(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) **1-0053164**

(51)[2022.01] **H04W 12/04**

(13) **B**

(21) 1-2022-07998
(22) 13/05/2021
(86) PCT/CN2021/093704 13/05/2021
(87) WO 2021/233208 25/11/2021
(30) 202010441150.1 22/05/2020 CN
(45) 25/11/2025 452
(43) 25/07/2023 424A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) GUO, Longhua (CN); LI, He (CN); WU, Rong (CN).
(74) Công ty Cổ phần Sở hữu công nghiệp INVESTIP (INVESTIP)

(54) PHƯƠNG PHÁP BẢO VỆ TRUYỀN THÔNG, THIẾT BỊ TRUYỀN THÔNG, VÀ PHƯƠNG TIỆN LƯU TRỮ ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(21) 1-2022-07998

(57) Sáng chế đề cập đến phương pháp bảo vệ truyền thông, thiết bị truyền thông, và phương tiện đọc được bằng máy tính. Phương pháp bảo vệ truyền thông bao gồm: Thiết bị đầu cuối gửi thông điệp yêu cầu thiết lập phiên ứng dụng đến bộ phận mạng chức năng ứng dụng (application function, AF) thứ nhất, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa xác thực và quản lý khóa đối với ứng dụng AKMA (Authentication and Key Management for Application, AKMA); và thiết bị đầu cuối nhận thông điệp phản hồi thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật. Chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA. Bằng cách này, các phương án của sáng chế có thể thực hiện bảo vệ bảo mật đầu cuối giữa thiết bị người dùng UE (user equipment, UE) và AF đối với các yêu cầu dịch vụ khác nhau.

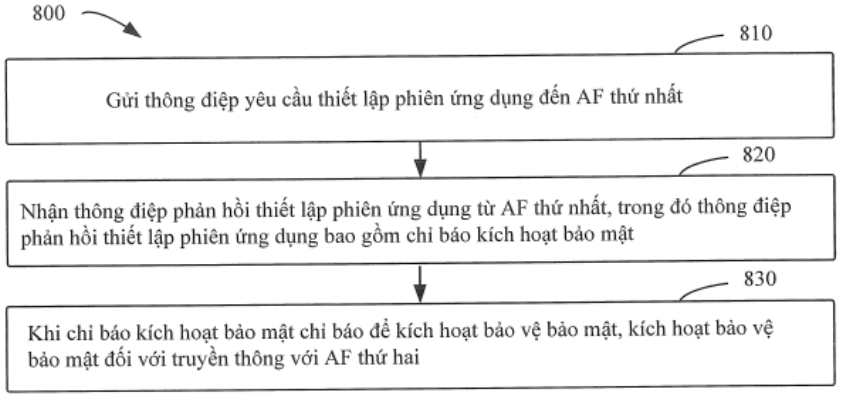

FIG. 8

Lĩnh vực kỹ thuật được đề cập

Các phương án của sáng chế đề cập đến lĩnh vực truyền thông, và cụ thể hơn, đến phương pháp bảo vệ truyền thông và thiết bị truyền thông.

Tình trạng kỹ thuật của sáng chế

Hệ thống truyền thông thế hệ thứ năm (5G) xác định kiến trúc xác thực và quản lý khóa đối với ứng dụng (Authentication and Key Management for Application, AKMA). Thiết bị đầu cuối (ví dụ, thiết bị người dùng, UE (user equipment, UE)) và bộ phận mạng chức năng ứng dụng (Application Function, AF) có thể thực hiện thương lượng khóa dựa trên kiến trúc AKMA, để tạo ra một cách riêng biệt khóa để bảo vệ truyền thông giữa thiết bị đầu cuối và AF.

Trong kiến trúc AKMA đang có, khóa ở mức độ chi tiết của mã định danh (Identifier, ID) AF được thương lượng giữa UE và AF. Do đó, khóa ở mức độ chi tiết hơn nữa không thể được thương lượng giữa UE và AF. Kết quả là, bảo vệ bảo mật đầu cuối giữa UE và AF không thể được thực hiện đối với các yêu cầu dịch vụ khác nhau.

Bản chất kỹ thuật của sáng chế

Nói chung, các phương án của sáng chế đề xuất phương pháp bảo vệ truyền thông, thiết bị truyền thông, và phương tiện đọc được bằng máy tính, để việc bảo vệ bảo mật đầu cuối giữa thiết bị đầu cuối và AF có thể được thực hiện đối với các yêu cầu dịch vụ khác nhau.

Theo khía cạnh thứ nhất, phương pháp bảo vệ truyền thông được đề xuất, và gồm: bước gửi, bởi thiết bị đầu cuối, thông điệp yêu cầu thiết lập phiên ứng dụng tới AF thứ nhất, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng gồm mã định danh khóa AKMA; và bước nhận, bởi thiết bị đầu cuối, thông điệp phản hồi thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, và bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn; và khi chỉ báo kích hoạt bảo mật chỉ báo kích hoạt bảo mật, bước kích hoạt, bởi thiết bị đầu cuối dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với

truyền thông với AF thứ hai, trong đó khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA. Bằng cách này, phương án này của sáng chế có thể thực hiện bảo vệ bảo mật đầu cuối giữa thiết bị đầu cuối và AF đối với các yêu cầu dịch vụ khác nhau.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật và/hoặc chính sách bảo mật mà được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn mà được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ sự kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không. Bằng cách này, phương án này của sáng chế có thể thực hiện thương lượng khả năng bảo mật giữa thiết bị đầu cuối và AF. Thương lượng khả năng bảo mật bao gồm việc thiết bị đầu cuối và AF thương lượng xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF hay không, thiết bị đầu cuối và AF thương lượng về thuật toán bảo vệ bí mật, thuật toán bảo vệ toàn vẹn, và/hoặc tương tự được sử dụng chung bởi thiết bị đầu cuối và AF.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai. Bước kích hoạt, bởi thiết bị đầu cuối dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với AF thứ hai bao gồm: bước kích hoạt, bởi thiết bị đầu cuối dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với AF thứ hai. Bằng cách này, thiết bị đầu cuối và AF có thể thương lượng về thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được sử dụng chung bởi thiết bị đầu cuối và AF.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật. Phương pháp còn bao gồm: bước tạo ra, bởi thiết bị đầu cuối, khóa bảo mật dựa trên khóa AKMA và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật được định danh bởi mã định danh khóa. Bằng cách này, thiết bị đầu cuối có thể xác định ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF, và tạo ra khóa bảo mật trong ngữ cảnh bảo mật dựa trên thuật toán bảo mật được thương lượng với AF.

Trong một số phương án, AF thứ nhất giống với AF thứ hai, và bước tạo ra khóa bảo

mật bao gồm: bước tạo ra, bởi thiết bị đầu cuối, khóa AF của AF thứ nhất dựa trên khóa AKMA; và bước tạo ra, bởi thiết bị đầu cuối, khóa bảo mật dựa trên hóa AF và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn. Bằng cách này, thiết bị đầu cuối có thể tạo ra, dựa trên thuật toán bảo mật được thương lượng với AF, khóa bảo mật để bảo vệ truyền thông giữa thiết bị đầu cuối và AF.

Trong một số phương án, AF thứ nhất khác với AF thứ hai, và bước tạo ra khóa bảo mật bao gồm: bước tạo ra, bởi thiết bị đầu cuối, khóa AF thứ nhất của AF thứ nhất dựa trên khóa AKMA; bước tạo ra, bởi thiết bị đầu cuối, khóa AF thứ hai của AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất; và bước tạo ra, bởi thiết bị đầu cuối, khóa bảo mật dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn. Bằng cách này, thiết bị đầu cuối có thể tạo ra, dựa trên thuật toán bảo mật được thương lượng với AF, khóa bảo mật để bảo vệ truyền thông giữa thiết bị đầu cuối và AF.

Trong một số phương án, thông số tạo ra khóa bao gồm ít nhất một trong số các nội dung sau đây: thông tin nhận dạng được sử dụng bởi thiết bị đầu cuối trong AF thứ nhất hoặc AF thứ hai; loại dịch vụ được yêu cầu bởi thiết bị đầu cuối; thông tin nhận dạng của AF thứ hai; hoặc thông số làm mới khóa. Thông tin nhận dạng giúp thực hiện cách ly bảo mật giữa các tên người dùng khác nhau. Loại dịch vụ giúp thực hiện cách ly bảo mật dữ liệu giữa các loại dịch vụ khác nhau. Thông tin nhận dạng của AF thứ hai có thể được sử dụng làm cơ sở cho AF thứ nhất để phân biệt giữa các AF khác nhau với cùng ID của AF, và giúp thực hiện cách ly bảo mật giữa các AF khác nhau với cùng ID của AF. Thông số làm mới khóa giúp thực hiện định kỳ cập nhật khóa tùy chỉnh.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa. Bằng cách này, thông số tạo ra khóa có thể được tạo ra bởi thiết bị đầu cuối và được chia sẻ với AF.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa. Bằng cách này, thông số tạo ra khóa có thể được tạo ra bởi AF và được chia sẻ với thiết bị đầu cuối.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và phương pháp còn bao gồm: bước tính toán, bởi thiết bị đầu

cuối, thông số xác minh toàn vẹn thứ hai đối với thông điệp phản hồi thiết lập phiên ứng dụng dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai và khóa bảo vệ toàn vẹn tương ứng với AF thứ hai; và nếu thông số xác minh toàn vẹn thứ nhất phù hợp với thông số xác minh toàn vẹn thứ hai, bước xác định bởi thiết bị đầu cuối, rằng thông điệp phản hồi thiết lập phiên ứng dụng không bị giả mạo; hoặc nếu thông số xác minh toàn vẹn thứ nhất không phù hợp với thông số xác minh toàn vẹn thứ hai, bước xác định, bởi thiết bị đầu cuối, rằng thông điệp phản hồi thiết lập phiên ứng dụng không bị giả mạo. Bằng cách này, thiết bị đầu cuối có thể thực hiện xác minh toàn vẹn đối với thông điệp được gửi bởi AF.

Trong một số phương án, phương pháp còn bao gồm: bước gửi, bởi thiết bị đầu cuối, thông điệp hoàn thành thiết lập phiên ứng dụng đến AF thứ hai nếu nó xác định được rằng thông điệp phản hồi thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ ba, và thông số xác minh toàn vẹn thứ ba được tính toán dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai và khóa bảo vệ toàn vẹn tương ứng với AF thứ hai. Bằng cách này, AF có thể thực hiện xác minh toàn vẹn đối với thông điệp được gửi bởi thiết bị đầu cuối.

Trong một số phương án, chỉ báo kích hoạt bảo mật bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Khi chỉ báo bảo vệ bí mật được thiết đặt đến giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng việc bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt. Khi chỉ báo bảo vệ bí mật được thiết đặt đến giá trị được thiết đặt trước thứ hai khác với giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt, và thuật toán bảo vệ bí mật được chỉ báo bởi giá trị được thiết đặt trước thứ hai được sử dụng để bảo vệ bí mật. Khi chỉ báo bảo vệ toàn vẹn được thiết đặt đến giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng việc bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt. Khi chỉ báo bảo vệ toàn vẹn được thiết đặt đến giá trị được thiết đặt trước thứ ba khác với giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt, và thuật toán bảo vệ toàn vẹn được chỉ báo bởi giá trị được thiết đặt trước thứ ba được sử dụng để bảo vệ toàn vẹn. Bằng cách này, chỉ báo kích hoạt bảo mật có thể chỉ báo hoàn toàn thuật toán bảo mật được sử dụng giữa thiết bị đầu cuối và AF.

Trong một số phương án, chỉ báo kích hoạt bảo mật được chỉ báo bởi thuật toán bảo mật được lựa chọn, trong đó khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo

rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt.

Trong một số phương án, AF thứ nhất và AF thứ hai có cùng mã định danh của AF. Bằng cách này, với kịch bản trong đó nhiều AF chia sẻ cùng ID của AF, giải pháp có thể tạo ra một cách riêng biệt các khóa tương ứng để thực hiện cách ly bảo mật trong kịch bản. AF có thể thực hiện thương lượng khóa với thiết bị đầu cuối thay mặt các AF khác. Do đó, không cần yêu cầu rằng có giao diện giữa mỗi AF và mạng di động mặt đất công cộng (public land mobile network, PLMN).

Theo khía cạnh thứ hai, phương pháp bảo vệ truyền thông được đề xuất, và bao gồm: bước nhận, bởi AF thứ nhất, thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA; và bước gửi, bởi AF thứ nhất, thông điệp phản hồi thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng gồm chỉ báo kích hoạt bảo mật, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, và bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn; và khi chỉ báo kích hoạt bảo mật chỉ báo kích hoạt bảo mật, bước khởi động, bởi AF thứ nhất, AF thứ hai để kích hoạt, dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối, trong đó khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA. Bằng cách này, phương án này của sáng chế có thể thực hiện bảo vệ bảo mật đầu cuối giữa thiết bị đầu cuối và AF đối với các yêu cầu dịch vụ khác nhau.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật và/hoặc chính sách bảo mật mà được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn mà được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ sự kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không. Bằng cách này, phương án

này của sáng chế có thể thực hiện thương lượng khả năng bảo mật giữa thiết bị đầu cuối và AF. Thương lượng khả năng bảo mật bao gồm việc thiết bị đầu cuối và AF thương lượng xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF hay không, thiết bị đầu cuối và AF thương lượng về thuật toán bảo vệ bí mật, thuật toán bảo vệ toàn vẹn, và/hoặc tương tự được sử dụng chung bởi thiết bị đầu cuối và AF.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai. Bước khởi động, bởi AF thứ nhất, AF thứ hai để kích hoạt, dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối bao gồm: bước khởi động, bởi AF thứ nhất, AF thứ hai để kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối. Bằng cách này, phương án này của sáng chế có thể kích hoạt, dựa trên kết quả thương lượng bảo mật giữa thiết bị đầu cuối và AF, bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF. Kết quả thương lượng bảo mật bao gồm thuật toán bảo mật và khóa bảo mật mà được thương lượng giữa thiết bị đầu cuối và AF.

Trong một số phương án, AF thứ nhất khác với AF thứ hai, và phương pháp còn bao gồm: bước tạo ra, bởi AF thứ nhất, khóa AF thứ nhất của AF thứ nhất dựa trên khóa AKMA; và bước tạo ra, bởi AF thứ nhất, khóa AF thứ hai của AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất. Bằng cách này AF thứ nhất có thể giúp AF thứ hai tạo ra khóa AF của AF thứ hai.

Trong một số phương án, phương pháp còn bao gồm: bước gửi, bởi AF thứ nhất, thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật và/hoặc chính sách bảo mật mà được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai; và bước nhận, bởi AF thứ nhất, thông điệp báo nhận từ AF thứ hai, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn, chỉ báo kích hoạt bảo mật, và mã định danh khóa, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật. Bằng cách này, AF thứ hai có thể tự thương lượng về khả năng bảo mật với thiết bị đầu cuối dựa trên thông tin khả năng bảo mật của thiết bị đầu cuối mà được chuyển tiếp bởi AF thứ nhất.

Trong một số phương án, bước gửi, bởi AF thứ nhất, thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối bao gồm: bước chuyển tiếp, bởi AF thứ nhất, thông điệp

báo nhận đến thiết bị đầu cuối làm một phần của thông điệp phản hồi thiết lập phiên ứng dụng. Bằng cách này, thiết bị đầu cuối có thể thu được kết quả thương lượng bảo mật giữa thiết bị đầu cuối và AF thứ hai thông qua AF thứ nhất.

Trong một số phương án, phương pháp còn bao gồm: bước nhận, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối; và bước chuyển tiếp, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng đến AF thứ hai. Bằng cách này, thiết bị đầu cuối có thể thực hiện xác minh toàn vẹn của thông điệp giữa thiết bị đầu cuối và AF thứ hai thông qua AF thứ nhất.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không; và phương pháp còn bao gồm: bước tạo ra, bởi AF thứ nhất, chỉ báo kích hoạt bảo mật theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi AF thứ hai, trong đó chính sách bảo mật được hỗ trợ bởi AF thứ hai chỉ báo xem AF thứ hai có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không. Bằng cách này, chỉ báo kích hoạt bảo mật có thể được tạo ra dựa trên kết quả thương lượng chính sách bảo mật.

Trong một số phương án, phương pháp còn bao gồm: bước xác định, bởi AF thứ nhất thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo mật được hỗ trợ bởi AF thứ hai. Bằng cách này, AF có thể thương lượng với thiết bị đầu cuối về thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được sử dụng chung bởi AF và thiết bị đầu cuối.

Trong một số phương án, phương pháp còn bao gồm: bước tạo ra, bởi AF thứ nhất, chỉ báo kích hoạt bảo mật dựa trên thuật toán bảo mật được lựa chọn, trong đó nếu thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai, chỉ báo kích hoạt bảo mật được tạo ra chỉ báo để kích hoạt bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai; và nếu thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai, chỉ báo kích hoạt bảo mật được tạo ra chỉ báo để kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai. Bằng cách này, chỉ báo kích hoạt bảo mật có thể được tạo ra dựa trên kết quả thương lượng thuật toán bảo mật.

Trong một số phương án, AF thứ nhất giống với AF thứ hai, và phương pháp còn bao

gồm: bước tạo ra, bởi AF thứ nhất, khóa AF của AF thứ nhất dựa trên khóa AKMA; và bước tạo ra, bởi AF thứ nhất, khóa bảo mật và mã định danh khóa của khóa bảo mật dựa trên khóa AF và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn. Bằng cách này, AF thứ nhất có thể tạo ra, dựa trên thuật toán bảo mật được thương lượng với thiết bị đầu cuối, khóa bảo mật để bảo vệ truyền thông giữa AF thứ nhất và thiết bị đầu cuối.

Trong một số phương án, AF thứ nhất khác với AF thứ hai, và phương pháp còn bao gồm: bước tạo ra, bởi AF thứ nhất, khóa AF thứ nhất của AF thứ nhất dựa trên khóa AKMA; bước tạo ra, bởi AF thứ nhất, khóa AF thứ hai của AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất; và bước tạo ra, bởi AF thứ nhất, khóa bảo mật và mã định danh khóa của khóa bảo mật dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn. Bằng cách này, AF thứ nhất có thể thay thế AF thứ hai để tạo ra khóa bảo mật để bảo vệ truyền thông giữa thiết bị đầu cuối và AF thứ hai.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa. Bằng cách này, thông số tạo ra khóa có thể được tạo ra bởi thiết bị đầu cuối và được chia sẻ với AF.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa. Bằng cách này, thông số tạo ra khóa có thể được tạo ra bởi AF và được chia sẻ với thiết bị đầu cuối.

Trong một số phương án, thông số tạo ra khóa bao gồm ít nhất một trong số các nội dung sau đây: thông tin nhận dạng được sử dụng bởi thiết bị đầu cuối trong AF thứ nhất hoặc AF thứ hai; loại dịch vụ được yêu cầu bởi thiết bị đầu cuối; thông tin nhận dạng của AF thứ hai; hoặc thông số làm mới khóa. Thông tin nhận dạng giúp thực hiện cách ly bảo mật giữa các tên người dùng khác nhau. Loại dịch vụ giúp thực hiện cách ly bảo mật dữ liệu giữa các loại dịch vụ khác nhau. Thông tin nhận dạng của AF thứ hai có thể được sử dụng làm cơ sở cho AF thứ nhất để phân biệt giữa các AF khác nhau với cùng ID của AF, và giúp thực hiện cách ly bảo mật giữa các AF khác nhau với cùng ID của AF. Thông số làm mới khóa giúp thực hiện định kỳ cập nhật khóa tùy chỉnh.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm mã định danh khóa, và mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu

cuối và AF thứ hai. Bằng cách này, thiết bị đầu cuối có thể xác định ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và xác định khóa bảo mật trong ngữ cảnh bảo mật.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và thông số xác minh toàn vẹn thứ nhất được tính toán dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ nhất và khóa bảo vệ toàn vẹn tương ứng với AF thứ nhất. Bằng cách này, thiết bị đầu cuối có thể thực hiện xác minh toàn vẹn đối với thông điệp được gửi bởi AF thứ nhất.

Trong một số phương án, phương pháp còn bao gồm: bước nhận, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai, và thông số xác minh toàn vẹn thứ hai được tính toán dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ nhất và khóa bảo vệ toàn vẹn tương ứng với AF thứ nhất; bước tính toán, bởi AF thứ nhất, thông số xác minh toàn vẹn thứ ba cho thông điệp phản hồi thiết lập phiên ứng dụng dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ nhất và khóa bảo vệ toàn vẹn tương ứng với AF thứ nhất; và nếu thông số xác minh toàn vẹn thứ hai phù hợp với thông số xác minh toàn vẹn thứ ba, bước xác định, bởi AF thứ nhất, rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo; và nếu thông số xác minh toàn vẹn thứ hai không phù hợp với thông số xác minh toàn vẹn thứ ba, bước xác định, bởi AF thứ nhất, rằng thông điệp hoàn thành thiết lập phiên ứng dụng bị giả mạo. Bằng cách này, AF thứ nhất có thể thực hiện xác minh toàn vẹn đối với thông điệp được gửi bởi thiết bị đầu cuối.

Trong một số phương án, bước khởi động, bởi AF thứ nhất, AF thứ hai để kích hoạt, dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối bao gồm: bước gửi, bởi AF thứ nhất, thông điệp kích hoạt đến AF thứ hai khi xác định rằng thông điệp thiết lập phiên ứng dụng không bị giả mạo, để chỉ báo AF thứ hai kích hoạt, dựa trên khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối. Bằng cách này, AF thứ nhất có thể kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai.

Trong một số phương án, chỉ báo kích hoạt bảo mật bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Khi chỉ báo bảo vệ bí mật được thiết đặt đến giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng việc bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt. Khi chỉ báo bảo vệ bí mật được thiết đặt đến

giá trị được thiết đặt trước thứ hai khác với giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt, và thuật toán bảo vệ bí mật được chỉ báo bởi giá trị được thiết đặt trước thứ hai được sử dụng để bảo vệ bí mật. Khi chỉ báo bảo vệ toàn vẹn được thiết đặt đến giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng việc bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt. Khi chỉ báo bảo vệ toàn vẹn được thiết đặt đến giá trị được thiết đặt trước thứ ba khác với giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt, và thuật toán bảo vệ toàn vẹn được chỉ báo bởi giá trị được thiết đặt trước thứ ba được sử dụng để bảo vệ toàn vẹn. Bằng cách này, chỉ báo kích hoạt bảo mật có thể chỉ báo hoàn toàn thuật toán bảo mật được sử dụng giữa thiết bị đầu cuối và AF.

Trong một số phương án, AF thứ nhất và AF thứ hai có cùng mã định danh của AF. Bằng cách này, với kịch bản trong đó nhiều AF chia sẻ cùng ID của AF, giải pháp này có thể tạo ra một cách riêng biệt các khóa tương ứng để thực hiện cách ly bảo mật trong kịch bản. AF có thể thực hiện thương lượng khóa với thiết bị đầu cuối thay mặt các AF khác. Do đó, không cần yêu cầu rằng có giao diện giữa mỗi AF và PLMN.

Theo khía cạnh thứ ba, phương pháp bảo vệ truyền thông được đề xuất, và bao gồm: bước nhận, bởi AF thứ hai, thông điệp thông báo khóa từ AF thứ nhất trong đó thông điệp thông báo khóa bao gồm khóa AF của AF thứ hai, khóa AF được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA, và mã định danh khóa AKMA được gửi bởi thiết bị đầu cuối đến AF thứ nhất; bước gửi, bởi AF thứ hai, thông điệp báo nhận đến AF thứ nhất, trong đó thông điệp báo nhận bao gồm chỉ báo kích hoạt bảo mật, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, và bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn; và khi chỉ báo kích hoạt bảo mật chỉ báo kích hoạt bảo mật, bước kích hoạt, bởi AF thứ hai dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối, trong đó khóa bảo mật được tạo ra dựa trên khóa AF. Bằng cách này, phương án này của sáng chế có thể thực hiện bảo vệ bảo mật đầu cuối giữa thiết bị đầu cuối và AF đối với các yêu cầu dịch vụ khác nhau.

Trong một số phương án, thông điệp thông báo khóa còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, thuật toán bảo mật bao gồm thật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối, và phương pháp

còn bao gồm: bước xác định, bởi AF thứ hai, thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và thuật toán bảo mật được hỗ trợ bởi AF thứ hai, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối và AF thứ hai. Bằng cách này, AF thứ hai có thể tự thương lượng về khả năng bảo mật với thiết bị đầu cuối dựa trên thông tin khả năng bảo mật của thiết bị đầu cuối mà được chuyển tiếp bởi AF thứ nhất.

Trong một số phương án, thông điệp báo nhận còn bao gồm thông tin về thuật toán bảo mật được lựa chọn, và bước kích hoạt, bởi AF thứ hai dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối bao gồm: bước kích hoạt, bởi AF thứ hai dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối. Bằng cách này, phương án này của sáng chế có thể kích hoạt, dựa trên kết quả thương lượng bảo mật giữa thiết bị đầu cuối và AF, bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF. Kết quả thương lượng bảo mật bao gồm thuật toán bảo mật và khóa bảo mật mà được thương lượng giữa thiết bị đầu cuối và AF.

Trong một số phương án, phương pháp còn bao gồm: bước tạo ra, bởi AF thứ hai, chỉ báo kích hoạt bảo mật dựa trên thuật toán bảo mật được lựa chọn, trong đó nếu thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai, chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai; và nếu thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai, chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai. Bằng cách này, chỉ báo kích hoạt bảo mật có thể được tạo ra dựa trên kết quả thương lượng thuật toán bảo mật.

Trong một số phương án, thông điệp thông báo khóa còn bao gồm thông tin về chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không; và phương pháp còn bao gồm: bước tạo ra, bởi AF thứ hai, chỉ báo kích hoạt bảo mật theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi AF thứ hai, trong đó chính sách bảo mật được hỗ trợ bởi AF thứ hai chỉ báo xem AF thứ hai có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không. Bằng cách này, chỉ báo kích hoạt bảo mật có thể được tạo ra dựa trên kết quả thương lượng chính sách bảo mật.

Trong một số phương án, phương pháp còn bao gồm: bước tạo ra, bởi AF thứ hai, khóa bảo mật và mã định danh khóa của khóa bảo mật dựa trên khóa AF và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn. Bằng cách này, AF thứ hai có thể tạo ra, dựa trên thuật toán bảo mật được thương lượng với thiết bị đầu cuối, khóa bảo mật để bảo vệ truyền thông giữa AF thứ hai và thiết bị đầu cuối.

Trong một số phương án, thông điệp báo nhận còn bao gồm mã định danh khóa, và mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai. Bằng cách này, thiết bị đầu cuối có thể xác định ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và xác định khóa bảo mật trong ngữ cảnh bảo mật.

Trong một số phương án, thông điệp báo nhận bao gồm thông số xác minh toàn vẹn thứ nhất, và thông số xác minh toàn vẹn thứ nhất được tính toán dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai và khóa bảo vệ toàn vẹn tương ứng với AF thứ hai. Bằng cách này, thiết bị đầu cuối có thể thực hiện xác minh toàn vẹn đối với thông điệp được gửi bởi AF thứ hai.

Trong một số phương án, phương pháp còn bao gồm: bước nhận, bởi AF thứ hai, thông điệp hoàn thành thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai, và thông số xác minh toàn vẹn thứ hai được tính toán dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai và khóa bảo vệ toàn vẹn tương ứng với AF thứ hai; bước tính toán, bởi AF thứ hai, thông số xác minh toàn vẹn thứ hai cho thông điệp phản hồi thiết lập phiên ứng dụng dựa trên thuật toán bảo vệ toàn vẹn được hỗ trợ bởi cả thiết bị đầu cuối và AF thứ hai và khóa bảo vệ toàn vẹn tương ứng với AF thứ hai; và nếu thông số xác minh toàn vẹn thứ nhất phù hợp với thông số xác minh toàn vẹn thứ hai, bước xác định, bởi AF thứ hai, rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo; và nếu thông số xác minh toàn vẹn thứ nhất không phù hợp với thông số xác minh toàn vẹn thứ hai, bước xác định, bởi AF thứ hai, rằng thông điệp hoàn thành thiết lập phiên ứng dụng bị giả mạo; Bằng cách này, AF thứ hai có thể thực hiện xác minh toàn vẹn đối với thông điệp được gửi bởi thiết bị đầu cuối.

Trong một số phương án, bước kích hoạt, bởi AF thứ hai dựa trên khóa bảo mật tương ứng với AF thứ hai, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối bao gồm: nếu xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, bước kích hoạt, bởi AF thứ hai dựa trên khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị

đầu cuối. Bằng cách này, AF thứ hai có thể kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai.

Trong một số phương án, chỉ báo kích hoạt bảo mật bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Khi chỉ báo bảo vệ bí mật được thiết đặt đến giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng việc bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt. Khi chỉ báo bảo vệ bí mật được thiết đặt đến giá trị được thiết đặt trước thứ hai khác với giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt, và thuật toán bảo vệ bí mật được chỉ báo bởi giá trị được thiết đặt trước thứ hai được sử dụng để bảo vệ bí mật. Khi chỉ báo bảo vệ toàn vẹn được thiết đặt đến giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng việc bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt. Khi chỉ báo bảo vệ toàn vẹn được thiết đặt đến giá trị được thiết đặt trước thứ ba khác với giá trị được thiết đặt trước thứ nhất, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt, và thuật toán bảo vệ toàn vẹn được chỉ báo bởi giá trị được thiết đặt trước thứ ba được sử dụng để bảo vệ toàn vẹn. Bằng cách này, chỉ báo kích hoạt bảo mật có thể chỉ báo hoàn toàn thuật toán bảo mật được sử dụng giữa thiết bị đầu cuối và AF.

Trong một số phương án, AF thứ nhất và AF thứ hai có cùng mã định danh của AF. Bằng cách này, với kịch bản trong đó nhiều AF chia sẻ cùng ID của AF, giải pháp này có thể tạo ra một cách riêng biệt các khóa tương ứng để thực hiện cách ly bảo mật trong kịch bản. AF có thể thực hiện thương lượng khóa với thiết bị đầu cuối thay mặt các AF khác. Do đó, không cần yêu cầu rằng có giao diện giữa mỗi AF và PLMN.

Theo khía cạnh thứ tư, thiết bị truyền thông được đề xuất. Thiết bị truyền thông có thể là thiết bị đầu cuối, hoặc có thể là chíp. Thiết bị truyền thông có chức năng thực thi thiết bị đầu cuối theo khía cạnh bất kỳ trong các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên. Chức năng có thể được thực thi bởi phần cứng, hoặc có thể được thực thi bởi phần mềm tương ứng thực thi phần cứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều bộ phận tương ứng với chức năng phía trên.

Trong một số phương án, thiết bị truyền thông bao gồm: môđun thu phát, được tạo cấu hình để: gửi thông điệp yêu cầu thiết lập phiên ứng dụng đến AF thứ nhất, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA; và nhận thông điệp phản hồi thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên

ứng dụng bao gồm chỉ báo kích hoạt bảo mật, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị truyền thông, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị truyền thông bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị truyền thông và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị truyền thông; và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị truyền thông, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn.

Trong một số phương án, thiết bị truyền thông còn bao gồm: môđun bảo vệ bảo mật, được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với AF thứ hai.

Trong một số phương án, AF thứ nhất và AF thứ hai là AF giống nhau. Thiết bị truyền thông còn bao gồm: môđun tạo ra khóa bảo mật, được tạo cấu hình để: tạo ra khóa AF thứ nhất dựa trên khóa AKMA; và tạo ra khóa bảo mật dựa trên khóa AF thứ nhất và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, AF thứ nhất và AF thứ hai là các AF khác nhau. Thiết bị truyền thông còn bao gồm: môđun tạo ra khóa thứ hai, được tạo cấu hình để: tạo ra khóa AF thứ nhất dựa trên khóa AKMA; tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị truyền thông và AF thứ nhất; và tạo ra khóa bảo mật dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa, và thông số tạo ra khóa bao gồm ít nhất một trong số sau đây: thông tin định danh được sử dụng bởi thiết bị truyền thông trong AF thứ nhất hoặc AF thứ hai; loại dịch vụ được yêu cầu bởi thiết bị truyền thông từ AF thứ nhất hoặc AF thứ hai; thông tin định danh

của AF thứ hai; hoặc thông số làm mới khóa.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa, và thông số tạo ra khóa bao gồm thông số làm mới khóa.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất. Thiết bị truyền thông còn bao gồm: môđun xác minh toàn vẹn, được tạo cấu hình để: xác định, dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ nhất, xem thông điệp phản hồi thiết lập phiên ứng dụng có bị giả mạo hay không.

Trong một số phương án, môđun thu phát còn được tạo cấu hình để: gửi thông điệp hoàn thành thiết lập phiên ứng dụng đến AF thứ hai khi thông điệp phản hồi thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai được tính toán dựa trên khóa bảo mật.

Trong một số phương án, AF thứ nhất và AF thứ hai có cùng mã định danh của AF.

Theo khía cạnh thứ năm, thiết bị truyền thông được đề xuất. Thiết bị truyền thông có thể là AF thứ nhất, hoặc có thể là chíp. Thiết bị truyền thông có chức năng thực thi AF thứ nhất theo khía cạnh bất kỳ trong các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên. Chức năng có thể được thực thi bởi phần cứng, hoặc có thể được thực thi bởi phần mềm tương ứng thực thi phần cứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều bộ phận tương ứng với chức năng phía trên.

Trong một số phương án, thiết bị truyền thông bao gồm: môđun thu phát, được tạo cấu hình để: nhận thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA; và gửi thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật

được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối; và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn.

Trong một số phương án, thiết bị truyền thông còn bao gồm: môđun bảo vệ bảo mật, được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, khởi động AF thứ hai để kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Trong một số phương án, thiết bị truyền thông và AF thứ hai là AF giống nhau. Thiết bị truyền thông còn bao gồm: môđun tạo ra khóa thứ nhất, được tạo cấu hình để: tạo ra khóa AF thứ nhất dựa trên khóa AKMA; và tạo ra khóa bảo mật dựa trên khóa AF thứ nhất và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, thiết bị truyền thông và AF thứ hai là các AF khác nhau. Thiết bị truyền thông còn bao gồm: môđun tạo ra khóa thứ hai, được tạo cấu hình để: tạo ra khóa AF thứ nhất dựa trên khóa AKMA; tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và thiết bị truyền thông; và tạo ra khóa bảo mật mà mã định danh khóa dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, ngữ cảnh bảo mật bao gồm khóa bảo mật, và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa. Môđun thu phát còn được tạo cấu hình để gửi thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được lựa chọn, khóa bảo mật, và mã định danh khóa.

Trong một số phương án, chỉ báo kích hoạt bảo mật được chỉ báo bởi thuật toán bảo mật được lựa chọn, trong đó khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông

giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt.

Trong một số phương án, thiết bị truyền thông còn bao gồm: môđun tạo ra chỉ báo kích hoạt bảo mật, được tạo cấu hình để: xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định.

Trong một số phương án, môđun tạo ra chỉ báo kích hoạt bảo mật còn được tạo cấu hình để: xác định, phụ thuộc vào việc thuật toán bảo vệ bí mật có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF thứ hai hay không, xem có kích hoạt bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và/hoặc xác định, phụ thuộc vào việc thuật toán bảo vệ toàn vẹn có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ toàn vẹn được hỗ trợ bởi AF thứ hai hay không, xem có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không. Môđun tạo ra chỉ báo kích hoạt bảo mật còn được tạo cấu hình để xác định, theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi AF thứ hai, xem có kích hoạt bảo vệ bảo mật hay không, trong đó chính sách bảo mật được hỗ trợ bởi AF thứ hai chỉ báo xem AF thứ hai có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không.

Trong một số phương án, thiết bị truyền thông và AF thứ hai là các AF khác nhau. Thiết bị truyền thông còn bao gồm: môđun tạo ra khóa thứ ba, được tạo cấu hình để: tạo ra khóa AF thứ nhất dựa trên khóa AKMA; và tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và thiết bị truyền thông. Môđun thu phát còn được tạo cấu hình để: gửi thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai; và nhận thông điệp báo nhận từ AF thứ hai, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn, chỉ báo kích hoạt bảo mật, và mã định danh khóa, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật, trong đó thông điệp phản

hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa.

Trong một số phương án, môđun thu phát còn được tạo cấu hình để nhận thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai. Thiết bị truyền thông còn bao gồm: môđun xác minh toàn vẹn, được tạo cấu hình để xác định, dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thành thiết lập phiên ứng dụng có bị giả mạo hay không.

Trong một số phương án, môđun thu phát còn được tạo cấu hình để gửi thông điệp kích hoạt đến AF thứ hai khi xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp kích hoạt chỉ báo AF thứ hai để kích hoạt, dựa trên khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Theo khía cạnh thứ sáu, thiết bị truyền thông được đề xuất. Thiết bị truyền thông có thể là AF thứ hai, hoặc có thể là chíp. Thiết bị truyền thông có chức năng thực thi AF thứ hai theo khía cạnh bất kỳ trong các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên. Chức năng có thể được thực thi bởi phần cứng, hoặc có thể được thực thi bởi phần mềm tương ứng thực thi phần cứng. Phần cứng hoặc phần mềm bao gồm một hoặc nhiều bộ phận tương ứng với chức năng phía trên.

Trong một số phương án, thiết bị truyền thông bao gồm: môđun thu phát, được tạo cấu hình để nhận thông điệp thông báo khóa từ AF thứ nhất, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai; và gửi thông điệp báo nhận đến AF thứ nhất, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, chỉ báo kích hoạt bảo mật, và mã định danh khóa; và thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và thiết bị truyền thông hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, khóa bảo mật được tạo ra dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và thiết bị truyền thông, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

Trong một số phương án, thiết bị truyền thông còn bao gồm: môđun bảo vệ bảo mật, được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, khởi

động, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Trong một số phương án, thiết bị truyền thông còn bao gồm: môđun tạo ra chỉ báo kích hoạt bảo mật, được tạo cấu hình để: xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và thiết bị truyền thông hay không; và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định.

Trong một số phương án, môđun tạo ra chỉ báo kích hoạt bảo mật còn được tạo cấu hình để: xác định, phụ thuộc vào việc thuật toán bảo vệ bí mật có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị truyền thông hay không, xem có kích hoạt bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và thiết bị truyền thông hay không; và/hoặc xác định, phụ thuộc vào việc liệu thuật toán bảo vệ toàn vẹn có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị truyền thông hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và thiết bị truyền thông hay không.

Trong một số phương án, thông điệp thông báo khóa còn bao gồm chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị truyền thông hay không. Môđun tạo ra chỉ báo kích hoạt bảo mật còn được tạo cấu hình để xác định, theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi thiết bị truyền thông, xem có kích hoạt bảo vệ bảo mật hay không, trong đó chính sách bảo mật được hỗ trợ bởi thiết bị truyền thông chỉ báo xem thiết bị truyền thông có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không.

Trong một số phương án, thiết bị truyền thông còn bao gồm: môđun tạo ra khóa, được tạo cấu hình để tạo ra khóa bảo mật và mã định danh khóa dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, môđun thu phát còn được tạo cấu hình để nhận thông điệp hoàn thành thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai. Thiết bị truyền thông còn bao gồm: môđun xác minh toàn vẹn, được tạo cấu hình để xác định, dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thành thiết lập phiên ứng dụng có bị giả mạo hay không.

Trong một số phương án, môđun bảo vệ bảo mật còn được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật và khi xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Theo khía cạnh thứ bảy, thiết bị bảo vệ truyền thông được đề xuất. Thiết bị bao gồm một hoặc nhiều bộ xử lý và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ một hoặc nhiều chương trình. Khi một hoặc nhiều chương trình được thực thi bởi một hoặc nhiều bộ xử lý, thiết bị được cho phép thực hiện phương pháp của thiết bị đầu cuối theo khía cạnh bất kỳ trong số các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ tám, thiết bị bảo vệ truyền thông được đề xuất. Thiết bị bao gồm một hoặc nhiều bộ xử lý và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ một hoặc nhiều chương trình. Khi một hoặc nhiều chương trình được thực thi bởi một hoặc nhiều bộ xử lý, thiết bị được cho phép thực hiện phương pháp của AF thứ nhất theo khía cạnh bất kỳ trong số các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ chín, thiết bị bảo vệ truyền thông được đề xuất. Thiết bị bao gồm một hoặc nhiều bộ xử lý và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ một hoặc nhiều chương trình. Khi một hoặc nhiều chương trình được thực thi bởi một hoặc nhiều bộ xử lý, thiết bị được cho phép thực hiện phương pháp của AF thứ hai theo khía cạnh bất kỳ trong số các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ mười, hệ thống truyền thông được đề xuất. Hệ thống truyền thông bao gồm AF thứ nhất và AF thứ hai. AF thứ nhất được tạo cấu hình để: nhận thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA; và gửi thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị đầu cuối và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối; và thông điệp

phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn. Trong một số phương án, AF thứ nhất còn được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, khởi động AF thứ hai để kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Theo khía cạnh thứ mười một, hệ thống truyền thông được đề xuất. Hệ thống truyền thông bao gồm AF thứ nhất và AF thứ hai khác với AF thứ nhất. AF thứ nhất được tạo cấu hình để: nhận thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA và thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối; tạo ra khóa AF thứ nhất dựa trên khóa AKMA tương ứng với mã định danh AKMA; tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất; gửi thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai; nhận thông điệp báo nhận từ AF thứ hai, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, chỉ báo kích hoạt bảo mật, và mã định danh khóa; và gửi thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông tin về thuật toán bảo mật được lựa chọn, chỉ báo kích hoạt bảo mật, và mã định danh khóa. Thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn. Chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không. Bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, trong đó khóa bảo mật được tạo ra dựa trên khóa AF thứ hai. Mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật. AF thứ hai được tạo cấu hình để: nhận thông điệp thông báo khóa từ AF thứ nhất, tạo ra khóa bảo mật dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, và gửi thông điệp báo nhận đến AF thứ nhất. AF thứ hai còn được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Theo khía cạnh thứ mười hai, phương tiện lưu trữ đọc được bằng máy tính được đề xuất. Phương tiện lưu trữ đọc được bằng máy tính lưu trữ chương trình. Chương trình cho phép thiết bị đầu cuối thực hiện phương pháp của thiết bị đầu cuối theo khía cạnh bất kỳ trong số các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ mười ba, phương tiện lưu trữ đọc được bằng máy tính được đề xuất. Phương tiện lưu trữ đọc được bằng máy tính lưu trữ chương trình. Chương trình cho phép AF thứ nhất thực hiện phương pháp của AF thứ nhất theo khía cạnh bất kỳ trong số các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ mười bốn, phương tiện lưu trữ đọc được bằng máy tính được đề xuất. Phương tiện lưu trữ đọc được bằng máy tính lưu trữ chương trình. Chương trình cho phép AF thứ hai thực hiện phương pháp của AF thứ hai theo khía cạnh bất kỳ trong số các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ mười lăm, chíp truyền thông được đề xuất, trong đó chíp truyền thông lưu trữ các lệnh. Khi các lệnh được chạy trên chíp truyền thông, chíp truyền thông được cho phép thực hiện phương pháp theo khía cạnh bất kỳ trong các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Theo khía cạnh thứ mười lăm, sản phẩm chương trình máy tính được đề xuất. Khi sản phẩm chương trình máy tính chạy trên máy tính, máy tính được cho phép thực hiện phương pháp theo khía cạnh bất kỳ trong các khía cạnh phía trên hoặc các phương án khả thi của các khía cạnh phía trên.

Mô tả vắn tắt các hình vẽ

Fig.1A và Fig.1B là các sơ đồ khối của kiến trúc hệ thống 3GPP (3rd Generation Partnership Project, Dự án đối tác thế hệ thứ ba) trong 5G;

Fig.2 là sơ đồ khối của mô hình mạng ví dụ đối với AKMA trong 5G;

Fig.3A và Fig.3B là các sơ đồ trao đổi tín hiệu của quy trình AKMA trong giải pháp thông thường;

Fig.4A là sơ đồ khối của hệ thống ví dụ mà các phương án của sáng chế có thể được áp dụng;

Fig.4B là sơ đồ dạng giản đồ của kịch bản ứng dụng ví dụ mà các phương án của sáng chế có thể được áp dụng;

Fig.5 là sơ đồ trao đổi tín hiệu của quy trình bảo vệ truyền thông ví dụ theo phương án

của sáng chế;

Fig.6 là sơ đồ khối của kiến trúc khóa ví dụ theo phương án của sáng chế;

Fig.7A và Fig.7B là sơ đồ trao đổi tín hiệu của quy trình bảo vệ truyền thông ví dụ khác theo phương án của sáng chế;

Fig.8 là lưu đồ của phương pháp bảo vệ truyền thông ví dụ theo phương án của sáng chế;

Fig.9 là lưu đồ của phương pháp bảo vệ truyền thông ví dụ theo phương án của sáng chế;

Fig.10 là lưu đồ của phương pháp bảo vệ truyền thông ví dụ theo phương án của sáng chế;

Fig.11 là sơ đồ khối của thiết bị truyền thông ví dụ theo phương án của sáng chế;

Fig.12 là sơ đồ khối của thiết bị truyền thông ví dụ theo phương án của sáng chế;

Fig.13 là sơ đồ khối của thiết bị truyền thông ví dụ theo phương án của sáng chế;

Fig.14 là sơ đồ khối đơn giản hóa của thiết bị ví dụ có thể áp dụng để thực thi phương án của sáng chế; và

Fig.15 là sơ đồ dạng giản đồ của phương tiện đọc được bằng máy tính có thể áp dụng để thực thi phương án của sáng chế.

Trong các hình vẽ kèm theo, các số tham chiếu giống nhau hoặc tương ứng thể hiện các phần giống nhau hoặc tương ứng.

Mô tả chi tiết sáng chế

Các nguyên lý của sáng chế giờ sẽ được mô tả tham chiếu đến một số phương án ví dụ. Cần hiểu rằng các phương án này chỉ được mô tả nhằm mục đích minh họa, và giúp người có hiểu biết trung bình hiểu và thực hiện sáng chế, mà không ngụ ý bất kỳ giới hạn nào về phạm vi của sáng chế. Ngoài các cách được mô tả dưới đây, nội dung được bộc lộ được mô tả trong sáng chế có thể được thực thi theo các cách khác nhau.

Trong phần mô tả và các yêu cầu bảo hộ dưới đây, trừ khi được quy định khác, tất cả các thuật ngữ kỹ thuật và công nghệ được sử dụng trong bản mô tả này có cùng ý nghĩa như được hiểu thông thường bởi những người có hiểu biết trung bình trong lĩnh vực của sáng chế này.

Khi được sử dụng ở đây, các dạng số ít cũng nhằm để bao gồm các dạng số nhiều, trừ khi được quy định khác trong ngữ cảnh. Thuật ngữ "bao gồm" và những biến thể của nó cần

được diễn giải là các thuật ngữ mở, nghĩa là "bao gồm nhưng không bị giới hạn". Thuật ngữ "dựa trên" cần được diễn giải là "ít nhất dựa trên một phần". Các thuật ngữ "một phương án" và "phương án" cần được diễn giải là "ít nhất một phương án". Thuật ngữ "phương án khác" cần được hiểu là "ít nhất một phương án khác". Các thuật ngữ "thứ nhất", "thứ hai", và tương tự có thể thể hiện các đối tượng khác nhau hoặc giống nhau. Các định nghĩa khác (rõ ràng và ẩn) có thể được bao gồm dưới đây.

Trong một số ví dụ, giá trị, quy trình, hoặc thiết bị được đề cập đến là giá trị, quy trình, hoặc thiết bị, "tốt nhất", "cao nhất", "tối thiểu", hoặc "tối đa" hoặc tương tự. Cần hiểu rằng mô tả như vậy nhằm để thể hiện rằng việc lựa chọn có thể được thực hiện trong số nhiều thay thế về chức năng được sử dụng, và rằng lựa chọn như vậy không cần phải là tốt hơn, nhỏ hơn, lớn hơn, hoặc tốt hơn là khác với các lựa chọn khác.

Truyền thông được thảo luận trong sáng chế này có thể phù hợp với mọi tiêu chuẩn thích hợp, bao gồm nhưng không bị hạn chế bởi giao diện vô tuyến mới (new radio, NR), truy nhập vô tuyến thế hệ sau (long term evolution, LTE), truy cập vô tuyến thế hệ sau cải tiến (LTE-advanced, LTE-A), đa truy nhập phân chia theo mã băng rộng (wideband code division multiple access, WCDMA), đa truy nhập phân chi theo mã (code division multiple access, CDMA), và hệ thống thông tin di động toàn cầu (global system for mobile communications, GSM). Ngoài ra, truyền thông có thể được thực hiện theo giao thức truyền thông được biết hiện nay hoặc giao thức truyền thông theo thế hệ bất kỳ sẽ được phát triển trong tương lai. Các ví dụ về giao thức truyền thông bao gồm nhưng không bị hạn chế bởi các giao thức truyền thông thế hệ thứ nhất (1st-generation 1G), thế hệ thứ hai (2nd-generation, 2G), 2.5G, 2.75G, thế hệ thứ ba (3rd-generation, 3G), thế hệ thứ tư (4th-generation, 4G), 4.5G, và thế hệ thứ năm (5th-generation, 5G).

Nhằm mục đích mô tả, sau đây mô tả các phương án của sáng chế trong ngữ cảnh của hệ thống truyền thông 3 GPP 5G. Tuy nhiên, cần hiểu rằng các phương án của sáng chế không bị giới hạn ở việc được áp dụng với hệ thống truyền thông 3GPP 5G, mà còn có thể được áp dụng với hệ thống truyền thông bất kỳ có vấn đề tương tự, ví dụ, mạng cục bộ không dây (Wireless Local Area Network, WLAN), hệ thống truyền thông có dây, hoặc hệ thống truyền thông khác được phát triển trong tương lai.

Fig.1A và Fig.1B là các sơ đồ khối của kiến trúc hệ thống 3GPP 100 trong 5G. Như được thể hiện trên Fig.1A, kiến trúc hệ thống 100 bao gồm các chức năng (còn được gọi là "các bộ phận mạng") và các thực thể mạng sau đây: chức năng lựa chọn lát cắt mạng (Network

Slice Selection Function, NSSF) 101, chức năng máy chủ xác thực (Authentication Server Function, AUSF) 102, quản lý dữ liệu thống nhất (Unified Data Management, UDM) 103, chức năng quản lý truy cập và di động (Access and Mobility Management Function, AMF) 104, chức năng quản lý phiên (Session Management Function, SMF) 105, chức năng kiểm soát chính sách (Policy Control Function, PCF) 106, chức năng ứng dụng (Application Function, AF) 107, thiết bị người dùng (User Equipment, UE) 108, thiết bị mạng truy nhập vô tuyến (Radio Access Network, RAN) 109, chức năng mặt phẳng người dùng (User Plane Function, UPF) 110, và mạng dữ liệu (Data Network, DN) 111.

UE 108 được kết nối với AMF 104 thông qua giao diện N1. UE 108 được kết nối với RAN 109 bằng cách sử dụng giao thức điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC). RAN 109 được kết nối với AMF 104 thông qua giao diện N2, và RAN 109 được kết nối với UPF 110 thông qua giao diện N3. Nhiều UPF 110 được kết nối với nhau thông qua giao diện N9. UPF 110 được kết nối với DN 111 thông qua giao diện N6, và còn được kết nối với SMF 105 thông qua giao diện N4. SMF 105 được kết nối với PCF 106 thông qua giao diện N7, SMF 105 còn được kết nối với UDM 103 thông qua giao diện N10, và SMF 105 được kết nối với AMF 104 thông qua giao diện N11. Nhiều AMF 104 được kết nối với nhau thông qua giao diện N14. AMF 104 được kết nối với UDM 103 thông qua giao diện N8, AMF 104 còn được kết nối với AUSF 102 thông qua giao diện N12, và AMF 104 được kết nối với PCF 106 thông qua giao diện N15. AUSF 102 được kết nối với UDM 103 thông qua giao diện N13. AMF 104 và SMF 105 thu được dữ liệu thuê bao người dùng từ UDM 103 thông qua giao diện N8 và giao diện N10 tương ứng, và thu được dữ liệu chính sách từ PCF 106 thông qua giao diện N15 và giao diện N7 tương ứng. AF 107 được kết nối với PCF 106 thông qua giao diện N5. Một số giao diện trên Fig.1A có thể được thực thi bởi các giao diện dựa trên dịch vụ, như được thể hiện trên Fig.1B.

Trên Fig.1B, Nnssf thể hiện giao diện dựa trên dịch vụ được cung cấp bởi NSSF 101. Nnef thể hiện giao diện dựa trên dịch vụ được cung cấp bởi bộ phận mạng chức năng tiếp xúc mạng (Network Exposure Function, NEF) 112. Nnrf thể hiện giao diện dựa trên dịch vụ được cung cấp bởi bộ phận mạng chức năng kho chứa mạng (Network Repository Function, NRF) 113. Npcf thể hiện giao diện dựa trên dịch vụ được cung cấp bởi PCF 106. Nudm thể hiện giao diện dựa trên dịch vụ được cung cấp bởi UDM 103. Naf thể hiện giao diện dựa trên dịch vụ được cung cấp bởi AF 107. Nauf thể hiện giao diện dựa trên dịch vụ được cung cấp bởi AUSF 102. Namf thể hiện giao diện dựa trên dịch vụ được cung cấp bởi AMF 104. Nsmf thể

hiện giao diện dựa trên dịch vụ được cung cấp bởi SMF 105.

Sau đây mô tả vắn tắt một số thực thể và phần tử mạng trong kiến trúc hệ thống 3GPP trong 5G.

UE 108 thể hiện thiết bị đầu cuối, và thiết bị đầu cuối có thể là thiết bị đầu cuối cầm tay, máy tính xách tay, bộ phận thuê bao, điện thoại di động, điện thoại thông minh, thẻ dữ liệu không dây, thiết bị kỹ thuật số hỗ trợ cá nhân, máy tính bảng, bộ điện thoại không dây, hoặc trạm đường dây thuê bao vô tuyến (Wireless Local Loop, WLL), thiết bị đầu cuối truyền thông dạng máy (Machine Type Communication, MTC), hoặc thiết bị khác mà có thể truy nhập mạng. Thiết bị đầu cuối truyền thông với thiết bị mạng truy cập bằng cách sử dụng công nghệ giao diện vô tuyến.

RAN 109 chịu trách nhiệm chủ yếu việc quản lý tài nguyên vô tuyến, quản lý chất lượng của dịch vụ (Quality Of Service, QoS), nén và mã hóa dữ liệu, và các chức năng khác ở phía giao diện vô tuyến. RAN 109 có thể bao gồm các trạm gốc dưới các dạng khác nhau, bao gồm nhưng không bị giới hạn bởi trạm gốc vĩ mô, trạm gốc vi mô (còn được gọi là ô nhỏ), trạm chuyển tiếp, điểm truy cập, và tương tự. Trong các hệ thống sử dụng các công nghệ truy cập vô tuyến, tên của thiết bị có chức năng trạm gốc có thể thay đổi. Ví dụ, trong hệ thống thế hệ thứ ba (3rd generation, 3G), thiết bị được gọi là trạm phát sóng vô tuyến thế hệ thứ 3 NodeB (Node B); trong hệ thống LTE, thiết bị được gọi là trạm thu phát sóng vô tuyến thế hệ thứ tư NodeB (evolved NodeB, eNB hoặc eNodeB); và trong hệ thống thế hệ thứ năm (5th generation, 5G), thiết bị được gọi là gNB.

AMF 104 là bộ phận mạng lõi, và chủ yếu chịu trách nhiệm xử lý tín hiệu, bao gồm nhưng không bị hạn chế bởi các chức năng như là điều khiển truy cập, quản lý di động, đính kèm và tách rời, và lựa chọn cổng. Khi AMF 104 cung cấp dịch vụ cho phiên trong UE 108, AMF cung cấp tài nguyên lưu trữ mặt phẳng điều khiển cho phiên, để lưu trữ mã định danh phiên, mã định danh phần tử mạng SMF liên quan đến mã định danh phiên, và tương tự.

SMF 105 chịu trách nhiệm lựa chọn phần tử mạng mặt phẳng người dùng, chuyển hướng phần tử mạng mặt phẳng người dùng, gán địa chỉ giao thức mạng (Internet Protocol, IP), thiết lập kênh mang, sửa đổi, và giải phóng, và điều khiển QoS.

UPF 110 chịu trách nhiệm chuyển tiếp và nhận dữ liệu người dùng trong UE 108. UPF 110 có thể nhận dữ liệu người dùng từ DN 111, và truyền dữ liệu người dùng đến UE 108 thông qua RAN 109. UPF 110 có thể còn nhận dữ liệu người dùng từ UE 108 thông qua RAN 109, và chuyển tiếp dữ liệu người dùng đến DN 111. Tài nguyên truyền dẫn và chức năng lập

lịch mà được sử dụng bởi UPF 110 để cung cấp dịch vụ cho UE 108 được quản lý và được điều khiển bởi SMF 105.

PCF 106 chủ yếu hỗ trợ cung cấp khung chính sách thống nhất để điều khiển hành vi mạng, và cung cấp quy tắc chính sách cho chức năng mạng lớp điều khiển, và chịu trách nhiệm thu nhận thông tin thuê bao liên quan đến chính sách của thuê bao.

AUSF 102 chủ yếu cung cấp chức năng xác thực, và hỗ trợ xác thực đối với truy cập 3GPP và truy cập không phải 3GPP.

NEF 112 hỗ trợ chủ yếu tương tác bảo mật giữa mạng 3GPP và ứng dụng bên thứ ba. NEF 112 có thể thể hiện một cách bảo mật các khả năng và các sự kiện mạng với bên thứ ba để nâng cao hoặc cải thiện chất lượng dịch vụ ứng dụng. Mạng 3GPP cũng có thể thu được một cách an toàn dữ liệu liên quan từ bên thứ ba để nâng cao khả năng ra quyết định mạng thông minh. Ngoài ra NEF 112 hỗ trợ khôi phục dữ liệu cấu trúc từ kho chứa dữ liệu đồng nhất hoặc khôi phục dữ liệu cấu trúc trong kho chứa dữ liệu.

UDM 103 chủ yếu chịu trách nhiệm khôi phục dữ liệu cấu trúc. Nội dung được lưu trữ bao gồm dữ liệu thuê bao và dữ liệu chính sách, dữ liệu cấu trúc được thể hiện bên ngoài, và dữ liệu liên quan đến ứng dụng.

AF 107 chủ yếu hỗ trợ tương tác với mạng lõi 3GPP để cung cấp dịch vụ, ví dụ, dịch vụ mà tác động đến quyết định định tuyến dữ liệu hoặc chức năng kiểm soát chính sách, hoặc một số dịch vụ bên thứ ba được cung cấp cho phía mạng.

Kiến trúc AKMA được xác định trong hệ thống truyền thông 5G. Thiết bị đầu cuối (ví dụ, UE) và AF có thể thực hiện thỏa thuận khóa dựa trên kiến trúc AKMA, để tạo ra riêng biệt khóa để bảo vệ truyền thông giữa UE và AF.

Fig.2 là sơ đồ khối của mô hình mạng ví dụ 200 đối với AKMA trong 5G. Các bộ phận mạng liên quan đến mô hình mạng 200 bao gồm chức năng neo AKMA (AKMA Anchor Function, AAnF) 201, AF 107, NEF 112, AUSF 102, và tương tự.

AAnF 201 cho phép rút ra khóa gốc AKMA (K_{AKMA}) cho dịch vụ AKMA, nghĩa là, AAnF 201 tương tác với AUSF 102 để thu được khóa gốc AKMA K_{AKMA}, và chịu trách nhiệm để tạo ra, cho AF, khóa K_{AF} được sử dụng bởi AF và thời hạn hiệu lực của K_{AF}.

AF 107 tương tác với bộ phận mạng lõi 3GPP để cung cấp dịch vụ. Ví dụ, AF 107 có thể tương tác với PCF để thực hiện kiểm soát chính sách (như là kiểm soát QoS). AF 107 có thể tương tác với bộ phận mạng lõi 3GPP để cung cấp thông tin về tác động lên định tuyến dịch vụ, và tương tự. Trong kịch bản AKMA, AF 107 cần tương tác với AAnF 201 để thu

được khóa K_{AF} được sử dụng bởi AF và thời hạn hiệu lực của K_{AF}. Dựa trên việc triển khai của nhà vận hành, AF 107 có thể là bộ phận mạng được tin cậy bởi nhà vận hành, và được cho phép để tương tác trực tiếp với chức năng mạng; hoặc có thể là bộ phận mạng không được tin cậy bởi nhà vận hành, và cần tương tác với chức năng mạng liên quan thông qua NEF 112.

NEF 112 là để thể hiện khả năng và sự kiện, dịch thông tin bên trong - bên ngoài, truyền gói không phải IP, và tương tự. Trong kịch bản AKMA, AF 107 thu được dịch vụ của AAnF 201 thông qua NEF 112.

AUSF 102 hỗ trợ xác thực cho truy cập 3GPP và truy cập không phải 3GPP. Trong kịch bản AKMA, AUSF 102 tạo ra khóa gốc AKMA K_{AKMA}, và cung cấp khóa gốc K_{AKMA} cho AAnF 201.

Trên Fig.2, Ua* thể hiện điểm tham chiếu giữa UE 108 và AF 107, và để trao đổi thông điệp giữa UE 108 và AF 107 để hỗ trợ tạo ra khóa trong quy trình AKMA.

Fig.3A và Fig.3B là các sơ đồ trao đổi tín hiệu của quy trình AKMA trong giải pháp thông thường. Fig.3A thể hiện quy trình 310 để tạo ra khóa gốc AKMA K_{AKMA} trong quy trình đăng ký UE. Fig.3B thể hiện quy trình 320 để tạo ra khóa K_{AF} trong quy trình AKMA.

Như được thể hiện trên Fig.3A, trong quy trình trong đó UE 108 đăng ký với mạng lõi 5G, UE 108 và AUSF 102 thực hiện quy trình xác thực chính (311). Sau quy trình xác thực chính, AUSF 102 tạo ra (312) khóa gốc AKMA K_{AKMA} bằng cách sử dụng khóa AUSF K_{AUSF} được tạo ra trong quy trình xác thực chính, và tạo ra (313) ID thông tin định danh khóa K_{AKMA} của K_{AKMA}. AUSF 102 còn cung cấp khóa gốc AKMA K_{AKMA} được tạo ra cho AAnF 201. AAnF 201 tạo ra khóa K_{AF} cho AF 107 dựa trên khóa gốc AKMA K_{AKMA}. Ở phía UE, UE 108 tạo ra (314) khóa gốc AKMA K_{AKMA} bằng cách sử dụng khóa AUSF K_{AUSF} được tạo ra trong quy trình xác thực chính và tạo ra (315) ID mã định danh khóa K_{AKMA} của AKMA.

Sau khi xác thực chính được hoàn thành, UE 108 khởi tạo dịch vụ AKMA.

Như được thể hiện trên Fig.3B, UE 108 gửi (311) thông điệp yêu cầu thiết lập phiên ứng dụng (Application Session Establishment Request) đến AF 107, trong đó thông điệp bao gồm ID mã định danh khóa K_{AKMA}.

Để phản hồi thông điệp yêu cầu thiết lập phiên ứng dụng nhận được, AF 107 gửi (312) thông điệp đến AAnF 201 để yêu cầu khóa K_{AF}. Ví dụ, AF 107 có thể gửi thông điệp yêu cầu khóa (Key Request) đến AAnF 201 để yêu cầu khóa K_{AF}. Ví dụ, đối với giao diện dựa trên dịch vụ, AF 107 có thể gửi thông điệp khác với tên thông điệp dựa trên dịch vụ đến AAnF 201 để yêu cầu khóa K_{AF}. Thông điệp được gửi bởi AF 107 có thể bao gồm ID mã định danh

khóa K_{AKMA} và ID của AF của AF 107.

Nếu khóa gốc AKMA K_{AKMA} tương ứng với ID mã định danh khóa K_{AKMA} tồn tại tại AAnF 201, AAnF 201 có thể tạo ra trực tiếp khóa K_{AF} và thời hạn hiệu lực của K_{AF} dựa trên K_{AKMA}. Nếu không có khóa gốc AKMA K_{AKMA} nào tương ứng với ID mã định danh khóa K_{AKMA} tồn tại tại AAnF 201, AAnF 201 gửi (313) thông điệp đến AUSF 102 để yêu cầu khóa gốc AKMA K_{AKMA}. Ví dụ, AAnF 201 có thể gửi thông điệp yêu cầu khóa AKMA (AKMA Key Request) AKMA đến AUSF 102 để yêu cầu khóa gốc AKMA K_{AKMA}. Ví dụ, đối với giao diện dựa trên dịch vụ, AAnF 201 có thể gửi thông điệp khác với tên thông điệp dựa trên dịch vụ đến AUSF 102 để yêu cầu khóa gốc AKMA K_{AKMA}. Thông điệp được gửi bởi AAnF 201 có thể bao gồm ID mã định danh khóa K_{AKMA}.

AUSF 102 tìm ra khóa gốc AKMA K_{AKMA} tương ứng với ID mã định danh khóa K_{AKMA}. Khi đó, AUSF 102 bao gồm khóa gốc AKMA K_{AKMA} trong thông điệp phản hồi khóa AKMA (AKMA Key Response), và gửi (314) thông điệp phản hồi khóa AKMA đến AAnF 201. AAnF 201 tạo ra (315) khóa K_{AF} và thời hạn hiệu lực của K_{AF} dựa trên khóa gốc AKMA K_{AKMA}. AAnF 201 bao gồm khóa K_{AF} được tạo ra và thời hạn hiệu lực của K_{AF} trong thông điệp phản hồi khóa (Key Response), và gửi (316) thông điệp phản hồi khóa đến AF 107. Để phản hồi thông điệp phản hồi khóa nhận được từ AAnF 201, AF 107 gửi (317) thông điệp phản hồi thiết lập phiên ứng dụng (Application Session Establishment Response) đến UE 108.

Có thể nhận biết được từ phần mô tả phía trên rằng, trong kiến trúc AKMA đang có, khóa ở mức độ chi tiết của mã định danh AF (Identifier, ID) được thương lượng giữa UE và AF. Do đó, khóa ở mức độ chi tiết hơn nữa không thể được thương lượng giữa UE và AF. Kết quả là, bảo vệ bảo mật đầu cuối giữa UE và AF không thể được thực hiện đối với các yêu cầu dịch vụ khác nhau.

Các phương án của sáng chế đề xuất giải pháp bảo vệ truyền thông. Giải pháp này có thể thực hiện thương lượng về khóa chi tiết hơn giữa UE và AF, bằng cách đó kích hoạt bảo vệ bảo mật đầu cuối, chẳng hạn như bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE và AF đối với các yêu cầu dịch vụ khác nhau. Cụ thể, giải pháp này có thể thực hiện thương lượng khả năng bảo mật giữa UE và AF, và có thể tạo ra, dựa trên kết quả thương lượng, khóa được chia sẻ bởi phía UE và phía AF. Thương lượng khả năng bảo mật bao gồm: UE và AF thương lượng xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE và AF hay không, và UE và AF thương lượng về thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn để được sử dụng chung bởi UE và AF, và v.v. Đối với kịch bản trong đó nhiều

AF chia sẻ cùng ID của AF, giải pháp này có thể tạo ra một cách riêng biệt các khóa tương ứng để thực hiện cách ly bảo mật trong kịch bản. AF có thể thực hiện thương lượng khóa với UE thay mặt các AF khác. Do đó, không cần yêu cầu rằng có giao diện giữa mỗi AF và PLMN. Giải pháp cho phép tạo ra nhiều mức độ khóa bảo mật (ví dụ, các khóa bảo vệ bí mật và/hoặc các khóa bảo vệ toàn vẹn) dựa trên các yêu cầu dịch vụ khác nhau (ví dụ, các yêu cầu bảo vệ bí mật và/hoặc các yêu cầu bảo vệ toàn vẹn) giữa UE và AF.

Fig.4A là sơ đồ khối của hệ thống ví dụ 400 mà các phương án của sáng chế có thể được áp dụng. Như được thể hiện trên Fig.4A, hệ thống 400 có thể bao gồm thiết bị đầu cuối 410, AF 420 (sau đây còn được gọi là "AF thứ nhất"), và AF 430 (sau đây còn được gọi là "AF thứ hai').

Trong một số phương án, có thể có giao diện giữa AF 420 và PLMN. Ngoài ra hoặc theo tùy chọn, có thể có giao diện hoặc không có giao diện giữa AF 430 và PLMN. Trong một số phương án, AF 420 có thể được thực hiện ở phía nhà vận hành, trong khi AF 430 có thể được thực hiện ở phía doanh nghiệp. Theo tùy chọn, cả AF 420 và AF 430 có thể được thực hiện ở phía nhà vận hành, hoặc cả AF 420 và AF 430 có thể được thực hiện ở phía doanh nghiệp. Trong một số phương án, AF 420 và AF 430 có cùng ID của AF. Cần hiểu rằng AF 420 và AF 430 có thể được thực hiện trên các thiết bị thực thể khác nhau, hoặc có thể được thực hiện trên cùng thiết bị thực thể. Phạm vi của sáng chế không bị giới hạn ở khía cạnh này.

UE 410 có thể gửi thông tin khả năng bảo mật của UE 410 đến AF 420. Thông tin khả năng bảo mật có thể bao gồm thuật toán bảo mật, chính sách bảo mật, và tương tự được hỗ trợ bởi UE 410.

Trong bản mô tả này, "thuật toán bảo mật" có thể bao gồm thuật toán xác thực, thuật toán bảo vệ bí mật, thuật toán toàn vẹn, và/hoặc tương tự. "Chính sách bảo mật" có thể cho biết xem bảo vệ bí mật và/hoặc bảo vệ toàn vẹn có được hỗ trợ hay không, mà có thể còn được chia nhỏ thành xem bảo vệ bí mật mặt phẳng người dùng/mặt phẳng dữ liệu và/hoặc bảo vệ toàn vẹn có được hỗ trợ hay không, xem bảo vệ bí mật mặt phẳng tín hiệu và/hoặc bảo vệ toàn vẹn có được hỗ trợ hay không, và tương tự.

Để phản hồi thông tin khả năng bảo mật nhận được của UE 410, AF 420 có thể thực hiện thương lượng bảo mật giữa UE 410 và AF 420. AF 420 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 420 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 420, xem có kích hoạt

bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 420 hay không. AF 420 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 420 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 420 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 hay không. AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 hay không. AF 420 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, bao gồm nhưng không bị giới hạn ở thuật toán xác thực, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Theo tùy chọn, AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên thuật toán bảo mật được lựa chọn, hoặc chỉ báo kích hoạt bảo mật có thể được chỉ báo hoàn toàn bởi thuật toán bảo mật được lựa chọn. AF 420 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420, và mã định danh khóa và thời hạn hiệu lực của khóa bảo mật. Theo tùy chọn, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420 có thể không phụ thuộc vào thuật toán bảo mật, nghĩa là, mã định danh thuật toán của thuật toán bảo mật có thể không được sử dụng làm thông số đầu vào để tạo ra khóa bảo mật. Khóa bảo mật có thể bao gồm khóa AF K_{AF1} của AF 420, và các mức độ khác nhau của các khóa bảo mật được tạo ra dựa trên khóa K_{AF1}, bao gồm nhưng không bị giới hạn ở khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn. Mã định danh khóa là để định danh ngữ cảnh bảo mật giữa UE 410 và AF 420. Việc lựa chọn thuật toán và việc tạo ra khóa có thể phụ thuộc vào chỉ báo kích hoạt bảo mật. Cụ thể, lựa chọn thuật toán tương ứng và tạo ra khóa được thực hiện chỉ khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420. Theo tùy chọn, việc lựa chọn thuật toán và việc tạo ra khóa có thể không phụ thuộc vào chỉ báo kích hoạt bảo mật. Trong trường hợp này, chỉ báo kích hoạt bảo mật chỉ để kích hoạt sử dụng thuật toán và khóa bảo mật tương ứng.

Bằng cách này, AF 420 có thể thu được kết quả thương lượng bảo mật thứ nhất giữa UE 410 và AF 420, trong đó kết quả thương lượng bảo mật thứ nhất bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE

410 và AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 420, và thông số tạo ra khóa.

Để phản hồi thông tin khả năng bảo mật nhận được của UE 410, AF 420 có thể còn thực hiện thương lượng bảo mật giữa UE 410 và AF 430. AF 420 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 420 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 430, xem có kích hoạt bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 430 hay không. AF 420 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không. AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không. AF 420 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, ví dụ, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Theo tùy chọn, AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên thuật toán bảo mật được lựa chọn, hoặc chỉ báo kích hoạt bảo mật có thể được chỉ báo hoàn toàn bởi thuật toán bảo mật được lựa chọn. AF 420 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn và thông số tạo ra khóa, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430 và mã định danh khóa của khóa bảo mật. Theo tùy chọn, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430 có thể không phụ thuộc vào thuật toán bảo mật, nghĩa là, mã định danh thuật toán của thuật toán bảo mật có thể không được sử dụng làm thông số đầu vào để tạo ra khóa bảo mật. Khóa bảo mật có thể bao gồm khóa AF K_{AF2} của AF 430, và khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn được tạo ra dựa trên khóa K_{AF2}. Mã định danh khóa là để định danh ngữ cảnh bảo mật giữa UE 410 và AF 430. Việc lựa chọn thuật toán và việc tạo ra khóa có thể phụ thuộc vào chỉ báo kích hoạt bảo mật. Cụ thể, lựa chọn thuật toán tương ứng và tạo ra khóa được thực hiện chỉ khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430. Theo tùy chọn, việc lựa chọn thuật toán

và việc tạo ra khóa có thể không phụ thuộc vào chỉ báo kích hoạt bảo mật. Trong trường hợp này, chỉ báo kích hoạt bảo mật chỉ để kích hoạt sử dụng thuật toán và khóa bảo mật tương ứng.

Bằng cách này, AF 420 có thể thu được kết quả thương lượng bảo mật thứ hai giữa UE 410 và AF 430, trong đó kết quả thương lượng bảo mật thứ hai bao gồm một hoặc nhiều nội dung trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 430, và thông số tạo ra khóa. AF 420 có thể gửi kết quả thương lượng bảo mật thứ hai đến AF 430.

Theo tùy chọn, AF 420 có thể gửi thông tin khả năng bảo mật của UE 410, khóa K_{AF2}, và mã định danh khóa của khóa đến AF 430, để AF 430 tự thực hiện thương lượng bảo mật giữa UE 410 và AF 430. AF 430 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 430 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 430, xem có kích hoạt bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 430 hay không. AF 430 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không. AF 430 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không. AF 430 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, ví dụ, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Theo tùy chọn, AF 430 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên thuật toán bảo mật được lựa chọn, hoặc chỉ báo kích hoạt bảo mật có thể được chỉ báo hoàn toàn bởi thuật toán bảo mật được lựa chọn. AF 430 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn và thông số tạo ra khóa, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430 và mã định danh khóa của khóa bảo mật. Theo tùy chọn, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430 có thể không phụ thuộc vào thuật

toán bảo mật, nghĩa là, mã định danh thuật toán của thuật toán bảo mật có thể không được sử dụng làm thông số đầu vào để tạo ra khóa bảo mật. Khóa bảo mật có thể bao gồm, và khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn được tạo ra dựa trên khóa K_{AF2}. Mã định danh khóa là để định danh ngữ cảnh bảo mật giữa UE 410 và AF 430. Việc lựa chọn thuật toán và việc tạo ra khóa có thể phụ thuộc vào chỉ báo kích hoạt bảo mật. Cụ thể, lựa chọn thuật toán tương ứng và tạo ra khóa được thực hiện chỉ khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430. Theo tùy chọn, việc lựa chọn thuật toán và việc tạo ra khóa có thể không phụ thuộc vào chỉ báo kích hoạt bảo mật. Trong trường hợp này, chỉ báo kích hoạt bảo mật chỉ để kích hoạt sử dụng thuật toán và khóa bảo mật tương ứng.

Bằng cách này, AF 430 có thể thu được kết quả thương lượng bảo mật thứ hai giữa UE 410 và AF 430. AF 430 có thể gửi kết quả thương lượng bảo mật thứ hai đến AF 420.

AF 420 có thể gửi kết quả thương lượng bảo mật thứ nhất và/hoặc kết quả thương lượng bảo mật thứ hai đến UE 410. UE 410 có thể tạo ra, dựa trên một số hoặc tất cả thuật toán bảo mật, mã định danh khóa, và thông số tạo ra khóa mà được bao gồm trong kết quả thương lượng bảo mật thứ nhất, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420. Khóa bảo mật có thể bao gồm khóa AF K_{AF1} của AF 420, và khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn được tạo ra dựa trên khóa K_{AF1}. Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, UE 410 có thể sử dụng khóa bảo mật được tạo ra để thực hiện bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420. UE 410 có thể tạo ra, dựa trên thuật toán bảo mật, mã định danh khóa, và thông số tạo ra khóa mà được bao gồm trong kết quả thương lượng bảo mật thứ hai, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430. Khóa bảo mật có thể bao gồm khóa AF K_{AF2} của AF 430, và khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn được tạo ra dựa trên khóa K_{AF2}. Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, UE 410 có thể sử dụng khóa bảo mật được tạo ra để thực hiện bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430.

Khi kết quả thương lượng bảo mật thứ hai được tạo ra bởi AF 420, AF 420 có thể thực hiện, bằng cách sử dụng khóa bảo vệ toàn vẹn được tạo ra dựa trên K_{AF1}, bảo vệ toàn vẹn đối với thông điệp mà được gửi đến UE 410 và mang kết quả thương lượng bảo mật. Ví dụ, thông điệp có thể bao gồm thông số bảo vệ toàn vẹn được tạo ra dựa trên khóa bảo vệ toàn vẹn. UE 410 có thể xác minh thông số bảo vệ toàn vẹn trong thông điệp bằng cách sử dụng khóa bảo

vệ toàn vẹn được tạo ra dựa trên K_{AF1}. Khi xác minh thành công, UE 410 có thể gửi thông điệp trả lời đến AF 420, trong đó thông điệp trả lời mang thông số bảo vệ toàn vẹn được tạo ra bởi UE 410 dựa trên khóa bảo vệ toàn vẹn. AF 420 có thể xác minh thông số bảo vệ toàn vẹn trong thông điệp bằng cách sử dụng khóa bảo vệ toàn vẹn được tạo ra dựa trên K_{AF1}. Khi xác minh thành công, nếu chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, UE 410 và AF 420 có thể thực hiện, dựa trên khóa bảo mật tương ứng, bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, đối với truyền thông giữa UE 410 và AF 420. Khi xác minh thành công, nếu chỉ báo kích hoạt chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, AF 420 có thể gửi thông điệp kích hoạt đến AF 430 để chỉ báo AF 430 kích hoạt bảo vệ bảo mật đầu cuối đối với truyền thông giữa UE 410 và AF 430. Bằng cách này, UE 410 và AF 430 có thể thực hiện, dựa trên khóa bảo mật tương ứng, bảo vệ bảo mật như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, đối với truyền thông giữa UE 410 và AF 430.

Khi kết quả thương lượng bảo mật thứ hai được tạo ra bởi AF 430, AF 430 có thể thực hiện, bằng cách sử dụng khóa bảo vệ toàn vẹn được tạo ra dựa trên K_{AF2}, bảo vệ toàn vẹn đối với thông điệp mà được gửi đến UE 410 thông qua AF 420 và mang kết quả thương lượng bảo mật. Ví dụ, thông điệp có thể bao gồm thông số bảo vệ toàn vẹn được tạo ra dựa trên khóa bảo vệ toàn vẹn. UE 410 có thể xác minh thông số bảo vệ toàn vẹn trong thông điệp bằng cách sử dụng khóa bảo vệ toàn vẹn được tạo ra dựa trên K_{AF2}. Khi xác minh thành công, UE 410 có thể gửi thông điệp trả lời đến AF 430 thông qua AF 420, trong đó thông điệp trả lời mang thông số bảo vệ toàn vẹn được tạo ra bởi UE 410 dựa trên khóa bảo vệ toàn vẹn. AF 430 có thể xác minh thông số bảo vệ toàn vẹn trong thông điệp bằng cách sử dụng khóa bảo vệ toàn vẹn được tạo ra dựa trên K_{AF2}. Khi xác minh thành công, để phản hồi chỉ báo kích hoạt bảo mật mà chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, UE 410 và AF 430 có thể thực hiện, dựa trên khóa bảo mật tương ứng, bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, đối với truyền thông giữa UE 410 và AF 430.

Fig.4B là sơ đồ dạng giản đồ của kịch bản ứng dụng ví dụ 405 mà các phương án của sáng chế có thể được áp dụng. Trên Fig.4B, UE 410 được thể hiện trên Fig.4A được thực thi như phương tiện bay không người lái (UncrewedAerial Vehicle, UAV), AF 420 được thực thi như thực thể quản lý hệ thống máy bay không người lái (UncrewedAircraft System Traffic Management, UTM), và AF 430 được thực thi như thực thể được ủy quyền của bên thứ ba

(Third Party Authorized Entity, TPAE). Cần hiểu rằng, trong thực thi cụ thể, kịch bản ứng dụng 405 có thể bao gồm một hoặc nhiều TPAE 430. Phạm vi của sáng chế không bị giới hạn ở khía cạnh này.

UAV 410 có thể sử dụng hệ thống 3GPP để truyền thông với UTM 420 và TPAE 430. TPAE 430 có thể đóng vai trò là tổ chức bên thứ ba được ủy quyền để thực hiện quản lý dịch vụ kỹ thuật số đối với phương tiện bay không người lái, và thu nhận thông tin như là danh tính, vị trí, và tốc độ của UAV 410 bằng cách trao đổi thông tin với UAV 410, để giám sát và quản lý UAV. UAV 410 và TPAE 430 có thể truyền thông với nhau thông qua giao diện UAV7, bao gồm nhưng không bị hạn chế ở phương thức quảng bá. Khi UAV 410 truyền thông với TPAE 430 thông qua giao diện UAV7, nội dung thông tin được gửi bởi UAV 410 có thể bao gồm thông tin như là danh tính, vị trí, và tốc độ của UAV 410. Các chức năng chính của UTM 420 bao gồm nhưng không bị giới hạn ở việc thực hiện giám sát UAV, bao gồm quản lý danh tính, theo dõi, thu thập các số liệu thống kê, và tương tự, và có thể được thực thi bởi nền tảng đám mây giám sát. UAV 410 và UTM 420 truyền thông với nhau thông qua giao diện UAV9.

UTM 420 và TPAE 430 có thể sử dụng cùng ID của AF. Các phương án của sáng chế có thể thực hiện bảo vệ bảo mật đầu cuối giữa UAV 410 và UTM 420 và bảo vệ bảo mật đầu cuối giữa UAV 410 và TPAE 430, bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn. Khóa được sử dụng giữa UAV 410 và UTM 420 là khác với khóa được sử dụng giữa UAV 410 và TPAE 430. Sau đây còn mô tả chi tiết các phương án khác nhau của sáng chế với sự tham chiếu đến kịch bản ví dụ được thể hiện trên Fig.4B.

Fig.5 là sơ đồ trao đổi tín hiệu của quy trình bảo vệ truyền thông ví dụ 500 theo phương án của sáng chế. Trong ví dụ được thể hiện trên Fig.5, AF 420 thay thế AF 430 đối với lựa chọn thuật toán và tạo ra khóa.

Như được thể hiện trên Fig.5, xác thực chính (310) được hoàn thành giữa UE 410 và AAnF 105 để tạo ra khóa gốc AKMA K_{AKMA} và ID mã định danh khóa K_{AKMA} của chúng. Quy trình xác thực chính là giống với quy trình 310 được thể hiện trên Fig.3. Chi tiết không được mô tả lại ở đây.

UE 410 có thể gửi (501) thông điệp yêu cầu thiết lập phiên ứng dụng (Application Session Establishment Request) đến AF 420. Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng có thể bao gồm ID mã định danh khóa K_{AKMA}.

Ngoài ra hoặc theo tùy chọn, thông điệp yêu cầu thiết lập phiên ứng dụng có thể bao gồm thông tin định danh của AF 430, để AF 420 lựa chọn AF 430 dựa trên thông tin định

danh. Thông tin định danh có thể là tên hoặc ID của AF 430.

Ngoài ra hoặc theo tùy chọn, thông điệp yêu cầu thiết lập phiên ứng dụng có thể còn bao gồm thông tin khả năng bảo mật của UE 410. Thông tin khả năng bảo mật có thể bao gồm thuật toán bảo mật, chính sách bảo mật, và tương tự được hỗ trợ bởi UE 410. Thuật toán bảo mật có thể bao gồm thuật toán xác thực, thuật toán bảo vệ bí mật, thuật toán toàn vẹn, và/hoặc tương tự. Thuật toán xác thực, có thể là, ví dụ, thuật toán EAP-TLS (giao thức xác thực mở rộng - bảo mật lớp vận chuyển -Extensible Authentication Protocol – Transport Layer Security, EAP-TLS). Chính sách bảo mật bao gồm liệu UE 410 có hỗ trợ bảo vệ bí mật và/hoặc bảo vệ toàn vẹn hay không, mà có thể còn được chia nhỏ thành liệu bảo vệ bí mật mặt phẳng người dùng/mặt phẳng dữ liệu và/hoặc bảo vệ toàn vẹn có được hỗ trợ hay không, và liệu bảo vệ bí mật mặt phẳng tín hiệu và/hoặc bảo vệ toàn vẹn có được hỗ trợ hay không. Theo tùy chọn, thông tin khả năng bảo mật có thể còn bao gồm mã định danh khả năng bảo mật, phiên bản phần mềm khách hàng của AF 420 hoặc AF 430 tại UE 410, và/hoặc tương tự.

Ngoài ra hoặc theo tùy chọn, thông điệp yêu cầu thiết lập phiên ứng dụng có thể còn bao gồm thông số tạo ra khóa được sử dụng bởi UE 410, để chia sẻ với AF 420 và AF 430. Thông số tạo ra khóa có thể bao gồm ít nhất một trong số sau đây: thông tin nhận dạng được sử dụng bởi UE 410 trong AF 420 và/hoặc AF 430, loại dịch vụ được yêu cầu bởi UE 410, thông tin định danh của AF 430, thông số làm mới, tên mạng dữ liệu (Data Network Name, DNN), hoặc tương tự.

Thông tin nhận dạng có thể là tên người dùng, ID người dùng, hoặc tương tự được sử dụng bởi UE 410 trong AF 420 hoặc AF 430. Ví dụ, nếu UE 410 đã đăng ký nhiều tên người dùng trong AF 420 hoặc AF 430, thông tin nhận dạng có thể thể hiện tên bất kỳ trong nhiều tên người dùng. Thông tin nhận dạng giúp thực hiện cách ly bảo mật giữa các tên người dùng khác nhau. Ví dụ, giả định rằng UE 410 là thiết bị công cộng, và người dùng A và người dùng B sử dụng riêng rẽ UE để thương lượng với AF về khóa. Trong giải pháp hiện tại, khóa của người dùng A và khóa của người dùng B sẽ giống nhau do họ sử dụng UE giống nhau. Việc sử dụng thông tin nhận dạng của UE làm thông số tạo ra khóa có thể thực hiện cách ly bảo mật giữa các tên người dùng khác nhau.

Các ví dụ về loại dịch vụ có thể bao gồm nhưng không bị giới hạn ở dịch vụ phương tiện bay không người lái, dịch vụ định vị, và tương tự. Việc sử dụng loại dịch vụ làm thông số tạo ra khóa giúp thực hiện cách ly bảo mật dữ liệu giữa các loại dịch vụ khác nhau.

Thông tin định danh của AF 430 có thể là tên ứng dụng, tên bộ phận, hoặc ID của AF

430. Các dịch vụ của Tencent được sử dụng là ví dụ. Các ứng dụng khác nhau như là WeChat và QQ có thể tồn tại dưới dùng ID của AF. Việc sử dụng tên ứng dụng cụ thể làm thông số tạo ra khóa giúp thực hiện cách ly bảo mật dữ liệu giữa các ứng dụng khác nhau. Kịch bản ứng dụng phương tiện bay không người lái được thể hiện trên Fig.4B được sử dụng làm ví dụ. Các ví dụ về thông tin định danh của AF 430 bao gồm nhưng không bị giới hạn ở TAPE, hệ thống con quản lý bay UAV (UAV Flight Management Subsystem, UFMS), nhà cung cấp dịch vụ UAV (UAV Service Supplier, USS), cơ quan hàng không dân dụng (Civil Aviation Authority), và tương tự. AF 420 có thể lựa chọn AF 430 dựa trên thông tin định danh của AP 430.

Thông số làm mới có thể là số ngẫu nhiên, giá trị đếm, hoặc tương tự được tạo ra tại chỗ bởi UE 410. Thông số làm mới giúp thực hiện định kỳ cập nhật khóa tùy chỉnh. Mặt khác, các chu kỳ cập nhật ở các mức độ khác nhau đối với các khóa bảo mật được tạo ra bởi chu kỳ cập nhật khóa AF, nghĩa là, các chu kỳ cập nhật ở các mức độ khác nhau của các khóa bảo mật được tạo ra phù hợp nhiều nhất với chu kỳ cập nhật khóa AF.

Để phản hồi thông điệp yêu cầu thiết lập phiên ứng dụng nhận được, AF 420 có thể lưu trữ thông tin khả năng bảo mật của UE và thông số tạo ra khóa mà được mang trong thông điệp. Sau đó, AF 420 gửi (502) thông điệp đến AAnF 201 để yêu cầu khóa AF K_{AF1} của AF 420. Ví dụ, AF 420 có thể gửi thông điệp yêu cầu khóa (Key Request) đến AAnF 201 để yêu cầu khóa K_{AF1}. Ví dụ, đối với giao diện dựa trên dịch vụ, AF 420 có thể gửi thông điệp khác với tên thông điệp dựa trên dịch vụ đến AAnF 201 để yêu cầu khóa K_{AF1}. Thông điệp được gửi bởi AF 420 có thể bao gồm ID mã định danh khóa K_{AKMA} và ID của AF của AF 420.

Nếu khóa gốc AKMA K_{AKMA} tương ứng với ID mã định danh khóa K_{AKMA} tồn tại tại AAnF 201, AAnF 201 có thể tạo ra trực tiếp khóa K_{AF1} và khoảng thời hạn hiệu lực của K_{AF1} dựa trên K_{AKMA}. Nếu không có khóa gốc AKMA K_{AKMA} nào tương ứng với ID mã định danh khóa K_{AKMA} tồn tại tại AAnF 201, AAnF 201 gửi (503) thông điệp đến AUSF 102 để yêu cầu khóa gốc AKMA K_{AKMA}. Ví dụ, AAnF 201 có thể gửi thông điệp yêu cầu khóa AKMA (AKMA Key Request) AKMA đến AUSF 102 để yêu cầu khóa gốc AKMA K_{AKMA}. Ví dụ, đối với giao diện dựa trên dịch vụ, AAnF 201 có thể gửi thông điệp khác với tên thông điệp dựa trên dịch vụ đến AUSF 102 để yêu cầu khóa gốc AKMA K_{AKMA}. Thông điệp được gửi bởi AAnF 201 có thể bao gồm ID mã định danh khóa K_{AKMA}.

AUSF 102 tìm ra khóa gốc AKMA K_{AKMA} tương ứng với ID mã định danh khóa K_{AKMA}. Khi đó, AUSF 102 bao gồm khóa gốc AKMA K_{AKMA} trong thông điệp phản hồi khóa

AKMA (AKMA Key Response), và gửi (504) thông điệp phản hồi khóa AKMA đến AAnF 201. AAnF 201 tạo ra (505) khóa AF K_{AF1} của AF 420 và khoảng thời hạn hiệu lực của K_{AF1} dựa trên khóa gốc AKMA K_{AKMA}. AAnF 201 bao gồm khóa K_{AF1} được tạo ra và thời hạn hiệu lực của K_{AF1} trong thông điệp phản hồi khóa (Key Response), và gửi (506) thông điệp phản hồi khóa đến AF 420. Cần hiểu rằng quy trình trao đổi tín hiệu được thể hiện trong các bước từ 502 đến 506 trên Fig.5 là giống với trong quy trình trao đổi tín hiệu được thể hiện trong các bước từ 312 đến 316 trên Fig.3. Chi tiết không được mô tả lại ở đây.

Như được thể hiện trên Fig.5, AF 420 có thể thực hiện riêng biệt việc thương lượng bảo mật (507) giữa AF 420 và UE 410, để thu nhận kết quả thương lượng bảo mật thứ nhất. Kết quả thương lượng bảo mật thứ nhất có thể bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 420, và thông số tạo ra khóa.

Cần hiểu rằng mặc dù quy trình thương lượng bảo mật được thể hiện trong các bước từ 507 đến 512 trên Fig.5 được thể hiện sau quy trình AKMA được thể hiện trong các bước từ 502 đến 506, điều này đơn thuần là thực thi ví dụ của sáng chế, và không ngụ ý giới hạn đối với phạm vi của sáng chế. Trong cách triển khai khác của sáng chế, quy trình thương lượng bảo mật được thể hiện trong các bước từ 507 đến 512 có thể không phụ thuộc vào các bước từ 502 đến 506 phía trên. Nói cách khác, quy trình thương lượng bảo mật có thể được áp dụng với quy trình AKMA, hoặc có thể độc lập với quy trình AKMA.

Trong một số phương án, AF 420 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 420 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 420, xem có kích hoạt bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 420 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. Ví dụ, nếu UE 410 hỗ trợ bảo vệ bí mật và AF 420 cũng hỗ trợ bảo vệ bí mật, AF 420 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ bí mật, AF 420 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 không cần được kích hoạt. Ví dụ khác, nếu UE 410 hỗ trợ bảo vệ toàn vẹn và AF 420 cũng hỗ trợ bảo vệ toàn vẹn, AF 420 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ toàn vẹn, AF

420 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 không cần được kích hoạt. Theo tùy chọn, AF 420 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 420 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 420 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 hay không. AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 hay không.

Trong một số phương án, chỉ báo kích hoạt bảo mật được tạo ra bởi AF 420 bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Dạng thể hiện của chỉ báo kích hoạt bảo mật có thể là chỉ báo rõ ràng. Ví dụ, '11' chỉ báo rằng cả hai bảo vệ bí mật và bảo vệ toàn vẹn được kích hoạt; '10' chỉ báo rằng bảo vệ bí mật được kích hoạt nhưng bảo vệ toàn vẹn không được kích hoạt; '00' chỉ báo rằng bảo vệ bí mật và bảo vệ toàn vẹn đều không được kích hoạt; và '01' chỉ báo rằng bảo vệ bí mật không được kích hoạt nhưng bảo vệ toàn vẹn được kích hoạt. Theo tùy chọn, chỉ báo kích hoạt bảo mật có thể được thể hiện hoàn toàn bởi thuật toán bảo mật được lựa chọn. Khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn được kích hoạt. Ví dụ, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 1, NEA=thuật toán bảo vệ bí mật 2", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 1 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 2 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=không, NEA=thuật toán bảo vệ bí mật 3", trong đó thông tin chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt và thuật toán bảo vệ bí mật 3 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật

toán bảo vệ toàn vẹn 4, NEA=thuật toán bảo vệ bí mật 5", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 4 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 5 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 6, NEA=không", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 6 được sử dụng để kích hoạt bảo vệ toàn vẹn và bảo vệ bí mật không được kích hoạt.

Trong một số phương án, AF 420 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, bao gồm nhưng không bị giới hạn ở thuật toán xác thực, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Ví dụ, AF 420 có thể xác định các thuật toán bảo mật cùng được hỗ trợ bởi UE 410 và AF 420, và ưu tiên các thuật toán bảo mật, trong đó thuật toán bảo mật có mức ưu tiên cao nhất được lựa chọn. AF 420 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420, và mã định danh khóa của khóa bảo mật.

Trong một số phương án, khóa bảo mật có thể bao gồm các mức độ khác nhau của các khóa bảo mật được tạo ra dựa trên khóa AF K_{AF1} của AF 420, bao gồm nhưng không bị giới hạn ở khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn. Ví dụ, AF 420 có thể tạo ra khóa xác thực dựa trên khóa K_{AF1} và mã định danh của thuật toán xác thực được lựa chọn, trong đó khóa xác thực là để thực hiện xác thực giữa UE 410 và AF 420. AF 420 có thể tạo ra khóa bảo vệ bí mật dựa trên khóa K_{AF1} và mã định danh của thuật toán bảo vệ bí mật được lựa chọn, trong đó khóa bảo vệ bí mật là để thực hiện mã hóa và giải mã đối với nội dung truyền thông giữa UE 410 và AF 420. AF 420 có thể tạo ra khóa bảo vệ toàn vẹn dựa trên khóa K_{AF1} và mã định danh của thuật toán toàn vẹn được lựa chọn, trong đó khóa bảo vệ toàn vẹn là để thực hiện bảo vệ toàn vẹn và xác minh đối với nội dung truyền thông giữa UE 410 và AF 420.

Trong một số phương án, việc lựa chọn thuật toán và việc tạo ra khóa có thể phụ thuộc vào chỉ báo kích hoạt bảo mật. Nghĩa là, lựa chọn thuật toán tương ứng và tạo ra khóa được thực hiện chỉ khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420. Theo tùy chọn, việc lựa chọn thuật toán và việc tạo ra khóa có thể không phụ thuộc vào chỉ báo kích hoạt bảo mật. Trong trường hợp này, chỉ báo kích hoạt bảo mật chỉ để kích hoạt sử dụng thuật toán và khóa bảo mật tương ứng.

Ngoài ra, như được thể hiện trên Fig.5, AF 420 có thể thực hiện việc thương lượng bảo mật (507) giữa AF 430 và UE 410, để thu nhận kết quả thương lượng bảo mật thứ hai. Kết quả thương lượng bảo mật thứ hai có thể bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 430, và thông số tạo ra khóa.

Trong một số phương án, AF 420 có thể xác định, dựa trên thông tin định danh của AF 430 được chứa trong thông điệp yêu cầu thiết lập phiên ứng dụng, AF 430 được truy nhập bởi UE 410. Theo tùy chọn, AF 420 có thể lựa chọn AF 430 dựa trên thông tin thuộc tính của UE 410. Ví dụ, thông tin thuộc tính có thể là thông tin định vị, thông tin tải, hoặc tương tự. Kịch bản phương tiện bay không người lái 405 được thể hiện trên Fig.4B được sử dụng làm ví dụ. Khi kịch bản ứng dụng 405 bao gồm nhiều TPAE, các khóa của tất cả các TPAE có thể giống nhau; hoặc các khóa của các TPAE trong khu vực cụ thể có thể giống nhau nhưng các khóa của TPAE trong các khu vực khác nhau có thể khác nhau. Khi khu vực được sử dụng làm mức độ chi tiết, UTM có thể xác định, dựa trên vị trí gần đây của UAV, khu vực trong đó UAV được đặt và lựa chọn, dựa trên thông tin khu vực, TPAE mà đóng vai trò là UAV.

Trong một số phương án, AF 420 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 420 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 430, xem có kích hoạt bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 430 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. Ví dụ, nếu UE 410 hỗ trợ bảo vệ bí mật và AF 430 cũng hỗ trợ bảo vệ bí mật, AF 420 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ bí mật, AF 420 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 không cần được kích hoạt. Ví dụ khác, nếu UE 410 hỗ trợ bảo vệ toàn vẹn và AF 430 cũng hỗ trợ bảo vệ toàn vẹn, AF 420 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ toàn vẹn, AF 420 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 không cần được kích hoạt. Theo tùy chọn, AF 420 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF

430 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không. AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không.

Trong một số phương án, chỉ báo kích hoạt bảo mật được tạo ra bởi AF 420 bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Dạng thể hiện của chỉ báo kích hoạt bảo mật có thể là chỉ báo rõ ràng. Ví dụ, '11' chỉ báo rằng cả hai bảo vệ bí mật và bảo vệ toàn vẹn được kích hoạt; '10' chỉ báo rằng bảo vệ bí mật được kích hoạt nhưng bảo vệ toàn vẹn không được kích hoạt; '00' chỉ báo rằng bảo vệ bí mật và bảo vệ toàn vẹn đều không được kích hoạt; và '01' chỉ báo rằng bảo vệ bí mật không được kích hoạt nhưng bảo vệ toàn vẹn được kích hoạt. Theo tùy chọn, chỉ báo kích hoạt bảo mật có thể được thể hiện hoàn toàn bởi thuật toán bảo mật được lựa chọn. Khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn được kích hoạt. Ví dụ, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 1, NEA=thuật toán bảo vệ bí mật 2", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 1 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 2 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=không, NEA=thuật toán bảo vệ bí mật 3", trong đó thông tin chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt và thuật toán bảo vệ bí mật 3 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 4, NEA=thuật toán bảo vệ bí mật 5", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 4 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 5 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập

phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 6, NEA=không", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 6 được sử dụng để kích hoạt bảo vệ toàn vẹn và bảo vệ bí mật không được kích hoạt.

Trong một số phương án, AF 420 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, bao gồm nhưng không bị giới hạn ở thuật toán xác thực, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Thuật toán bảo mật được hỗ trợ bởi AF 430 có thể được tạo cấu hình trước tại AF 420 hoặc có thể được thu nhận bằng cách truy vấn AF 430 bởi AF 420. Ví dụ, AF 420 có thể xác định các thuật toán bảo mật cùng được hỗ trợ bởi UE 410 và AF 430, và ưu tiên các thuật toán bảo mật, trong đó thuật toán bảo mật có mức ưu tiên cao nhất được lựa chọn. AF 420 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn và thông số tạo ra khóa, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430 và mã định danh khóa của khóa bảo mật.

Trong một số phương án, khóa bảo mật có thể bao gồm khóa AF K_{AF2} của AF 430, và các mức độ khác nhau của các khóa bảo mật được tạo ra dựa trên khóa AF K_{AF2} của AF 430, bao gồm nhưng không bị giới hạn ở khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn. Ví dụ, AF 420 có thể tạo ra khóa AF K_{AF2} của AF 430 dựa trên khóa AF K_{AF1} của AF 420 và thông số tạo ra khóa. AF 420 có thể tạo ra khóa xác thực dựa trên khóa K_{AF2} và mã định danh của thuật toán xác thực được lựa chọn, trong đó khóa xác thực là để thực hiện xác thực giữa UE 410 và AF 430. AF 420 có thể tạo ra khóa bảo vệ bí mật dựa trên khóa K_{AF2} và mã định danh của thuật toán bảo vệ bí mật được lựa chọn, trong đó khóa bảo vệ bí mật là để thực hiện mã hóa và giải mã đối với nội dung truyền thông giữa UE 410 và AF 430. AF 420 có thể tạo ra khóa bảo vệ toàn vẹn dựa trên khóa K_{AF2} và mã định danh của thuật toán toàn vẹn được lựa chọn, trong đó khóa bảo vệ toàn vẹn là để thực hiện bảo vệ toàn vẹn và xác minh đối với nội dung truyền thông giữa UE 410 và AF 430.

Trong một số phương án, thông số tạo ra khóa được sử dụng bởi AF 420 trong việc tạo ra khóa AF K_{AF2} của AF 430 có thể là thông số tạo ra khóa được chia sẻ bởi UE 410 trong thông điệp yêu cầu thiết lập phiên ứng dụng. Theo tùy chọn, thông số tạo ra khóa được sử dụng bởi AF 420 có thể là thông số tạo ra khóa được tạo ra bởi AF 420 hoặc AF 430. Ví dụ, thông số tạo ra khóa được tạo ra bởi AF 420 có thể bao gồm ít nhất một trong số sau đây: thông tin nhận dạng được sử dụng bởi UE 410 trong AF 420 và/hoặc AF 430, loại dịch vụ được yêu cầu bởi UE 410, thông tin định danh của AF 430, thông số làm mới, tên mạng dữ

liệu (Data Network Name, DNN), hoặc tương tự. Thông số làm mới có thể là số ngẫu nhiên, giá trị đếm, hoặc tương tự được tạo ra bởi AF 420.

Trong một số phương án, việc lựa chọn thuật toán và việc tạo ra khóa có thể phụ thuộc vào chỉ báo kích hoạt bảo mật. Cụ thể, lựa chọn thuật toán tương ứng và tạo ra khóa được thực hiện chỉ khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430. Theo tùy chọn, việc lựa chọn thuật toán và việc tạo ra khóa có thể không phụ thuộc vào chỉ báo kích hoạt bảo mật. Trong trường hợp này, chỉ báo kích hoạt bảo mật chỉ để kích hoạt sử dụng thuật toán và khóa bảo mật tương ứng.

Như được thể hiện trên Fig.5, AF 420 có thể gửi (508) thông điệp thông báo khóa đến AF 430, để chỉ báo kết quả thương lượng bảo mật thứ hai đến AF 430. Thông điệp thông báo khóa có thể bao gồm khóa bảo mật của AF 430, ví dụ, khóa AF K_{AF2} của AF 430, và các mức độ khác nhau của các khóa bảo mật được tạo ra dựa trên khóa AF K_{AF2} của AF 430. Để phản hồi thông điệp thông báo khóa nhận được, AF 430 có thể lưu trữ một phần hoặc tất cả kết quả thương lượng bảo mật thứ hai và khóa bảo mật của AF 430. Sau khi nhận thông điệp kích hoạt từ AF 420, AF 430 có thể thực hiện bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430 bằng cách sử dụng thuật toán bảo mật và/hoặc khóa tương ứng dựa trên chỉ báo kích hoạt bảo mật trong kết quả thương lượng bảo mật thứ hai.

Như được thể hiện trên Fig.5, AF 430 có thể gửi (509) thông điệp báo nhận đối với thông điệp thông báo khóa đến AF 420. AF 420 có thể gửi (510) thông điệp phản hồi thiết lập phiên ứng dụng đến UE 410.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng có thể bao gồm kết quả thương lượng bảo mật thứ nhất và/hoặc kết quả thương lượng bảo mật thứ hai. Như được đề cập phía trên, kết quả thương lượng bảo mật thứ nhất có thể bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 420, và thông số tạo ra khóa. Kết quả thương lượng bảo mật thứ hai có thể bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 430, và thông số tạo ra khóa, và mã định danh khóa của khóa tương ứng được tạo ra dựa trên kết quả thương lượng bảo mật thứ nhất. UE 410 có thể lưu trữ một phần hoặc tất cả trong số kết quả thương lượng bảo mật thứ nhất và/hoặc kết quả thương lượng bảo

mật thứ hai.

Trong một số phương án, kết quả thương lượng bảo mật thứ nhất và/hoặc kết quả thương lượng bảo mật thứ hai có thể được mang trong thông điệp phiên ứng dụng đường xuống khác.

Trong một số phương án, AF 420 có thể xác định, dựa trên khóa K_{AF1}, khóa bảo vệ toàn vẹn để bảo vệ thông điệp phản hồi thiết lập phiên ứng dụng. Khóa bảo vệ toàn vẹn có thể là khóa K_{AF1} hoặc khóa bắt nguồn từ K_{AF1}. AF 420 có thể tính toán giá trị băm MAC1 của thông điệp phản hồi thiết lập phiên ứng dụng bằng cách sử dụng khóa bảo vệ toàn vẹn, để bảo vệ toàn vẹn thông điệp phản hồi thiết lập phiên ứng dụng. Giá trị băm MAC1 có thể được gửi đến UE 410 cùng với thông điệp phản hồi thiết lập phiên ứng dụng.

Đề phản hồi thông điệp phản hồi thiết lập phiên ứng dụng nhận được từ AF 420, UE 410 có thể tạo ra (511) khóa ở phía UE 410 theo cách giống với AF 420.

Trong một số phương án, UE 410 có thể tạo ra khóa gốc thứ nhất K_{AF} dựa trên khóa gốc AKMA K_{AKMA} thu được trong quy trình xác thực chính. Để phản hồi giá trị băm MAC1 nhận được được gửi cùng với thông điệp phản hồi thiết lập phiên ứng dụng từ AF 420, UE 410 có thể xác định, dựa trên khóa gốc thứ nhất K_{AF} theo cách giống với AF 420, khóa bảo vệ toàn vẹn để xác minh thông điệp phản hồi thiết lập phiên ứng dụng. UE 410 có thể tính toán giá trị băm của thông điệp phản hồi thiết lập phiên ứng dụng dựa trên khóa bảo vệ toàn vẹn và so sánh giá trị băm với giá trị băm MAC1 nhận được. Nếu hai giá trị là giống nhau, nó chỉ báo rằng thông điệp phản hồi thiết lập phiên ứng dụng đã không bị giả mạo. Nếu hai giá trị là khác nhau, nó chỉ báo rằng phản hồi thiết lập phiên ứng dụng đã không bị giả mạo. Bằng cách này, UE 410 có thể xác minh sự toàn vẹn của thông điệp phản hồi thiết lập phiên ứng dụng.

Trong một số phương án, ví dụ, khi xác minh toàn vẹn thành công, nếu thông điệp phản hồi thiết lập phiên ứng dụng bao gồm kết quả thương lượng bảo mật thứ nhất, UE 410 có thể tạo ra, dựa trên kết quả thương lượng bảo mật thứ nhất theo cách giống với AF 420, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420. Nếu thông điệp phản hồi thiết lập phiên ứng dụng bao gồm kết quả thương lượng bảo mật thứ hai, UE 410 có thể tạo ra, dựa trên kết quả thương lượng bảo mật thứ hai theo cách giống với AF 420, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430.

Như được thể hiện trên Fig.5, UE 410 có thể gửi (512) thông điệp hoàn thành thiết lập phiên ứng dụng đến AF 420.

Trong một số phương án, UE 410 có thể tính toán giá trị băm MAC2 của thông điệp hoàn thành thiết lập phiên ứng dụng bằng cách sử dụng khóa bảo vệ toàn vẹn được xác định, để bảo vệ toàn vẹn thông điệp hoàn thành thiết lập phiên ứng dụng. Giá trị băm MAC2 có thể được gửi đến AF 420 cùng với thông điệp hoàn thành thiết lập phiên ứng dụng. Để phản hồi thông điệp hoàn thành thiết lập phiên ứng dụng nhận được và giá trị băm MAC2 nhận được, AF 420 có thể tính toán giá trị băm của thông điệp hoàn thành thiết lập phiên ứng dụng dựa trên cùng khóa bảo vệ toàn vẹn, và so sánh giá trị băm với giá trị băm MAC2 nhận được. Nếu hai giá trị là giống nhau, nó chỉ báo rằng thông điệp hoàn thành thiết lập phiên ứng dụng đã không bị giả mạo. Nếu hai giá trị là khác nhau, nó chỉ báo rằng hoàn thành thiết lập phiên ứng dụng đã bị giả mạo. Bằng cách này, AF 420 có thể xác minh sự toàn vẹn của thông điệp hoàn thành thiết lập phiên ứng dụng.

Trong một số phương án, ví dụ, khi toàn vẹn của thông điệp hoàn thành thiết lập phiên ứng dụng được xác minh, nếu chỉ báo kích hoạt bảo mật trong kết quả thương lượng bảo mật thứ nhất chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, UE 410 và AF 420 có thể thực hiện bảo vệ bảo mật đầu cuối đối với truyền thông giữa UE 410 và AF 420 dựa trên thuật toán bảo mật và khóa tương ứng trong kết quả thương lượng bảo mật thứ nhất. Ví dụ, nếu chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420, UE 410 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất để mã hóa thông điệp/dữ liệu được gửi đến AF 420. AF 420 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420, AF 420 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất để mã hóa thông điệp/dữ liệu được gửi đến UE 410. UE 410 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420, UE 410 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến AF 420. AF 420 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất. AF 420 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất để thực hiện bảo

vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến UE 410, và UE 410 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất.

Trong một số phương án, AF 420 có thể gửi thông điệp kích hoạt đến AF 430, để chỉ báo AF 430 kích hoạt bảo vệ bảo mật đầu cuối giữa UE 410 và AF 430 dựa trên kết quả thương lượng bảo mật thứ hai.

Trong một số phương án, nếu chỉ báo kích hoạt bảo mật trong kết quả thương lượng bảo mật thứ hai chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, UE 410 và AF 430 có thể thực hiện bảo vệ bảo mật đầu cuối đối với truyền thông giữa UE 410 và AF 430 dựa trên thuật toán bảo mật và khóa tương ứng trong kết quả thương lượng bảo mật thứ hai. Ví dụ, nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430, UE 410 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai để mã hóa thông điệp/dữ liệu được gửi đến AF 430. AF 430 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430, AF 430 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai để mã hóa thông điệp/dữ liệu được gửi đến UE 410. UE 410 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430, UE 410 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến AF 430. AF 430 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai. AF 430 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến UE 410, và UE 410 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai.

Kịch bản ứng dụng phương tiện bay không người lái được thể hiện trên Fig.4B được sử dụng làm ví dụ. UAV có thể thực hiện bảo vệ bảo mật đối với thông điệp quảng bá bằng cách sử dụng khóa bảo mật được thương lượng và thuật toán bảo mật. Sau khi nhận được

thông điệp quảng bá, và TPAE thực hiện bỏ bảo vệ bảo mật đối với thông điệp quảng bá bằng cách sử dụng khóa tương ứng và thuật toán bảo mật, để thu nhận văn bản gốc của thông điệp quảng bá. Thông điệp quảng bá có thể bao gồm một số hoặc tất cả trong số các thông số sau đây: thông tin định danh của UAV, mã định danh khóa, bản mã được mã hóa, mã xác minh thông điệp để bảo vệ toàn vẹn, và tương tự.

Fig.6 là sơ đồ khối của kiến trúc khóa ví dụ 600 theo phương án của sáng chế. Kiến trúc khóa ví dụ 600 minh họa cách tạo ra khóa theo phương án của sáng chế. Như được thể hiện trên Fig.6, khóa gốc AKMA K_{AKMA} được tạo ra dựa trên khóa K_{AUSF} được tạo ra trong quy trình xác thực chính. Chức năng tạo ra khóa 610 tạo ra khóa AF K_{AF1} cho AF 420 dựa trên khóa gốc AKMA K_{AKMA}. Ví dụ, chức năng tạo ra khóa 610 có thể được tạo cấu hình trước tại UE 410 và AF 420. Chức năng tạo ra khóa 620 có thể tạo ra các khóa gốc tương ứng của chúng K_{AF2}, K_{AF3}, ..., và K_{AFn} (trong đó $n\geq2$) cho nhiều AF (ví dụ, bao gồm AF 430) có cùng ID của AF dựa trên khóa K_{AF1} và thông số tạo ra khóa 601. Ví dụ, chức năng tạo ra khóa 620 có thể được tạo cấu hình trước tại UE 410 và AF 420 hoặc AF 430. Chức năng tạo ra khóa 630 có thể tạo ra nhiều khóa bảo mật dựa trên khóa AF K_{AF2} cho AF 430 và thuật toán bảo mật 602 được sử dụng bởi UE 410 và AF 430, bao gồm nhưng không bị hạn chế ở khóa xác thực K_{AF2_auth}, khóa bảo vệ bí mật K_{AF2_enc}, và/hoặc khóa bảo vệ toàn vẹn K_{AF2_int}. Ngoài ra, chức năng tạo ra khóa 620 có thể tạo ra các khóa gốc tương ứng của chúng K_{AF2}, K_{AF3}, ..., và K_{AFn} (trong đó $n\geq2$) cho AF giống nhau (ví dụ, bao gồm AF 420) dựa trên khóa K_{AF1} và thông số tạo ra khóa 601. Ví dụ, khi thông số tạo ra khóa 601 là thông tin nhận dạng, thông số tạo ra khóa 601 có thể là tên người dùng, ID người dùng, hoặc tương tự được sử dụng bởi UE 410 trong AF 420 hoặc AF 430. Trong trường hợp này, K_{AF2}, K_{AF3}, ..., và K_{AFn} thể hiện các khóa gốc có các định danh khác nhau trong AF giống nhau.

Fig.7A và Fig.7B là sơ đồ trao đổi tín hiệu của quy trình bảo vệ truyền thông ví dụ khác 700 theo phương án của sáng chế. Trong ví dụ được thể hiện trên Fig.7A và Fig.7B, AF 420 gửi thông tin khả năng bảo mật của UE 410 đến AF 430, để AF 430 tự thực hiện lựa chọn thuật toán và tạo ra khóa.

Quy trình trao đổi tín hiệu được thể hiện trong các bước 310 và từ 501 đến 506 trên Fig.7A và Fig.7B là giống với quy trình trao đổi tín hiệu được thể hiện trong các bước 310 và từ 501 đến 506 trên Fig.5. Chi tiết không được mô tả lại ở đây.

Như được thể hiện trên Fig.7A và Fig.7B, AF 420 có thể thực hiện riêng biệt thương lượng bảo mật (701) giữa AF 420 và UE 410, để thu nhận kết quả thương lượng bảo mật thứ

nhất. Kết quả thương lượng bảo mật thứ nhất có thể bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 420, và thông số tạo ra khóa.

Trong một số phương án, AF 420 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 420 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 420, xem có kích hoạt bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 420 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. Ví dụ, nếu UE 410 hỗ trợ bảo vệ bí mật và AF 420 cũng hỗ trợ bảo vệ bí mật, AF 420 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ bí mật, AF 420 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 không cần được kích hoạt. Ví dụ khác, nếu UE 410 hỗ trợ bảo vệ toàn vẹn và AF 420 cũng hỗ trợ bảo vệ toàn vẹn, AF 420 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ toàn vẹn, AF 420 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 không cần được kích hoạt. Theo tùy chọn, AF 420 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 420 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 420 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 hay không. AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420 hay không.

Trong một số phương án, chỉ báo kích hoạt bảo mật được tạo ra bởi AF 420 bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Dạng thể hiện của chỉ báo kích hoạt bảo mật có thể là chỉ báo rõ ràng. Ví dụ, '11' chỉ báo rằng cả hai bảo vệ bí mật và bảo vệ toàn vẹn được kích hoạt; '10' chỉ báo rằng bảo vệ bí mật được kích hoạt nhưng bảo vệ toàn vẹn không được kích hoạt; '00' chỉ báo rằng bảo vệ bí mật và bảo vệ toàn vẹn đều không được kích hoạt; và '01' chỉ báo rằng bảo vệ bí mật không được kích hoạt nhưng bảo vệ toàn vẹn

được kích hoạt. Theo tùy chọn, chỉ báo kích hoạt bảo mật có thể được thể hiện hoàn toàn bởi thuật toán bảo mật được lựa chọn. Khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn được kích hoạt. Ví dụ, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 1, NEA=thuật toán bảo vệ bí mật 2", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 1 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 2 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=không, NEA=thuật toán bảo vệ bí mật 3", trong đó thông tin chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt và thuật toán bảo vệ bí mật 3 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 4, NEA=thuật toán bảo vệ bí mật 5", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 4 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 5 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 420 cho UE 410 thông qua thông điệp phản hồi thiết lập phiên ứng dụng có thể là "NIA=thuật toán bảo vệ toàn vẹn 6, NEA=không", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 6 được sử dụng để kích hoạt bảo vệ toàn vẹn và bảo vệ bí mật không được kích hoạt.

Trong một số phương án, AF 420 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 420, thuật toán bảo mật được sử dụng bởi UE 410 và AF 420, bao gồm nhưng không bị giới hạn ở thuật toán xác thực, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Ví dụ, AF 420 có thể xác định các thuật toán bảo mật cùng được hỗ trợ bởi UE 410 và AF 420, và ưu tiên các thuật toán bảo mật, trong đó thuật toán bảo mật có mức ưu tiên cao nhất được lựa chọn. AF 420 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420, và mã định danh khóa của khóa bảo mật.

Theo một số phương án, AF 420 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên thuật

toán bảo mật được lựa chọn, hoặc chỉ báo kích hoạt bảo mật có thể được chỉ báo hoàn toàn bởi thuật toán bảo mật được lựa chọn. Ví dụ, nếu thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật, chỉ báo kích hoạt chỉ báo để kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420. Nếu thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật, chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420.

Trong một số phương án, khóa bảo mật có thể bao gồm các mức độ khác nhau của các khóa bảo mật được tạo ra dựa trên khóa AF K_{AF1} của AF 420, bao gồm nhưng không bị giới hạn ở khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn. Ví dụ, AF 420 có thể tạo ra khóa xác thực dựa trên khóa K_{AF1} và mã định danh của thuật toán xác thực được lựa chọn, trong đó khóa xác thực là để thực hiện xác thực giữa UE 410 và AF 420. AF 420 có thể tạo ra khóa bảo vệ bí mật dựa trên khóa K_{AF1} và mã định danh của thuật toán bảo vệ bí mật được lựa chọn, trong đó khóa bảo vệ bí mật là để thực hiện mã hóa và giải mã đối với nội dung truyền thông giữa UE 410 và AF 420. AF 420 có thể tạo ra khóa bảo vệ toàn vẹn dựa trên khóa K_{AF1} và mã định danh của thuật toán toàn vẹn được lựa chọn, trong đó khóa bảo vệ toàn vẹn là để thực hiện bảo vệ toàn vẹn và xác minh đối với nội dung truyền thông giữa UE 410 và AF 420.

Trong một số phương án, việc lựa chọn thuật toán và việc tạo ra khóa có thể phụ thuộc vào chỉ báo kích hoạt bảo mật. Nghĩa là, lựa chọn thuật toán tương ứng và tạo ra khóa được thực hiện chỉ khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420. Theo tùy chọn, việc lựa chọn thuật toán và việc tạo ra khóa có thể không phụ thuộc vào chỉ báo kích hoạt bảo mật. Trong trường hợp này, chỉ báo kích hoạt bảo mật chỉ để kích hoạt sử dụng thuật toán và khóa bảo mật tương ứng.

Trong một số phương án, AF 420 có thể tạo ra khóa AF K_{AF2} của AF 430 dựa trên khóa AF K_{AF1} của AF 420 và thông số tạo ra khóa. Trong một số phương án, thông số tạo ra khóa được sử dụng bởi AF 420 trong việc tạo ra khóa được chia sẻ bởi UE 410 trong thông điệp yêu cầu thiết lập phiên ứng dụng. Theo tùy chọn, thông số tạo ra khóa được sử dụng bởi AF 420 có thể là thông số tạo ra khóa được tạo ra bởi AF 420. Ví dụ, thông số tạo ra khóa được tạo ra bởi AF 420 hoặc AF 430 có thể bao gồm ít nhất một trong số sau đây: thông tin nhận dạng được sử dụng bởi UE 410 trong AF 420 và/hoặc AF 430, loại dịch vụ được yêu cầu bởi UE 410, thông tin định danh của AF 430, thông số làm mới, tên mạng dữ liệu (Data Network Name, DNN), hoặc tương tự. Thông số làm mới có thể là số ngẫu nhiên, giá trị đếm, hoặc

tương tự được tạo ra bởi AF 420.

Như được thể hiện trên Fig.7A và Fig.7B, AF 420 có thể gửi (702) thông điệp thông báo khóa đến AF 430. Trong một số phương án, thông điệp thông tin khóa có thể bao gồm thông tin khả năng bảo mật của UE 410. Ngoài ra hoặc theo tùy chọn, thông điệp thông báo khóa có thể còn bao gồm khóa AF K_{AF2} của AF 430, và mã định danh và thời hạn hiệu lực của khóa AF.

Trong một số phương án, AF 420 có thể xác định, dựa trên thông tin định danh của AF 430 được chứa trong yêu cầu thiết lập phiên ứng dụng, AF 430 được truy nhập bởi UE 410. Theo tùy chọn, AF 420 có thể lựa chọn AF 430 dựa trên thông tin thuộc tính của UE 410. Ví dụ, thông tin thuộc tính có thể là thông tin định vị, thông tin tải, hoặc tương tự. Kịch bản phương tiện bay không người lái 405 được thể hiện trên Fig.4B được sử dụng làm ví dụ. Khi kịch bản ứng dụng 405 bao gồm nhiều TPAE, các khóa của tất cả các TPAE có thể giống nhau; hoặc các khóa của các TPAE trong khu vực cụ thể có thể giống nhau nhưng các khóa của TPAE trong các khu vực khác nhau có thể khác nhau. Khi khu vực được sử dụng làm mức độ chi tiết, UTM có thể xác định, dựa trên vị trí gần đây của UAV, khu vực trong đó UAV được đặt và lựa chọn, dựa trên thông tin khu vực, TPAE mà đóng vai trò là UAV.

Để phản hồi thông điệp thông tin khóa nhận được, AF 430 có thể thực hiện thương lượng bảo mật (703) với UE 410, để thu nhận kết quả thương lượng bảo mật thứ hai. Kết quả thương lượng bảo mật thứ hai có thể bao gồm một hoặc nhiều trong số sau đây: chỉ báo kích hoạt bảo mật để bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, mã định danh khóa của khóa bảo mật được sử dụng bởi UE 410 và AF 430, và thông số tạo ra khóa.

Trong một số phương án, AF 430 có thể xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. AF 430 có thể xác định, dựa trên chính sách bảo mật được hỗ trợ bởi UE 410 và chính sách bảo mật được hỗ trợ bởi AF 430, xem có kích hoạt bảo vệ bảo mật, như là bảo vệ bí mật và/hoặc bảo vệ toàn vẹn, giữa UE 410 và AF 430 hay không, và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định. Ví dụ, nếu UE 410 hỗ trợ bảo vệ bí mật và AF 430 cũng hỗ trợ bảo vệ bí mật, AF 430 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ bí mật, AF 430 có thể xác định rằng bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 không cần được kích hoạt. Ví dụ khác, nếu UE 410 hỗ trợ bảo vệ toàn vẹn và AF 430 cũng

hỗ trợ bảo vệ toàn vẹn, AF 430 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 cần được kích hoạt. Nếu một trong hai không hỗ trợ bảo vệ toàn vẹn, AF 430 có thể xác định rằng bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 không cần được kích hoạt. Theo tùy chọn, AF 430 có thể xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi UE 410 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430 hay không, và/hoặc xác định, phụ thuộc vào việc liệu thuật toán toàn vẹn có được hỗ trợ bởi UE 410 bao gồm thuật toán toàn vẹn có được hỗ trợ bởi AF 430 hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không. AF 430 có thể tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định phía trên, trong đó chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bí mật và/hoặc bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430 hay không.

Trong một số phương án, chỉ báo kích hoạt bảo mật được tạo ra bởi AF 430 bao gồm chỉ báo bảo vệ bí mật và/hoặc chỉ báo bảo vệ toàn vẹn. Dạng thể hiện của chỉ báo kích hoạt bảo mật có thể là chỉ báo rõ ràng. Ví dụ, '11' chỉ báo rằng cả hai bảo vệ bí mật và bảo vệ toàn vẹn được kích hoạt; '10' chỉ báo rằng bảo vệ bí mật được kích hoạt nhưng bảo vệ toàn vẹn không được kích hoạt; '00' chỉ báo rằng bảo vệ bí mật và bảo vệ toàn vẹn đều không được kích hoạt; và '01' chỉ báo rằng bảo vệ bí mật không được kích hoạt nhưng bảo vệ toàn vẹn được kích hoạt. Theo tùy chọn, chỉ báo kích hoạt bảo mật có thể được thể hiện hoàn toàn bởi thuật toán bảo mật được lựa chọn. Khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn được kích hoạt. Ví dụ, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 430 cho UE 410 thông qua thông điệp báo nhận đối với thông điệp thông báo khóa có thể là "NIA=thuật toán bảo vệ toàn vẹn 1, NEA=thuật toán bảo vệ bí mật 2", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 1 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 2 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 430 cho UE 410 thông qua thông điệp báo nhận có thể là "NIA=không, NEA=thuật toán bảo vệ bí mật 3", trong đó thông tin chỉ báo rằng bảo vệ toàn vẹn không được kích hoạt và thuật toán bảo vệ bí mật 3 được sử dụng để kích hoạt bảo vệ bí

mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 430 cho UE 410 thông qua thông điệp báo nhận có thể là "NIA=thuật toán bảo vệ toàn vẹn 4, NEA=thuật toán bảo vệ bí mật 5", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 4 được sử dụng để kích hoạt bảo vệ toàn vẹn và thuật toán bảo vệ bí mật 5 được sử dụng để kích hoạt bảo vệ bí mật. Ví dụ khác, thông tin về thuật toán bảo mật được lựa chọn được trả về bởi AF 430 cho UE 410 thông qua thông điệp báo nhận có thể là "NIA=thuật toán bảo vệ toàn vẹn 6, NEA=không", trong đó thông tin chỉ báo rằng thuật toán bảo vệ toàn vẹn 6 được sử dụng để kích hoạt bảo vệ toàn vẹn và bảo vệ bí mật không được kích hoạt.

Trong một số phương án, AF 430 có thể lựa chọn, dựa trên thuật toán bảo mật được hỗ trợ bởi UE 410 và thuật toán bảo mật được hỗ trợ bởi AF 430, thuật toán bảo mật được sử dụng bởi UE 410 và AF 430, bao gồm nhưng không bị giới hạn ở thuật toán xác thực, thuật toán bảo vệ bí mật, và/hoặc thuật toán toàn vẹn. Ví dụ, AF 430 có thể xác định các thuật toán bảo mật cùng được hỗ trợ bởi UE 410 và AF 430, và ưu tiên các thuật toán bảo mật, trong đó thuật toán bảo mật có mức ưu tiên cao nhất được lựa chọn. AF 430 có thể tạo ra, dựa trên thuật toán bảo mật được lựa chọn và thông số tạo ra khóa, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430 và mã định danh khóa của khóa bảo mật.

Trong một số phương án, AF 430 có thể tạo ra các mức độ khác nhau của các khóa bảo mật, bao gồm nhưng không bị giới hạn ở khóa xác thực, khóa bảo vệ bí mật, và/hoặc khóa bảo vệ toàn vẹn, dựa trên khóa AF K_{AF2} của AF 430 và thuật toán bảo mật được lựa chọn. Ví dụ, AF 430 có thể tạo ra khóa xác thực dựa trên khóa K_{AF2} và mã định danh của thuật toán xác thực được lựa chọn, trong đó khóa xác thực là để thực hiện xác thực giữa UE 410 và AF 430. AF 430 có thể tạo ra khóa bảo vệ bí mật dựa trên khóa K_{AF2} và mã định danh của thuật toán bảo vệ bí mật được lựa chọn, trong đó khóa bảo vệ bí mật là để thực hiện mã hóa và giải mã đối với nội dung truyền thông giữa UE 410 và AF 430. AF 430 có thể tạo ra khóa bảo vệ toàn vẹn dựa trên khóa K_{AF2} và mã định danh của thuật toán toàn vẹn được lựa chọn, trong đó khóa bảo vệ toàn vẹn là để thực hiện bảo vệ toàn vẹn và xác minh đối với nội dung truyền thông giữa UE 410 và AF 430.

Như được thể hiện trên Fig.7A và Fig.7B, AF 430 có thể gửi (704) thông điệp báo nhận đối với thông điệp thông báo khóa đến AF 420. Thông điệp báo nhận có thể bao gồm kết quả thương lượng bảo mật thứ hai.

Trong một số phương án, AF 430 có thể xác định, dựa trên khóa K_{AF2}, khóa bảo vệ toàn vẹn để bảo vệ thông điệp báo nhận. Khóa bảo vệ toàn vẹn có thể là khóa K_{AF2} hoặc khóa

bắt nguồn từ K_{AF2}. AF 430 có thể tính toán giá trị băm MAC3 của thông điệp báo nhận bằng cách sử dụng khóa bảo vệ toàn vẹn, để bảo vệ toàn vẹn của thông điệp báo nhận. Giá trị băm MAC3 có thể được gửi đến AF 420 cùng với thông điệp báo nhận.

Để phản hồi thông điệp báo nhận nhận được đối với thông điệp thông báo khóa từ AF 430, AF 420 có thể gửi (705) thông điệp phản hồi thiết lập phiên ứng dụng đến UE 410.

Trong một số phương án, thông điệp báo nhận cùng với giá trị băm MAC3 của nó, có thể được gửi đến UE 410 như ít nhất một phần của thông điệp phản hồi thiết lập phiên ứng dụng. Ngoài ra hoặc theo tùy chọn, thông điệp phản hồi thiết lập phiên ứng dụng có thể có thể còn bao gồm kết quả thương lượng bảo mật thứ nhất giữa AF 420 và UE 410.

Đề phản hồi thông điệp phản hồi thiết lập phiên ứng dụng nhận được từ AF 420, UE 410 có thể tạo ra (706) khóa ở phía UE 410 theo cách giống với AF 420 và AF 430.

Trong một số phương án, UE 410 có thể tạo ra khóa AF K_{AF1} của AF 420 dựa trên khóa gốc AKMA K_{AKMA} thu được trong quy trình xác thực chính. UE 410 có thể tạo ra khóa AF K_{AF2} của AF 430 dựa trên khóa AF K_{AF1} theo cách giống với AF 420. Để phản hồi giá trị băm MAC3 nhận được từ AF 420, UE 410 có thể xác định, dựa trên khóa gốc K_{AF2} theo cách giống với AF 430, khóa bảo vệ toàn vẹn để xác minh thông điệp phản hồi thiết lập phiên ứng dụng. UE 410 có thể tính toán, dựa trên khóa bảo vệ toàn vẹn, giá trị băm của thông điệp báo nhận được chứa trong thông điệp phản hồi thiết lập phiên ứng dụng và so sánh giá trị băm với giá trị băm MAC3 nhận được. Nếu hai giá trị là giống nhau, nó chỉ báo rằng thông điệp báo nhận được bao gồm trong thông điệp phản hồi thiết lập phiên ứng dụng đã không bị giả mạo. Nếu hai giá trị là khác nhau, nó chỉ báo rằng thông điệp báo nhận được bao gồm trong thông điệp phản hồi thiết lập phiên ứng dụng đã bị giả mạo.

Trong một số phương án, ví dụ, khi xác minh toàn vẹn thành công, nếu thông điệp phản hồi thiết lập phiên ứng dụng bao gồm kết quả thương lượng bảo mật thứ hai, UE 410 có thể tạo ra, dựa trên kết quả thương lượng bảo mật thứ hai theo cách giống với AF 430, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 430. Nếu thông điệp phản hồi thiết lập phiên ứng dụng bao gồm kết quả thương lượng bảo mật thứ nhất, UE 410 có thể tạo ra, dựa trên kết quả thương lượng bảo mật thứ nhất theo cách giống với AF 420, khóa bảo mật để bảo vệ truyền thông giữa UE 410 và AF 420.

Như được thể hiện trên Fig.7A và Fig.7B, UE 410 có thể gửi (707) thông điệp hoàn thành thiết lập phiên ứng dụng đến AF 420. AF 420 có thể chuyển tiếp (708) thông điệp hoàn thành thiết lập phiên ứng dụng đến AF 430.

Trong một số phương án, để phản hồi thông điệp hoàn thành thiết lập phiên ứng dụng nhận được từ UE 410, nếu chỉ báo kích hoạt bảo mật trong kết quả thương lượng bảo mật thứ nhất chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 420, UE 410 và AF 420 có thể thực hiện bảo vệ bảo mật đầu cuối đối với truyền thông giữa UE 410 và AF 420 dựa trên thuật toán bảo mật và khóa tương ứng trong kết quả thương lượng bảo mật thứ nhất. Ví dụ, nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420, UE 410 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất để mã hóa thông điệp/dữ liệu được gửi đến AF 420. AF 420 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 420, AF 420 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất để mã hóa thông điệp/dữ liệu được gửi đến UE 410. UE 410 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ nhất. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 420, UE 410 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến AF 420. AF 420 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất. AF 420 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến UE 410, và UE 410 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ nhất.

Trong một số phương án, UE 410 có thể tính toán giá trị băm MAC4 của thông điệp hoàn thành thiết lập phiên ứng dụng bằng cách sử dụng khóa bảo vệ toàn vẹn được xác định, để bảo vệ toàn vẹn thông điệp hoàn thành thiết lập phiên ứng dụng. Giá trị băm MAC4 có thể được gửi đến AF 420 cùng với thông điệp hoàn thành thiết lập phiên ứng dụng. AF 420 có thể chuyển tiếp thông điệp hoàn thành thiết lập phiên ứng dụng đến AF 430. Để phản hồi thông điệp hoàn thành thiết lập phiên ứng dụng nhận được và giá trị băm MAC4 nhận được, AF 430 có thể tính toán giá trị băm của thông điệp hoàn thành thiết lập phiên ứng dụng dựa trên cùng khóa bảo vệ toàn vẹn, và so sánh giá trị băm với giá trị băm MAC4 nhận được. Nếu hai giá

trị là giống nhau, nó chỉ báo rằng thông điệp hoàn thành thiết lập phiên ứng dụng đã không bị giả mạo. Nếu hai giá trị là khác nhau, nó chỉ báo rằng hoàn thành thiết lập phiên ứng dụng đã bị giả mạo. Bằng cách này, AF 430 có thể xác minh toàn vẹn của thông điệp hoàn thành thiết lập phiên ứng dụng.

Trong một số phương án, ví dụ, khi toàn vẹn của thông điệp hoàn thành thiết lập phiên ứng dụng được xác minh, nếu chỉ báo kích hoạt bảo mật trong kết quả thương lượng bảo mật thứ hai chỉ báo để kích hoạt bảo vệ bảo mật đối với truyền thông giữa UE 410 và AF 430, UE 410 và AF 430 có thể thực hiện bảo vệ bảo mật đầu cuối đối với truyền thông giữa UE 410 và AF 430 dựa trên thuật toán bảo mật và khóa tương ứng trong kết quả thương lượng bảo mật thứ hai. Ví dụ, nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430, UE 410 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai để mã hóa thông điệp/dữ liệu được gửi đến AF 430. AF 430 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ bí mật đối với truyền thông giữa UE 410 và AF 430, AF 430 có thể sử dụng thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai để mã hóa thông điệp/dữ liệu được gửi đến UE 410. UE 410 có thể giải mã thông điệp/dữ liệu nhận được dựa trên thuật toán bảo vệ bí mật và khóa bảo vệ bí mật trong kết quả thương lượng bảo mật thứ hai. Nếu chỉ báo kích hoạt bảo mật kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa UE 410 và AF 430, UE 410 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến AF 430. AF 430 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai. AF 430 có thể sử dụng thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai để thực hiện bảo vệ toàn vẹn đối với thông điệp/dữ liệu được gửi đến UE 410, và UE 410 có thể xác minh sự toàn vẹn của thông điệp/dữ liệu nhận được dựa trên thuật toán toàn vẹn và khóa bảo vệ toàn vẹn trong kết quả thương lượng bảo mật thứ hai.

Kịch bản ứng dụng phương tiện bay không người lái được thể hiện trên Fig.4B được sử dụng làm ví dụ. UAV có thể thực hiện bảo vệ bảo mật đối với thông điệp quảng bá bằng cách sử dụng khóa bảo mật được thương lượng và thuật toán bảo mật. Sau khi nhận được thông điệp quảng bá, và TPAE thực hiện bỏ bảo vệ bảo mật đối với thông điệp quảng bá bằng

cách sử dụng khóa tương ứng và thuật toán bảo mật, để thu nhận văn bản gốc của thông điệp quảng bá. Thông điệp quảng bá có thể bao gồm một số hoặc tất cả trong số các thông số sau đây: thông tin định danh của UAV, mã định danh khóa, bản mã được mã hóa, mã xác minh thông điệp để bảo vệ toàn vẹn, và tương tự.

Fig.8 là lưu đồ của phương pháp bảo vệ truyền thông ví dụ 800 theo phương án của sáng chế. Phương pháp 800 có thể được thực hiện bởi thiết bị đầu cuối, và thiết bị đầu cuối là, ví dụ, UE 410 được thể hiện trên Fig.4A. Cần hiểu rằng phương pháp 800 có thể còn bao gồm các hoạt động bổ sung mà không được thể hiện và/hoặc có thể bỏ qua các hoạt động mà được thể hiện. Phạm vi của sáng chế không bị giới hạn ở mặt này.

810. Thiết bị đầu cuối gửi thông điệp yêu cầu thiết lập phiên ứng dụng đến AF thứ nhất, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA.

820. Thiết bị đầu cuối nhận thông điệp phản hồi thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật. Chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị đầu cuối và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối; và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn.

830. Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, thiết bị đầu cuối kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với AF thứ hai.

Trong một số phương án, AF thứ nhất và AF thứ hai là AF giống nhau, và phương pháp còn bao gồm: Thiết bị đầu cuối tạo ra khóa AF dựa trên khóa AKMA; và thiết bị đầu cuối tạo ra khóa bảo mật dựa trên khóa AF thứ nhất và thuật toán bảo mật được lựa chọn, trong đó

khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, AF thứ nhất và AF thứ hai là các AF khác nhau, và phương pháp còn bao gồm: Thiết bị đầu cuối tạo ra khóa AF thứ nhất dựa trên khóa AKMA; thiết bị đầu cuối tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất; và thiết bị đầu cuối tạo ra khóa bảo mật dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa, và thông số tạo ra khóa bao gồm ít nhất một trong số sau đây: thông tin nhận dạng được sử dụng bởi thiết bị đầu cuối trong AF thứ nhất hoặc AF thứ hai; loại dịch vụ được yêu cầu bởi thiết bị đầu cuối từ AF thứ nhất hoặc AF thứ hai; thông tin định danh của AF thứ hai; hoặc thông số làm mới khóa.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa, và thông số tạo ra khóa bao gồm thông số làm mới khóa.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

Trong một số phương án, thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và phương pháp còn bao gồm: Thiết bị đầu cuối xác định, dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ nhất, xem thông điệp phản hồi thiết lập phiên ứng dụng có bị giả mạo hay không.

Trong một số phương án, phương pháp còn bao gồm: Thiết bị đầu cuối gửi thông điệp hoàn thành thiết lập phiên ứng dụng đến AF thứ hai khi thông điệp phản hồi thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai được tính toán dựa trên khóa bảo mật.

Trong một số phương án, AF thứ nhất và AF thứ hai có cùng mã định danh của AF.

Fig.9 là lưu đồ của phương pháp bảo vệ truyền thông ví dụ 900 theo phương án của sáng chế. Phương pháp 900 có thể được thực hiện bởi AF thứ nhất, và AF thứ nhất là, ví dụ, AF 420 được thể hiện trên Fig.4A. Cần hiểu rằng phương pháp 900 có thể còn bao gồm các hoạt động bổ sung mà không được thể hiện và/hoặc có thể bỏ qua các hoạt động mà được thể hiện. Phạm vi của sáng chế không bị giới hạn ở mặt này.

910. AF thứ nhất nhận thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA;

920. AF thứ nhất gửi thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật. Chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị đầu cuối và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối; và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn.

930. Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, AF thứ nhất khởi động AF thứ hai để kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Trong một số phương án, AF thứ nhất và AF thứ hai là AF giống nhau, và phương pháp còn bao gồm: AF thứ nhất tạo ra khóa AF thứ nhất dựa trên khóa AKMA; và AF thứ nhất tạo ra khóa bảo mật dựa trên khóa AF thứ nhất và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, AF thứ nhất và AF thứ hai là các AF khác nhau, và phương pháp còn bao gồm: AF thứ nhất tạo ra khóa AF thứ nhất dựa trên khóa AKMA; AF thứ nhất tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất; AF thứ nhất tạo ra khóa bảo mật và mã định danh khóa dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật đối với bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, ngữ cảnh bảo mật bao gồm khóa bảo mật, và thông điệp phản hồi thiết lập phiên ứng dụng

còn bao gồm mã định danh khóa; và AF thứ nhất gửi thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được lựa chọn, khóa bảo mật, và mã định danh khóa.

Trong một số phương án, chỉ báo kích hoạt bảo mật được chỉ báo bởi thuật toán bảo mật được lựa chọn, trong đó khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt; khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; và khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt.

Trong một số phương án, phương pháp còn bao gồm: Thiết bị đầu cuối thứ nhất xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và AF thứ nhất tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định.

Trong một số phương án, việc xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không bao gồm: xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF thứ hai hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và/hoặc xác định, phụ thuộc vào việc liệu thuật toán bảo vệ toàn vẹn có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ toán vẹn được hỗ trợ bởi AF thứ hai hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không.

Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không; và xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không bao gồm: xác định, bởi AF thứ nhất theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi AF thứ hai, xem có kích hoạt bảo vệ bảo mật hay không, trong đó chính sách bảo mật được hỗ trợ bởi AF thứ hai hay không chỉ báo xem AF thứ hai có hỗ trợ kích hoạt đối với bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không.

Trong một số phương án, AF thứ nhất và AF thứ hai là các AF khác nhau, và phương pháp còn bao gồm: AF thứ nhất tạo ra khóa AF thứ nhất dựa trên khóa AKMA; AF thứ nhất tạo ra khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất; AF thứ nhất gửi thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai; và AF thứ nhất nhận thông điệp báo nhận từ AF thứ hai, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn, chỉ báo kích hoạt bảo mật, và mã định danh khóa, mã định danh khóa để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật, trong đó thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa.

Trong một số phương án, phương pháp còn bao gồm: AF thứ nhất nhận thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai; và AF thứ nhất xác định, dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thành thiết lập phiên ứng dụng có bị giả mạo hay không.

Trong một số phương án, phương pháp còn bao gồm: AF thứ nhất gửi thông điệp kích hoạt đến AF thứ hai khi xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp kích hoạt chỉ báo AF thứ hai để kích hoạt, dựa trên khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Fig.10 là lưu đồ của phương pháp bảo vệ truyền thông ví dụ 1000 theo phương án của sáng chế. Phương pháp 1000 có thể được thực hiện bởi AF thứ hai và AF thứ hai là, ví dụ, AF 430 được thể hiện trên Fig.4A. Cần hiểu rằng phương pháp 1000 có thể còn bao gồm các hoạt động bổ sung mà không được thể hiện và/hoặc có thể bỏ qua các hoạt động mà được thể hiện. Phạm vi của sáng chế không bị giới hạn ở mặt này.

1010. AF thứ hai nhận thông điệp thông báo khóa từ AF thứ nhất, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai;

1020. AF thứ hai gửi thông điệp báo nhận đến AF thứ nhất, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, chỉ báo kích hoạt bảo mật, và mã định danh khóa. Thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo

mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, Bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, khóa bảo mật được tạo ra dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

1030. Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, AF thứ hai kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Trong một số phương án, phương pháp còn bao gồm: AF thứ hai xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và tạo ra chỉ báo kích hoạt bảo mật dựa trên kết quả xác định.

Trong một số phương án, việc xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không bao gồm: AF thứ hai xác định, phụ thuộc vào việc liệu thuật toán bảo vệ bí mật có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF hay không, liệu có kích hoạt bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và/hoặc xác định, phụ thuộc vào việc liệu thuật toán bảo vệ toàn vẹn có được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ toàn vẹn được hỗ trợ bởi AF thứ hai hay không, liệu có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không.

Trong một số phương án, thông điệp thông báo khóa còn bao gồm chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không. Việc xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không bao gồm: AF thứ hai xác định, theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi AF thứ hai, xem có kích hoạt bảo vệ bảo mật hay không, trong đó chính sách bảo mật được hỗ trợ bởi AF thứ hai chỉ báo xem AF thứ hai có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không.

Trong một số phương án, phương pháp còn bao gồm: AF thứ hai tạo ra khóa bảo mật mà mã định danh khóa dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

Trong một số phương án, phương pháp còn bao gồm: AF thứ hai nhận thông điệp hoàn thành thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai; và AF thứ hai xác định, dựa trên khóa bảo mật và thống số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thành thiết lập phiên ứng dụng có bị giả mạo hay không.

Trong một số phương án, phương pháp còn bao gồm: Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật và khi xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, AF thứ hai kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Fig.11 là sơ đồ khối của thiết bị truyền thông ví dụ 1100 theo phương án của sáng chế. Thiết bị 1100 có thể được thực thi như thiết bị hoặc chíp trong thiết bị. Phạm vi của sáng chế không bị giới hạn ở khía cạnh này. Thiết bị 1100 có thể được thực thi như UE 410 được thể hiện trên Fig.4A hoặc một phần của UE 410.

Như được thể hiện trên Fig.11, thiết bị 1100 bao gồm môđun thu phát 1110. Môđun thu phát 1110 được tạo cấu hình để: gửi thông điệp yêu cầu thiết lập phiên ứng dụng đến AF thứ nhất, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA. Môđun thu phát 1110 còn được tạo cấu hình để nhận thông điệp phản hồi thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật. Chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị 1100 và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA. Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị 1100, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị 1100 bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị 1100 và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị 1100; và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị 1100, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn. Trong một số phương án, thiết bị thiết bị 1100 còn bao gồm: môđun bảo vệ bảo mật 1120, được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với

AF thứ hai.

Cần hiểu rằng thiết bị 1100 có thể tương ứng với phương pháp được thực hiện bởi thiết bị đầu cuối hoặc UE 410 trong các phương án phía trên. Các hoạt động và các dấu hiệu của các môđun trong thiết bị 1100 được sử dụng riêng biệt để thực hiện các bước tương ứng của phương pháp được thực hiện bởi thiết bị đầu cuối hoặc UE 410 trong các phương án phía trên, và có cùng các hiệu quả có lợi. Nhằm mục đích đơn giản hóa, các chi tiết cụ thể không được mô tả lại.

Fig.12 là sơ đồ khối của thiết bị truyền thông ví dụ 1200 theo các phương án của sáng chế. Thiết bị 1200 có thể được thực thi như thiết bị hoặc chíp trong thiết bị. Phạm vi của sáng chế không bị giới hạn ở khía cạnh này. Thiết bị 1200 có thể được thực thi như AF 420 được thể hiện trên Fig.4A hoặc một phần của AF 420.

Như được thể hiện trên Fig.12, thiết bị 1200 bao gồm ít nhất môđun thu phát 1210. Môđun thu phát 1210 được tạo cấu hình để: nhận thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA. Môđun thu phát 1210 còn được tạo cấu hình để gửi thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm chỉ báo kích hoạt bảo mật. Chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA. Trong một số phương án, thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối; và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn. Trong một số phương án, thiết bị 1200 còn bao gồm môđun bảo vệ bảo mật 1220. Môđun bảo vệ bảo mật 1220 được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, khởi động AF thứ hai để kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Cần hiểu rằng thiết bị 1200 có thể tương ứng với phương pháp được thực hiện bởi AF

thứ nhất hoặc AF 420 trong các phương án phía trên. Các hoạt động và các dấu hiệu của các môđun trong thiết bị 1200 được sử dụng riêng biệt để thực hiện các bước tương ứng của phương pháp được thực hiện bởi AF thứ nhất hoặc AF 420 trong các phương án phía trên, và có cùng các hiệu quả có lợi. Nhằm mục đích đơn giản hóa, các chi tiết cụ thể không được mô tả lại.

Fig.13 là sơ đồ khối của thiết bị truyền thông ví dụ 1300 theo phương án của sáng chế; Thiết bị 1300 có thể được thực thi như thiết bị hoặc chíp trong thiết bị. Phạm vi của sáng chế không bị giới hạn ở khía cạnh này. Thiết bị 1300 có thể được thực thi như AF 430 được thể hiện trên Fig.4A hoặc một phần của AF 430.

Như được thể hiện trên Fig.13, thiết bị 1300 bao gồm ít nhất môđun thu phát 1310. Môđun thu phát 1310 được tạo cấu hình để nhận thông điệp thông báo khóa từ AF thứ nhất, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai. Môđun thu phát 1310 còn được tạo cấu hình để gửi thông điệp báo nhận đến AF thứ nhất, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, chỉ báo kích hoạt bảo mật, và mã định danh khóa. Thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn, chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và thiết bị 1300 hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, khóa bảo mật được tạo ra dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, mã định danh khóa là để định danh ngữ cảnh bảo mật giữa thiết bị đầu cuối và thiết bị 1300, và ngữ cảnh bảo mật bao gồm khóa bảo mật. Trong một số phương án, thiết bị 1300 còn bao gồm môđun bảo vệ bảo mật 1320. Môđun bảo vệ bảo mật 1320 được tạo cấu hình để: khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

Cần hiểu rằng thiết bị 1300 có thể tương ứng với phương pháp được thực hiện bởi AF thứ hai hoặc AF 430 trong các phương án phía trên. Các hoạt động và các dấu hiệu của các môđun trong thiết bị 1300 được sử dụng riêng biệt để thực hiện các bước tương ứng của phương pháp được thực hiện bởi AF thứ hai hoặc AF 430 trong các phương án phía trên, và có cùng các hiệu quả có lợi. Nhằm mục đích đơn giản hóa, các chi tiết cụ thể không được mô tả lại.

Fig.14 là sơ đồ khối đơn giản hóa của thiết bị ví dụ 1400 có thể áp dụng để thực thi phương án của sáng chế. Thiết bị 1400 có thể được tạo cấu hình để thực thi UE 410, AF thứ nhất 420, và/hoặc AF thứ hai 430 được thể hiện trên Fig.4A. Như được thể hiện trên hình vẽ, thiết bị 1400 bao gồm một hoặc nhiều bộ xử lý 1410, một hoặc nhiều bộ nhớ 1420 được ghép nối với các bộ xử lý 1410, và môđun truyền thông 1440 được ghép nối với các bộ xử lý 1410.

Môđun truyền thông 1440 có thể được tạo cấu hình để thực hiện truyền thông hai chiều. Môđun truyền thông 1440 có thể có ít nhất một giao diện truyền thông để truyền thông. Giao diện truyền thông có thể bao gồm giao diện bất kỳ cần thiết để truyền thông với thiết bị khác.

Bộ xử lý 1410 có thể là loại bất kỳ thích hợp cho mạng kỹ thuật cục bộ, và có thể bao gồm nhưng không bị giới hạn ở một hoặc nhiều máy tính đa dụng, máy tính chuyên dụng, thiết bị vi điều khiển, bộ xử lý tín hiệu số (digital signal processor, DSP), và kiến trúc bộ điều khiển đa lõi dựa trên bộ điều khiển. Thiết bị 1400 có thể có nhiều bộ xử lý, như là các chíp mạch tích hợp chuyên dụng, mà có thời gian phụ thuộc vào đồng hồ được đồng bộ với bộ xử lý chính.

Bộ nhớ 1420 có thể bao gồm một hoặc nhiều bộ nhớ bất biến và một hoặc nhiều bộ nhớ khả biến. Các ví dụ về bộ nhớ bất biến bao gồm nhưng không bị giới hạn ở bộ nhớ chỉ đọc (read-only memory, ROM) 1424, bộ nhớ chỉ đọc có thể lập trình lại (erasable programmable read-only memory, EPROM), bộ nhớ cực nhanh, đĩa cứng, đĩa quang (optical disc, CD), đĩa video kỹ thuật số (digital video disc, DVD), và bộ lưu trữ từ tính khác và/hoặc bộ lưu trữ quang. Các ví dụ về bộ nhớ khả biến bao gồm nhưng không bị giới hạn ở bộ nhớ truy cập ngẫu nhiên (random access memory, RAM) 1422 và bộ nhớ khả biến khác mà không kéo dài cho khoảng thời gian ngắt nguồn.

Chương trình máy tính 1430 bao gồm các lệnh thực thi máy tính được thực thi bởi bộ xử lý 1410 liên quan. Chương trình 1430 có thể được lưu trữ trong ROM 1420. Bộ xử lý 1410 có thể thực hiện các hành động phù hợp bất kỳ và xử lý bằng cách tải chương trình 1430 vào RAM 1420.

Các phương án của sáng chế có thể được thực thi với sự hỗ trợ của chương trình 1430, để thiết bị 1400 có thể thực hiện quy trình bất kỳ được thảo luận tham chiếu đến Fig.5, Fig.7A và Fig.7B, và từ Fig.8 đến Fig.10. Các phương án của sáng chế có thể được thực thi thay thế bằng cách sử dụng phần cứng hoặc sự kết hợp của phần mềm và phần cứng.

Trong các phương án, chương trình 1430 có thể được bao gồm một cách rõ ràng trong phương tiện đọc được bằng máy tính, và phương tiện đọc được bằng máy tính có thể được

chứa trong thiết bị 1400 (ví dụ, trong bộ nhớ 1420) hoặc thiết bị lưu trữ khác mà có thể được truy nhập bởi thiết bị 1400. Chương trình 1430 có thể được tải từ phương tiện đọc được bằng máy tính vào RAM 1422 để thực thi. Phương tiện đọc được bằng máy tính có thể chứa dạng bất kỳ của bộ nhớ bất biến hữu hình, như là ROM, EPROM, bộ nhớ cực nhanh, đĩa cứng, CD, DVD, hoặc tương tự. Fig.15 thể hiện ví dụ về phương tiện đọc được bằng máy tính 1500 dưới dạng CD hoặc DVD. Phương tiện đọc được bằng máy tính lưu trữ chương trình 1430.

Nói chung, các phương án khác nhau của sáng chế có thể được thực thi bởi phần cứng hoặc mạch chuyên dụng, phần mềm, logic, hoặc sự kết hợp bất kỳ của chúng. Một số khía cạnh có thể được thực thi bởi phần cứng, và các khía cạnh khác có thể được thực thi bởi chương trình cơ sở hoặc phần mềm, và có thể được thực hiện bởi bộ điều khiển, bộ vi xử lý, hoặc thiết bị tính toán khác. Mặc dù các khía cạnh của các phương án của sáng chế được thể hiện và được minh họa như các sơ đồ khối, các lưu đồ, hoặc các chương trình khác, cần hiểu rằng các khối, các thiết bị, các hệ thống, các kỹ thuật, hoặc các phương pháp được mô tả trong bản mô tả này có thể được thực thi như, ví dụ, các ví dụ không giới hạn, phần cứng, phần mềm, chương trình cơ sở, các mạch chuyên dụng, logic, phần cứng đa dụng, các bộ điều khiển, các thiết bị tính toán khác, hoặc sự kết hợp của chúng.

Sáng chế còn đề xuất ít nhất một chương trình máy tính được lưu trữ rõ ràng trên phương tiện lưu trữ đọc được bằng máy tính không nhất thời. Sản phẩm chương trình máy tính bao gồm các lệnh thực thi máy tính, như là các lệnh được chứa trong môđun chương trình, được thực thi trong thiết bị trên bộ xử lý mục tiêu thực hoặc ảo để thực hiện phương pháp 900, phương pháp 1000, và/hoặc phương pháp 1100 như được mô tả phía trên với sự tham chiếu đến các hình từ Fig.9 đến Fig.11. Nói chung, môđun chương trình bao gồm đoạn chương trình, chương trình, thư viện, đối tượng, lớp, bộ phận, kết cấu dữ liệu, và tương tự mà thực thi nhiệm vụ cụ thể hoặc thực thi loại dữ liệu trừu tượng cụ thể. Trong các phương án khác nhau, các chức năng của các môđun chương trình có thể được kết hợp hoặc chức năng của môđun chương trình có thể được tách khi cần thiết. Các lệnh thực thi máy tính đối với môđun chương trình có thể được thực thi cục bộ hoặc trong thiết bị được phân phối. Trong thiết bị được phân phối, môđun chương trình có thể được đặt trong phương tiện lưu trữ cục bộ hoặc từ xa.

Mã chương trình máy tính được sử dụng để thực hiện các phương pháp được bộc lộ trong sáng chế có thể được viết trong một hoặc nhiều ngôn ngữ lập trình. Mã chương trình máy tính có thể được cung cấp cho bộ xử lý của máy tính đa dụng, máy tính chuyên dụng,

thiết bị xử lý dữ liệu lập trình khác, để khi mã chương trình được thực thi bởi máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, các hoạt động/các vận hành được xác định trong các lưu đồ và/hoặc các sơ đồ khối có thể được thực thi. Mã chương trình có thể được thực thi hoàn toàn trên máy tính, một phần trên máy tính, như gói phần mềm độc lập, một phần trên máy tính và một phần trên máy tính từ xa, hoặc hoàn toàn trên máy tính hoặc máy chủ từ xa.

Trong ngữ cảnh của sáng chế, mã chương trình máy tính hoặc dữ liệu liên quan có thể được mang bởi vật mang phù hợp, để thiết bị, thiết bị, hoặc bộ xử lý có thể thực hiện các hoạt động và xử lý khác nhau được mô tả ở trên. Các ví dụ về vật mang bao gồm tín hiệu, phương tiện đọc được bằng máy tính, hoặc tương tự. Các ví dụ về tín hiệu có thể bao gồm các tín hiệu lan truyền dưới dạng điện, quang, vô tuyến, âm, hoặc các dạng khác, như là các sóng mang hoặc các tín hiệu hồng ngoại.

Phương tiện đọc được bằng máy tính có thể là phương tiện hữu hình mà bao gồm hoặc chứa chương trình được sử dụng để hoặc liên quan đến hệ thống, thiết bị hoặc thiết bị thực thi lệnh. Phương tiện đọc được bằng máy tính có thể là phương tiện tín hiệu đọc được bằng máy tính hoặc phương tiện lưu trữ đọc được bằng máy tính. Phương tiện đọc được bằng máy tính có thể bao gồm nhưng không bị giới hạn ở hệ thống, thiết bị, hoặc thiết bị điện, từ, quang, điện từ, hồng ngoại hoặc bán dẫn hoặc sự kết hợp phù hợp bất kỳ của chúng. Nhiều ví dụ chi tiết về phương tiện lưu trữ đọc được bằng máy tính bao gồm phần kết nối điện với một hoặc nhiều dây, ổ đĩa máy tính di động, ổ cứng, bộ nhớ truy cập ngẫu nhiên (random access memory, RAM), bộ nhớ chỉ đọc read-only memory (ROM), bộ nhớ chỉ đọc có thể lập trình và xóa được (EPROM hoặc bộ nhớ cực nhanh), thiết bị lưu trữ quang, thiết bị lưu trữ từ, hoặc sự kết hợp phù hợp bất kỳ của chúng.

Ngoài ra, mặc dù các vận hành của các phương pháp được bộc lộ trong sáng chế này được mô tả theo thứ tự cụ thể trong các hình vẽ kèm theo, điều này không yêu cầu hoặc ngụ ý rằng các vận hành này cần được thực hiện theo thứ tự cụ thể hoặc tất cả trong các vận hành được thể hiện cần được thực hiện để đạt được kết quả mong muốn. Thay vì thế, các thứ tự thực thi của các bước được mô tả trong các lưu đồ có thể thay đổi. Ngoài ra hoặc theo tùy chọn, một số bước có thể được bỏ qua, nhiều bước có thể được kết hợp thành một bước hoặc thực thi, và/hoặc một bước có thể được tách thành nhiều bước để thực thi. Cần lưu ý thêm rằng các dấu hiệu và các chức năng của hai hoặc nhiều thiết bị theo sáng chế có thể được xác định trong một thiết bị. Ngược lại, các dấu hiệu và các chức năng của một thiết bị được mô tả phía trên có thể còn được chia thành nhiều thiết bị để cụ thể hóa.

Mặc dù sáng chế đã được mô tả với sự tham chiếu đến một số phương án cụ thể, cần hiểu rằng sáng chế không bị giới hạn bởi các phương án cụ thể được bộc lộ. Sáng chế nhằm bao trùm các sửa đổi khác nhau và những sắp xếp tương đương được bao gồm trong phạm vi của các yêu cầu bảo hộ kèm theo.

YÊU CẦU BẢO HỘ

1. Phương pháp bảo vệ truyền thông, bao gồm:

bước gửi, bởi thiết bị truyền thông, thông điệp yêu cầu thiết lập phiên ứng dụng đến bộ phận mạng chức năng ứng dụng AF (application function) thứ nhất, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa xác thực và quản lý khóa đối với ứng dụng AKMA (Authentication and Key Management for Application, AKMA); và

bước nhận, bởi thiết bị truyền thông, thông điệp phản hồi thiết lập phiên ứng dụng từ bộ phận mạng chức năng ứng dụng thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật, trong đó

chỉ báo kích hoạt bảo mật được sử dụng để chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị truyền thông và bộ phận mạng chức năng ứng dụng thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

2. Phương pháp theo điểm 1, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị truyền thông, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị truyền thông bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị truyền thông và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị truyền thông; và

thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị truyền thông, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn.

3. Phương pháp theo điểm 2, trong đó phương pháp này còn bao gồm:

khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, bước kích hoạt, bởi thiết bị truyền thông dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với bộ phận mạng chức năng ứng dụng thứ hai.

4. Phương pháp theo điểm 2 hoặc điểm 3, trong đó AF thứ nhất và AF thứ hai là cùng một AF, và phương pháp này còn bao gồm:

bước tạo ra, bởi thiết bị truyền thông, khóa AF thứ nhất dựa trên khóa AKMA; và

bước tạo ra, bởi thiết bị truyền thông, khóa bảo mật dựa trên khóa AF thứ nhất và thuật toán bảo mật được lựa chọn, trong đó

khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

5. Phương pháp theo điểm 2 hoặc điểm 3, trong đó AF thứ nhất và AF thứ hai là các AF khác nhau, và phương pháp này còn bao gồm:

bước tạo ra, bởi thiết bị truyền thông, khóa AF thứ nhất dựa trên khóa AKMA;

bước tạo ra, bởi thiết bị truyền thông, khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị truyền thông và AF thứ nhất; và

bước tạo ra, bởi thiết bị truyền thông, khóa bảo mật dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó

khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

6. Phương pháp theo điểm 5, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa; và

thông số tạo ra khóa bao gồm ít nhất một trong số các nội dung sau đây:

thông tin nhận dạng được sử dụng bởi thiết bị truyền thông trong AF thứ nhất hoặc AF thứ hai;

loại dịch vụ được yêu cầu bởi thiết bị truyền thông từ AF thứ nhất hoặc AF thứ hai;

thông tin nhận dạng của AF thứ hai; hoặc

thông số làm mới khóa.

7. Phương pháp theo điểm 5, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số tạo ra khóa, và thông số tạo ra khóa bao gồm thông số làm mới khóa.

8. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, 6 hoặc 7, trong đó thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa, mã định danh khóa này để xác định ngữ cảnh bảo mật giữa thiết bị truyền thông và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

9. Phương pháp theo điểm 4, trong đó thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa, mã định danh khóa này dùng để xác định ngữ cảnh bảo mật giữa thiết bị truyền thông và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

10. Phương pháp theo điểm 5, trong đó thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa, mã định danh khóa này dùng để xác định ngữ cảnh bảo mật giữa thiết bị truyền thông và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật.

11. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, 6, 7, 9 hoặc 10, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và phương pháp này còn bao gồm:

bước xác định, bởi thiết bị truyền thông dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ nhất, xem thông điệp phản hồi thiết lập phiên ứng dụng có bị giả mạo hay không.

12. Phương pháp theo điểm 4, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và phương pháp này còn bao gồm:

bước xác định, bởi thiết bị truyền thông dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ nhất, xem thông điệp phản hồi thiết lập phiên ứng dụng có bị giả mạo hay không.

13. Phương pháp theo điểm 5, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và phương pháp này còn bao gồm:

bước xác định, bởi thiết bị truyền thông dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ nhất, xem thông điệp phản hồi thiết lập phiên ứng dụng có bị giả mạo hay không.

14. Phương pháp theo điểm 8, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ nhất, và phương pháp này còn bao gồm:

bước xác định, bởi thiết bị truyền thông dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ nhất, xem thông điệp phản hồi thiết lập phiên ứng dụng có bị giả mạo hay không.

15. Phương pháp theo điểm 11, trong đó phương pháp này còn bao gồm:

bước gửi, bởi thiết bị truyền thông, thông điệp hoàn thành thiết lập phiên ứng dụng đến bộ phận mạng chức năng ứng dụng thứ hai khi thông điệp phản hồi thiết lập phiên ứng dụng

không bị giả mạo, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai được tính toán dựa trên khóa bảo mật.

16. Phương pháp theo điểm bất kỳ trong số các điểm từ 12 đến 14, trong đó phương pháp này còn bao gồm:

bước gửi, bởi thiết bị truyền thông, thông điệp hoàn thành thiết lập phiên ứng dụng đến bộ phận mạng chức năng ứng dụng thứ hai khi thông điệp phản hồi thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai được tính toán dựa trên khóa bảo mật.

17. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, 6, 7, 9, 10 hoặc từ 12 đến 15, trong đó AF thứ nhất và AF thứ hai có cùng mã định danh AF.

18. Phương pháp theo điểm 4, trong đó AF thứ nhất và AF thứ hai có cùng mã định danh AF.

19. Phương pháp theo điểm 5, trong đó AF thứ nhất và AF thứ hai có cùng mã định danh AF.

20. Phương pháp theo điểm 8, trong đó AF thứ nhất và AF thứ hai có cùng mã định danh AF.

21. Phương pháp theo điểm 11, trong đó AF thứ nhất và AF thứ hai có cùng mã định danh AF.

22. Phương pháp theo điểm 16, trong đó AF thứ nhất và AF thứ hai có cùng mã định danh AF.

23. Phương pháp bảo vệ truyền thông, bao gồm:

bước nhận, bởi bộ phận mạng chức năng ứng dụng thứ nhất AF, thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa xác thực và quản lý khóa đối với ứng dụng AKMA; và

bước gửi, bởi AF thứ nhất, thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật, trong đó

chỉ báo kích hoạt bảo mật chỉ báo xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không, bảo vệ bảo mật bao gồm bảo vệ bí mật và/hoặc

bảo vệ toàn vẹn được thực hiện dựa trên khóa bảo mật, và khóa bảo mật được tạo ra dựa trên khóa AKMA tương ứng với mã định danh khóa AKMA.

24. Phương pháp theo điểm 23, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị đầu cuối và/hoặc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị đầu cuối; và

thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm thông tin về thuật toán bảo mật được lựa chọn dựa trên thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối, trong đó thuật toán bảo mật được lựa chọn bao gồm thuật toán bảo vệ bí mật được lựa chọn và/hoặc thuật toán bảo vệ toàn vẹn được lựa chọn.

25. Phương pháp theo điểm 24, trong đó phương pháp này còn bao gồm:

khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, bước kích hoạt, bởi AF thứ nhất, AF thứ hai để kích hoạt, dựa trên thuật toán bảo mật được lựa chọn và khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

26. Phương pháp theo điểm 24, trong đó AF thứ nhất và AF thứ hai là cùng một AF, và phương pháp này còn bao gồm:

bước tạo ra, bởi AF thứ nhất, khóa AF thứ nhất dựa trên khóa AKMA; và

bước tạo ra, bởi AF thứ nhất, khóa bảo mật dựa trên khóa AF thứ nhất và thuật toán bảo mật được lựa chọn, trong đó

khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn.

27. Phương pháp theo điểm 24, trong đó AF thứ nhất và AF thứ hai là các AF khác nhau, và phương pháp này còn bao gồm:

bước tạo ra, bởi AF thứ nhất, khóa AF thứ nhất dựa trên khóa AKMA;

bước tạo ra, bởi AF thứ nhất, khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất;

bước tạo ra, bởi AF thứ nhất, khóa bảo mật và mã định danh khóa dựa trên khóa AF thứ hai và thuật toán bảo mật được lựa chọn, trong đó

khóa bảo mật bao gồm khóa bảo vệ bí mật để bảo vệ bí mật và/hoặc khóa bảo vệ toàn vẹn để bảo vệ toàn vẹn, mã định danh khóa dùng để xác định ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, ngữ cảnh bảo mật bao gồm khóa bảo mật, và thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa; và

bước gửi, bởi AF thứ nhất, thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được lựa chọn, khóa bảo mật, và mã định danh khóa.

28. Phương pháp theo điểm bất kỳ trong số các điểm từ 24 đến 27, trong đó chỉ báo kích hoạt bảo mật được chỉ báo bởi thuật toán bảo mật được lựa chọn, trong đó

khi thuật toán bảo vệ bí mật được lựa chọn là không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt;

khi thuật toán bảo vệ bí mật được lựa chọn là khác không, nó chỉ báo rằng bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt;

khi thuật toán bảo vệ toàn vẹn được lựa chọn là không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai không được kích hoạt; và

khi thuật toán bảo vệ toàn vẹn được lựa chọn là khác không, nó chỉ báo rằng bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai được kích hoạt.

29. Phương pháp theo điểm bất kỳ trong số các điểm từ 24 đến 27, trong đó phương pháp này còn bao gồm:

bước xác định, bởi AF thứ nhất, xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và

bước tạo ra, bởi AF thứ nhất, chỉ báo kích hoạt bảo mật dựa trên kết quả xác định.

30. Phương pháp theo điểm 29, trong đó bước xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không bao gồm:

bước xác định, phụ thuộc vào việc thuật toán bảo vệ bí mật được hỗ trợ bởi thiết bị đầu cuối có bao gồm thuật toán bảo vệ bí mật được hỗ trợ bởi AF thứ hai hay không, và có kích hoạt tính bảo vệ bí mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không; và/hoặc

bước xác định, phụ thuộc vào việc thuật toán bảo vệ toàn vẹn được hỗ trợ bởi thiết bị

đầu cuối có bao gồm thuật toán bảo vệ toàn vẹn được hỗ trợ bởi AF thứ hai hay không, có kích hoạt bảo vệ toàn vẹn đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không.

31. Phương pháp theo điểm 29, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng còn bao gồm chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối, và chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối chỉ báo xem thiết bị đầu cuối có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai hay không; và bước xác định xem có kích hoạt bảo vệ bảo mật đối với truyền thông giữa thiết bị đầu cuối và AF thứ hai hay không bao gồm:

bước xác định, bởi AF thứ nhất theo chính sách bảo mật được hỗ trợ bởi thiết bị đầu cuối và chính sách bảo mật được hỗ trợ bởi AF thứ hai, xem có kích hoạt bảo vệ bảo mật hay không, trong đó chính sách bảo mật được hỗ trợ bởi AF thứ hai chỉ báo xem AF thứ hai có hỗ trợ kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối hay không.

32. Phương pháp theo điểm 24 hoặc điểm 25, trong đó AF thứ nhất và AF thứ hai là các AF khác nhau, và phương pháp này còn bao gồm:

bước tạo ra, bởi AF thứ nhất, khóa AF thứ nhất dựa trên khóa AKMA;

bước tạo ra, bởi AF thứ nhất, khóa AF thứ hai dựa trên khóa AF thứ nhất và thông số tạo ra khóa mà được chia sẻ bởi thiết bị đầu cuối và AF thứ nhất;

bước gửi, bởi AF thứ nhất, thông điệp thông báo khóa đến AF thứ hai, trong đó thông điệp thông báo khóa bao gồm thông tin về thuật toán bảo mật được hỗ trợ bởi thiết bị đầu cuối và khóa AF thứ hai; và

bước nhận, bởi AF thứ nhất, thông điệp báo nhận từ AF thứ hai, trong đó thông điệp báo nhận bao gồm thông tin về thuật toán bảo mật được lựa chọn, chỉ báo kích hoạt bảo mật, và mã định danh khóa, mã định danh khóa dùng để xác định ngữ cảnh bảo mật giữa thiết bị đầu cuối và AF thứ hai, và ngữ cảnh bảo mật bao gồm khóa bảo mật, trong đó

thông điệp phản hồi thiết lập phiên ứng dụng còn bao gồm mã định danh khóa.

33. Phương pháp theo điểm bất kỳ trong số các điểm từ 23 đến 27 hoặc từ 30 đến 31, trong đó phương pháp này còn bao gồm:

bước nhận, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai; và

bước xác định, bởi AF thứ nhất dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thành thiết lập phiên ứng dụng có bị giả mạo hay không.

34. Phương pháp theo điểm 28, trong đó phương pháp này còn bao gồm:

bước nhận, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai; và

bước xác định, bởi AF thứ nhất dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thiện thiết lập phiên ứng dụng có bị giả mạo hay không.

35. Phương pháp theo điểm 29, trong đó phương pháp này còn bao gồm:

bước nhận, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai; và

bước xác định, bởi AF thứ nhất dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thiện thiết lập phiên ứng dụng có bị giả mạo hay không.

36. Phương pháp theo điểm 32, trong đó phương pháp này còn bao gồm:

bước nhận, bởi AF thứ nhất, thông điệp hoàn thành thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp hoàn thành thiết lập phiên ứng dụng bao gồm thông số xác minh toàn vẹn thứ hai; và

bước xác định, bởi AF thứ nhất dựa trên khóa bảo mật và thông số xác minh toàn vẹn thứ hai, xem thông điệp hoàn thiện thiết lập phiên ứng dụng có bị giả mạo hay không.

37. Phương pháp theo điểm 33, trong đó phương pháp này còn bao gồm:

bước gửi, bởi AF thứ nhất, thông điệp kích hoạt đến AF thứ hai khi xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp kích hoạt chỉ báo AF thứ hai kích hoạt, dựa trên khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

38. Phương pháp theo điểm bất kỳ trong số các điểm từ 34 đến 36, trong đó phương pháp này còn bao gồm:

bước gửi, bởi AF thứ nhất, thông điệp kích hoạt đến AF thứ hai khi xác định rằng thông điệp hoàn thành thiết lập phiên ứng dụng không bị giả mạo, trong đó thông điệp kích hoạt chỉ báo AF thứ hai kích hoạt, dựa trên khóa bảo mật, bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối.

39. Thiết bị truyền thông, bao gồm môđun được tạo cấu hình để thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 28.

40. Thiết bị truyền thông, bao gồm bộ xử lý, trong đó bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trữ trong bộ nhớ để cho phép thiết bị truyền thông thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 22.

41. Thiết bị truyền thông, bao gồm bộ xử lý, trong đó bộ xử lý được tạo cấu hình để thực thi chương trình được lưu trữ trong bộ nhớ để cho phép thiết bị truyền thông thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 23 đến 38.

42. Phương tiện lưu trữ đọc được bằng máy tính, trong đó phương tiện lưu trữ đọc được bằng máy tính lưu trữ các lệnh; và khi các lệnh được chạy trên thiết bị truyền thông, thiết bị truyền thông được cho phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 22.

43. Phương tiện lưu trữ đọc được bằng máy tính, trong đó phương tiện lưu trữ đọc được bằng máy tính lưu trữ các lệnh; và khi các lệnh được chạy trên thiết bị truyền thông, thiết bị truyền thông được cho phép thực hiện phương pháp theo điểm bất kỳ trong số các điểm từ 23 đến 38.

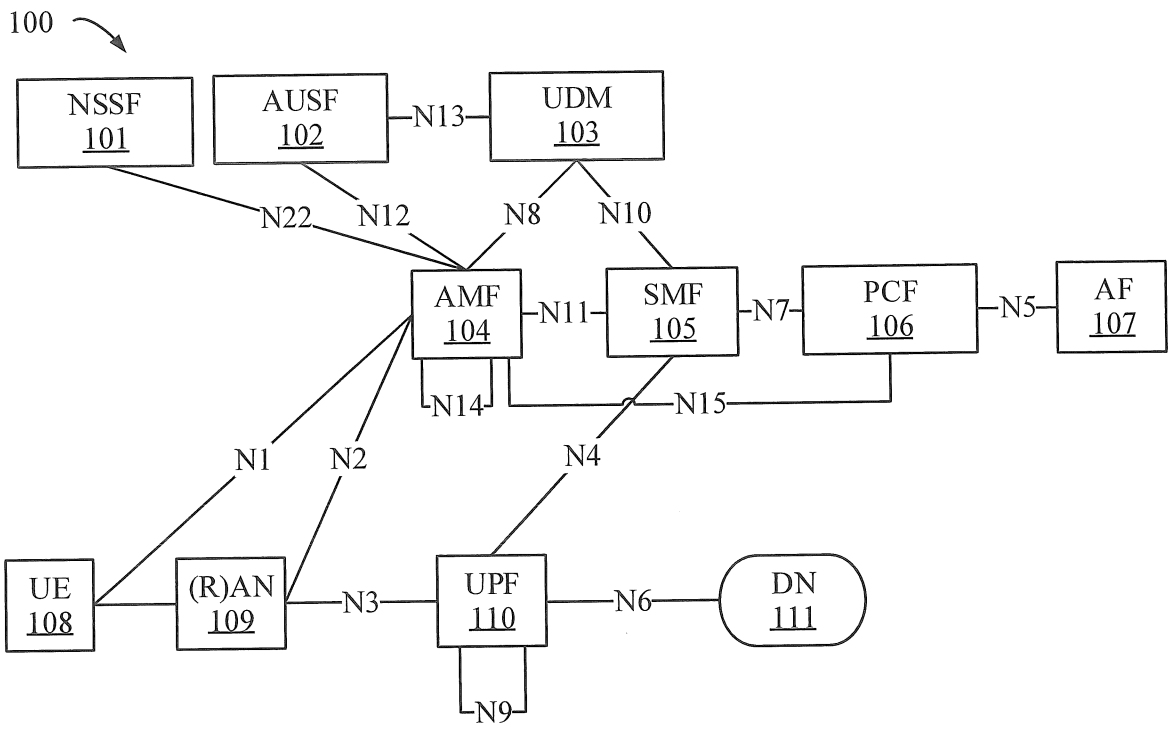
100
NSSF 101
AUSF 102
N13
UDM 103
N22
N12
N8
N10
AMF 104
N11
SMF 105
N7
PCF 106
N5
AF 107
N14
N15
N1
N2
N4
UE 108
(R)AN 109
N3
UPF 110
N6
DN 111
N9

FIG. 1A

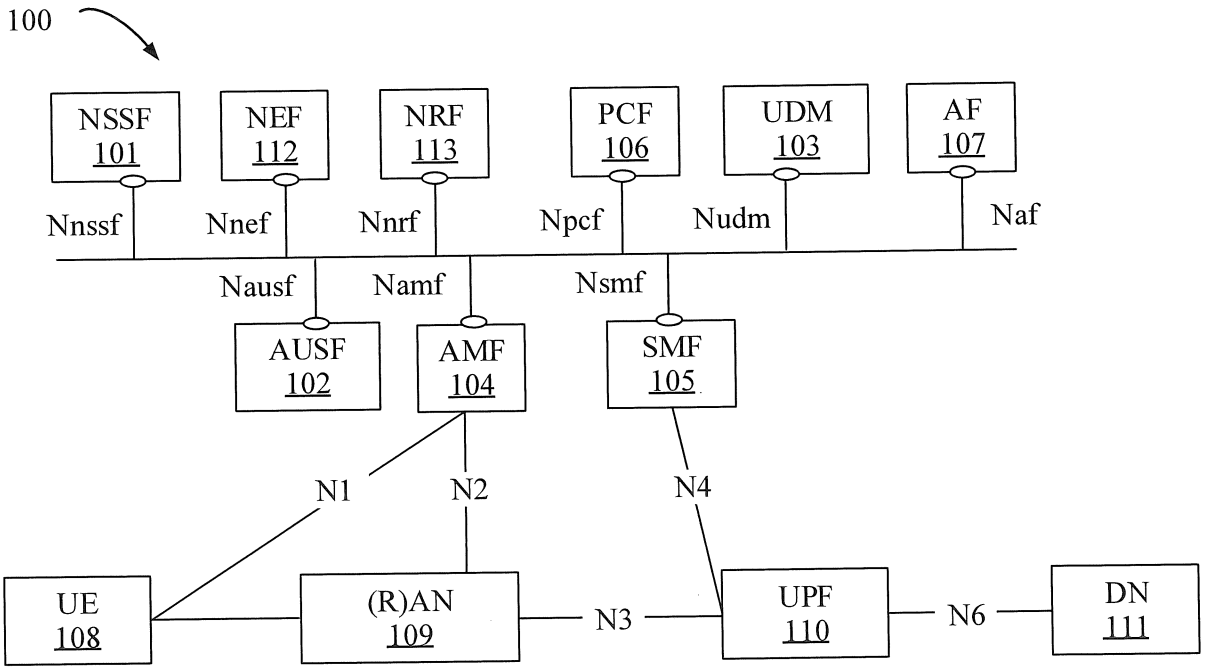
100
NSSF 101
NEF 112
NRF 113
PCF 106
UDM 103
AF 107
Nnssf
Nnef
Nnrf
Npcf
Nudm
Naf
Nausf
Namf
Nsmf
AUSF 102
AMF 104
SMF 105
N1
N2
N4
UE 108
(R)AN 109
N3
UPF 110
N6
DN 111

FIG. 1B

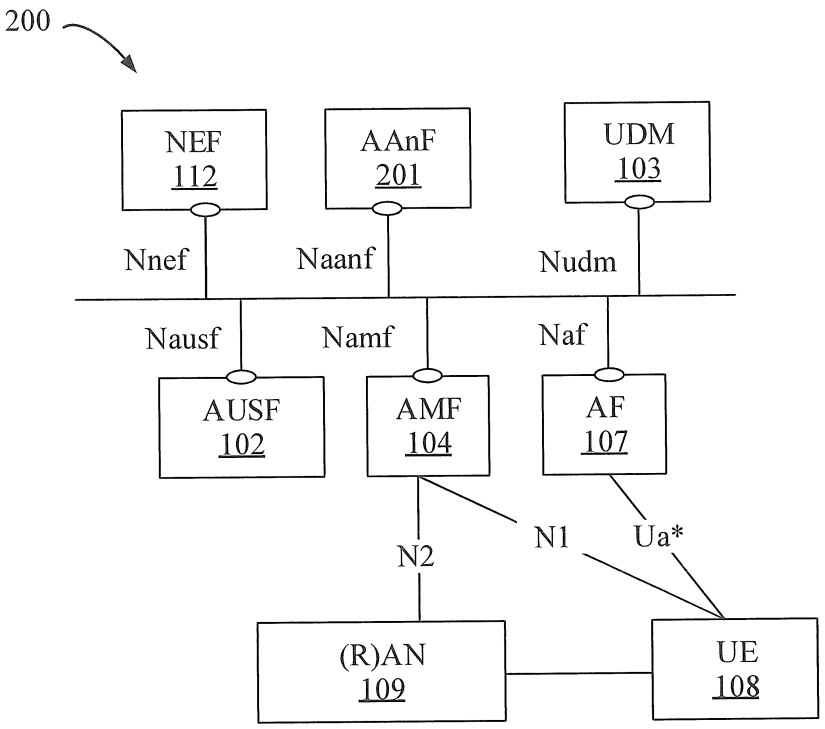
200
NEF
112
AAnF
201
UDM
103
Nnef
Naanf
Nudm
Nausf
Namf
Naf
AUSF
102
AMF
104
AF
107
N2
N1
Ua*
(R)AN
109
UE
108

FIG. 2

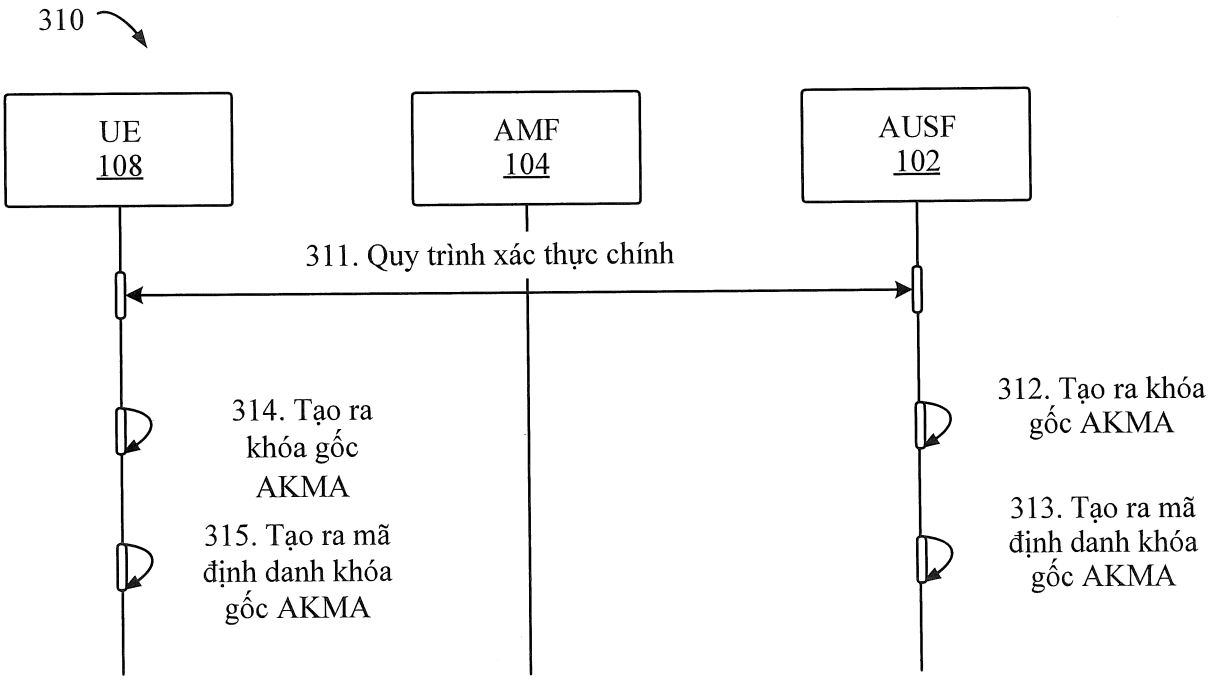
310
UE
108
AMF
104
AUSF
102
311. Quy trình xác thực chính
314. Tạo ra khóa gốc AKMA
315. Tạo ra mã định danh khóa gốc AKMA
312. Tạo ra khóa gốc AKMA
313. Tạo ra mã định danh khóa gốc AKMA

FIG. 3A

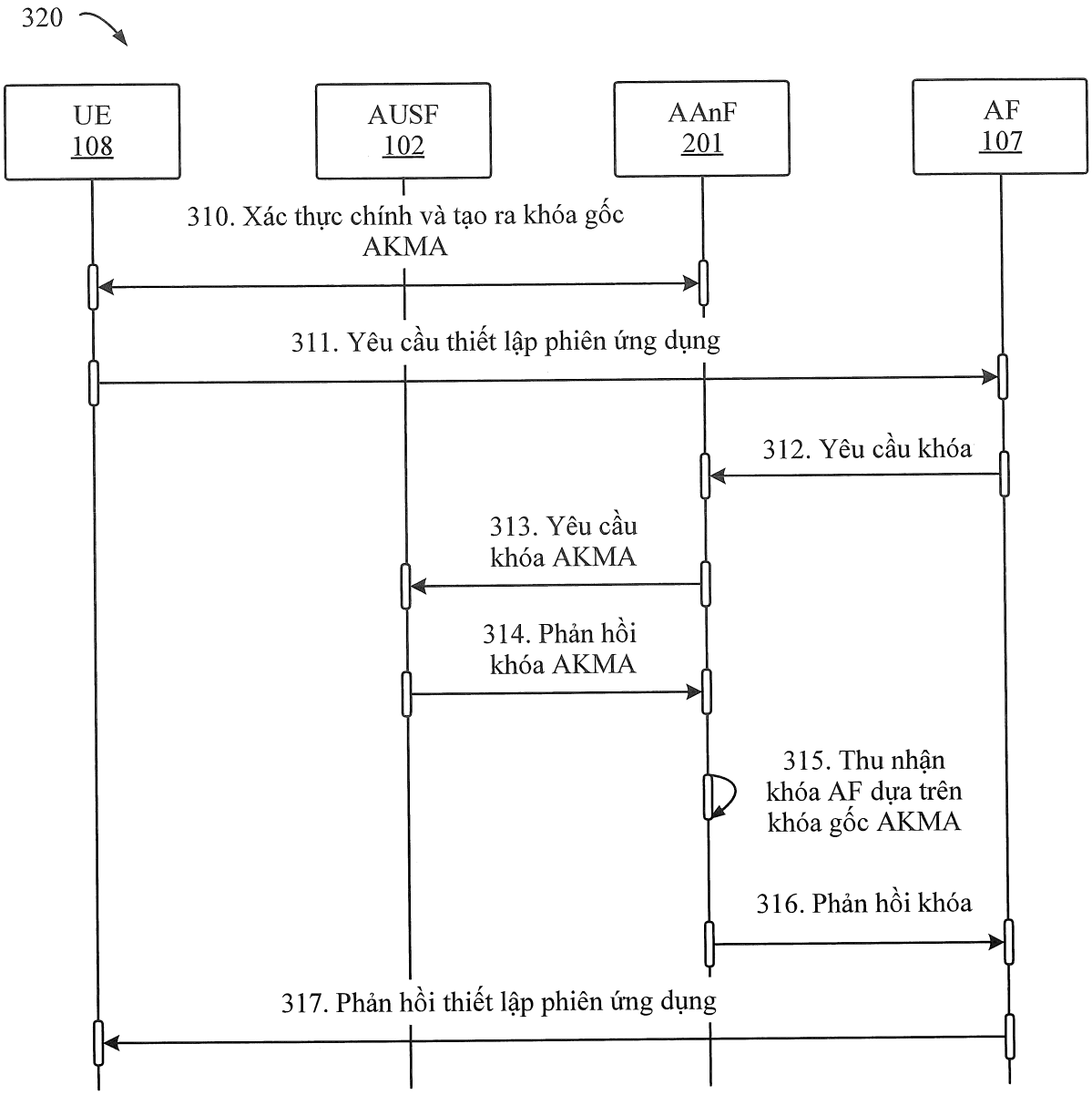
320
UE
108
AUSF
102
AAnF
201
AF
107
310. Xác thực chính và tạo ra khóa gốc AKMA
311. Yêu cầu thiết lập phiên ứng dụng
312. Yêu cầu khóa
313. Yêu cầu khóa AKMA
314. Phản hồi khóa AKMA
315. Thu nhận khóa AF dựa trên khóa gốc AKMA
316. Phản hồi khóa
317. Phản hồi thiết lập phiên ứng dụng

FIG. 3B

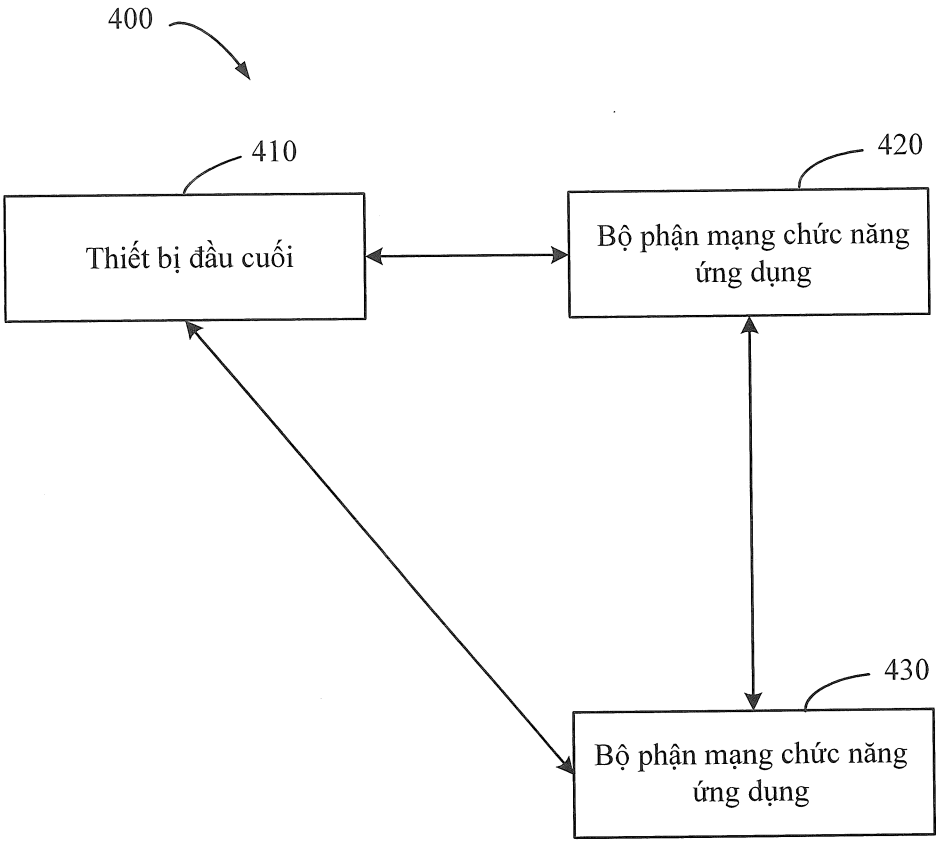
400
410
Thiết bị đầu cuối
420
Bộ phận mạng chức năng ứng dụng
430
Bộ phận mạng chức năng ứng dụng

FIG. 4A

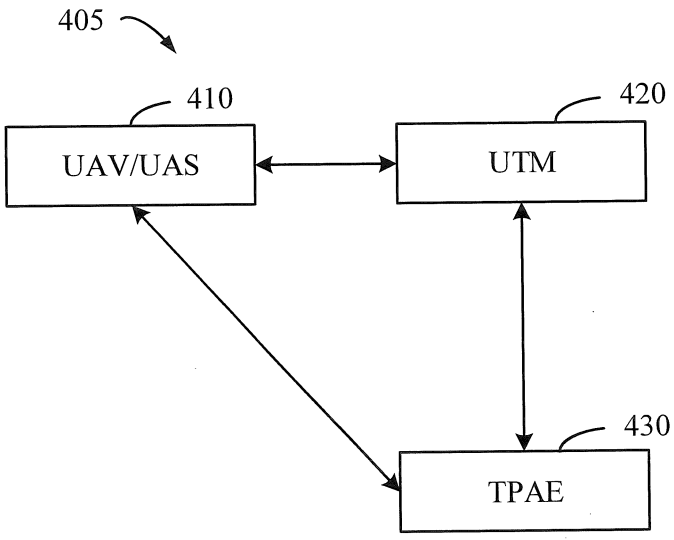
405
410
UAV/UAS
420
UTM
430
TPAE

FIG. 4B

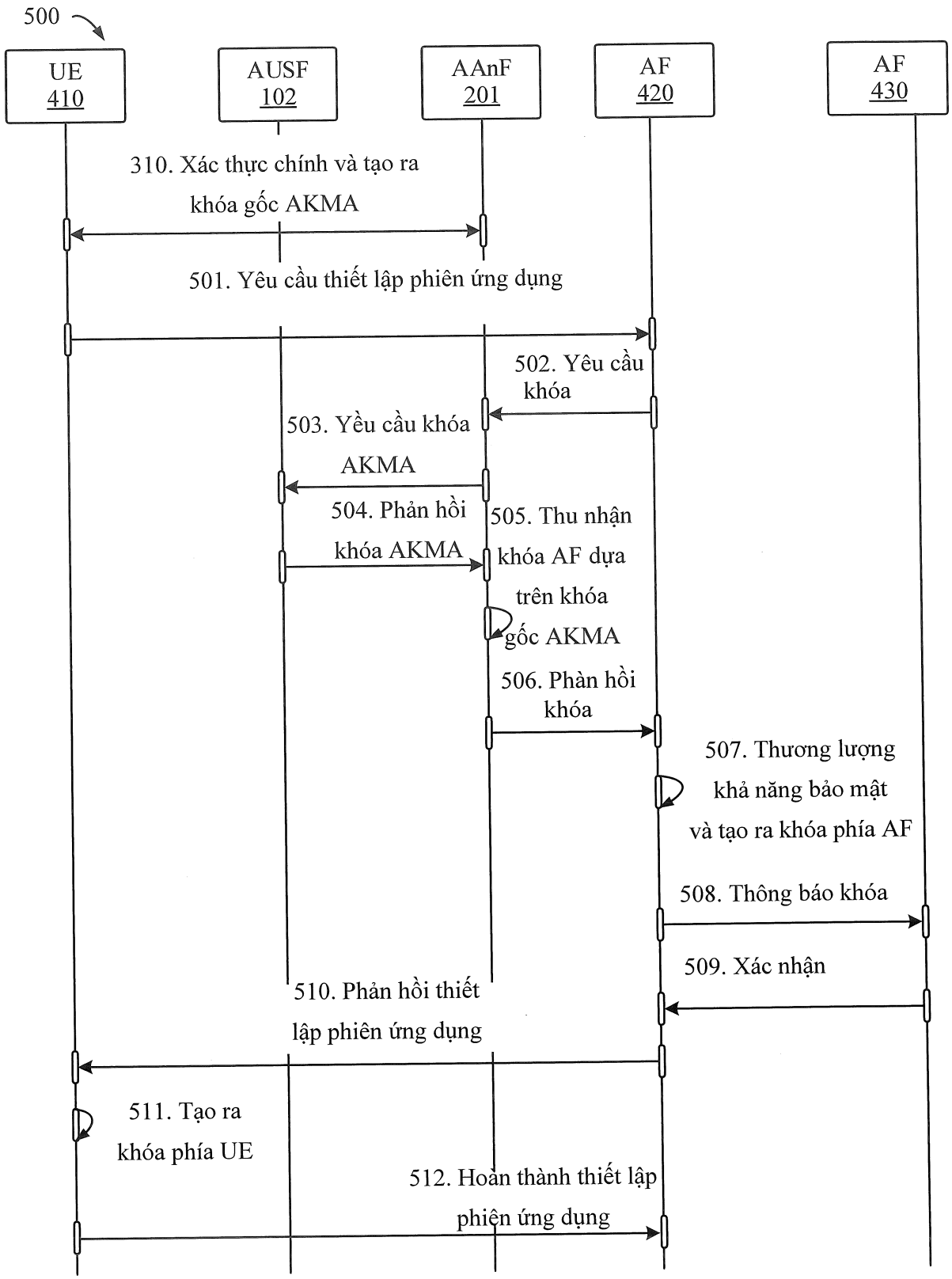
500
UE
410
AUSF
102
AAnF
201
AF
420
AF
430
310. Xác thực chính và tạo ra khóa gốc AKMA
501. Yêu cầu thiết lập phiên ứng dụng
502. Yêu cầu khóa
503. Yều cầu khóa AKMA
504. Phản hồi khóa AKMA
505. Thu nhận khóa AF dựa trên khóa gốc AKMA
506. Phản hồi khóa
507. Thương lượng khả năng bảo mật và tạo ra khóa phía AF
508. Thông báo khóa
509. Xác nhận
510. Phản hồi thiết lập phiên ứng dụng
511. Tạo ra khóa phía UE
512. Hoàn thành thiết lập phiên ứng dụng

FIG. 5

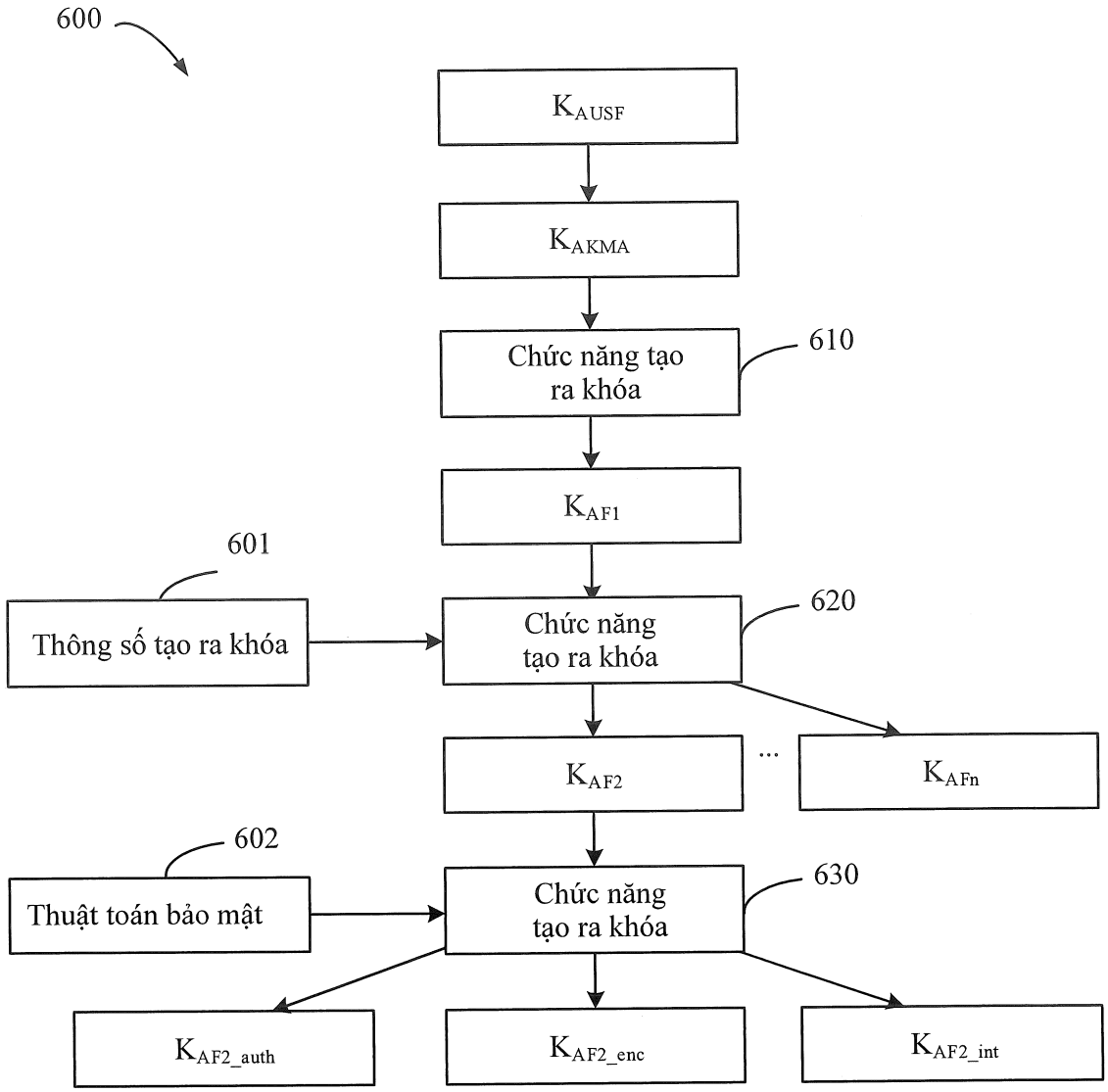
600
K_{AUSF}
K_{AKMA}
Chức năng tạo ra khóa
610
K_{AF1}
601
Thông số tạo ra khóa
Chức năng tạo ra khóa
620
K_{AF2}
...
K_{AFn}
602
Thuật toán bảo mật
Chức năng tạo ra khóa
630
K_{AF2_auth}
K_{AF2_enc}
K_{AF2_int}

FIG. 6

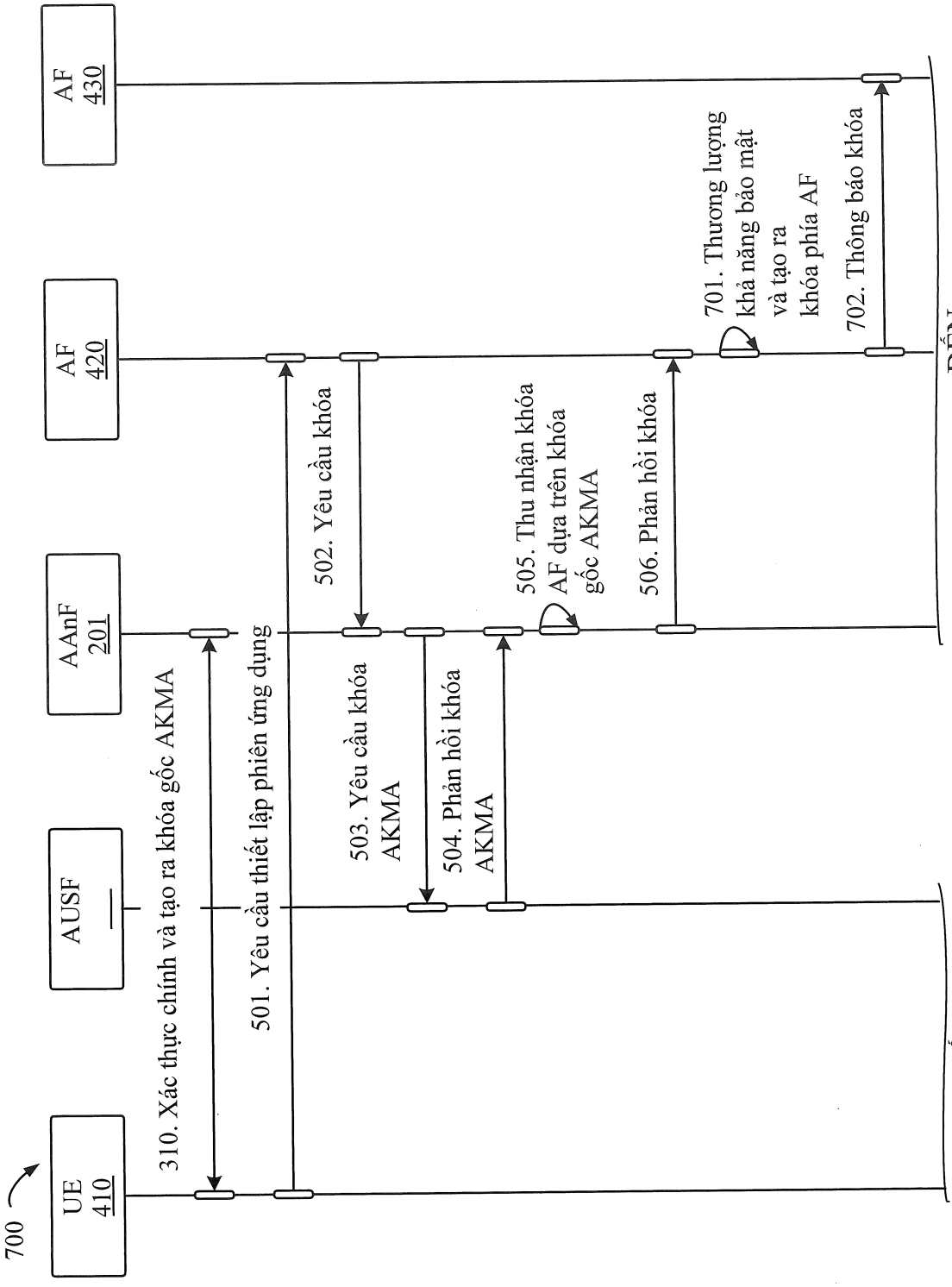
700
UE 410
AUSF
AAnF 201
AF 420
AF 430
310. Xác thực chính và tạo ra khóa gốc AKMA
501. Yêu cầu thiết lập phiên ứng dụng
502. Yêu cầu khóa
503. Yêu cầu khóa AKMA
504. Phản hồi khóa AKMA
505. Thu nhận khóa AF dựa trên khóa gốc AKMA
506. Phản hồi khóa
701. Thương lượng khả năng bảo mật và tạo ra khóa phía AF
702. Thông báo khóa
ĐẾN FIG. 7B
ĐẾN FIG. 7B

FIG. 7A

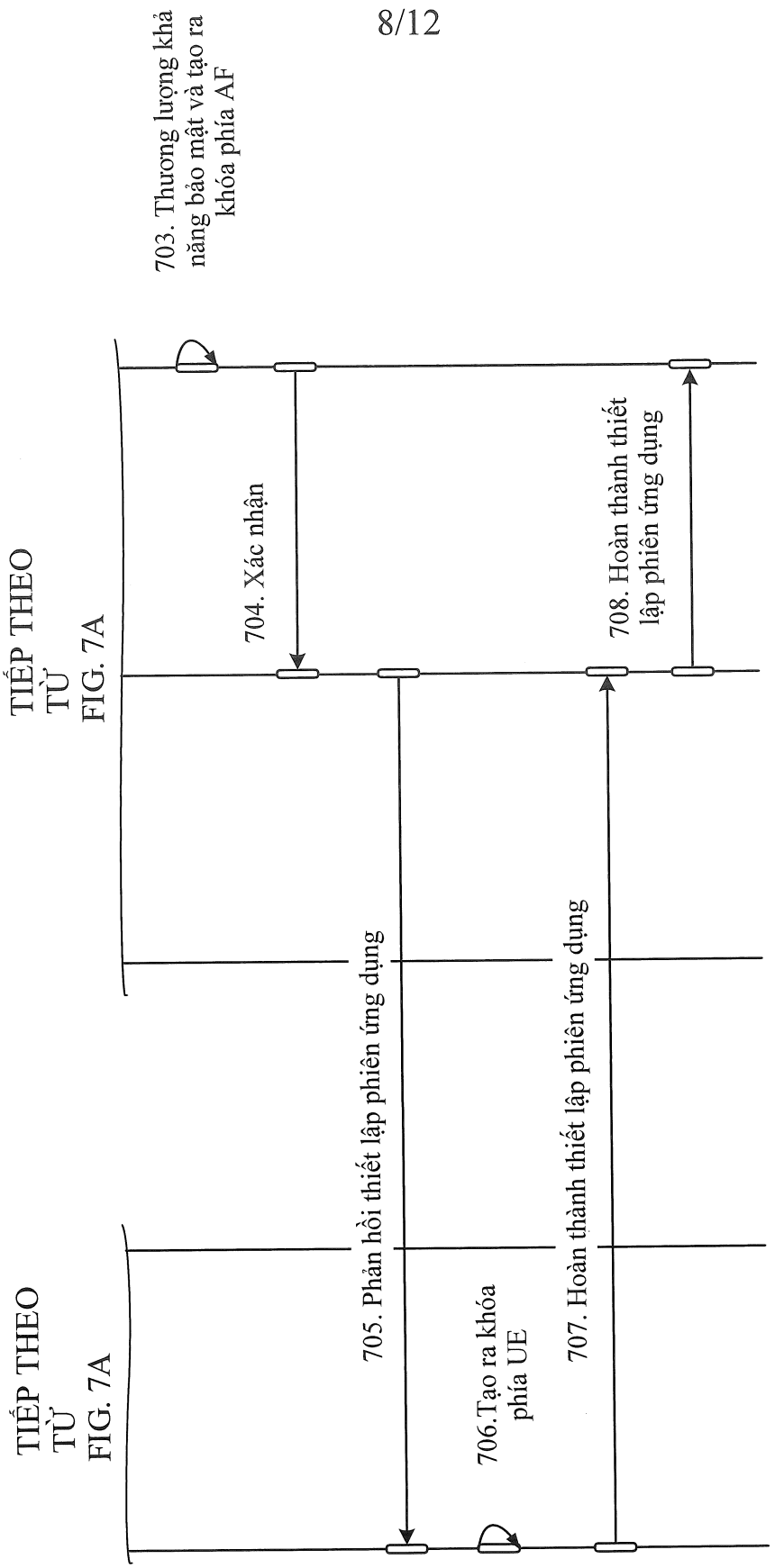
TIẾP THEO
TỪ
FIG. 7A
703. Thương lượng khả năng bảo mật và tạo ra khóa phía AF
704. Xác nhận
708. Hoàn thành thiết lập phiên ứng dụng
705. Phản hồi thiết lập phiên ứng dụng
706.Tạo ra khóa phía UE
707. Hoàn thành thiết lập phiên ứng dụng
TIẾP THEO
TỪ
FIG. 7A

FIG. 7B

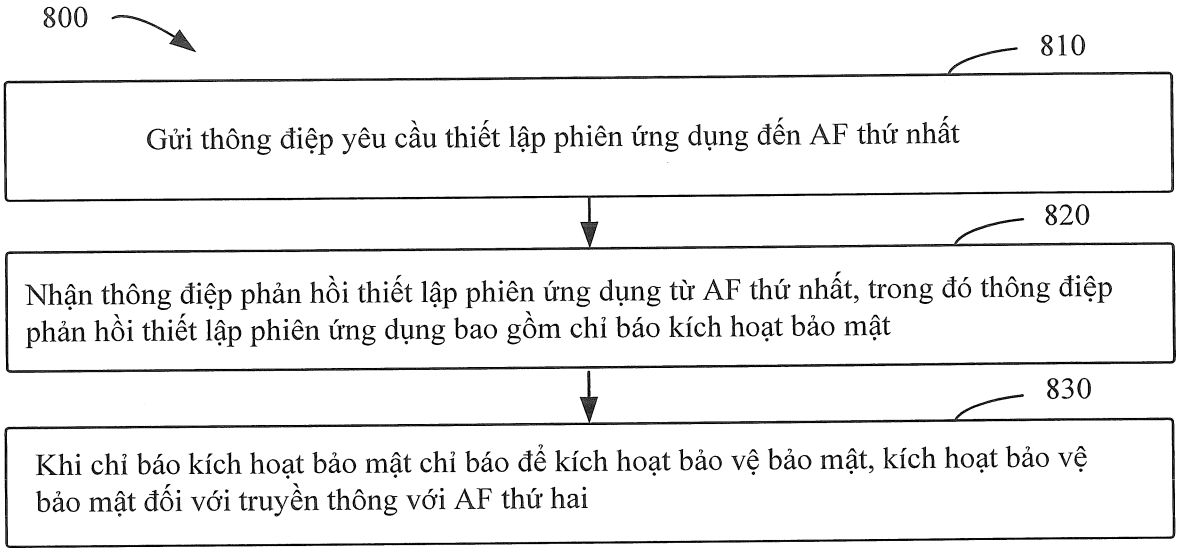
800
810
Gửi thông điệp yêu cầu thiết lập phiên ứng dụng đến AF thứ nhất
820
Nhận thông điệp phản hồi thiết lập phiên ứng dụng từ AF thứ nhất, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật
830
Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, kích hoạt bảo vệ bảo mật đối với truyền thông với AF thứ hai

FIG. 8

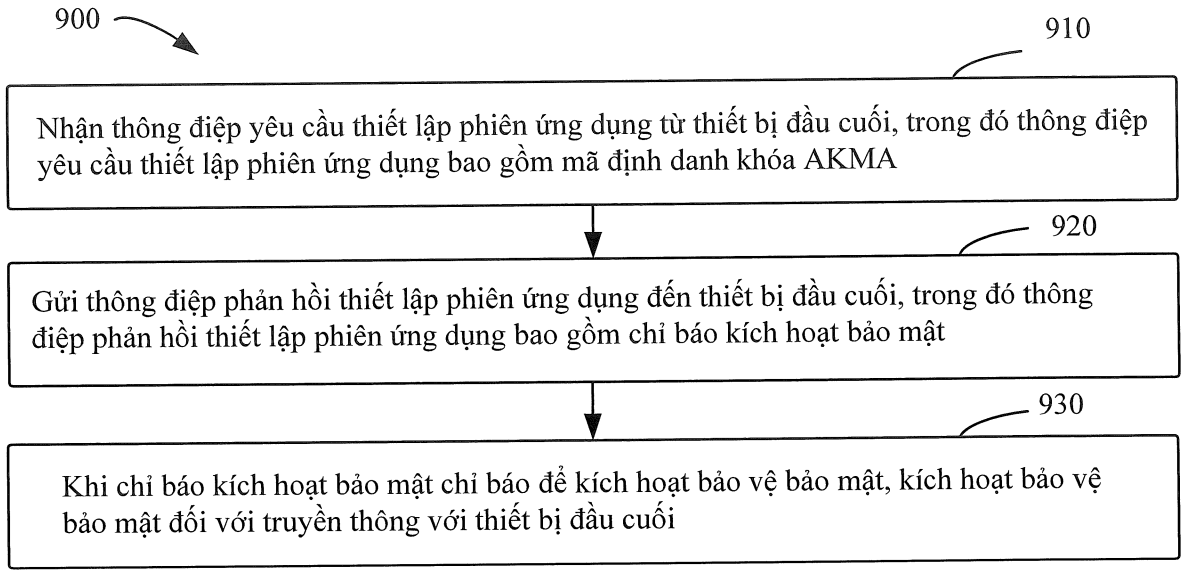
900
910
Nhận thông điệp yêu cầu thiết lập phiên ứng dụng từ thiết bị đầu cuối, trong đó thông điệp yêu cầu thiết lập phiên ứng dụng bao gồm mã định danh khóa AKMA
920
Gửi thông điệp phản hồi thiết lập phiên ứng dụng đến thiết bị đầu cuối, trong đó thông điệp phản hồi thiết lập phiên ứng dụng bao gồm chỉ báo kích hoạt bảo mật
930
Khi chỉ báo kích hoạt bảo mật chỉ báo để kích hoạt bảo vệ bảo mật, kích hoạt bảo vệ bảo mật đối với truyền thông với thiết bị đầu cuối

FIG. 9

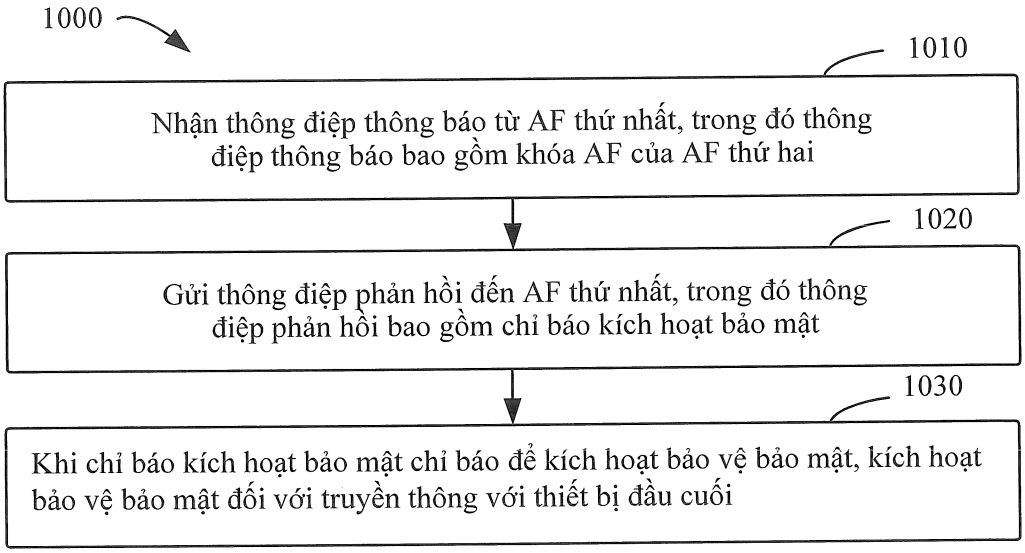

FIG. 10

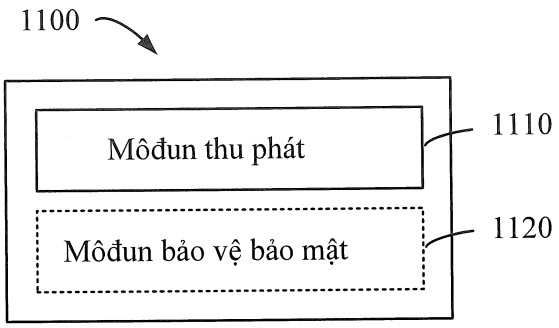

FIG. 11

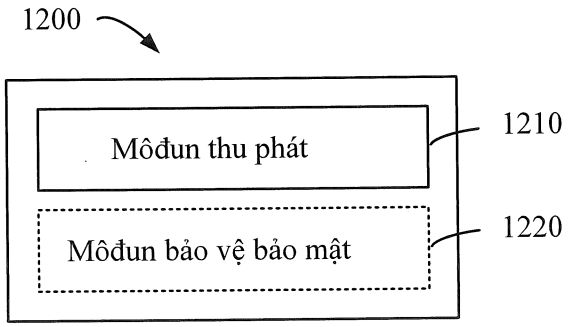

FIG. 12

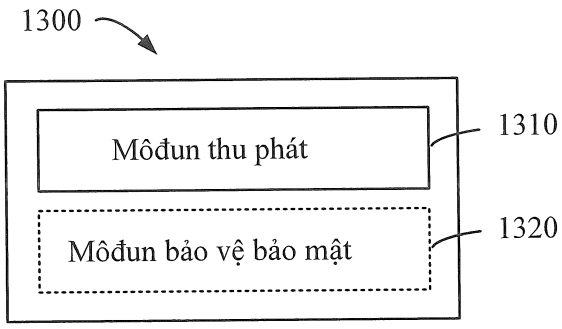
1300
Môđun thu phát
1310
Môđun bảo vệ bảo mật
1320

FIG. 13

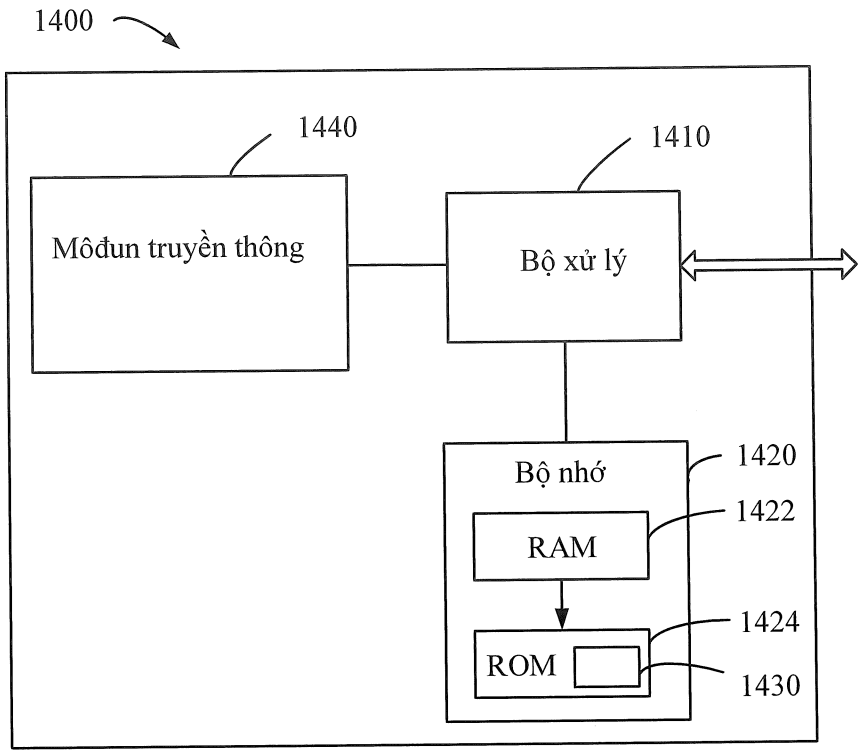
1400
1440
1410
Môđun truyền thông
Bộ xử lý
Bộ nhớ
1420
RAM
1422
ROM
1424
1430

FIG. 14

12/12

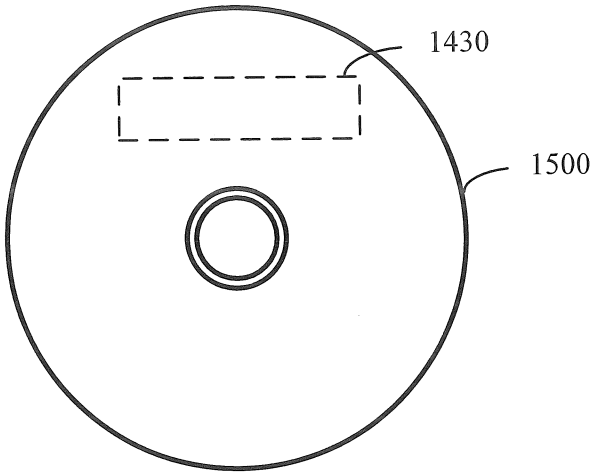

FIG. 15