, hoặc tổ hợp của phần mềm và phần cứng. Thiết bị có thể bao gồm môđun nhận 81 và môđun xác định 83.

Môđun nhận 81 được tạo cấu hình để nhận SMC NAS được gửi bởi thực thể AMF đích, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, hoặc thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{AUF}) được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Môđun xác định 83 được tạo cấu hình để xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo.

Chẳng hạn, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Chẳng hạn, khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Theo thiết kế khả thi thứ nhất, môđun xác định 83 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, và sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết

bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{AUF}) được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và sử dụng khóa thứ ba (K_{AUF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Theo thiết kế khả thi thứ hai, môđun xác định 83 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi thứ ba, môđun xác định 83 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích.

Theo thiết kế khả thi thứ tư, môđun xác định 83 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên a số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}); hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}).

Theo thiết kế khả thi thứ năm, môđun xác định 83 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ năm (K_{nAMF}') và khóa thứ sáu (K_{DH}); hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức

năng xác thực, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ sáu (K_{DH}) và khóa thứ bảy (K_{nAUF}').

Một cách tùy chọn trong ứng dụng thực, môđun xác định 83 có thể còn được tạo cấu hình cụ thể để: dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, hoặc dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tùy chọn trong ứng dụng thực, môđun xác định 83 có thể còn được tạo cấu hình cụ thể để: dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối, hoặc dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn thiết bị có thể còn bao gồm môđun gửi 82. Trong ứng dụng thực, môđun gửi 82 có thể được tạo cấu hình để gửi thông điệp thứ nhất đến (R)AN, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối; hoặc gửi thông điệp thứ nhất đến thực thể AMF đích, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối.

Ngoài ra, thông điệp thứ nhất có thể mang số ngẫu nhiên của thiết bị đầu cuối.

Thiết bị thu thập khóa theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thiết bị đầu cuối theo phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.9 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.9, thiết bị có thể được triển khai dưới

dạng một phần hoặc tất cả thực thể AMF nguồn bằng cách sử dụng phần mềm, phần cứng, hoặc tổ hợp của phần mềm và phần cứng. Thiết bị có thể bao gồm môđun nhận 91, môđun gửi 92, và môđun dẫn xuất khóa 93.

Môđun nhận 91 được tạo cấu hình để nhận thông điệp thứ hai từ thực thể AMF đích, trong đó thông điệp thứ hai được sử dụng để yêu cầu ngữ cảnh bảo mật của thiết bị đầu cuối, thông điệp thứ hai có thể là thông điệp yêu cầu thông tin, và thông điệp thứ hai bao gồm ID của thiết bị đầu cuối.

Môđun dẫn xuất khóa 93 được tạo cấu hình để dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Môđun gửi 92 được tạo cấu hình để gửi thông điệp thứ ba đến thực thể AMF đích, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai, thông điệp thứ ba được sử dụng để gửi ngữ cảnh bảo mật của thiết bị đầu cuối đến thực thể AMF đích, thông điệp thứ ba có thể là thông điệp đáp ứng thông tin, và thông điệp thứ ba mang khóa thứ nhất (K_{oAMF}').

Chẳng hạn, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Một cách tùy chọn, trong ứng dụng thực, môđun dẫn xuất khóa 93 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun dẫn xuất khóa 93 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn thông điệp thứ hai có thể mang số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, môđun dẫn xuất khóa 93 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối và

số ngẫu nhiên của thực thể AMF nguồn.

Thiết bị thu thập khóa theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể AMF nguồn ở phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.10 là sơ đồ cấu trúc của thiết bị thu thập khóa theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.10, thiết bị có thể được triển khai dưới dạng một phần hoặc tất cản thực thể chức năng xác thực bằng cách sử dụng phần mềm, phần cứng, hoặc tổ hợp của phần mềm và phần cứng. Thiết bị có thể bao gồm môđun nhận 101, môđun gửi 102, và môđun dẫn xuất khóa 103.

Môđun nhận được tạo cấu hình để nhận thông điệp thứ tư được gửi bởi thực thể AMF, trong đó thông điệp thứ tư được sử dụng để yêu cầu khóa, thông điệp thứ tư có thể là thông điệp yêu cầu khóa, và thông điệp thứ tư bao gồm ID của thiết bị đầu cuối.

Môđun dẫn xuất khóa 103 được tạo cấu hình để dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Môđun gửi 102 được tạo cấu hình để gửi thông điệp thứ năm đến thực thể AMF đích, trong đó thông điệp thứ năm được sử dụng để đáp ứng thông điệp thứ tư, thông điệp thứ năm có thể là thông điệp đáp ứng khóa, và thông điệp thứ năm mang khóa thứ ba (K_{AUF}').

Chẳng hạn, khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Một cách tùy chọn, trong ứng dụng thực, môđun dẫn xuất khóa 103 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Một cách tùy chọn, trong ứng dụng thực, môđun dẫn xuất khóa 103 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng

KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn, thông điệp thứ tư có thể mang số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn, trong ứng dụng thực, môđun dẫn xuất khóa 103 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

Thiết bị thu thập khóa theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể chức năng xác thực ở phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Dựa trên ý tưởng giống như ý tưởng của phương pháp nêu trên các phương án thực hiện, các phương án thực hiện sáng chế còn đề xuất các thiết bị mạng và thiết bị đầu cuối. Các thiết bị mạng và thiết bị đầu cuối có thể được tạo cấu hình để triển khai phương pháp thu thập khóa được nêu ở phương pháp nêu trên các phương án thực hiện. Bộ phận thiết bị tương ứng với phương pháp nêu trên, và nội dung và hiệu quả kỹ thuật tương ứng của bộ phận thiết bị giống như của phương pháp nêu trên và không được mô tả lại ở đây.

Fig.11 là sơ đồ cấu trúc của thực thể AMF theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.11, thực thể AMF bao gồm bộ thu phát 111, bộ nhớ 112, bộ xử lý 113, và ít nhất một đường truyền thông 114.

Bộ nhớ 112 lưu trữ chương trình phần mềm, bộ nhớ 112 có thể bao gồm bộ nhớ RAM cao tốc, và có thể còn bao gồm bộ nhớ bất biến (non-volatile memory, NVM), chẳng hạn, ít nhất một bộ nhớ đĩa từ, và bộ nhớ 112 có thể lưu trữ các chương trình khác nhau, để hoàn thành các chức năng xử lý khác nhau và triển khai các bước phương pháp theo phương án thực hiện. Bộ xử lý 113 được ghép nối với bộ nhớ 112, và đường truyền thông 114 được tạo cấu hình để triển khai kết nối truyền thông giữa các phần tử. Một cách tùy chọn bộ thu phát 111 theo phương án thực hiện có thể là môđun tần số vô tuyến, môđun băng

gốc, hoặc môđun giao diện truyền thông.

Theo phương án thực hiện, bộ thu phát 111 được tạo cấu hình để: nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối; gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm ID của thiết bị đầu cuối; và nhận thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai, thông điệp thứ ba mang khóa thứ nhất (K_{oAMF}'), và khóa thứ nhất (K_{oAMF}') thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Chẳng hạn, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Theo phương án thực hiện, bộ xử lý 113 được tạo cấu hình để xác định khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa thứ nhất (K_{oAMF}').

Chẳng hạn, thông tin liên quan đến bảo mật có thể bao gồm: chính sách được tiền tạo cấu hình, trong đó chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực; hoặc thông tin cô lập khóa của thực thể AMF, trong đó thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn; hoặc trạng thái bảo mật của thực thể AMF nguồn, trong đó trạng thái bảo mật được sử dụng để chỉ báo liệu thực thể AMF nguồn có bảo mật hay không.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là thông tin cô

lập khóa của thực thể AMF và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}'); hoặc khi thực thể AMF xác định, dựa trên thông tin liên quan đến bảo mật, để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}').

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể còn được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, xác định sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định sử dụng khóa được nhận từ thực thể AMF nguồn.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu

nhiên của thực thể AMF và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}).

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 113 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất và số ngẫu nhiên của thực thể AMF, và dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ sáu (K_{DH}) và khóa thứ năm (K_{nAMF}').

Trong ứng dụng thực, khóa thứ nhất (K_{oAMF}') có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

Trong ứng dụng thực, khóa thứ nhất (K_{oAMF}') có thể thu được bởi thực thể AMF nguồn thông qua dẫn xuất dựa trên khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF nguồn.

Trong ứng dụng thực, thông điệp thứ nhất có thể bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ thu phát 111 có thể còn được tạo cấu hình để gửi SMC NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF bằng cách sử dụng khóa (K_{oAMF}) giữa thực thể AMF nguồn và thiết bị đầu cuối.

Thực thể AMF theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi AMF đích ở phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.12 là sơ đồ cấu trúc của thực thể AMF theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.12, thực thể AMF bao gồm bộ thu phát 121, bộ nhớ 122, bộ xử lý 123, và ít nhất một đường truyền thông 124.

Bộ nhớ 122 lưu trữ chương trình phần mềm, bộ nhớ 122 có thể bao gồm bộ nhớ RAM cao tốc, và có thể còn bao gồm NVM, chẳng hạn, ít nhất một bộ nhớ

đĩa từ, và bộ nhớ 122 có thể lưu trữ các chương trình khác nhau, để hoàn thành các chức năng xử lý khác nhau và triển khai các bước phương pháp theo phương án thực hiện. Bộ xử lý 123 được ghép nối với bộ nhớ 122, và đường truyền thông 124 được tạo cấu hình để triển khai kết nối truyền thông giữa các phần tử. Một cách tùy chọn bộ thu phát 111 theo phương án thực hiện có thể là môđun tần số vô tuyến, môđun băng gốc, hoặc môđun giao diện truyền thông trên thiết bị mạng.

Theo phương án thực hiện, bộ thu phát 121 được tạo cấu hình để: nhận thông điệp thứ nhất, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối; gửi thông điệp thứ hai đến thực thể AMF nguồn dựa trên thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm ID của thiết bị đầu cuối; nhận thông điệp thứ ba từ thực thể AMF nguồn, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai; gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông điệp thứ ba, trong đó thông điệp thứ tư được sử dụng để yêu cầu khóa, và thông điệp thứ tư bao gồm ID của thiết bị đầu cuối; và nhận thông điệp thứ năm từ thực thể chức năng xác thực, trong đó thông điệp thứ năm mang khóa thứ ba (K_{AUF}'), và khóa thứ ba (K_{AUF}') thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Theo phương án thực hiện, bộ xử lý 123 được tạo cấu hình để xác định khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}').

Chẳng hạn, khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Chẳng hạn, bộ thu phát 121 có thể được tạo cấu hình cụ thể để: gửi thông điệp thứ tư đến thực thể chức năng xác thực dựa trên thông tin liên quan đến bảo mật; hoặc khi bộ xử lý 123 xác định, dựa trên thông tin liên quan đến bảo mật, không sử dụng khóa được nhận từ thực thể AMF nguồn, gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Chẳng hạn, thông tin liên quan đến bảo mật có thể cụ thể bao gồm: chính

sách được tiền tạo cấu hình, trong đó chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, hoặc chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực; hoặc thông tin cô lập khóa của thực thể AMF, trong đó thông tin cô lập khóa được sử dụng để chỉ báo liệu khóa của thực thể AMF được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn; hoặc trạng thái bảo mật của thực thể AMF nguồn, trong đó trạng thái bảo mật được sử dụng để chỉ báo liệu thực thể AMF nguồn có bảo mật hay không.

Một cách tùy chọn trong ứng dụng thực, bộ thu phát 121 có thể được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể chức năng xác thực, gửi thông điệp thứ tư đến thực thể chức năng xác thực; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF hoàn toàn bị cô lập khỏi khóa của thực thể AMF nguồn, gửi thông điệp thứ tư đến thực thể chức năng xác thực; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn không bảo mật, gửi thông điệp thứ tư đến thực thể chức năng xác thực.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 123 có thể còn được tạo cấu hình cụ thể để: khi thông tin liên quan đến bảo mật là chính sách được tiền tạo cấu hình và chính sách được sử dụng để chỉ báo để sử dụng khóa được nhận từ thực thể AMF nguồn, xác định không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là thông tin cô lập khóa của thực thể AMF và thông tin cô lập khóa được sử dụng để chỉ báo rằng khóa của thực thể AMF không được hoàn toàn cô lập khỏi khóa của thực thể AMF nguồn, xác định không sử dụng khóa được nhận từ thực thể AMF nguồn; hoặc khi thông tin liên quan đến bảo mật là trạng thái bảo mật của thực thể AMF nguồn và trạng thái bảo mật được sử dụng để chỉ báo rằng thực thể AMF nguồn có bảo mật hay không, xác định không sử dụng khóa được nhận từ thực thể AMF nguồn.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 123 có thể sử dụng khóa thứ ba (K_{AUF}') làm khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 123 có thể dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 123 có thể dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 123 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}).

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 123 có thể dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF và số ngẫu nhiên của thiết bị đầu cuối, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF, và dẫn xuất khóa truyền thông giữa thực thể AMF và thiết bị đầu cuối dựa trên khóa thứ sáu (K_{DH}) và khóa thứ bảy (K_{nAUF}').

Một cách tùy chọn khóa thứ ba (K_{AUF}') thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn khóa thứ ba (K_{AUF}') thu được bởi thực thể chức năng xác thực thông qua dẫn xuất dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn thông điệp thứ nhất bao gồm số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ thu phát 121 có thể còn được tạo cấu hình để gửi SMC NAS đến thiết bị đầu cuối, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF dựa

trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Thực thể AMF theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể AMF đích ở phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.13 là sơ đồ cấu trúc của thiết bị đầu cuối theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.13, thiết bị đầu cuối bao gồm bộ thu phát 131, bộ nhớ 132, bộ xử lý 133, và ít nhất một đường truyền thông 134.

Bộ nhớ 132 lưu trữ chương trình phần mềm, bộ nhớ 132 có thể bao gồm bộ nhớ RAM cao tốc, và có thể còn bao gồm NVM, chẳng hạn, ít nhất một bộ nhớ đĩa từ, và bộ nhớ 132 có thể lưu trữ các chương trình khác nhau, để hoàn thành các chức năng xử lý khác nhau và triển khai các bước phương pháp theo phương án thực hiện. Bộ xử lý 133 được ghép nối với bộ nhớ 132, và đường truyền thông 134 được tạo cấu hình để triển khai kết nối truyền thông giữa các phần tử. Môt cách tùy chọn bộ thu phát 131 theo phương án thực hiện có thể là môđun tần số vô tuyến hoặc môđun băng gốc trên thiết bị đầu cuối.

Theo phương án thực hiện, bộ thu phát 131 được tạo cấu hình để nhận SMC NAS được gửi bởi thực thể AMF đích, trong đó SMC NAS mang thông tin chỉ báo, và thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, hoặc thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{AUF}) được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực.

Theo phương án thực hiện, bộ xử lý 133 được tạo cấu hình để xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo.

Chẳng hạn, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo

dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Chẳng hạn, khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Theo thiết kế khả thi thứ nhất, bộ xử lý 133 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thiết bị đầu cuối và thực thể AMF nguồn, và sử dụng khóa thứ nhất (K_{oAMF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa (K_{AUF}) được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và sử dụng khóa thứ ba (K_{AUF}') làm khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích.

Theo thiết kế khả thi thứ hai, bộ xử lý 133 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thiết bị đầu cuối; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thiết bị đầu cuối.

Theo thiết kế khả thi thứ ba, bộ xử lý 133 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa

truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích; hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích.

Theo thiết kế khả thi thứ tư, bộ xử lý 133 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ nhất (K_{oAMF}') và khóa thứ sáu (K_{DH}); hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ ba (K_{AUF}') và khóa thứ sáu (K_{DH}).

Theo thiết kế khả thi thứ năm, bộ xử lý 133 được tạo cấu hình cụ thể để: khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa giữa

thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn, dẫn xuất khóa thứ năm (K_{nAMF}') dựa trên khóa thứ nhất (K_{oAMF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ năm (K_{nAMF}') và khóa thứ sáu (K_{DH}); hoặc khi thông tin chỉ báo được sử dụng để chỉ báo thiết bị đầu cuối để dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực, dẫn xuất khóa thứ bảy (K_{nAUF}') dựa trên khóa thứ ba (K_{AUF}') và số ngẫu nhiên của thực thể AMF đích, dẫn xuất khóa thứ sáu (K_{DH}) bằng cách sử dụng thuật toán trao đổi khóa dựa trên số ngẫu nhiên của thực thể AMF đích và số ngẫu nhiên của thiết bị đầu cuối, và dẫn xuất khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích dựa trên khóa thứ sáu (K_{DH}) và khóa thứ bảy (K_{nAUF}').

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 133 có thể còn được tạo cấu hình cụ thể để: dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thiết bị đầu cuối, hoặc dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa giữa thiết bị đầu cuối và thực thể AMF nguồn và số ngẫu nhiên của thực thể AMF nguồn.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 133 có thể còn được tạo cấu hình cụ thể để: dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thiết bị đầu cuối, hoặc dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa được chia sẻ giữa thiết bị đầu cuối và thực thể chức năng xác thực và số ngẫu nhiên của thực thể chức năng xác thực.

Một cách tùy chọn trong ứng dụng thực, bộ thu phát 131 có thể được tạo cấu hình để gửi thông điệp thứ nhất đến (R)AN, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối; hoặc gửi thông điệp thứ

nhất đến thực thể AMF đích, trong đó thông điệp thứ nhất được sử dụng để yêu cầu đăng ký thiết bị đầu cuối.

Ngoài ra, thông điệp thứ nhất có thể mang số ngẫu nhiên của thiết bị đầu cuối.

Thiết bị đầu cuối theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thiết bị đầu cuối ở phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.14 là sơ đồ cấu trúc của thực thể chức năng xác thực theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.14, thực thể chức năng xác thực bao gồm bộ thu phát 141, bộ nhớ 142, bộ xử lý 143, và ít nhất một đường truyền thông 144.

Bộ nhớ 142 lưu trữ chương trình phần mềm, bộ nhớ 142 có thể bao gồm bộ nhớ RAM cao tốc, và có thể còn bao gồm NVM, chẳng hạn, ít nhất một bộ nhớ đĩa từ, và bộ nhớ 142 có thể lưu trữ các chương trình khác nhau, để hoàn thành các chức năng xử lý khác nhau và triển khai các bước phương pháp theo phương án thực hiện. Bộ xử lý 143 được ghép nối với bộ nhớ 142, và đường truyền thông 144 được tạo cấu hình để triển khai kết nối truyền thông giữa các phần tử. Một cách tùy chọn bộ thu phát 141 theo phương án thực hiện có thể là môđun tần số vô tuyến, môđun băng gốc, hoặc môđun giao diện truyền thông trên thiết bị mạng.

Theo phương án thực hiện, bộ thu phát 141 được tạo cấu hình để nhận thông điệp thứ tư được gửi bởi thực thể AMF, trong đó thông điệp thứ tư được sử dụng để yêu cầu khóa, thông điệp thứ tư có thể là thông điệp yêu cầu khóa, và thông điệp thứ tư bao gồm ID của thiết bị đầu cuối. Bộ xử lý 143 được tạo cấu hình để dẫn xuất khóa thứ ba (K_{AUF}') dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối. Bộ thu phát 141 còn được tạo cấu hình để gửi thông điệp thứ năm đến thực thể AMF đích, trong đó thông điệp thứ năm được sử dụng để đáp ứng thông điệp thứ tư, thông điệp thứ năm có thể là thông điệp đáp ứng khóa, và thông điệp thứ năm mang khóa thứ ba (K_{AUF}').

Chẳng hạn, khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối là EMSK, hoặc khóa được tạo dựa trên EMSK, hoặc khóa được tạo dựa trên CK và IK.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 143 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 143 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn thông điệp thứ tư có thể mang số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 143 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ ba (K_{AUF}') bằng cách sử dụng KDF dựa trên khóa (K_{AUF}) được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối và số ngẫu nhiên của thực thể chức năng xác thực.

Thực thể chức năng xác thực theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể chức năng xác thực ở phương án thực hiện phương pháp nêu trên. Nguyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Fig.15 là sơ đồ cấu trúc của thực thể AMF theo phương án thực hiện sáng chế. Như được thể hiện trên Fig.15, thực thể AMF bao gồm bộ thu phát 151, bộ nhớ 152, bộ xử lý 153, và ít nhất một đường truyền thông 154.

Bộ nhớ 152 lưu trữ chương trình phần mềm, bộ nhớ 152 có thể bao gồm bộ nhớ RAM cao tốc, và có thể còn bao gồm NVM, chẳng hạn, ít nhất một bộ nhớ đĩa từ, và bộ nhớ 152 có thể lưu trữ các chương trình khác nhau, để hoàn thành các chức năng xử lý khác nhau và triển khai các bước phương pháp theo phương án thực hiện. Bộ xử lý 153 được ghép nối với bộ nhớ 152, và đường truyền thông 154 được tạo cấu hình để triển khai kết nối truyền thông giữa các phần tử. Một cách tùy chọn bộ thu phát 151 theo phương án thực hiện có thể là

môđun tần số vô tuyến, môđun băng gốc, hoặc môđun giao diện truyền thông trên thiết bị mạng.

Theo phương án thực hiện, bộ thu phát 151 được tạo cấu hình để nhận thông điệp thứ hai từ thực thể AMF đích, trong đó thông điệp thứ hai được sử dụng để yêu cầu ngữ cảnh bảo mật của thiết bị đầu cuối, thông điệp thứ hai có thể là thông điệp yêu cầu thông tin, và thông điệp thứ hai bao gồm ID của thiết bị đầu cuối. Bộ xử lý 153 được tạo cấu hình để dẫn xuất khóa thứ nhất (K_{oAMF}') dựa trên khóa (K_{oAMF}) giữa thực thể AMF và thiết bị đầu cuối. Bộ thu phát 151 còn được tạo cấu hình để gửi thông điệp thứ ba đến thực thể AMF đích, trong đó thông điệp thứ ba được sử dụng để đáp ứng thông điệp thứ hai, thông điệp thứ ba được sử dụng để gửi ngữ cảnh bảo mật của thiết bị đầu cuối đến thực thể AMF đích, thông điệp thứ ba có thể là thông điệp đáp ứng thông tin, và thông điệp thứ ba mang khóa thứ nhất (K_{oAMF}').

Chẳng hạn, khóa giữa thực thể AMF nguồn và thiết bị đầu cuối bao gồm khóa truyền thông giữa thực thể AMF nguồn và thiết bị đầu cuối hoặc khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối, và khóa được chia sẻ giữa thực thể AMF nguồn và thiết bị đầu cuối là MSK, hoặc khóa được tạo dựa trên MSK, hoặc khóa được tạo dựa trên CK và IK.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 153 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF và thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 153 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF và thiết bị đầu cuối và số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn thông điệp thứ hai có thể mang số ngẫu nhiên của thiết bị đầu cuối.

Một cách tùy chọn trong ứng dụng thực, bộ xử lý 153 có thể được tạo cấu hình cụ thể để dẫn xuất khóa thứ nhất (K_{oAMF}') bằng cách sử dụng KDF dựa trên khóa (K_{oAMF}) giữa thực thể AMF và thiết bị đầu cuối và số ngẫu nhiên của thực thể AMF.

Thực thể AMF theo phương án thực hiện có thể thực hiện các chức năng được thực hiện bởi thực thể AMF nguồn ở phương án thực hiện phương pháp nêu trên. Nuyên lý triển khai và hiệu quả kỹ thuật của phương án thực hiện giống như của phương án thực hiện phương pháp và không được mô tả lại ở đây.

Ngoài ra, phương án thực hiện sáng chế còn đề xuất các hệ thống truyền thông.

Hệ thống truyền thông thứ nhất bao gồm thực thể AMF đích có thiết bị thu thập khóa theo phương án thực hiện nêu trên được thể hiện trên Fig.6 hoặc Fig.7, thực thể AMF nguồn có thiết bị thu thập khóa theo phương án thực hiện nêu trên được thể hiện trên Fig.9, thực thể chức năng xác thực có thiết bị thu thập khóa theo phương án thực hiện nêu trên được thể hiện trên Fig.10, và thiết bị đầu cuối có thiết bị thu thập khóa theo phương án thực hiện nêu trên được thể hiện trên Fig.8.

Hệ thống truyền thông thứ hai bao gồm thực thể AMF đích theo phương án thực hiện nêu trên được thể hiện trên Fig.11 hoặc Fig.12, thực thể AMF nguồn theo phương án thực hiện nêu trên được thể hiện trên Fig.15, thực thể chức năng xác thực theo phương án thực hiện nêu trên được thể hiện trên Fig.14, và thiết bị đầu cuối theo phương án thực hiện nêu trên được thể hiện trên Fig.13.

Các phương pháp hoặc các bước thuật toán được mô tả dựa vào nội dung được bộc lộ theo sáng chế có thể được triển khai bởi phần cứng, có thể được triển khai bởi bộ xử lý bằng cách thực thi lệnh phần mềm, hoặc có thể được triển khai bằng cách sử dụng sản phẩm chương trình máy tính. Lệnh phần mềm có thể bao gồm môđun phần mềm tương ứng. Môđun phần mềm có thể được lưu trữ trong RAM, bộ nhớ nhanh, ROM, EPROM, EEPROM, thanh ghi, đĩa cứng, đĩa cứng tháo được, CD-ROM, hoặc vật lưu trữ ở các dạng khác bất kỳ đã biết theo giải pháp kỹ thuật đã biết. Vật lưu trữ được sử dụng làm ví dụ được ghép nối với bộ xử lý, sao cho bộ xử lý có thể đọc thông tin từ vật lưu trữ, và có thể viết thông tin vào vật lưu trữ. Chắc chắn là, vật lưu trữ có thể là thành phần của bộ xử lý. Bộ xử lý và vật lưu trữ có thể được đặt trong ASIC. Ngoài ra, ASIC có thể được đặt trong UE. Chắc chắn là, bộ xử lý và vật lưu trữ có thể

tồn tại trong UE dưới dạng các thành phần rời rạc.

Các chuyên gia trong lĩnh vực nên hiểu rằng trong một hoặc nhiều ví dụ nêu trên, các chức năng được mô tả theo sáng chế có thể được triển khai bằng cách sử dụng phần cứng, phần mềm, firmware, hoặc tổ hợp bất kỳ của nó. Khi được triển khai bởi phần mềm, các chức năng này có thể được lưu trữ trong vật lưu trữ máy tính đọc được hoặc được truyền dưới dạng một hoặc nhiều lệnh hoặc mã trong vật lưu trữ máy tính đọc được. Vật lưu trữ máy tính đọc được bao gồm vật lưu trữ máy tính và phương tiện truyền thông, và phương tiện truyền thông bao gồm phương tiện bất kỳ cho phép chương trình máy tính được truyền từ một điểm sang điểm khác. Vật lưu trữ có thể là phương tiện khả dụng mà máy tính đa năng hoặc dành riêng truy nhập được.

Theo các phương án thực hiện sáng chế, nên hiểu rằng hệ thống, thiết bị và phương pháp được bộc lộ có thể được triển khai theo các cách thức khác mà không xa rời phạm vi của sáng chế. Chẳng hạn, phương án thực hiện được mô tả chỉ là ví dụ. Chẳng hạn, việc phân chia khối hoặc mô đun chỉ là phân chia chức năng lôgic và có thể là phân chia khác khi triển khai thực. Chẳng hạn, các khối hoặc các thành phần có thể được kết hợp hoặc tích hợp vào hệ thống khác, hoặc một số dấu hiệu có thể bị bỏ qua hoặc không được thực hiện. Các khối được mô tả dưới dạng các phần riêng rẽ có thể hoặc không thể riêng rẽ về mặt vật lý, và các phần được hiển thị dưới dạng các khối có thể hoặc không thể là các khối vật lý, có thể được đặt ở một vị trí, hoặc có thể được phân tán trên các khối mạng. Một số hoặc tất cả các môđun có thể được lựa chọn dựa trên các nhu cầu thực để đạt được các mục đích của các giải pháp theo các phương án thực hiện. Những người có hiểu biết trung bình trong lĩnh vực có thể hiểu và triển khai các phương án thực hiện sáng chế mà không cần nỗ lực sáng tạo.

Ngoài ra, các sơ đồ minh họa hệ thống, thiết bị, phương pháp, và các phương án thực hiện khác có thể được kết hợp hoặc tích hợp với các hệ thống khác, các môđun, các công nghệ hoặc các phương pháp mà không xa rời phạm vi của sáng chế. Ngoài ra, các ghép nối lẫn nhau được hiển thị hoặc đề cập hoặc các ghép nối trực tiếp hoặc kết nối truyền thông có thể được triển khai qua một số giao diện. Các ghép nối gián tiếp hoặc kết nối truyền thông giữa các

thiết bị hoặc các khối có thể được triển khai ở dạng điện tử, cơ khí, hoặc các dạng khác.

Có thể hiểu rằng "các" theo các phương án thực hiện sáng chế đề cập đến hai hoặc nhiều hơn hai. Các phần mô tả chẳng hạn "thứ nhất" và "thứ hai" theo các phương án thực hiện sáng chế chỉ được sử dụng để chỉ báo và phân biệt giữa các đối tượng, không thể hiện chuỗi, không biểu diễn việc số lượng thiết bị hoặc các thông điệp bị giới hạn cụ thể theo các phương án thực hiện sáng chế, chẳng hạn, có thể có một hoặc nhiều khóa thứ nhất, và không giới hạn ở các phương án thực hiện sáng chế.

Cuối cùng, nên lưu ý rằng các phương án thực hiện nêu trên chỉ nhằm mô tả các giải pháp kỹ thuật sáng chế khác thay vì giới hạn sáng chế. Mặc dù sáng chế được mô tả chi tiết dựa vào các phương án thực hiện nêu trên, song những người có hiểu biết trung bình trong lĩnh vực nên hiểu rằng họ vẫn có thể thực hiện các cải biến với các giải pháp kỹ thuật được mô tả theo các phương án thực hiện nêu trên hoặc thay thế tương đương với một số hoặc tất cả các dấu hiệu kỹ thuật của nó, mà không xa rời phạm vi của các giải pháp kỹ thuật theo các phương án thực hiện sáng chế.

YÊU CẦU BẢO HỘ

1. Phương pháp xử lý bảo mật khi thiết bị đầu cuối di chuyển bao gồm các bước:

nhận, bởi thực thể chức năng quản lý di động và truy nhập đích, thông điệp thứ nhất để đăng ký thông điệp đầu cuối;

gửi, bởi thực thể chức năng quản lý di động và truy nhập đích, thông điệp thứ hai đến thực thể chức năng quản lý di động và truy nhập nguồn sau khi nhận thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm định danh của thông điệp đầu cuối; dẫn xuất, bởi thực thể chức năng quản lý di động và truy nhập nguồn, khóa thứ nhất dựa trên khóa giữa thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối, trong đó khóa thứ nhất là để dẫn xuất khóa truyền thông để thực hiện bảo vệ tính toàn vẹn với báo hiệu giữa thực thể chức năng quản lý di động và truy nhập đích và thông điệp đầu cuối;

gửi, bởi thực thể chức năng quản lý di động và truy nhập nguồn, khóa thứ nhất đến thực thể chức năng quản lý di động và truy nhập đích;

xác định, bởi thực thể chức năng quản lý di động và truy nhập đích sau khi nhận khóa thứ nhất, liệu có sử dụng khóa thứ nhất dựa trên thông tin liên quan bảo mật hay không;

xác định, bởi thực thể chức năng quản lý di động và truy nhập đích sau khi xác định sử dụng khóa thứ nhất, khóa truyền thông giữa thực thể chức năng quản lý di động và truy nhập đích và thông điệp đầu cuối dựa trên khóa thứ nhất; và

gửi, bởi thực thể chức năng quản lý di động và truy nhập đích và đến thông điệp đầu cuối, lệnh chế độ bảo mật (security mode command, SMC) tầng không truy nhập (non-access stratum, NAS) mà mang thông tin chỉ báo ra lệnh thông điệp đầu cuối dẫn xuất khóa thứ nhất.

2. Phương pháp theo điểm 1, trong đó phương pháp còn bao gồm các bước:

nhận, bởi thông điệp đầu cuối, NAS SMC;

dẫn xuất, bởi thông điệp đầu cuối, khóa thứ nhất dựa trên khóa giữa thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối; và

dẫn xuất, bởi thông điệp đầu cuối, khóa truyền thông giữa thông điệp đầu cuối và thực thể chức năng quản lý di động và truy nhập đích theo khóa thứ nhất.

3. Phương pháp theo điểm 1, trong đó thông tin liên quan bảo mật bao gồm thông tin cô lập khóa của thực thể chức năng quản lý di động và truy nhập đích.

4. Phương pháp theo điểm 1, trong đó thông tin liên quan bảo mật bao gồm chính sách được tiền cấu hình chỉ báo sử dụng khóa thứ nhất từ thực thể chức năng quản lý di động và truy nhập nguồn.

5. Phương pháp theo điểm 1, trong đó thông điệp thứ hai là để yêu cầu ngữ cảnh bảo mật của thông điệp đầu cuối.

6. Phương pháp theo điểm 1, trong đó khóa thứ nhất bao gồm KoAMF′, trong đó dẫn xuất khóa thứ nhất bao gồm dẫn xuất, bởi thực thể chức năng quản lý di động và truy nhập nguồn, KoAMF′ dựa trên khóa khác (KoAMF) giữa thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối, và trong đó KoAMF′ là để dẫn xuất khóa truyền thông để thực hiện quá trình bảo vệ tính toàn vẹ với báo hiệu giữa thông điệp đầu cuối và thực thể chức năng quản lý di động và truy nhập đích.

7. Phương pháp xử lý bảo mật khi thiết bị đầu cuối di chuyển bao gồm các bước:

nhận, bởi thực thể chức năng quản lý di động và truy nhập đích, thông điệp thứ nhất để đăng ký thông điệp đầu cuối;

gửi, bởi thực thể chức năng quản lý di động và truy nhập đích, thông điệp thứ hai đến thực thể chức năng quản lý di động và truy nhập nguồn sau khi nhận thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm định danh của thông điệp đầu cuối; nhận, bởi thực thể chức năng quản lý di động và truy nhập đích, khóa thứ nhất từ thực thể chức năng quản lý di động và truy nhập nguồn,

trong đó khóa thứ nhất dựa trên khóa giữa thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối;

xác định, bởi thực thể chức năng quản lý di động và truy nhập đích sau khi nhận khóa thứ nhất, liệu có sử dụng khóa thứ nhất dựa trên thông tin liên quan bảo mật;

xác định, bởi thực thể chức năng quản lý di động và truy nhập đích sau khi xác định sử dụng khóa thứ nhất, khóa truyền thông giữa thực thể chức năng quản lý di động và truy nhập đích và thông điệp đầu cuối dựa trên khóa thứ nhất, trong đó khóa truyền thông là để thực hiện bảo vệ tính toàn vẹn với báo hiệu giữa thực thể chức năng quản lý di động và truy nhập đích và thông điệp đầu cuối; và

gửi, bởi thực thể chức năng quản lý di động và truy nhập đích, đến thông điệp đầu cuối, NAS SMC mà mang thông tin chỉ báo ra lệnh thông điệp đầu cuối dẫn xuất khóa thứ nhất.

8. Phương pháp theo điểm 7, trong đó thông tin liên quan bảo mật bao gồm thông tin cô lập khóa của thực thể chức năng quản lý di động và truy nhập đích.

9. Phương pháp theo điểm 7, trong đó thông tin liên quan bảo mật bao gồm chính sách được tiền cấu hình chỉ báo sử dụng khóa thứ nhất từ thực thể chức năng quản lý di động và truy nhập nguồn.

10. Phương pháp theo điểm 7, trong đó thông điệp thứ hai là để yêu cầu ngữ cảnh bảo mật của thông điệp đầu cuối.

11. Phương pháp thu thập khóa bao gồm các bước:

gửi, bởi thiết bị, thông điệp thứ nhất đến thực thể chức năng quản lý di động và truy nhập đích, trong đó thông điệp thứ nhất yêu cầu đăng ký thiết bị;

nhận, bởi thiết bị, NAS SMC từ thực thể chức năng quản lý di động và truy nhập đích, trong đó NAS SMC mang thông tin chỉ báo ra lệnh thiết bị dẫn xuất khóa thứ nhất giữa thiết bị và thực thể chức năng quản lý di động và truy

nhập đích;

dẫn xuất, bởi thiết bị, khóa thứ nhất giữa thiết bị và thực thể chức năng quản lý di động và truy nhập đích dựa trên khóa chia sẻ giữa thực thể chức năng quản lý di động và truy nhập nguồn và thiết bị; và

xác định, bởi thiết bị, khóa truyền thông giữa thiết bị và thực thể chức năng quản lý di động và truy nhập đích theo khóa thứ nhất,

trong đó khóa truyền thông là để thực hiện bảo vệ tính toàn vẹn với báo hiệu giữa thực thể chức năng quản lý di động và truy nhập đích và thiết bị.

12. Phương pháp thu thập khóa theo điểm 11, trong đó phương pháp còn bao gồm bước gửi, bởi thiết bị, thông điệp hoàn thành chế độ bảo mật NAS đến thực thể chức năng quản lý di động và truy nhập đích.

13. Phương pháp thu thập khóa theo điểm 12, trong đó phương pháp còn bao gồm bước nhận, bởi thiết bị, thông điệp từ thực thể chức năng quản lý di động và truy nhập đích, trong đó thông điệp thông báo thiết bị rằng đăng ký của thiết bị được chấp nhận.

14. Thiết bị thu thập khóa bao gồm:

bộ xử lý được ghép nối với bộ nhớ lưu trữ các lệnh và được tạo cấu hình để thực thi các lệnh để khiến thiết bị thu thập khóa:

nhận thông điệp thứ nhất để đăng ký thiết bị đầu cuối;

gửi thông điệp thứ hai đến thực thể chức năng quản lý di động và truy nhập nguồn sau khi nhận thông điệp thứ nhất, trong đó thông điệp thứ hai bao gồm định danh của thông điệp đầu cuối;

nhận khóa thứ nhất từ thực thể chức năng quản lý di động và truy nhập nguồn, trong đó khóa thứ nhất được dẫn xuất dựa trên khóa giữa thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối;

xác định, sau khi nhận khóa thứ nhất, liệu có sử dụng khóa thứ nhất dựa trên thông tin liên quan bảo mật hay không;

xác định, sau khi xác định sử dụng khóa thứ nhất, khóa truyền thông giữa

thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối dựa trên khóa thứ nhất, trong đó khóa truyền thông là để thực hiện bảo vệ tính toàn vẹn với báo hiệu giữa thực thể chức năng quản lý di động và truy nhập nguồn và thông điệp đầu cuối; và

gửi, đến thông điệp đầu cuối NAS SMC mà mang thông tin chỉ báo ra lệnh thông điệp đầu cuối dẫn xuất khóa thứ nhất.

15. Thiết bị thu thập khóa theo điểm 14, trong đó thông tin liên quan bảo mật bao gồm thông tin cô lập khóa của thực thể chức năng quản lý di động và truy nhập nguồn.

16. Thiết bị thu thập khóa theo điểm 14, trong đó thông tin liên quan bảo mật bao gồm chính sách được tiền cấu hình chỉ báo sử dụng khóa thứ nhất từ thực thể chức năng quản lý di động và truy nhập nguồn.

17. Thiết bị thu thập khóa theo điểm 14, trong đó thông điệp thứ hai là để yêu cầu ngữ cảnh bảo mật của thông điệp đầu cuối.

18. Thiết bị truyền thông bao gồm:

bộ xử lý được ghép nối với bộ nhớ lưu trữ các lệnh và được tạo cấu hình để thực thi các lệnh để khiến thiết bị để:

gửi thông điệp thứ nhất đến thực thể chức năng quản lý di động và truy nhập đích, trong đó thông điệp thứ nhất yêu cầu đăng ký thiết bị;

nhận NAS SMC từ thực thể chức năng quản lý di động và truy nhập đích, trong đó NAS SMC mang thông tin chỉ báo ra lệnh thiết bị dẫn xuất khóa thứ nhất giữa thiết bị và thực thể chức năng quản lý di động và truy nhập đích;

dẫn xuất khóa thứ nhất giữa thiết bị và thực thể chức năng quản lý di động và truy nhập đích dựa trên khóa được chia sẻ giữa thực thể chức năng quản lý di động và truy nhập nguồn và thiết bị; và

xác định khóa truyền thông giữa thiết bị và thực thể chức năng quản lý di động và truy nhập đích theo khóa thứ nhất, trong đó khóa truyền thông là để

thực hiện bảo vệ tính toàn vẹn với báo hiệu giữa thực thể chức năng quản lý di động và truy nhập đích và thiết bị.

19. Thiết bị theo điểm 18, trong đó các lệnh khi được thực thi còn khiến thiết bị gửi thông điệp hoàn thành chế độ bảo mật NAS đến thực thể chức năng quản lý di động và truy nhập đích.

20. Thiết bị theo điểm 19, trong đó các lệnh khi được thực thi còn khiến thiết bị nhận thông điệp từ thực thể chức năng quản lý di động và truy nhập đích, trong đó thông điệp thông báo thiết bị rằng việc đăng ký của thiết bị được chấp nhận.

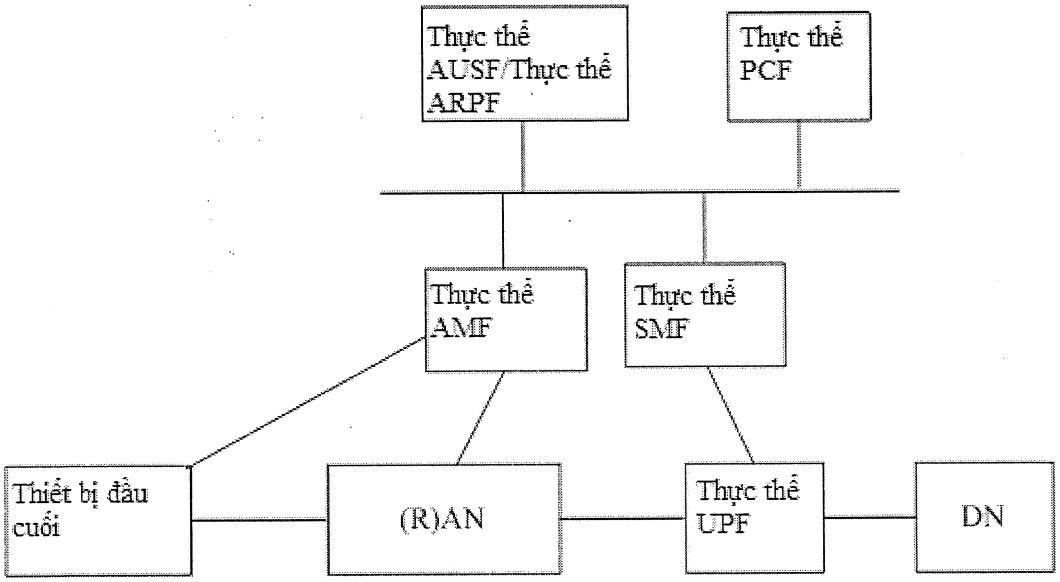

Thực thể AUSF/Thực thể ARPF
Thực thể PCF
Thực thể AMF
Thực thể SMF
Thiết bị đầu cuối
(R)AN
Thực thể UPF
DN

Fig.1

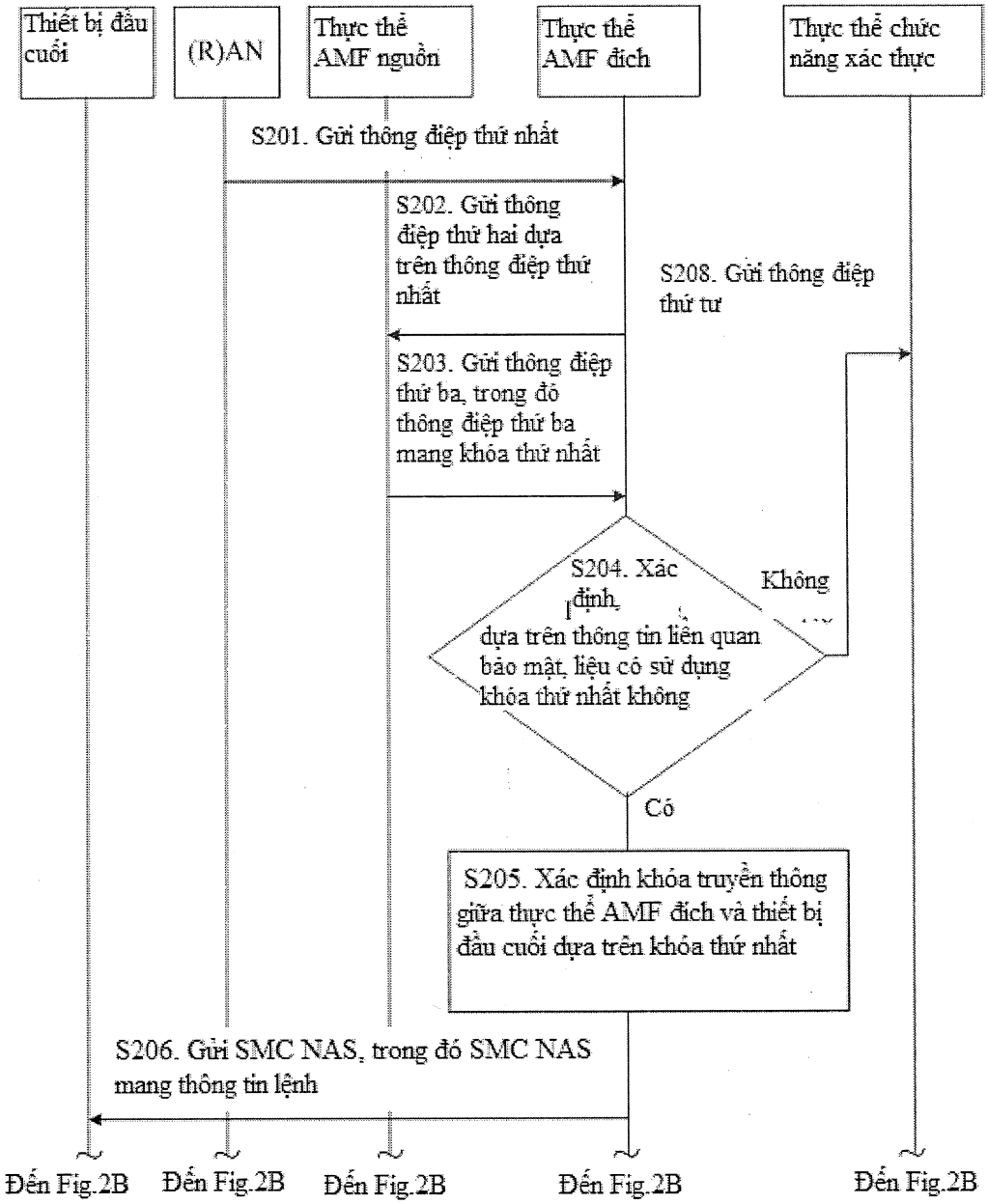

Thiết bị đầu cuối
(R)AN
Thực thể AMF nguồn
Thực thể AMF đích
Thực thể chức năng xác thực
S201. Gửi thông điệp thứ nhất
S202. Gửi thông điệp thứ hai dựa trên thông điệp thứ nhất
S208. Gửi thông điệp thứ tư
S203. Gửi thông điệp thứ ba, trong đó thông điệp thứ ba mang khóa thứ nhất
S204. Xác định, dựa trên thông tin liên quan bảo mật, liệu có sử dụng khóa thứ nhất không
Không
Có
S205. Xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ nhất
S206. Gửi SMC NAS, trong đó SMC NAS mang thông tin lệnh
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B

Fig.2A

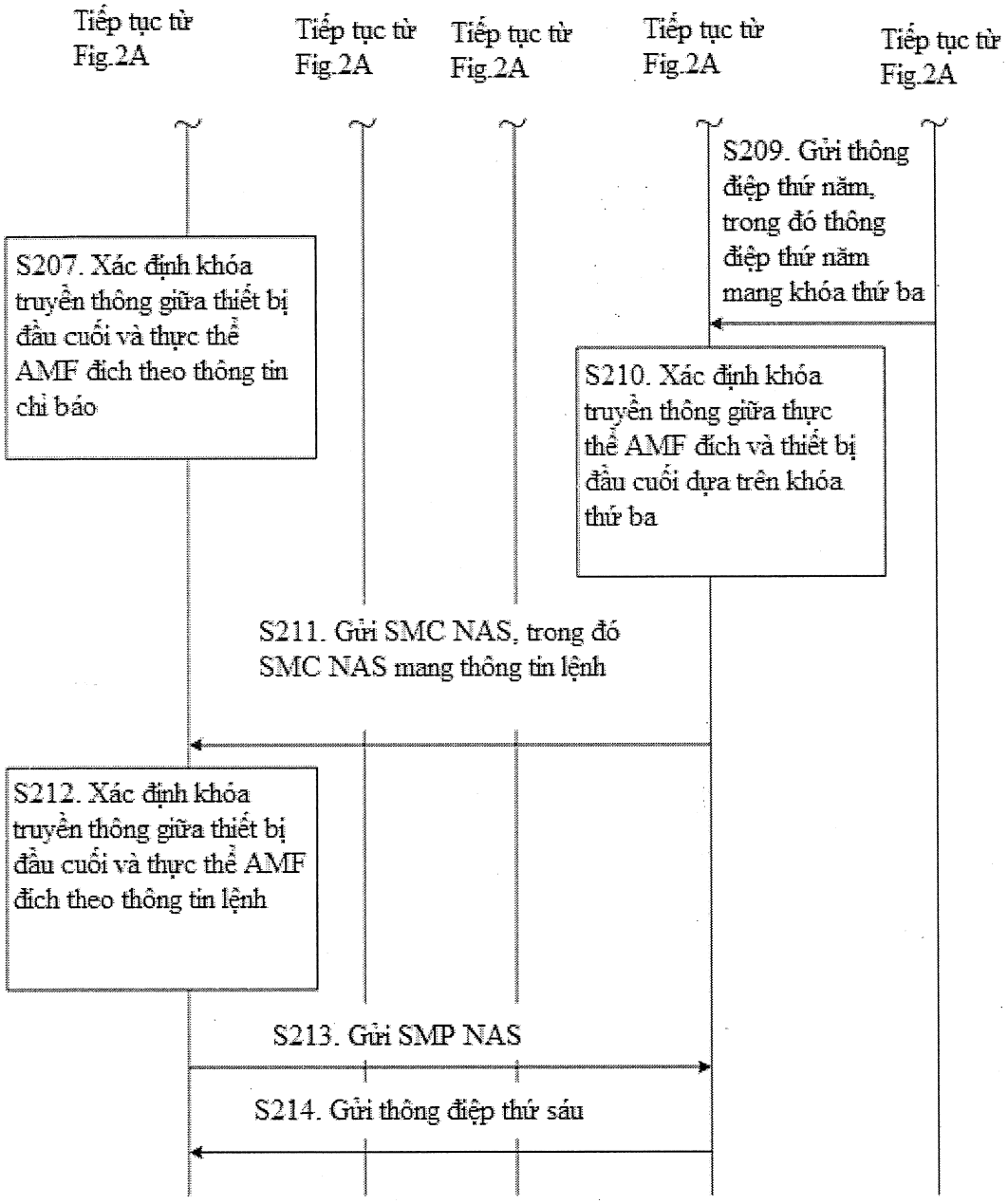

Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
S209. Gửi thông điệp thứ năm, trong đó thông điệp thứ năm mang khóa thứ ba
S207. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin chỉ báo
S210. Xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba
S211. Gửi SMC NAS, trong đó SMC NAS mang thông tin lệnh
S212. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin lệnh
S213. Gửi SMP NAS
S214. Gửi thông điệp thứ sáu

Fig.2B

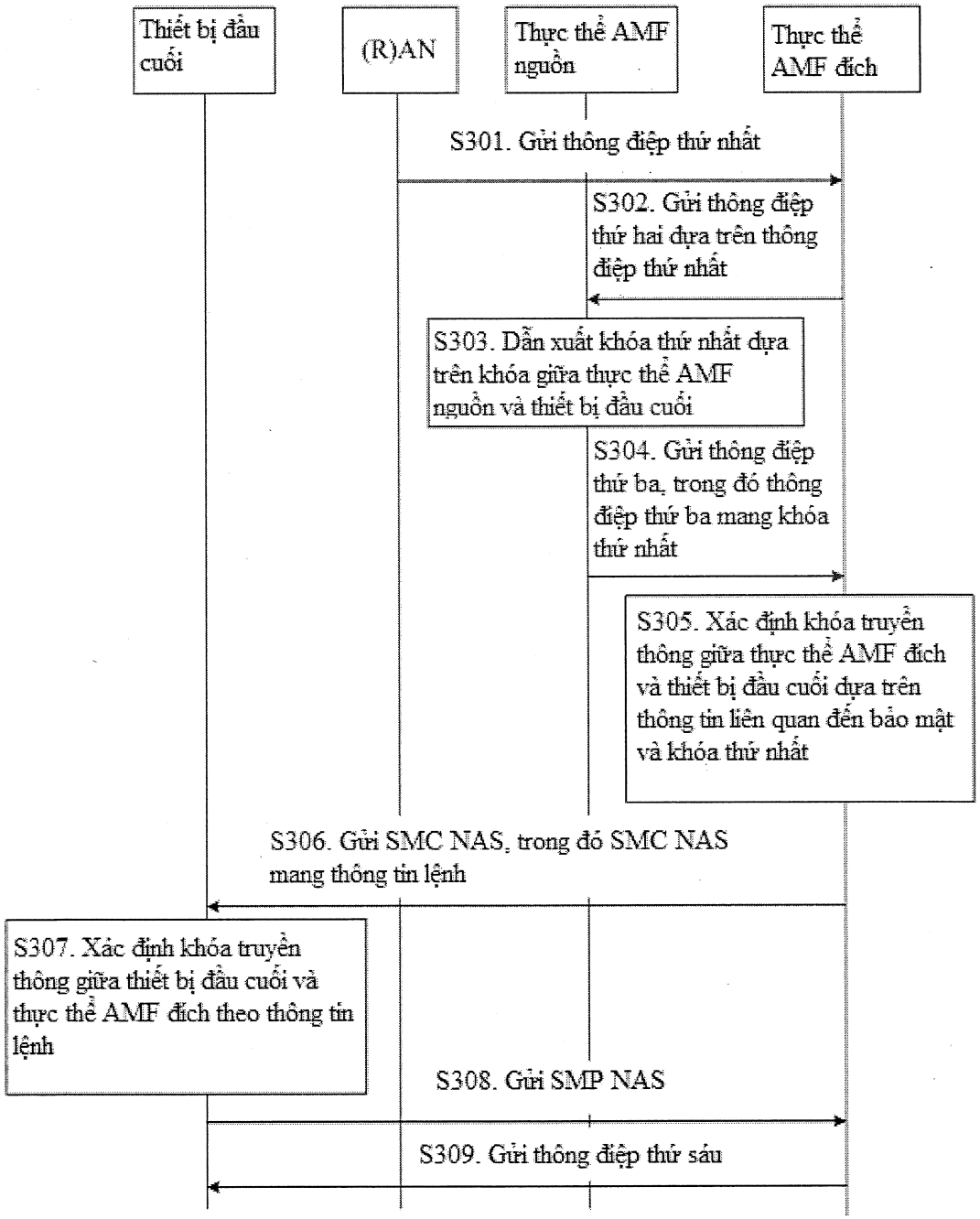

Thiết bị đầu cuối
(R)AN
Thực thể AMF nguồn
Thực thể AMF đích
S301. Gửi thông điệp thứ nhất
S302. Gửi thông điệp thứ hai dựa trên thông điệp thứ nhất
S303. Dẫn xuất khóa thứ nhất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối
S304. Gửi thông điệp thứ ba, trong đó thông điệp thứ ba mang khóa thứ nhất
S305. Xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên thông tin liên quan đến bảo mật và khóa thứ nhất
S306. Gửi SMC NAS, trong đó SMC NAS mang thông tin lệnh
S307. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin lệnh
S308. Gửi SMP NAS
S309. Gửi thông điệp thứ sáu

Fig.3

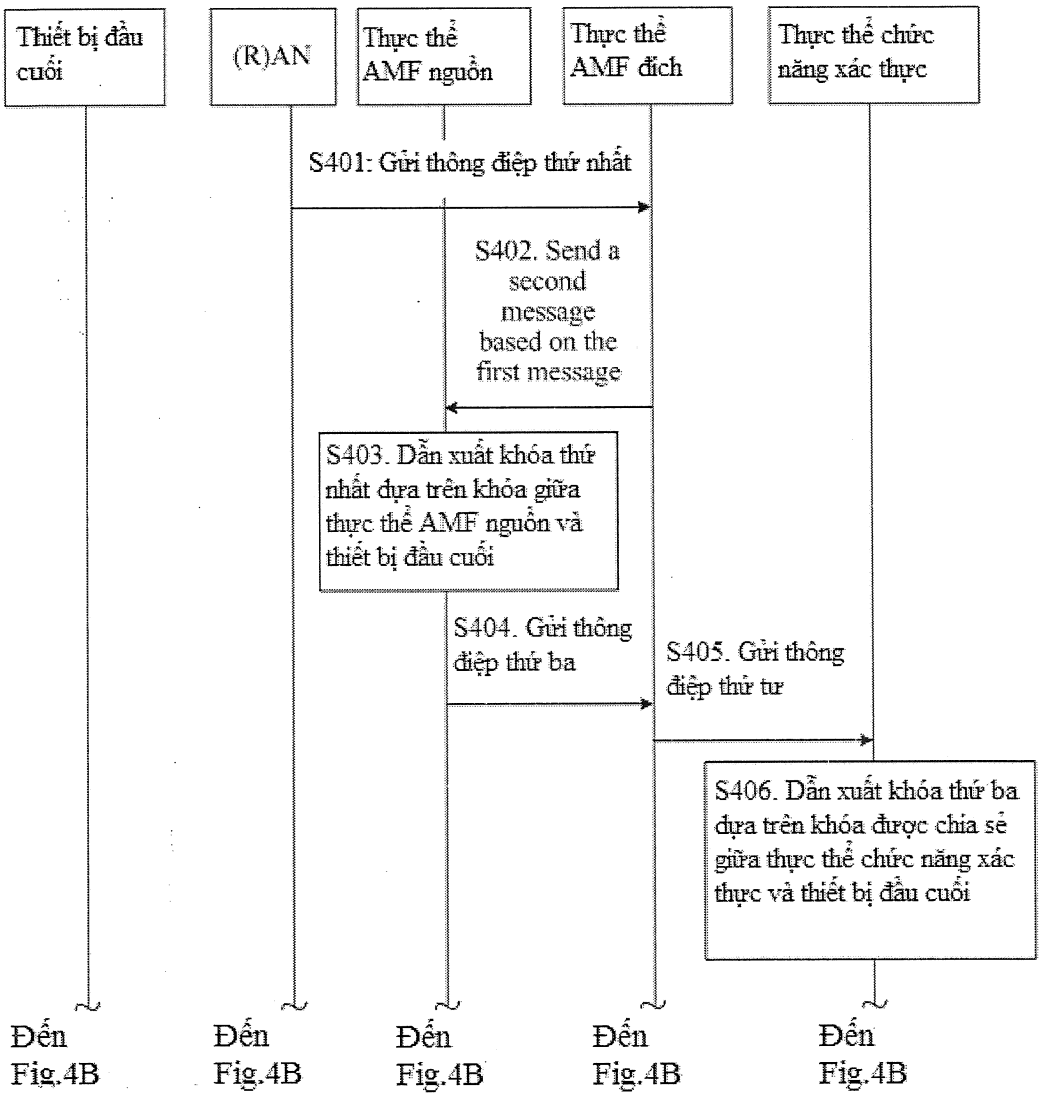

Thiết bị đầu cuối
(R)AN
Thực thể AMF nguồn
Thực thể AMF đích
Thực thể chức năng xác thực
S401: Gửi thông điệp thứ nhất
S402. Send a second message based on the first message
S403. Dẫn xuất khóa thứ nhất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối
S404. Gửi thông điệp thứ ba
S405. Gửi thông điệp thứ tư
S406. Dẫn xuất khóa thứ ba dựa trên khóa được chia sẻ giữa thực thể chức năng xác thực và thiết bị đầu cuối
Đến Fig.4B
Đến Fig.4B
Đến Fig.4B
Đến Fig.4B
Đến Fig.4B

Fig.4A

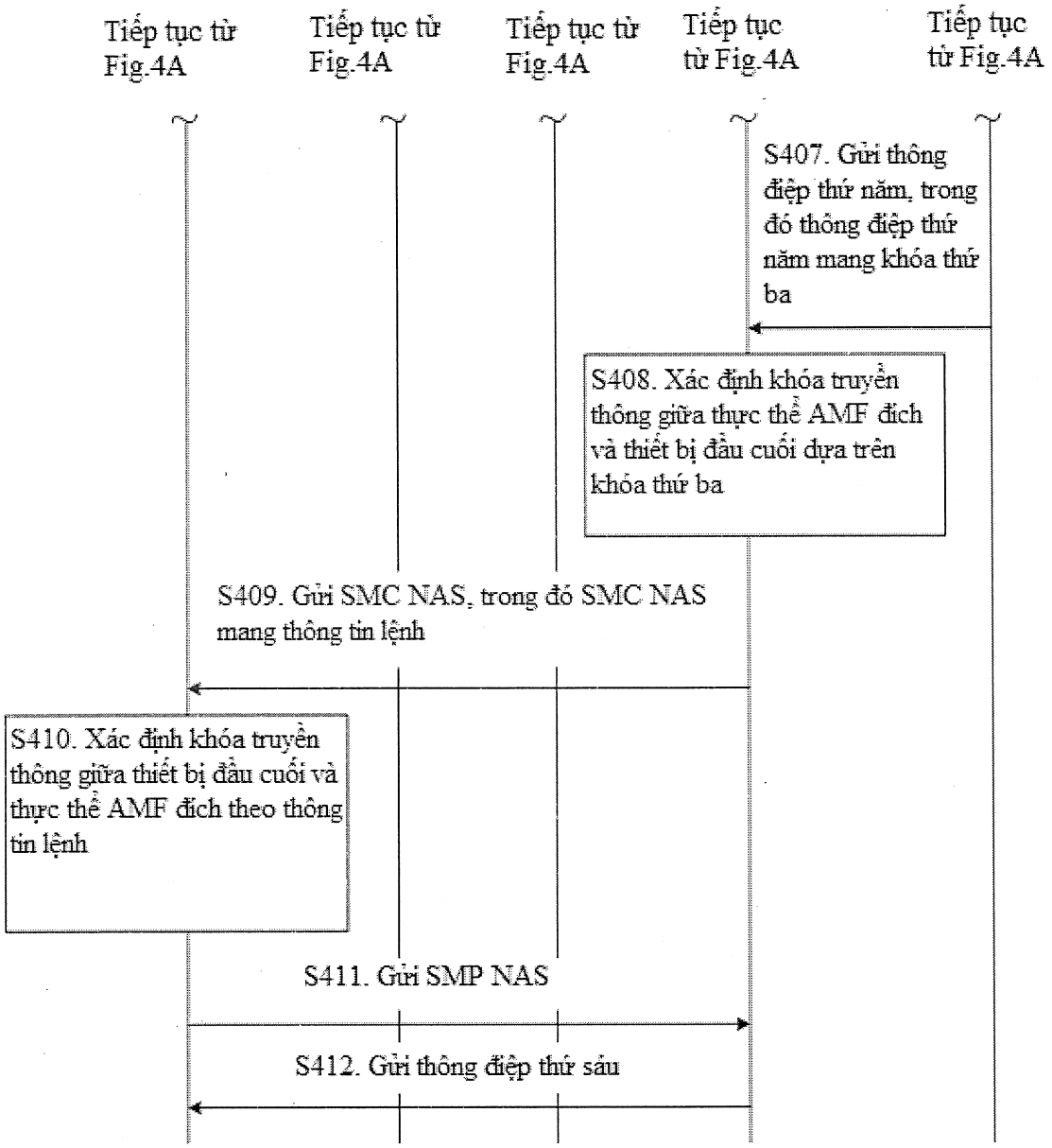

Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
S407. Gửi thông điệp thứ năm, trong đó thông điệp thứ năm mang khóa thứ ba
S408. Xác định khóa truyền thông giữa thực thể AMF đích và thiết bị đầu cuối dựa trên khóa thứ ba
S409. Gửi SMC NAS, trong đó SMC NAS mang thông tin lệnh
S410. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo thông tin lệnh
S411. Gửi SMP NAS
S412. Gửi thông điệp thứ sáu

Fig.4B

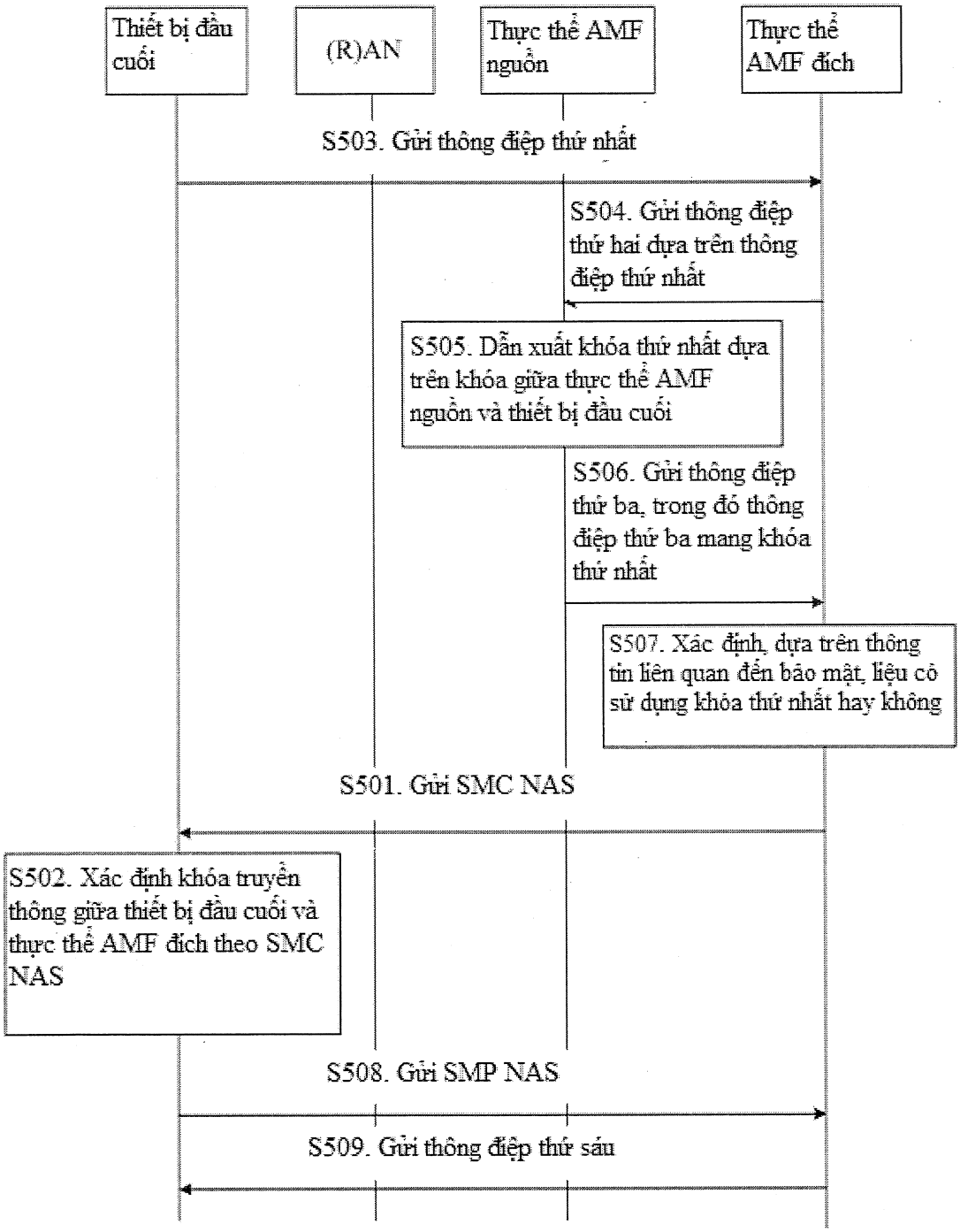

Thiết bị đầu cuối
(R)AN
Thực thể AMF nguồn
Thực thể AMF đích
S503. Gửi thông điệp thứ nhất
S504. Gửi thông điệp thứ hai dựa trên thông điệp thứ nhất
S505. Dẫn xuất khóa thứ nhất dựa trên khóa giữa thực thể AMF nguồn và thiết bị đầu cuối
S506. Gửi thông điệp thứ ba, trong đó thông điệp thứ ba mang khóa thứ nhất
S507. Xác định, dựa trên thông tin liên quan đến bảo mật, liệu có sử dụng khóa thứ nhất hay không
S501. Gửi SMC NAS
S502. Xác định khóa truyền thông giữa thiết bị đầu cuối và thực thể AMF đích theo SMC NAS
S508. Gửi SMP NAS
S509. Gửi thông điệp thứ sáu

Fig.5

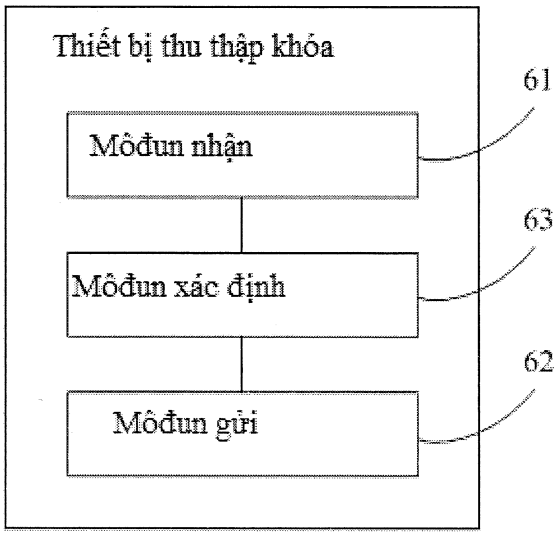

Thiết bị thu thập khóa
Môđun nhận
Môđun xác định
Môđun gửi
61
63
62

Fig.6

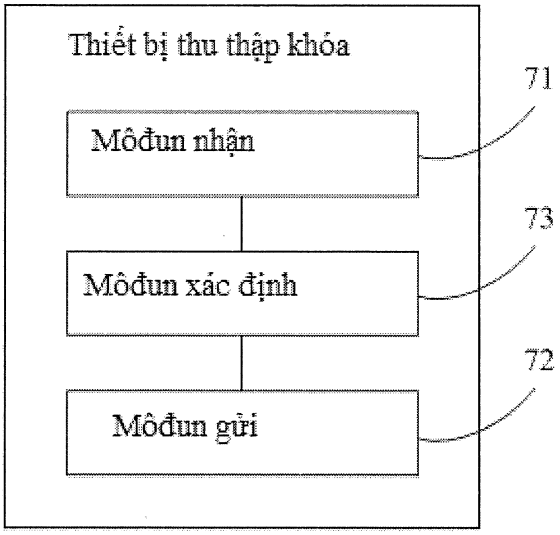

Thiết bị thu thập khóa
Môđun nhận
Môđun xác định
Môđun gửi
71
73
72

Fig.7

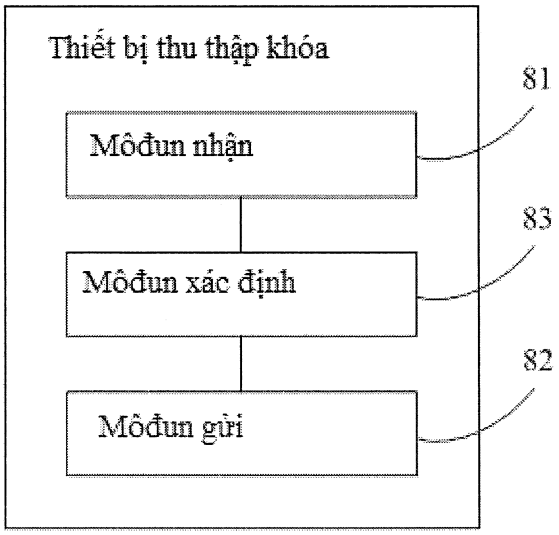

Thiết bị thu thập khóa
81
Môđun nhận
83
Môđun xác định
82
Môđun gửi

Fig.8

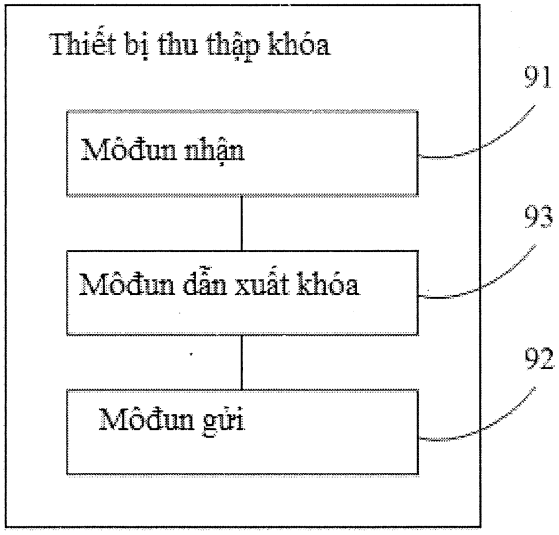

Thiết bị thu thập khóa
91
Môđun nhận
93
Môđun dẫn xuất khóa
92
Môđun gửi

Fig.9

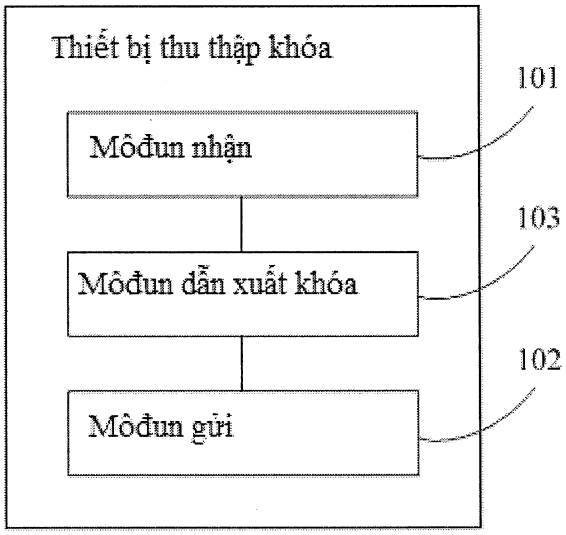

Thiết bị thu thập khóa
101
Môđun nhận
103
Môđun dẫn xuất khóa
102
Môđun gửi

Fig.10

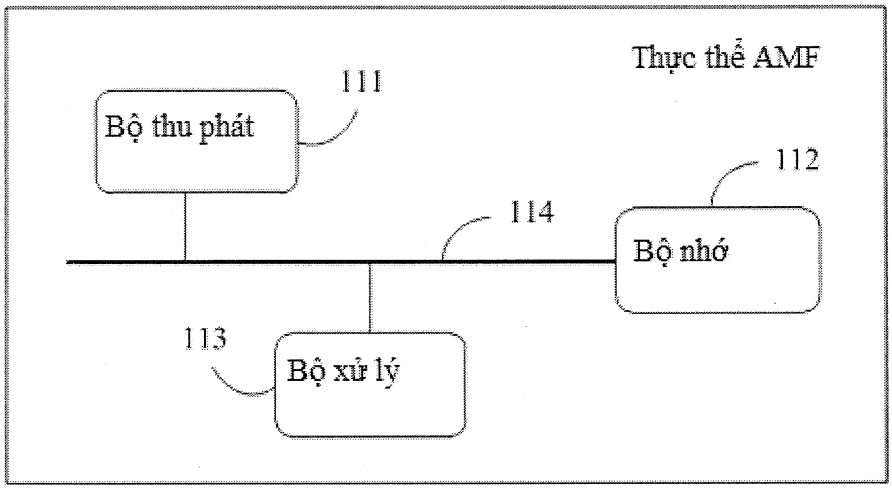

Thực thể AMF
111
Bộ thu phát
112
114
Bộ nhớ
113
Bộ xử lý

Fig.11

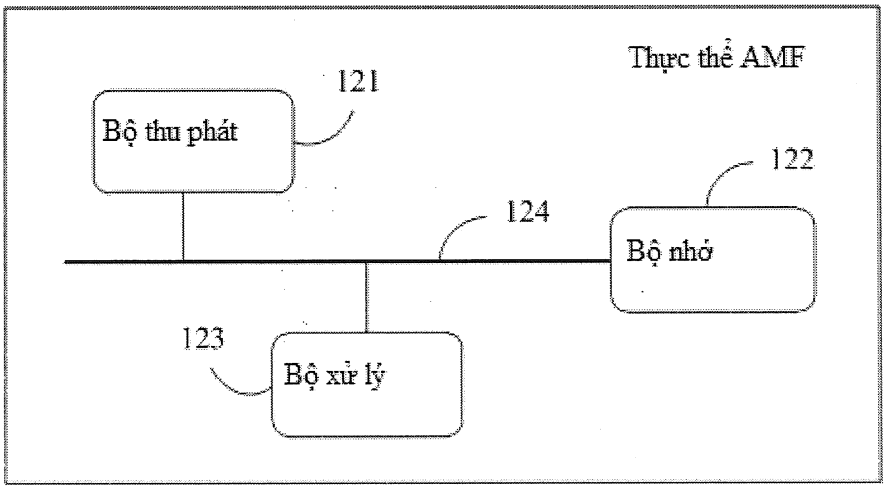

Thực thể AMF
121
Bộ thu phát
122
124
Bộ nhớ
123
Bộ xử lý

Fig.12

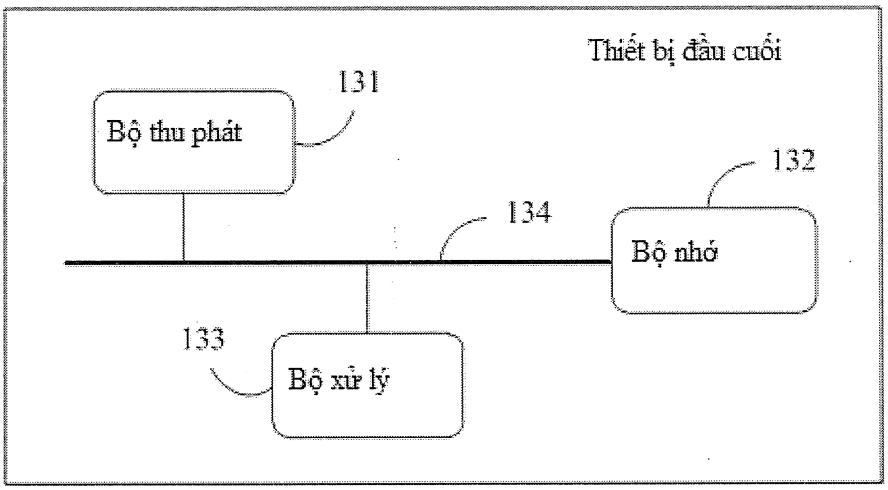

Thiết bị đầu cuối
131
Bộ thu phát
132
134
Bộ nhớ
133
Bộ xử lý

Fig.13

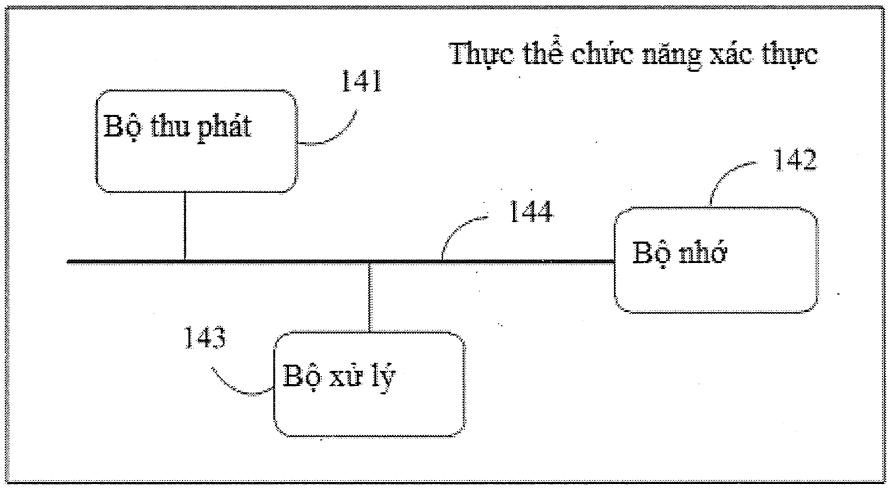

Thực thể chức năng xác thực
141
Bộ thu phát
142
144
Bộ nhớ
143
Bộ xử lý

Fig.14

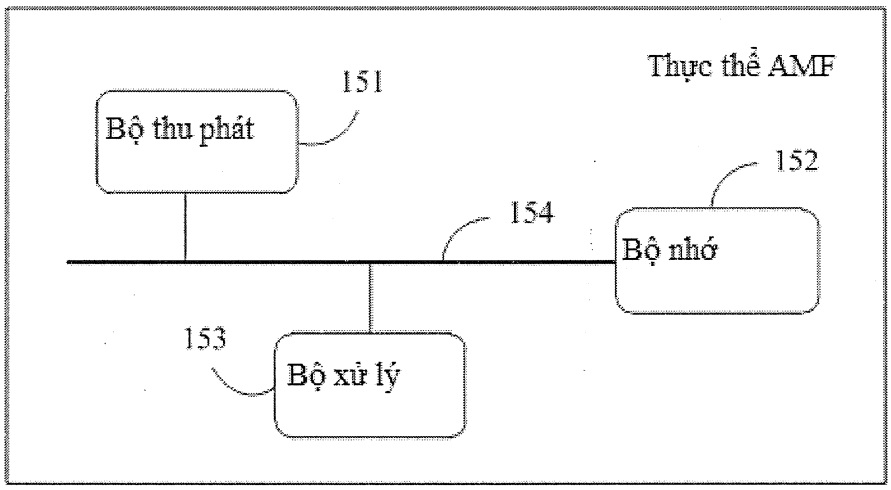

Thực thể AMF
151
Bộ thu phát
152
154
Bộ nhớ
153
Bộ xử lý

Fig.15