(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) **1-0043929**

(51)[2020.01] **H04W 24/00**

(13) **B**

(21) 1-2020-05092
(22) 07/01/2019
(86) PCT/CN2019/070712 07/01/2019
(87) WO2019/153994 15/08/2019
(30) 201810119888.9 06/02/2018 CN
(45) 25/03/2025 444
(43) 25/12/2020 393A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) WU, Rong (CN); ZHANG, Bo (CN); TAN, Shuaishuai (CN).
(74) Công ty TNHH Tầm nhìn và Liên danh (VISION & ASSOCIATES CO.LTD.)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ THỎA THUẬN BẢO MẬT

(21) 1-2020-05092

(57) Sáng chế đề cập đến phương pháp và thiết bị thỏa thuận bảo mật. Phương pháp này bao gồm các bước: nhận, bởi thiết bị đầu cuối, thông tin thỏa thuận bảo mật được gửi bởi CU-CP/CU-UP, trong đó thông tin thỏa thuận bảo mật này bao gồm mã nhận dạng chỉ báo việc bảo vệ trạng thái nguyên vẹn của CU-UP; và xác định, bởi thiết bị đầu cuối dựa trên mã nhận dạng chỉ báo việc bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không. Theo cách này, thỏa thuận bảo mật mặt phẳng người dùng với thiết bị đầu cuối có thể được hoàn thành theo kịch bản trong đó CU-CP và CU-UP được tách rời khỏi nhau.

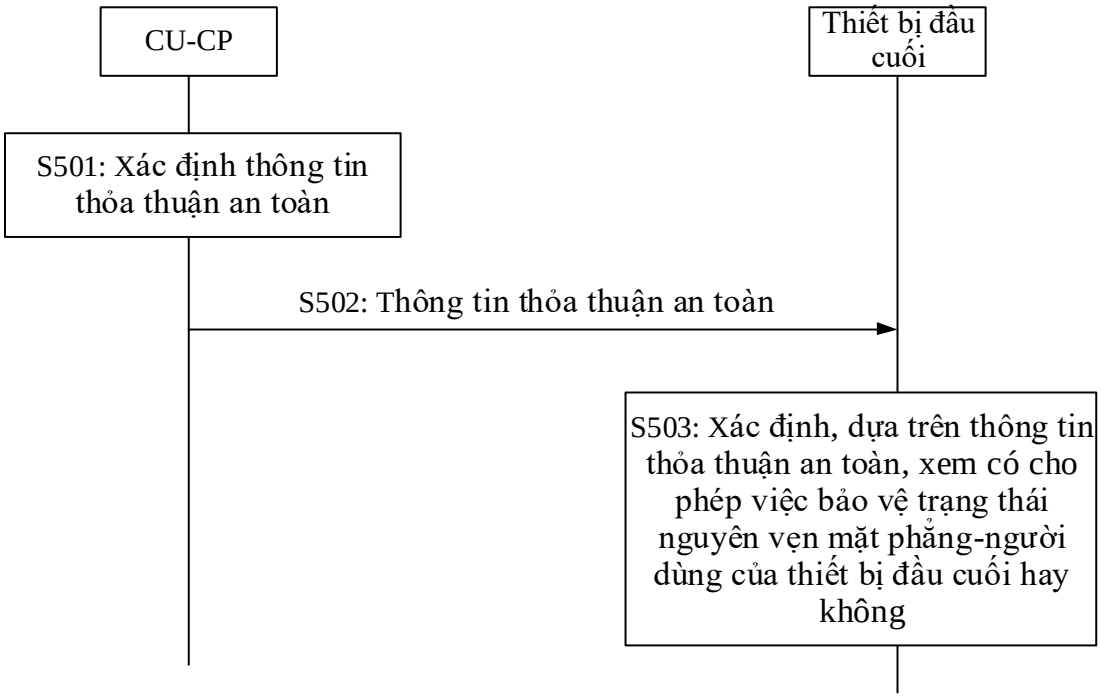

FIG.5

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực truyền thông không dây, và cụ thể là đến phương pháp và thiết bị thỏa thuận bảo mật.

Tình trạng kỹ thuật của sáng chế

Bộ phận xử lý cơ bản của mạng tương lai trên phía mạng truy cập được chia thành bộ phận tập trung (Centralized Unit, CU) và bộ phận phân tán (Distributed Unit, DU). Bộ phận tập trung có thể được chia thêm thành thực thể chức năng mặt phẳng-điều khiển và thực thể chức năng mặt phẳng người dùng, và một cách tương ứng, có thiết bị phần tử mạng chức năng mặt phẳng-điều khiển và thiết bị phần tử mạng chức năng mặt phẳng người dùng. Cụ thể, sự tách rời chức năng này chủ yếu là sự phân chia chức năng thêm của bộ phận tập trung của thiết bị mạng truy cập. Để bảo đảm bảo mật truyền thông theo kịch bản này, cần đề xuất cơ chế thỏa thuận bảo mật truy cập có hiệu quả.

Tuy nhiên, cơ chế thỏa thuận bảo mật hiện này chủ yếu là quy trình SMC máy chủ xác thực (Authentication Server, AS) trong công nghệ tiến hóa dài hạn (Long Term Evolution, LTE), cụ thể là quy trình tương tác giữa thiết bị đầu cuối và trạm cơ sở. Cơ chế thỏa thuận bảo mật theo giải pháp kỹ thuật đã biết không áp dụng được cho kịch bản trong đó thực thể chức năng mặt phẳng-điều khiển và thực thể chức năng mặt phẳng người dùng được tách rời khỏi nhau.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp và thiết bị thỏa thuận bảo mật để thực hiện việc thỏa thuận bảo mật trong kịch bản trong đó thực thể chức năng mặt phẳng-điều khiển và thực thể chức năng mặt phẳng người dùng được tách rời khỏi nhau.

Theo khía cạnh thứ nhất, sáng chế đề xuất phương pháp thỏa thuận bảo mật. Phương pháp này bao gồm các bước:

nhận, bởi thiết bị đầu cuối, thông tin thỏa thuận bảo mật được gửi bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, trong đó thông tin thỏa thuận bảo mật này bao

gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

nhận, bởi thiết bị đầu cuối, thông tin giao diện không gian được gửi bởi CU-CP, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, yêu cầu thiết lập phiên thứ nhất đến thực thể chức năng quản lý phiên SMF, trong đó yêu cầu thiết lập phiên thứ nhất bao gồm một hoặc nhiều tham số sau: một đoạn hoặc nhiều đoạn của S-NSSAI, DNN, ID phiên PDU, kiểu yêu cầu (Request Type), ID phiên PDU cũ, và côngtenơ N1 SM (PDU Session Establishment Request (yêu cầu thiết lập phiên PDU)).

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối, sau khi gửi yêu cầu thiết lập phiên thứ nhất đến SMF, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên của thiết bị đầu cuối.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép,

để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Một cách tuỳ chọn, sau khi xác định, bởi thiết bị đầu cuối, để cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, tham số bảo vệ trạng thái nguyên vẹn đến CU-CP.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là không được phép, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối.

Một cách tuỳ chọn, sau khi xác định, bởi thiết bị đầu cuối, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, phản hồi thỏa thuận bảo mật đến CU-CP, trong đó phản hồi thỏa thuận bảo mật này bao gồm tham số bảo vệ trạng thái nguyên vẹn và mã định danh chỉ báo được sử dụng để chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối là được phép.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và phương pháp còn bao gồm bước:

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và phương pháp còn bao gồm bước:

xác định, bởi thiết bị đầu cuối, sau khi yêu cầu thiết lập phiên thứ nhất được gửi đến SMF, dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa dựa vào phiên đối với thiết bị đầu cuối hay không.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Theo khía cạnh thứ hai, sáng chế đề xuất phương pháp thỏa thuận bảo mật. phương pháp này bao gồm các bước:

nhận, bởi thiết bị đầu cuối, thông tin thỏa thuận bảo mật được gửi bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã

định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

nhận, bởi thiết bị đầu cuối, thông tin giao diện không gian được gửi bởi CU-CP, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

Phương pháp này còn bao gồm bước:

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, yêu cầu thiết lập phiên thứ nhất đến thực thể chức năng quản lý phiên SMF, trong đó yêu cầu thiết lập phiên thứ nhất bao gồm một hoặc nhiều tham số sau: một đoạn hoặc nhiều đoạn của S-NSSAI, DNN, ID phiên PDU, kiểu yêu cầu (Request Type), ID phiên PDU cũ, và côngtenơ N1 SM (PDU Session Establishment Request (Yêu cầu thiết lập phiên PDU)).

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối, sau khi gửi yêu cầu thiết lập phiên thứ nhất đến SMF, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên của thiết bị đầu cuối.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép,

để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Một cách tuỳ chọn, sau khi xác định, bởi thiết bị đầu cuối, để cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, tham số bảo vệ trạng thái nguyên vẹn đến CU-CP.

Một cách tuỳ chọn, bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là không được phép, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối.

Một cách tuỳ chọn, sau khi xác định, bởi thiết bị đầu cuối, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, phản hồi thỏa thuận bảo mật đến CU-CP, trong đó phản hồi thỏa thuận bảo mật này bao gồm tham số bảo vệ trạng thái nguyên vẹn và mã định danh chỉ báo được sử dụng để chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối là được phép.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

Phương pháp này còn bao gồm bước:

xác định, bởi thiết bị đầu cuối, sau khi yêu cầu thiết lập phiên thứ nhất được gửi đến SMF, dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa dựa vào phiên đối với thiết bị đầu cuối hay không.

Theo khía cạnh thứ ba, sáng chế đề xuất phương pháp thỏa thuận bảo mật. Phương pháp này bao gồm các bước:

nhận, bởi thiết bị đầu cuối, thông tin thỏa thuận bảo mật được gửi bởi bộ phận tập trung mặt phẳng người dùng CU-UP, trong đó thông tin thỏa thuận bảo mật này bao

gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

nhận, bởi thiết bị đầu cuối, thông tin giao diện không gian được gửi bởi CU-UP, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và phương pháp còn bao gồm bước:

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa.

Theo khía cạnh thứ tư, sáng chế đề xuất phương pháp thỏa thuận bảo mật. phương pháp này bao gồm các bước:

nhận, bởi thiết bị đầu cuối, thông tin thỏa thuận bảo mật được gửi bởi bộ phận tập trung mặt phẳng người dùng CU-UP, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-

CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

nhận, bởi thiết bị đầu cuối, thông tin giao diện không gian được gửi bởi CU-UP, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và phương pháp còn bao gồm bước:

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa.

Theo khía cạnh thứ năm, sáng chế đề xuất phương pháp thỏa thuận bảo mật. Phương pháp này bao gồm các bước:

xác định, bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, thông tin thỏa thuận bảo mật, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

gửi, bởi CU-CP, thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP này dựa vào tham số tạo khóa.

Một cách tuỳ chọn, sau bước tạo ra, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa, phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP đến CU-UP này.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-CP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP đến CU-UP này.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-CP, khóa cơ sở; và

gửi, bởi CU-CP, khóa cơ sở này đến CU-UP.

Một cách tuỳ chọn, phương pháp này còn bao gồm các bước:

nhận, bởi CU-CP, yêu cầu thiết lập phiên thứ hai được gửi bởi thực thể chức năng quản lý phiên SMF sau khi SMF nhận yêu cầu thiết lập phiên thứ nhất được gửi bởi thiết bị đầu cuối; và

gửi, bởi CU-CP, phản hồi thiết lập phiên đến SMF.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định

danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

Theo khía cạnh thứ sáu, sáng chế đề xuất phương pháp thỏa thuận bảo mật. Phương pháp này bao gồm các bước:

xác định, bởi CU-CP, thông tin thỏa thuận bảo mật, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

gửi, bởi CU-CP, thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu

thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-CP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP đến CU-UP này.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP này dựa vào tham số tạo khóa.

Một cách tuỳ chọn, sau bước tạo ra, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa, phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP đến CU-UP này.

Một cách tuỳ chọn, phương pháp này còn bao gồm các bước:

tạo ra, bởi CU-CP, khóa cơ sở; và

gửi, bởi CU-CP, khóa cơ sở này đến CU-UP.

Một cách tuỳ chọn, phương pháp này còn bao gồm các bước:

nhận, bởi CU-CP, yêu cầu thiết lập phiên thứ hai được gửi bởi thực thể chức năng quản lý phiên SMF sau khi SMF nhận yêu cầu thiết lập phiên thứ nhất được gửi bởi thiết bị đầu cuối; và

gửi, bởi CU-CP, phản hồi thiết lập phiên đến SMF.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

Theo khía cạnh thứ bảy, sáng chế đề xuất phương pháp thỏa thuận bảo mật. Phương pháp này bao gồm các bước:

xác định, bởi bộ phận tập trung mặt phẳng người dùng CU-UP, thông tin thỏa thuận bảo mật, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

gửi, bởi CU-UP, thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi CU-UP, thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu,

mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-UP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-UP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Theo khía cạnh thứ tám, sáng chế đề xuất phương pháp thỏa thuận bảo mật. phương pháp này bao gồm các bước:

xác định, bởi bộ phận tập trung mặt phẳng người dùng CU-UP, thông tin thỏa thuận bảo mật, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

gửi, bởi CU-UP, thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp

điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

gửi, bởi CU-UP, thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-UP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Một cách tuỳ chọn, phương pháp này còn bao gồm bước:

tạo ra, bởi CU-UP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Theo khía cạnh thứ chín, sáng chế đề xuất thiết bị thỏa thuận bảo mật, trong đó

thiết bị này bao gồm các môđun hoặc phương tiện (means) được tạo cấu hình để tiến hành các phương pháp được đề xuất trong các khía cạnh từ thứ nhất đến thứ tám và các phương án thực hiện khác nhau của các khía cạnh từ thứ nhất đến thứ tám.

Theo khía cạnh thứ mười, sáng chế đề xuất thiết bị thỏa thuận bảo mật. Thiết bị này bao gồm bộ xử lý và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ chương trình. Bộ xử lý gọi chương trình được lưu trong bộ nhớ, tiến hành phương pháp được đề xuất theo khía cạnh bất kỳ trong số các khía cạnh từ thứ nhất đến thứ tư của sáng chế. Thiết bị này có thể là thiết bị đầu cuối, hoặc có thể là chip trên thiết bị đầu cuối.

Theo khía cạnh thứ mười một, sáng chế đề xuất thiết bị thỏa thuận bảo mật. Thiết bị này bao gồm bộ xử lý và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ chương trình. Bộ xử lý gọi chương trình được lưu trong bộ nhớ, tiến hành phương pháp được đề xuất theo khía cạnh thứ năm hoặc khía cạnh thứ sáu của sáng chế. Thiết bị này có thể là CU-CP, hoặc có thể là chip trên CU-CP.

Theo khía cạnh thứ mười hai, sáng chế đề xuất thiết bị thỏa thuận bảo mật. Thiết bị này bao gồm bộ xử lý và bộ nhớ. Bộ nhớ được tạo cấu hình để lưu trữ chương trình. Bộ xử lý gọi chương trình được lưu trong bộ nhớ, tiến hành phương pháp được đề xuất theo khía cạnh thứ bảy hoặc khía cạnh thứ tám của sáng chế. Thiết bị này có thể là CU-UP, hoặc có thể là chip trên CU-UP.

Theo khía cạnh thứ mười ba, sáng chế đề xuất vật ghi lưu trữ máy tính. Vật ghi lưu trữ máy tính này được tạo cấu hình để lưu trữ chương trình, và chương trình này được tạo cấu hình để tiến hành phương pháp bất kỳ theo khía cạnh từ thứ nhất đến thứ tám.

Trong phương pháp và thiết bị thỏa thuận bảo mật được đề xuất theo sáng chế, CU-CP hoặc CU-UP xác định thông tin thỏa thuận bảo mật, và gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối. Sau khi nhận thông tin thỏa thuận bảo mật, thiết bị đầu cuối có thể xác định, dựa vào chỉ báo của thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không. Theo cách này, thỏa thuận bảo mật mặt phẳng người dùng với thiết bị đầu cuối có thể

được hoàn thành theo kịch bản trong đó CU-CP và CU-UP được tách rời khỏi nhau.

Mô tả vắn tắt các hình vẽ

FIG.1 là sơ đồ sơ lược của hệ thống truyền thông;

FIG.2 là sơ đồ sơ lược khác của kịch bản hệ thống truyền thông;

FIG.3 là sơ đồ sơ lược khác nữa của kịch bản hệ thống truyền thông;

FIG.4 là sơ đồ sơ lược khác nữa của kịch bản hệ thống truyền thông;

FIG.5 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án của sáng chế;

FIG.6 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.7 là sơ đồ sơ lược của việc tạo khóa theo sáng chế;

FIG.8 là sơ đồ sơ lược khác của việc tạo khóa theo sáng chế;

FIG.9 là sơ đồ sơ lược khác nữa của việc tạo khóa theo sáng chế;

FIG.10 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.11 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án khác nữa của sáng chế;

FIG.12 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án của sáng chế;

FIG.13 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.14 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.15 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.16 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương

án khác nữa của sáng chế;

FIG.17 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác nữa của sáng chế;

FIG.18 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.19 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế;

FIG.20 là sơ đồ cấu trúc sơ lược của thiết bị đầu cuối theo một phương án của sáng chế;

FIG.21 là sơ đồ cấu trúc sơ lược của CU-CP theo một phương án của sáng chế; và

FIG.22 là sơ đồ cấu trúc sơ lược của CU-UP theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

FIG.1 là sơ đồ sơ lược của hệ thống truyền thông. Như được thể hiện trên FIG.1, hệ thống này bao gồm một DU, mặt phẳng điều khiển của bộ phận tập trung (CU-Control Plane, CU-CP), và mặt phẳng người dùng của bộ phận tập trung (CU-User Plane, CU-UP).

Như được thể hiện trên FIG.1, hệ thống này có thể là hệ thiết bị mạng, và bao gồm một CU-CP, các DU, và các CU-UP. CU-CP và DU có thể được nối thông qua giao diện F1-C, CU-UP và DU có thể được nối thông qua giao diện F1-U, và CU-UP và CU-CP có thể được nối thông qua giao diện E1.

DU bao gồm một số chức năng của lớp vật lý để xử lý băng tần và lớp điều khiển truy cập môi trường (Media Access Control, MAC) / lớp điều khiển liên kết vô tuyến (Radio Link Control, RLC). Khi xem xét tài nguyên truyền dẫn giữa khối từ xa vô tuyến (Radio Remote Unit, RRU) và DU, các chức năng lớp vật lý của một phần của các DU có thể dịch chuyển lên đến RRU. Với sự giảm thiểu của RRU, thậm chí triệt để hơn, DU có thể được kết hợp với RRU. Việc triển khai các DU phụ thuộc vào môi trường mạng

thực tế. Ví dụ, trong vùng thành thị trung tâm, vùng có mật độ giao thông tương đối cao, vùng có khoảng cách liên vị trí nhỏ, và vùng có tài nguyên phòng thiết bị giới hạn, như trường đại học và phòng xử án hiệu suất cao, Các DU có thể được triển khai theo kiểu tập trung hóa. Trong vùng có giao thông tương đối thưa thớt và vùng có có khoảng cách liên vị trí lớn, như vùng ngoại ô và đồi núi, các DU có thể được triển khai theo kiểu phân bố.

CU bao gồm chồng lớp giao thức cao của mạng truy cập vô tuyến và một số chức năng của mạng lõi, ví dụ một số chức năng của lớp điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC), lớp giao thức hội tụ dữ liệu gói (Packet Data Convergence Protocol, PDCP), và tương tự, và thậm chí có thể còn hỗ trợ việc dịch chuyển một số chức năng mạng lõi hướng xuống mạng truy cập. Các chức năng mạng lõi có thể được xem là mạng điện toán biên, có thể đáp ứng yêu cầu cao của mạng truyền thông trong tương lại đối với thời gian trễ mạng của dịch vụ mới, như viđeo, mua sắm trực tuyến hoặc thực tế ảo/thực tế tăng cường.

Sau khi phân chia thêm, CU-CP bao gồm một số chức năng của lớp giao thức RRC và lớp giao thức PDCP, và chủ yếu quản lý và lập lịch biểu cho các tài nguyên của DU và CU-UP, và quản lý và chuyển tiếp báo hiệu điều khiển.

CU-UP chủ yếu bao gồm một số chức năng của lớp giao thức PDCP, và chủ yếu truyền dữ liệu người dùng (UP Traffic), và khi đến phiên, truyền dữ liệu.

Trong mạng thế hệ thứ 5 (5G) trong tương lai, đặc biệt được hỗ trợ bởi công nghệ đám mây, việc tách mặt phẳng người dùng và mặt phẳng điều khiển có thể thực hiện đồng thời kết nối của các mạng có các chuẩn khác nhau. Báo hiệu mặt phẳng-điều khiển liên quan đến phiên dịch vụ được mang trên mạng thông thường có phủ sóng liên tục được thực hiện. Trên mặt phẳng dữ liệu, dữ liệu tốc độ cao được mang trên mạng 5G trong vùng có phủ sóng mạng 5G, và được mang trên mạng thông thường trong vùng không có phủ sóng mạng 5G. Theo cách này, mạng 5G có thể được triển khai đầy đủ theo yêu cầu, và không nhất thiết phải xem xét việc phủ sóng liên tục.

Trong khi triển khai cụ thể, một DU có thể được nối với một CU-UP, và một CU-

UP được nối với một CU-CP. Trong trường hợp đặc biệt, CU-UP có thể được nối với nhiều CU-CP. Các CU-UP có thể được nối với một DU. Các DU có thể được nối với một CU-UP. Việc này không bị giới hạn trong sáng chế. Phần sau đây mô tả một số kịch bản điển hình, và các kịch bản này áp dụng được cho phương pháp được đề xuất theo sáng chế.

FIG.2 là sơ đồ sơ lược khác của kịch bản hệ thống truyền thông.

Như được thể hiện trên FIG.2, CU-CP và CU-UP nằm ở vị trí triển khai tập trung hóa, ví dụ, được triển khai trong phòng thiết bị.

Theo cách này, công nghệ đám mây được ưu tiên sử dụng, và cả CU-CP lẫn CU-UP có thể được thực hiện nhờ ảo hóa. CU-CP được bố trí ở trung tâm, cung cấp sự cân bằng tải và phối trí tài nguyên tốt hơn cho DU.

FIG.3 là sơ đồ sơ lược khác nữa của kịch bản hệ thống truyền thông.

Như được thể hiện trên FIG.3, một CU-CP được triển khai ngoài trời, giống như DU, và một CU-CP quản lý một DU. Điều này được áp dụng cho kịch bản trong đó có một số lượng lớn các hoạt động báo hiệu. CU-CP quản lý một DU duy nhất. Ví dụ, việc này được áp dụng cho truyền thông tới hạn (critical) và kịch bản trong đó khóa cần được thay đổi một cách định kỳ. Tuy nhiên, CU-UP có thể được thực hiện nhờ sử dụng đám mây, nghĩa là, được thực hiện nhờ sử dụng máy chủ đám mây (cloud).

Thời gian trễ giữa CU-CP và CU-UP tăng. Điều này được áp dụng cho kịch bản trong đó có số lượng lớn các thiết lập lại liên kết, chuyển vùng và chuyển tiếp trạng thái, đặc biệt là kịch bản di động như internet của xe ôtô chẳng hạn.

FIG.4 là sơ đồ sơ lược khác nữa của kịch bản hệ thống truyền thông.

Như được thể hiện trên FIG.4, ví dụ, kịch bản này có thể là kịch bản truyền thông độ tin cậy cao (Ultra Reliable & Low Latency Communication, URLLC), trong đó truyền dẫn UP (giao thông) sau một tương tác trung tâm có thể được tiến hành, hoặc phương án thực hiện đám mây có thể được tiến hành trên phía UP, để thực hiện thời gian trễ thấp của dữ liệu truyền dẫn, ví dụ, truyền thông nhiệm vụ tới hạn (critical) (Mission

Critical Communication, MTC).

Sáng chế đề xuất phương pháp thỏa thuận bảo mật, áp dụng cho kịch bản trong đó CU-CP và CU-UP được tách rời khỏi nhau, ví dụ kịch bản nêu trên. Tuy nhiên, không giới hạn ở kịch bản nêu trên.

Trong phương án này của sáng chế, thiết bị đầu cuối (terminal device) bao gồm, nhưng không bị giới hạn, trạm di động (MS, Mobile Station), thiết bị đầu cuối di động (Mobile Terminal), máy điện thoại di động (Mobile Telephone), bộ thu phát cầm tay (handset), thiết bị xách tay (portable equipment) và thiết bị tương tự. Thiết bị đầu cuối có thể truyền thông với một hoặc nhiều mạng lõi thông qua mạng truy cập vô tuyến (RAN, Radio Access Network). Ví dụ, thiết bị đầu cuối có thể là máy điện thoại di động (hoặc được gọi là điện thoại "tế bào"), hoặc máy tính có chức năng truyền thông không dây; thiết bị đầu cuối có thể là thiết bị xách tay, bỏ túi được, cầm tay, gắn trong máy tính, thiết bị hoặc máy di động lắp trên xe.

Thiết bị mạng có thể là thiết bị được tạo cấu hình để truyền thông với thiết bị đầu cuối. Ví dụ, mạng thiết bị có thể là trạm thu-phát cơ sở (Base Transceiver Station, BTS) trong hệ thống GSM hoặc hệ thống CDMA, hoặc có thể là Nút B (NodeB, NB) trong hệ thống WCDMA, hoặc có thể là Nút B tiến hóa (Evolved Node B, eNB hoặc eNode B) trong hệ thống LTE hoặc gNB trong mạng 5G tương lai.

FIG.5 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án của sáng chế. Như được thể hiện trên FIG.5, phương pháp này bao gồm các bước sau.

S501: CU-CP xác định thông tin thỏa thuận bảo mật.

S502: CU-CP gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn (UP integrity indication) của CU-UP.

Mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP được sử dụng để biểu thị việc bảo vệ trạng thái nguyên vẹn của CU-UP có được phép hay không.

Thông tin thỏa thuận bảo mật này có thể được mang trong lệnh chế độ bảo mật

AS (AS Security Mode Command), hoặc được mang trong lệnh chế độ bảo mật CP (Security Mode Command), hoặc được mang trong lệnh như tin nhắn tạo cấu hình lại giao diện không gian (RRC Reconfiguration Request). Việc này không bị giới hạn trong sáng chế.

Theo một phương án thực hiện tùy chọn, trước bước S501, CU-CP thu được các khóa của tất cả các CU-UP. CU-CP có thể tạo ra các khóa của tất cả các CU-UP, hoặc các CU-UP có thể gửi các khóa của các CU-UP đến CU-CP. Việc này không bị giới hạn ở đây.

Mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP có thể là giá trị 1-bit hoặc 1-byte hoặc ký hiệu bằng văn bản. Ví dụ, "0" chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn là không được phép, "1" chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn là được phép. Theo cách khác, ký hiệu bằng văn bản có thể biểu thị việc bảo vệ trạng thái nguyên vẹn có được phép hay không. Ví dụ, "ĐÚNG" chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn là được phép, và "SAI" chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn là không được phép.

Một cách tuỳ chọn, có thể xác định trước, ví dụ, được xác định theo tiêu chuẩn, hoặc được tạo cấu hình trước, rằng việc bảo vệ mã hóa của CU-UP là được phép theo mặc định.

S503: Thiết bị đầu cuối xác định, dựa vào thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

Sau khi nhận thông tin thỏa thuận bảo mật, thiết bị đầu cuối có thể xác định, dựa vào chỉ báo của thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không. Cụ thể, việc xác định xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không này có thể được xác định theo quy luật đặt trước.

Trong phương án này, CU-CP xác định thông tin thỏa thuận bảo mật, và gửi thông tin thỏa thuận bảo mật này đến thiết bị đầu cuối. Sau khi nhận thông tin thỏa thuận bảo

mật, thiết bị đầu cuối có thể xác định, dựa vào chỉ báo của thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không. Theo cách này, thỏa thuận bảo mật mặt phẳng người dùng với thiết bị đầu cuối có thể được hoàn thành theo kịch bản trong đó CU-CP và CU-UP được tách rời khỏi nhau.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật có thể còn bao gồm mã định danh bảo vệ mã hóa (Chỉ báo bí mật UP) của CU-UP. Mã định danh bảo vệ mã hóa của CU-UP được sử dụng để biểu thị việc bảo vệ mã hóa của CU-UP có được phép hay không.

Tương tự, mã định danh bảo vệ mã hóa của CU-UP có thể là giá trị 1-bit hoặc 1-byte hoặc ký hiệu bằng văn bản. Ví dụ, "0" chỉ báo rằng bảo vệ mã hóa là không được phép, "1" chỉ báo rằng bảo vệ mã hóa là được phép. Theo cách khác, ký hiệu bằng văn bản có thể biểu thị việc bảo vệ mã hóa có được phép hay không. Ví dụ, "ĐÚNG" chỉ báo rằng bảo vệ mã hóa là được phép, và "SAI" chỉ báo rằng bảo vệ mã hóa là không được phép.

Nếu mã định danh bảo vệ mã hóa của CU-UP chỉ báo rằng việc bảo vệ mã hóa của CU-UP là được phép, thiết bị đầu cuối xác định cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối. Theo cách khác, thiết bị đầu cuối không cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối.

FIG.6 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án khác của sáng chế. Như được thể hiện trên FIG.6, phương pháp này bao gồm các bước sau.

S601: CU-CP xác định thông tin thỏa thuận bảo mật.

S602: CU-CP gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh bảo vệ mã hóa của CU-UP.

Mã định danh bảo vệ mã hóa của CU-UP được sử dụng để biểu thị việc bảo vệ mã hóa của CU-UP có được phép hay không.

S603: Thiết bị đầu cuối xác định, dựa vào thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, khi thông tin thỏa thuận bảo mật bao gồm "mã định danh chỉ báo bảo vệ mã hóa của CU-UP", nó có thể được xác định trước, ví dụ, được xác định theo tiêu chuẩn, hoặc được tạo cấu hình trước, rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép theo mặc định.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Theo một phương án thực hiện, thông tin thỏa thuận bảo mật này còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

Cụ thể, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP có thể là mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển của CU-CP, và mã định danh thuật toán bảo vệ mã hóa của CU-CP có thể là mã định danh thuật toán bảo vệ mã hóa mặt phẳng-điều khiển của CU-CP. Cụ thể, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP có thể là mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, và mã định danh thuật toán bảo vệ mã hóa của CU-UP có thể là mã định danh thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP.

Một cách tuỳ chọn, theo một kịch bản, CU-CP và CU-UP có cùng thuật toán bảo vệ trạng thái nguyên vẹn, và trong trường hợp này, thông tin thỏa thuận bảo mật có thể biểu thị mã định danh thuật toán bảo vệ trạng thái nguyên vẹn; và/hoặc, CU-CP và CU-UP có cùng thuật toán bảo vệ mã hóa, và trong trường hợp này, thông tin thỏa thuận bảo mật có thể biểu thị mã định danh thuật toán bảo vệ mã hóa.

Cần lưu ý rằng CU-CP và CU-UP có thể thỏa thuận thuật toán bảo vệ trạng thái nguyên vẹn và/hoặc thuật toán bảo vệ mã hóa từ trước .

Ví dụ, CU-CP gửi thông tin thỏa thuận thuật toán đến CU-UP, và CU-UP này xác định thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP và/hoặc thuật toán bảo vệ mã hóa của CU-UP, và gửi phản hồi thỏa thuận thuật toán đến CU-CP. Phản hồi thỏa thuận thuật toán này biểu thị thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP và/hoặc thuật toán bảo vệ mã hóa của CU-UP. Ngoài ra, CU-CP còn xác định các thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP và CU-UP và/hoặc các thuật toán bảo vệ mã hóa của CU-CP và CU-UP dựa vào phản hồi thỏa thuận thuật toán.

Cần lưu ý rằng thuật toán bảo vệ trạng thái nguyên vẹn bao gồm thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển và thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng, và thuật toán mã hóa bao gồm thuật toán mã hóa mặt phẳng-điều khiển và thuật toán mã hóa mặt phẳng người dùng.

Thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển là thuật toán được sử dụng để tiến hành việc bảo vệ trạng thái nguyên vẹn trên tín hiệu truyền, và mặt phẳng-điều khiển thuật toán bảo vệ thuật toán mã hóa được sử dụng để tiến hành việc bảo vệ mã hóa trên tín hiệu truyền.

Thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng là thuật toán được sử dụng để tiến hành việc bảo vệ trạng thái nguyên vẹn trên dữ liệu người dùng, và thuật toán bảo vệ mã hóa mặt phẳng người dùng là thuật toán được sử dụng để tiến hành việc bảo vệ mã hóa trên dữ liệu.

Các thuật toán được xử lý bởi CU-CP chủ yếu bao gồm thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển và thuật toán mã hóa mặt phẳng-điều khiển, và ngoài ra còn bao gồm thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng và thuật toán mã hóa mặt phẳng người dùng. CU-UP chủ yếu xử lý thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng và thuật toán mã hóa mặt phẳng người dùng. Không loại trừ việc sau đó DU còn cần xử lý thuật toán bảo vệ trạng thái nguyên vẹn và thuật toán mã hóa trên mặt phẳng điều khiển và/hoặc mặt phẳng điều khiển và mặt phẳng người dùng.

Sau khi nhận thông tin thỏa thuận bảo mật, trước tiên thiết bị đầu cuối có thể xác

minh trạng thái nguyên vẹn của thông tin thỏa thuận bảo mật, và sau đó trước tiên cho phép giải mã đường xuống của tin nhắn điều khiển tài nguyên vô tuyến (Radio Resource Control, RRC) mặt phẳng-điều khiển và việc bảo vệ trạng thái nguyên vẹn của tin nhắn RRC, và sau đó xác định xem việc bảo vệ trạng thái nguyên vẹn của CU-UP và bảo vệ mã hóa của CU-UP có được phép hay không.

Một cách tuỳ chọn, thiết bị đầu cuối này xác định, dựa vào thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không và/hoặc việc bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối có thể bao gồm ít nhất một trường hợp trong số các trường hợp sau:

(1) Nếu thông tin thỏa thuận bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, và mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, thiết bị đầu cuối xác định cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Nếu mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là không được phép, thiết bị đầu cuối không cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

(2) Thông tin thỏa thuận bảo mật bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và mã định danh chỉ báo bảo vệ mã hóa của CU-UP chỉ báo rằng việc bảo vệ mã hóa của CU-UP là được phép. Trong trường hợp này, thiết bị đầu cuối xác định cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối.

Nếu mã định danh chỉ báo bảo vệ mã hóa của CU-UP chỉ báo rằng việc bảo vệ mã hóa của CU-UP là không được phép, thiết bị đầu cuối không cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối.

Ngoài ra, thiết bị đầu cuối gửi phản hồi thỏa thuận bảo mật đến CU-CP.

Nếu thiết bị đầu cuối xác định cho phép bảo vệ trạng thái nguyên vẹn của thiết bị

đầu cuối, phản hồi thỏa thuận bảo mật này bao gồm tham số bảo vệ trạng thái nguyên vẹn.

Nếu thiết bị đầu cuối xác định không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phản hồi thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn, tham số bảo vệ trạng thái nguyên vẹn và dấu hiệu tương tự của thiết bị đầu cuối. Mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối được sử dụng để biểu thị việc thiết bị đầu cuối có cho phép bảo vệ trạng thái nguyên vẹn hay không.

Tham số bảo vệ trạng thái nguyên vẹn có thể là mã bảo vệ trạng thái nguyên vẹn tin nhắn (Message Authentication Code for Integrity, MAC-I).

Cần lưu ý rằng nếu thiết bị đầu cuối xác định cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối, thiết bị đầu cuối có thể cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối sau khi nhận thông tin thỏa thuận bảo mật; và/hoặc

nếu thiết bị đầu cuối xác định cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối, thiết bị đầu cuối có thể cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối sau khi nhận thông tin thỏa thuận bảo mật.

Theo cách khác, nếu thiết bị đầu cuối xác định cho phép bảo vệ mã hóa, thiết bị đầu cuối này có thể cho phép bảo vệ mã hóa đối với thiết bị đầu cuối khi gửi phản hồi thỏa thuận bảo mật này; và/hoặc

nếu thiết bị đầu cuối xác định cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, thiết bị đầu cuối có thể cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối khi gửi phản hồi thỏa thuận bảo mật này.

Một cách tuỳ chọn, trước khi xác định thông tin thỏa thuận bảo mật bởi CU-CP, phương pháp có thể còn bao gồm bước: xác định, bởi CU-CP, xem mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP có được kích hoạt hay không.

Nếu mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP được kích hoạt, việc bảo vệ giải mã đường xuống của CU-UP được xác định là được phép. Ngoài ra, CU-CP và/hoặc CU-UP còn ghi lại giá trị hiện tại của mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Ngoài ra, CU-CP còn thiết lập giá trị mã định danh của CU-CP, và giá trị mã định danh này được biểu thị dưới dạng "mã định danh CU-CP (chỉ báo CP)". Sau khi CU-CP xác định rằng cả thiết bị đầu cuối và CU-UP đều cho phép bảo vệ mã hóa, giá trị của mã định danh CU-CP được thiết lập thành "được kích hoạt". Ví dụ, mã định danh CU-CP "1" biểu thị "được kích hoạt", và mã định danh CU-CP "0" biểu thị "không được kích hoạt". Theo cách khác, giá trị của mã định danh CU-CP có thể là ký hiệu bằng văn bản. Ví dụ, "ĐÚNG" biểu thị "được phép", và "SAI" biểu thị "không được phép". Theo cách khác, mã định danh CU-CP có thể bao gồm mã định danh bảo vệ mã hóa của CU-CP và mã định danh bảo vệ trạng thái nguyên vẹn của CU-CP. CU-CP có thể thông báo cho thiết bị đầu cuối ngay sau khi kích hoạt, hoặc CU-CP có thể thông báo cho thiết bị đầu cuối về một số thông tin có liên quan (ví dụ, thông tin mẫu CU-UP được tạo cấu hình, ID đường hầm của CU-UP và thông tin bảo vệ có liên quan), và thiết bị đầu cuối xác định xem mã định danh bảo vệ trạng thái nguyên vẹn của CU-CP có được kích hoạt hay không. Việc này không bị giới hạn trong sáng chế.

Một cách tuỳ chọn, theo cách khác, CU-CP gửi mã định danh CU-CP đến thiết bị đầu cuối, và thiết bị đầu cuối xác định, dựa vào mã định danh CU-CP, xem có cho phép bảo vệ mã hóa mặt phẳng-điều khiển của thiết bị đầu cuối hay không. Ví dụ, khi mã định danh CU-CP biểu thị "được kích hoạt", thiết bị đầu cuối cho phép bảo vệ mã hóa mặt phẳng-điều khiển của thiết bị đầu cuối. Nếu mã định danh CU-CP chỉ báo rằng "không được kích hoạt", thiết bị đầu cuối không cho phép bảo vệ mã hóa mặt phẳng-điều khiển của thiết bị đầu cuối.

Dựa vào phương án nêu trên, cả CU-CP lẫn thiết bị đầu cuối đều cần tạo ra khóa. Cụ thể, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP và khóa tương tự được tạo ra.

CU-CP và thiết bị đầu cuối có thể tạo ra khóa bảo vệ trạng thái nguyên vẹn, khóa mã hóa và khóa tương tự dựa vào khóa bảo mật (được biểu thị dưới dạng K-AN) của mạng truy cập (Access Network, AN). Mạng truy cập này có thể là một thiết bị trong số các thiết bị mạng nêu trên. Các chi tiết không được mô tả lại ở đây. Khóa bảo mật có thể là khóa bảo mật được chia sẻ bởi thiết bị mạng, thiết bị đầu cuối và thiết bị tương tự.

Cần lưu ý rằng thuật toán tạo khóa có thể là hàm tạo khóa (Key Derivation Function, KDF) hoặc thuật toán HMAC-SHA256, nhưng không bị giới hạn ở đó. Khóa có thể được tạo ra nhờ việc nhập, vào thuật toán tạo khóa, tham số cần được sử dụng.

FIG.7 là sơ đồ sơ lược của việc tạo khóa theo sáng chế.

Trong phương án thực hiện này, như được thể hiện trên FIG.7, CU-CP tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, và K-AN; và/hoặc

CU-CP này tạo ra khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào mã định danh kiểu thuật toán bảo vệ mã hóa của CU-UP, mã định danh thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP này, và K-AN.

Tương tự, CU-CP tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-CP dựa vào mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển của CU-CP này, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển của CU-CP này, và K-AN. CU-CP tạo ra khóa bảo vệ mã hóa của CU-CP dựa vào mã định danh kiểu thuật toán bảo vệ mã hóa mặt phẳng-điều khiển của CU-CP này, mã định danh thuật toán bảo vệ mã hóa mặt phẳng-điều khiển của CU-CP này, và K-AN.

Mã định danh kiểu thuật toán biểu thị kiểu của thuật toán. Ví dụ, thuật toán bảo vệ mã hóa mặt phẳng người dùng là "UP-enc-alg", và giá trị kiểu của thuật toán là 0x05. đầu vào mã định danh của thuật toán bảo vệ mã hóa mặt phẳng người dùng có thể là mã định danh văn bản "UP-enc-alg", hoặc giá trị tương ứng 0x05, hoặc ký hiệu bằng văn bản của giá trị.

Thiết bị đầu cuối tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, và K-AN; và/hoặc

thiết bị đầu cuối tạo ra khóa mã hóa mặt phẳng người dùng dựa vào mã định danh kiểu thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và K-AN.

Một cách tuỳ chọn, thiết bị đầu cuối tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển của CU-CP dựa vào mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng-điều khiển của CU-CP, và K-AN, và tạo ra khóa bảo vệ mã hóa mặt phẳng-điều khiển của CU-CP dựa vào mã định danh kiểu thuật toán bảo vệ mã hóa mặt phẳng-điều khiển của CU-CP, mã định danh thuật toán bảo vệ mã hóa mặt phẳng-điều khiển của CU-CP, và K-AN.

Ngoài ra, thiết bị đầu cuối và CU-CP có thể còn có thông tin liên quan đên thỏa thuận thỏa thuận để tạo ra khóa.

Theo một phương án thực hiện, tham số tạo khóa được mang trong thông tin thỏa thuận bảo mật này.

Theo một phương án thực hiện khác, CU-CP gửi tham số tạo khóa đến thiết bị đầu cuối.

Tham số tạo khóa có thể là: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-

CP, hoặc tham số tương tự.

Mã định danh CU-UP có thể là mã định danh đường hầm, ví dụ TEID. Mã định danh mẫu có thể mã định danh mẫu CU-CP, mã định danh mẫu CU-UP, hoặc mã định danh mẫu DU.

Tham số làm mới có thể là số ngẫu nhiên Nonce hoặc số ngẫu nhiên hoặc tương tự. Mã định danh bearer có thể là DRB ID hoặc bearer ID.

Ví dụ, thuật toán bảo vệ trạng thái nguyên vẹn có thể là thuật toán không "NIA 0", và giá trị tương ứng là "0000" theo nhị phân. Thuật toán bảo vệ trạng thái nguyên vẹn có thể là thuật toán dựa vào 128-bit SNOW 3G "128-NIA 1", và giá trị tương ứng là "0001" theo nhị phân. Thuật toán bảo vệ trạng thái nguyên vẹn có thể là thuật toán dựa vào 128-bit AES "128-NIA 2", và giá trị tương ứng là "0010" theo nhị phân. Đầu vào mã định danh của thuật toán bảo vệ trạng thái nguyên vẹn có thể là mã định danh văn bản tên thuật toán, hoặc giá trị tương ứng, hoặc ký hiệu bằng văn bản của giá trị.

Theo cách khác, thuật toán bảo vệ mã hóa có thể là thuật toán mã hóa không "NEA 0", và giá trị tương ứng là "0000" theo nhị phân. Thuật toán bảo vệ mã hóa có thể là thuật toán dựa vào 128-bit SNOW 3G "128-NEA 1", và giá trị tương ứng là "0001" theo nhị phân. Thuật toán bảo vệ mã hóa có thể là thuật toán dựa vào 128-bit AES "128-NEA 2", và giá trị tương ứng là "0010" theo nhị phân. Thuật toán bảo vệ mã hóa có thể là thuật toán dựa vào 128-bit ZUC "128-NEA 3", và giá trị tương ứng là "0011" theo nhị phân. Đầu vào mã định danh của thuật toán bảo vệ mã hóa có thể là mã định danh văn bản tên thuật toán, hoặc giá trị tương ứng, hoặc ký hiệu bằng văn bản của giá trị.

FIG.8 là sơ đồ sơ lược khác của việc tạo khóa theo sáng chế.

Sau khi xác định thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP và/hoặc thuật toán bảo vệ mã hóa của CU-UP này, thiết bị đầu cuối có thể còn tạo ra khóa dựa vào tham số tạo khóa nêu trên.

Cụ thể, thiết bị đầu cuối tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa, mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt

phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, và K-AN; và/hoặc

thiết bị đầu cuối tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa, mã định danh kiểu thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và K-AN.

Tương tự, CU-CP có thể còn tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa, mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, và K-AN; và/hoặc

CU-CP tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa, mã định danh kiểu thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và K-AN.

FIG.9 là sơ đồ sơ lược khác nữa của việc tạo khóa theo sáng chế.

Trong quy trình tạo khóa, các mã định danh của các CU-UP khác nhau có thể được xem xét thêm. Theo cách này, mỗi CU-UP tương ứng với một khóa khác nhau.

Một cách tương ứng, có thể hiểu rằng CU-UP tương ứng với các khóa mặt phẳng người dùng khác nhau. Ví dụ, nếu CU-UP tương ứng với thủ tục thiết lập phiên, khóa bảo vệ mã hóa mặt phẳng người dùng và khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng có thể dựa vào độ hạt phiên, và hai phiên có các khóa bảo vệ mặt phẳng người dùng khác nhau. Nói cách khác, khóa mã hóa của một phiên khác với khóa mã hóa của phiên khác, và các khóa bảo vệ trạng thái nguyên vẹn của các phiên cũng khác nhau. Nếu CU-UP tương ứng với thủ tục thiết lập bearer, như bear hoặc DRB, khóa bảo vệ mã hóa mặt phẳng người dùng và khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng có thể dựa vào độ hạt bearer, và hai bearer có các khóa bảo vệ mặt phẳng người dùng khác nhau. Nói cách khác, khóa mã hóa của một bearer khác với khóa mã hóa của một bearer khác, và các khóa bảo vệ trạng thái nguyên vẹn của các bearer cũng khác nhau.

Như được thể hiện trên FIG.9, thiết bị đầu cuối tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa, mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, mã định danh của CU-UP, và K-AN; và/hoặc

thiết bị đầu cuối tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa, mã định danh kiểu thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, mã định danh thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, mã định danh của CU-UP, và K-AN.

Theo FIG.9, trước tiên thiết bị đầu cuối có thể tạo ra khóa ban đầu dựa vào tham số tạo khóa và K-AN, và sau đó thay thế mã định danh của CU-UP, mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn, (một cách tuỳ chọn, còn bao gồm tham số tạo khóa) và mã tương tự, để tạo ra khóa bảo vệ trạng thái nguyên vẹn. Tương tự, trước tiên thiết bị đầu cuối có thể tạo ra khóa ban đầu dựa vào tham số tạo khóa và K-AN, và sau đó thay thế mã định danh của CU-UP, mã định danh kiểu thuật toán bảo vệ mã hóa, mã định danh thuật toán bảo vệ mã hóa, (một cách tuỳ chọn, còn bao gồm tham số tạo khóa) và mã tương tự, để tạo ra khóa bảo vệ mã hóa.

Trong phương án này, sau khi nhận mã định danh của CU-UP, CU-CP còn gửi mã định danh của CU-UP đến thiết bị đầu cuối.

Mã định danh của CU-UP có thể là mã định danh liên quan đến sự phân biệt thực thể của CU-UP, như ID đường hầm (Tunnel) chẳng hạn.

Một cách tuỳ chọn, khóa có thể được tạo ra bởi CU-UP. Cụ thể, CU-CP tạo ra khóa cơ sở và gửi khóa cơ sở này đến CU-UP, và CU-UP tạo ra khóa bảo vệ trạng thái nguyên vẹn dựa vào mã định danh của CU-UP, khóa cơ sở và khóa này. Theo cách khác, CU-UP tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào mã định danh của CU-UP, khóa cơ sở, và tham số tạo khóa. Một cách tuỳ chọn, khi gửi khóa cơ sở, CU-CP còn gửi thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP và tham số tạo khóa đến

CU-UP.

Khóa cơ sở này có thể là K-AN, khóa bảo mật được chia sẻ với thiết bị đầu cuối, khóa bảo mật được tạo ra bởi CU-CP dựa vào K-AN này, hoặc dấu hiệu tương tự.

Tương tự, CU-UP tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào mã định danh của CU-UP, khóa cơ sở, mã định danh kiểu thuật toán bảo vệ mã hóa của CU-UP này, và thuật toán mã hóa mã định danh của CU-UP này. Theo cách khác, CU-UP tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào mã định danh của CU-UP này, khóa cơ sở, mã định danh kiểu thuật toán bảo vệ mã hóa của CU-UP này, và tham số tạo khóa.

Cần lưu ý rằng CU-UP và DU có thể được triển khai cùng nhau theo một cách phân bố. Do đó, DU có thể cũng có khả năng tạo khóa. Trong trường hợp này, cần xem xét rằng mã định danh của DU được bổ sung vào.

Dựa vào các phương án nêu trên, còn có thủ tục thiết lập phiên hoặc thủ tục thiết lập bearer.

FIG.10 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án khác của sáng chế. Như được thể hiện trên FIG.10, phương pháp này bao gồm các bước sau.

S111: Thiết bị đầu cuối gửi yêu cầu thiết lập phiên thứ nhất đến thực thể chức năng quản lý phiên (Session Management Function, SMF).

Nói cách khác, thiết bị đầu cuối khởi tạo việc thiết lập phiên. Tất nhiên, sáng chế không bị giới hạn ở đó. Theo cách khác, thiết bị ở phía mạng, như SMF chẳng hạn, có thể khởi tạo yêu cầu thiết lập phiên. Nói cách khác, SMF gửi yêu cầu thiết lập phiên thứ nhất đến thiết bị đầu cuối. Việc này không bị giới hạn ở đây.

Yêu cầu thiết lập phiên thứ nhất bao gồm một hoặc nhiều tham số sau: thông tin trợ giúp lựa chọn lát mạng phục vụ (Serving-Network Slice Selection Assistance Information, S-NSSAI), tên mạng dữ liệu (Data Network Name, DNN), khối dữ liệu giao thức (Protocol Data Unit, PDU) ID phiên (Session), kiểu yêu cầu (Request Type), ID phiên PDU cũ, và côngtenơ quản lý phiên N1 (Session Management, SM) (yêu cầu

thiết lập phiên (Session Establishment Request) PDU). N1 là tên của giao diện giữa thiết bị đầu cuối và AMF. Côngtenơ N1 SM là côngtenơ liên quan đến phiên giữa thiết bị đầu cuối và AMF.

S112: SMF gửi yêu cầu thiết lập phiên thứ hai đến CU-CP.

Yêu cầu thiết lập phiên thứ hai này bao gồm một hoặc nhiều tham số sau: thông tin quản lý phiên (thông tin N2 SM) giữa AMF và RAN, và tin nhắn lớp không truy cập (Non-Access Stratum, NAS) (ID phiên PDU và côngtenơ N1 SM (chấp nhận thiết lập phiên PDU)). N2 là tên của giao diện giữa AMF và mạng truy cập vô tuyến (RAN).

Một cách tuỳ chọn, SMF dễ dàng truyền yêu cầu thiết lập phiên thứ hai đến CU-CP nhờ thực thể chức năng điều khiển di động (Access and Mobility Function, AMF).

S113: CU-CP lựa chọn CU-UP đích. Có thể có một hoặc nhiều CU-UP đích.

Một cách tuỳ chọn, sau khi nhận yêu cầu thiết lập phiên thứ hai, trước tiên CU-CP lựa chọn CU-UP đích, nghĩa là CU-UP đích mà kết nối phiên cần được thiết lập.

Đối với quy trình cài đặt bearer, CU-CP lựa chọn yêu cầu cài đặt bearer và gửi yêu cầu cài đặt bearer đến CU-UP đích, và hoàn thành việc kích hoạt và thỏa thuận bảo mật mặt phẳng người dùng sau đó trong yêu cầu cài đặt bearer.

Theo một phương án, S113 được tiến hành trước khi CU-CP xác định thông tin thỏa thuận bảo mật. Sau khi lựa chọn CU-UP đích, CU-CP thu được mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên của CU-UP đích và/hoặc mã định danh chỉ báo bảo vệ mã hóa của CU-UP dựa vào mã định danh của CU-UP đích. Một điều kiện tiên quyết là trước tiên CU-CP thu nhận các mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của tất cả các CU-UP và/hoặc các mã định danh chỉ báo bảo vệ mã hóa của các CU-UP, lựa chọn, dựa vào mã định danh của CU-UP đích, mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP của CU-UP đích và/hoặc mã định danh chỉ báo bảo vệ mã hóa của CU-UP đích từ các mã định danh của các CU-UP.

Một cách tuỳ chọn, mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-

UP của CU-UP đích và mã định danh chỉ báo bảo vệ mã hóa của CU-UP có thể là không được tìm kiếm. Trong quy trình thiết lập phiên, theo mặc định, việc bảo vệ trạng thái nguyên vẹn của CU-UP có thể là không được phép và việc bảo vệ mã hóa của CU-UP có thể là không được phép. Cụ thể, việc này có thể được tạo cấu hình trước hoặc được xác định theo tiêu chuẩn hoặc giao thức. Việc này không bị giới hạn trong sáng chế.

S114: CU-CP tạo ra khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào mã định danh của CU-UP đích.

Nói cách khác, khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP có thể được tạo ra trong trong quy trình thiết lập phiên nhờ sử dụng phương pháp được thể hiện trên FIG.9. Tuy nhiên, việc này không bị giới hạn ở đó. Nếu khóa được tạo ra theo cách trên FIG.7 và FIG.8 trong đó mã định danh của CU-UP không được đưa vào, khóa này cũng có thể được tạo ra trước thỏa thuận bảo mật. Lý do đặc biệt để tạo ra khóa là không bị giới hạn trong sáng chế. Nếu CU-CP tạo ra khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP trước khi việc thiết lập phiên được khởi tạo, việc bảo vệ trạng thái nguyên vẹn của CU-UP bắt đầu được kích hoạt cần được xác định trong quy trình sau đó.

Mã định danh của CU-UP đích có thể là mã định danh liên quan đến sự phân biệt thực thể của CU-UP, như ID đường hầm chẳng hạn.

Theo cách khác, khi tạo ra khóa bảo vệ mã hóa của CU-CP và khóa bảo vệ trạng thái nguyên vẹn của CU-CP, CU-CP còn tạo ra khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP.

Khi có nhiều CU-UP đích, CU-CP tạo ra khóa bảo vệ mã hóa và khóa bảo vệ trạng thái nguyên vẹn của từng CU-UP.

S115: CU-CP gửi lệnh bảo mật đến CU-UP đích, trong đó lệnh bảo mật này bao gồm khóa bảo vệ mã hóa của CU-UP, khóa bảo vệ trạng thái nguyên vẹn của CU-UP, và mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Một cách tuỳ chọn, lệnh bảo mật có thể còn có mã định danh (ID) phiên và/hoặc

mã định danh chỉ báo bảo vệ mã hóa của CU-UP, thuật toán bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP này.

Cần lưu ý rằng, nếu CU-CP đã có khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP trước quy trình thiết lập phiên, S114 có thể không được tiến hành. Ngoài ra, lệnh bảo mật này không có khóa bảo vệ mã hóa của CU-UP hoặc khóa bảo vệ trạng thái nguyên vẹn của CU-UP.

S116: CU-UP đích gửi phản hồi bảo mật đến CU-CP, trong đó phản hồi bảo mật này mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, để biểu thị việc CU-UP có đang cho phép bảo vệ trạng thái nguyên vẹn hay không.

Sau khi nhận phản hồi bảo mật, CU-CP ghi lại mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn hiện tại của CU-UP.

Theo cách khác, phản hồi bảo mật có thể không mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn, và CU-CP xem xét theo mặc định rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép.

Sau bước S116, CU-CP gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối. CU-UP trong phương án nêu trên là CU-UP đích được lựa chọn bởi CU-CP.

Sau khi nhận thông tin thỏa thuận bảo mật, thiết bị đầu cuối có thể tạo ra khóa bảo vệ mã hóa tương ứng của CU-UP và khóa bảo vệ trạng thái nguyên vẹn tương ứng của CU-UP dựa vào thuật toán bảo vệ trạng thái nguyên vẹn và thuật toán bảo vệ mã hóa của CU-UP.

Ngoài ra, trong phương án nêu trên, cả thiết bị đầu cuối và CU-UP đều cho phép việc mã hóa và giải mã đường lên và đường xuống, hoặc cho phép bảo vệ trạng thái nguyên vẹn. Việc bảo vệ này dựa vào phiên hoặc bearer phụ thuộc vào việc thủ tục của sự tương tác giữa thiết bị đầu cuối và SMF và/hoặc CU-UP là thủ tục thiết lập phiên hoặc thủ tục thiết lập bearer (liên quan đến bearer vô tuyến (Data Radio Bear, DRB) giao diện không gian. Cả hai trường hợp này đều áp dụng được.

Cần lưu ý rằng nếu thiết bị đầu cuối xác định, trước khi phiên được thiết lập, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối, thiết bị đầu cuối cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào thiết bị đầu cuối và việc tạo khóa và thỏa thuận. Khóa được tạo ra này cũng dựa vào độ hạt thiết bị đầu cuối.

Ví dụ, nếu trong quy trình thiết lập phiên, trước tiên thiết bị đầu cuối khởi tạo thiết lập phiên, nói cách khác, sau khi gửi yêu cầu thiết lập phiên thứ nhất hoặc nhận yêu cầu thiết lập phiên thứ nhất, thiết bị đầu cuối xác định, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối, thiết bị đầu cuối cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên và việc tạo khóa và thỏa thuận. Khóa được tạo ra này dựa vào độ hạt phiên.

Nếu thiết bị đầu cuối gửi yêu cầu thiết lập phiên thứ nhất hoặc nhận yêu cầu thiết lập phiên thứ nhất, và yêu cầu thiết lập phiên thứ nhất bao gồm mã định danh DRB, thiết bị đầu cuối cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào DRB và việc tạo khóa và thỏa thuận. Khóa được tạo ra này dựa vào độ hạt DRB.

Nếu thiết bị đầu cuối và CU-UP tiến hành quy trình cài đặt bearer (Bearer), thiết bị đầu cuối cho phép và thỏa thuận việc bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào DRB và việc thỏa thuận khóa. Khóa được tạo ra này dựa dựa vào độ hạt bearer.

Một cách tuỳ chọn, dựa vào phương án nêu trên, CU-CP có thể còn gửi phản hồi thiết lập phiên thứ hai đến thực thể điều khiển chức năng truy cập và di động (Access and Mobility Function, AMF).

FIG.11 là lưu đồ sơ lược của phương pháp thỏa thuận bảo mật theo một phương án khác nữa của sáng chế. Một khác biệt với phương án nêu trên là ở chỗ CU-UP có thể tiến hành thỏa thuận bảo mật với thiết bị đầu cuối. Trong phương án này, CU-UP có khả năng xử lý tin nhắn cụ thể, và có thể tạo cấu hình cho danh sách thuật toán bảo mật CU-UP, hoặc nhận danh sách thuật toán bảo mật được gửi bởi CU-CP, hoặc tạo ra khóa bảo

vệ, bao gồm khóa bảo vệ trạng thái nguyên vẹn và khóa mã hóa, và có khả năng thỏa thuận với thiết bị đầu cuối, tiến hành việc tách rời bảo mật của mặt phẳng điều khiển và mặt phẳng người dùng.

Như được thể hiện trên FIG.11, phương pháp này bao gồm các bước sau.

S1101: CU-UP xác định thông tin thỏa thuận bảo mật.

S1102: CU-UP gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn (chỉ báo bí mật UP) của CU-UP. Mã định danh bảo vệ trạng thái nguyên vẹn của CU-UP biểu thị việc bảo vệ trạng thái nguyên vẹn của CU-UP có được phép hay không.

S1103: Thiết bị đầu cuối xác định, dựa vào thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

Trong phương án này, CU-UP xác định thông tin thỏa thuận bảo mật, và gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối. Sau khi nhận thông tin thỏa thuận bảo mật, thiết bị đầu cuối có thể xác định, dựa vào chỉ báo của thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không. Theo cách này, thỏa thuận bảo mật với thiết bị đầu cuối có thể được hoàn thành theo kịch bản trong đó CU-CP và CU-UP được tách rời khỏi nhau.

Trong một phương án thực hiện tùy chọn, nếu mã định danh bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, thiết bị đầu cuối xác định cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Nếu không thì thiết bị đầu cuối không cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật có thể còn có mã định danh bảo vệ mã hóa của CU-UP. Mã định danh bảo vệ mã hóa của CU-UP được sử dụng để biểu

thị việc bảo vệ mã hóa của CU-UP có được phép hay không.

Nếu mã định danh bảo vệ mã hóa của CU-UP chỉ báo rằng việc bảo vệ mã hóa của CU-UP là được phép, thiết bị đầu cuối xác định cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối. Nếu không thì thiết bị đầu cuối không cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối.

Theo cách khác, theo phương án được thể hiện trên FIG.11, thông tin thỏa thuận bảo mật bao gồm mã định danh bảo vệ mã hóa của CU-UP.

Bước S1103 có thể là: thiết bị đầu cuối xác định, dựa vào thông tin thỏa thuận bảo mật, xem có cho phép bảo vệ mã hóa mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tương ứng, theo cách khác, thông tin thỏa thuận bảo mật có thể còn có mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Theo một phương án thực hiện, thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

Một cách tuỳ chọn, theo một kịch bản, CU-CP và CU-UP có cùng thuật toán bảo vệ trạng thái nguyên vẹn; trong trường hợp này, thông tin thỏa thuận bảo mật có thể biểu thị mã định danh thuật toán bảo vệ trạng thái nguyên vẹn, và/hoặc, CU-CP và CU-UP có cùng thuật toán bảo vệ mã hóa; trong trường hợp này, thông tin thỏa thuận bảo mật có thể biểu thị mã định danh thuật toán bảo vệ mã hóa.

Theo kịch bản khác, CU-UP và CU-CP có thể lần lượt gửi các thuật toán của CU-UP và CU-CP đến thiết bị đầu cuối. Ví dụ, CU-UP gửi thuật toán bảo vệ mã hóa của CU-UP đến thiết bị đầu cuối, và CU-UP gửi thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP đến thiết bị đầu cuối; và CU-CP gửi thuật toán bảo vệ mã hóa của CU-CP đến thiết bị đầu cuối, và CU-CP gửi thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP đến

thiết bị đầu cuối. Việc này không bị giới hạn cụ thể trong sáng chế.

Dựa vào phương án nêu trên, CU-UP tạo ra khóa bảo vệ trạng thái nguyên vẹn, khóa bảo vệ mã hóa của CU-UP và khóa tương tự.

Cụ thể, CU-CP tạo ra khóa cơ sở và gửi khóa cơ sở này đến CU-UP, và CU-UP tạo ra khóa bảo vệ trạng thái nguyên vẹn dựa vào mã định danh của CU-UP, khóa cơ sở, mã định danh kiểu thuật toán trạng thái nguyên vẹn, và mã định danh thuật toán trạng thái nguyên vẹn. Theo cách khác, CU-UP tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào mã định danh của CU-UP, khóa cơ sở, và tham số tạo khóa. Theo cách khác, CU-UP tạo ra khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào mã định danh của CU-UP, khóa cơ sở, tham số tạo khóa, mã định danh kiểu thuật toán trạng thái nguyên vẹn, và mã định danh thuật toán trạng thái nguyên vẹn. Một cách tuỳ chọn, khi gửi khóa cơ sở, CU-CP còn gửi thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP và tham số tạo khóa đến CU-UP.

Khóa cơ sở này có thể là K-AN, khóa bảo mật được chia sẻ với thiết bị đầu cuối, khóa bảo mật được tạo ra bởi CU-CP dựa vào K-AN, hoặc khóa tương tự.

Tương tự, CU-UP tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào mã định danh của CU-UP, khóa cơ sở, mã định danh kiểu thuật toán bảo vệ mã hóa của CU-UP, và thuật toán mã hóa mã định danh của CU-UP. Theo cách khác, CU-UP tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào mã định danh của CU-UP, khóa cơ sở, mã định danh kiểu thuật toán bảo vệ mã hóa của CU-UP, và tham số tạo khóa.

Cần lưu ý rằng CU-UP và DU có thể được triển khai cùng nhau theo một cách phân bố. Do đó, DU có thể còn có khả năng tạo khóa. Trong trường hợp này, cần xem xét rằng mã định danh của DU được bổ sung vào.

Đối với quy trình tạo khóa cụ thể, xem các phương án trên trên trên FIG.7 đến FIG.9. Các chi tiết không được mô tả lại ở đây.

Theo một phương án thực hiện khác, CU-UP nhận khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP được gửi bởi CU-CP. Cụ thể, đối

với phương pháp để tạo ra, bởi CU-CP, khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP, xem các phương án nêu trên. Các chi tiết không được mô tả lại ở đây.

Cụ thể, đối với quy trình thiết lập phiên, xem các phương án về phương pháp nêu trên, và xem phương án được thể hiện trên FIG.10. Các chi tiết không được mô tả lại ở đây.

Nói cách khác, thiết bị đầu cuối có thể khởi tạo việc thiết lập phiên, hoặc phía mạng, như SMF chẳng hạn, có thể khởi tạo việc thiết lập phiên.

FIG.12 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án của sáng chế. Như được thể hiện trên FIG.12, thiết bị này bao gồm môđun nhận 121 và môđun xác định 122.

Môđun nhận 121 được tạo cấu hình để nhận thông tin thỏa thuận bảo mật được gửi bởi CU-CP, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Môđun xác định 122 được tạo cấu hình để xác định, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, và tham số làm mới.

Một cách tuỳ chọn, môđun nhận 121 còn được tạo cấu hình để nhận thông tin giao diện không gian được gửi bởi CU-CP, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu,

mã định danh CU-UP, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, và tham số làm mới.

FIG.13 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế. Như được thể hiện trên FIG.13, dựa vào FIG.12, thiết bị này còn bao gồm môđun tạo khóa 131, được tạo cấu hình để tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

FIG.14 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế. Như được thể hiện trên FIG.14, thiết bị này có thể còn có môđun gửi 141, được tạo cấu hình để gửi yêu cầu thiết lập phiên thứ nhất đến thực thể chức năng quản lý phiên SMF, trong đó yêu cầu thiết lập phiên thứ nhất bao gồm một hoặc nhiều tham số sau: một đoạn hoặc nhiều đoạn của S-NSSAI, DNN, ID phiên PDU, kiểu yêu cầu, ID phiên PDU cũ, và côngtenơ N1 SM.

Một cách tuỳ chọn, môđun xác định 122 được tạo cấu hình cụ thể để xác định, sau khi gửi yêu cầu thiết lập phiên thứ nhất đến SMF, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không.

Ngoài ra, môđun xác định 122 còn được tạo cấu hình cụ thể để xác định, khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên của thiết bị đầu cuối.

Ngoài ra, môđun xác định 122 còn được tạo cấu hình cụ thể để xác định, khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

Theo một phương án thực hiện, môđun gửi 141 được tạo cấu hình để gửi tham số bảo vệ trạng thái nguyên vẹn đến CU-CP.

Môđun xác định 122 được tạo cấu hình cụ thể để xác định, khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là không được phép, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối. Một cách tương ứng, môđun gửi 141 được tạo cấu hình để gửi phản hồi thỏa thuận bảo mật đến CU-CP, trong đó phản hồi thỏa thuận bảo mật này bao gồm tham số bảo vệ trạng thái nguyên vẹn và mã định danh chỉ báo được sử dụng để chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối là được phép.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

môđun xác định 122 còn được tạo cấu hình để xác định, dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không.

Theo một phương án thực hiện khác, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

Một cách tương ứng, môđun xác định 122 được tạo cấu hình cụ thể để xác định, sau khi yêu cầu thiết lập phiên thứ nhất được gửi đến SMF, dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa dựa vào phiên đối với thiết bị đầu cuối hay không.

Một cách tuỳ chọn, môđun tạo khóa 131 được tạo cấu hình để tạo ra khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

Thiết bị này có thể được tích hợp vào thiết bị đầu cuối hoặc chip của thiết bị đầu cuối. Phương pháp nêu trên được tiến hành bởi thiết bị đầu cuối trong phương án nêu

trên được thực hiện bởi thiết bị nêu trên. Các nguyên lý thực hiện và các hiệu quả kỹ thuật là tương tự. Các chi tiết không được mô tả lại ở đây.

FIG.15 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế. Như được thể hiện trên FIG.15, thiết bị bao gồm môđun xác định 151 và môđun gửi 152.

Môđun xác định 151 được tạo cấu hình để xác định thông tin thỏa thuận bảo mật, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Môđun gửi 152 được tạo cấu hình để gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, và tham số làm mới.

Một cách tuỳ chọn, môđun gửi 152 còn được tạo cấu hình để gửi thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, và tham số làm mới.

FIG.16 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác nữa của sáng chế. Thiết bị này còn bao gồm môđun tạo khóa 161, được tạo cấu hình để tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa

vào tham số tạo khóa.

Môđun gửi 152 còn được tạo cấu hình để gửi khóa bảo vệ trạng thái nguyên vẹn của CU-UP đến CU-UP này.

Theo một phương án thực hiện, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

Một cách tương ứng, môđun tạo khóa 161 được tạo cấu hình để tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, môđun gửi 152 còn được tạo cấu hình để gửi khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP đến CU-UP này.

Ngoài ra, theo phương án thực hiện, môđun tạo khóa 161 được tạo cấu hình để tạo ra khóa cơ sở.

Môđun gửi 152 còn được tạo cấu hình để gửi khóa cơ sở đến CU-UP.

FIG.17 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác nữa của sáng chế. Như được thể hiện trên FIG.17, thiết bị này còn bao gồm: môđun nhận 171, được tạo cấu hình để nhận yêu cầu thiết lập phiên thứ hai được gửi bởi thực thể chức năng quản lý phiên SMF sau khi SMF nhận yêu cầu thiết lập phiên thứ nhất được gửi bởi thiết bị đầu cuối.

Môđun gửi 152 còn được tạo cấu hình để gửi phản hồi thiết lập phiên đến SMF.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

Thiết bị này có thể được tích hợp vào CU-CP hoặc chip của CU-CP. Phương pháp nêu trên được tiến hành bởi CU-CP trong phương án nêu trên được thực hiện bởi thiết bị nêu trên. Các nguyên lý thực hiện và các hiệu quả kỹ thuật là tương tự. Các chi tiết không được mô tả lại ở đây.

FIG.18 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế. Như được thể hiện trên FIG.18, thiết bị này bao gồm môđun xác định 181 và môđun gửi 182.

Môđun xác định 181 được tạo cấu hình để xác định thông tin thỏa thuận bảo mật, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP.

Môđun gửi 182 được tạo cấu hình để gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, và tham số làm mới.

Môđun gửi 182 còn được tạo cấu hình để gửi thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, và tham số làm mới.

FIG.19 là sơ đồ cấu trúc sơ lược của thiết bị thỏa thuận bảo mật theo một phương án khác của sáng chế. Thiết bị này có thể có môđun tạo khóa 191, được tạo cấu hình để tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Một cách tuỳ chọn, thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

Một cách tương ứng, môđun tạo khóa 191 được tạo cấu hình để tạo ra khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

Thiết bị này có thể được tích hợp vào CU-UP hoặc chip của CU-UP. Phương pháp nêu trên được tiến hành bởi CU-CP trong phương án nêu trên được thực hiện bởi thiết bị nêu trên. Các nguyên lý thực hiện và các hiệu quả kỹ thuật là tương tự. Các chi tiết không được mô tả lại ở đây.

Cần lưu ý là cần hiểu rằng việc phân chia thành các môđun của thiết bị chỉ là sự phân chia chức năng lôgic. Theo một phương án thực hiện thực tế, tất cả hoặc một số môđun có thể được tích hợp vào một thực thể vật lý, hoặc các môđun có thể được tách rời vật lý. Ngoài ra, các môđun này có thể đều được thực hiện dưới dạng phần mềm được gọi bởi phần tử xử lý, hoặc có thể đều được thực hiện dưới dạng phần cứng; hoặc một số môđun có thể được thực hiện dưới dạng phần mềm được gọi bởi phần tử xử lý, và một số môđun được thực hiện dưới dạng phần cứng. Ví dụ, môđun xác định có thể là phần tử xử lý được bố trí riêng rẽ, hoặc có thể được tích hợp trong chip của thiết bị nếu trên để thực hiện. Ngoài ra, theo cách khác, môđun xác định có thể được lưu trong bộ nhớ của thiết bị nêu trên dưới dạng mã chương trình, và được gọi bởi phần tử xử lý của thiết bị nêu trên tiến hành chức năng của môđun xác định nêu trên. Các phương án thực hiện của các môđun khác là tương tự như phương án thực hiện của môđun xác định. Ngoài ra, tất cả hoặc một số môđun có thể được tích hợp với nhau, hoặc có thể được sử dụng riêng rẽ. Phần tử xử lý ở đây có thể là mạch tích hợp và có khả năng xử lý tín hiệu. Theo quy trình thực hiện, các bước theo các phương pháp hoặc các môđun có thể được thực hiện nhờ sử dụng mạch lôgic được tích hợp phần cứng trong phần tử xử lý, hoặc nhờ sử dụng các lệnh dưới dạng phần mềm.

Ví dụ, các môđun nêu trên có thể được tạo cấu hình dưới dạng một hoặc nhiều mạch tích hợp thực hiện các phương pháp nêu trên, ví dụ một hoặc nhiều mạch tích hợp dùng cho ứng dụng cụ thể (Application Specific Integrated Circuit, ASIC), một hoặc nhiều bộ vi xử lý (digital signal processor (bộ xử lý tín hiệu số), DSP), hoặc một hoặc nhiều mảng cổng lập trình được theo trường (Field Programmable Gate Array, FPGA).

Theo một ví dụ khác, khi môđun được thực hiện dưới dạng mã chương trình được gọi bởi phần tử xử lý, phần tử xử lý này có thể là bộ xử lý cho mục đích chung, ví dụ bộ xử lý trung tâm (Central Processing Unit, CPU) hoặc bộ xử lý khác mà có thể gọi mã chương trình. Theo một ví dụ khác, các môđun có thể được tích hợp với nhau, và được thực hiện dưới dạng hệ thống trên chip (system-on-a-chip, SOC).

FIG.20 là sơ đồ cấu trúc sơ lược của thiết bị đầu cuối theo một phương án của sáng chế. Như được thể hiện trên FIG.20, thiết bị đầu cuối này có thể bao gồm bộ nhớ 201 và bộ xử lý 202.

Bộ nhớ 201 có thể là bộ phận vật lý độc lập, và có thể được nối với bộ xử lý 202 nhờ bus. Bộ nhớ 201 và bộ xử lý 202 có thể được tích hợp với nhau, và được thực hiện nhờ sử dụng phần cứng hoặc bộ phận tương tự.

Bộ nhớ 201 được tạo cấu hình để lưu trữ chương trình để thực hiện các phương án phương pháp nêu trên, và bộ xử lý 202 gọi chương trình để tiến hành các hoạt động của các phương án phương pháp nêu trên được tiến hành bởi thiết bị đầu cuối.

FIG.21 là sơ đồ cấu trúc sơ lược của CU-CP theo một phương án của sáng chế. Như được thể hiện trên FIG.21, CU-CP có thể bao gồm bộ nhớ 211 và bộ xử lý 212.

Bộ nhớ 211 có thể là bộ phận vật lý độc lập, và có thể được nối với bộ xử lý 2102 nhờ bus. Bộ nhớ 211 và bộ xử lý 212 có thể được tích hợp với nhau, và được thực hiện nhờ sử dụng phần cứng, hoặc bộ phận tương tự.

Bộ nhớ 211 được tạo cấu hình để lưu trữ và thực hiện các phương án phương pháp nêu trên, và bộ xử lý 212 gọi chương trình để tiến hành các hoạt động của các phương án phương pháp nêu trên được tiến hành bởi CU-CP.

FIG.22 là sơ đồ cấu trúc sơ lược của CU-UP theo một phương án của sáng chế. Như được thể hiện trên FIG.22, CU-UP có thể bao gồm bộ nhớ 221 và bộ xử lý 222.

Bộ nhớ 221 có thể là bộ phận vật lý độc lập, và có thể được nối với bộ xử lý 222 nhờ bus. Bộ nhớ 201 và bộ xử lý 222 có thể được tích hợp với nhau, và được thực hiện nhờ sử dụng phần cứng, hoặc bộ phận tương tự.

Bộ nhớ 221 được tạo cấu hình để lưu trữ và thực hiện các phương án phương pháp nêu trên, và bộ xử lý 222 gọi chương trình để tiến hành các hoạt động của các phương án phương pháp nêu trên được tiến hành bởi CU-UP.

Một cách tuỳ chọn, khi một phần hoặc toàn bộ các phương pháp thỏa thuận bảo mật trong các phương án nêu trên được thực hiện nhờ sử dụng phần mềm, theo cách khác, thiết bị thỏa thuận bảo mật có thể chỉ có bộ xử lý. Bộ nhớ này được tạo cấu hình để lưu trữ chương trình được bố trí bên ngoài thiết bị. Bộ xử lý được nối với bộ nhớ thông qua mạch/dây điện, để đọc và chạy chương trình được lưu trong bộ nhớ.

Bộ xử lý có thể là bộ xử lý trung tâm (central processing unit, CPU), bộ xử lý mạng (network processor, NP), hoặc kết hợp của CPU và NP.

Bộ xử lý có thể còn có chip phần cứng. Chip phần cứng này có thể là mạch tích hợp dùng cho ứng dụng cụ thể (application-specific integrated circuit, ASIC), thiết bị lôgic lập trình được (programmable logic device, PLD), hoặc sự kết hợp của chúng. PLD có thể là thiết bị lôgic lập trình phức (complex programmable logic device, CPLD), mảng cổng lập trình được theo trường (field-programmable gate array, FPGA), lôgic ma trận chung (generic array logic, GAL), hoặc sự kết hợp bất kỳ của chúng.

Bộ nhớ có thể bao gồm bộ nhớ khả biến (volatile memory), ví dụ bộ nhớ truy cập ngẫu nhiên (random-access memory, RAM); hoặc bộ nhớ có thể bao gồm bộ nhớ bất khả biến (non-volatile memory), ví dụ bộ nhớ chớp (flash memory), ổ đĩa cứng (hard disk drive, HDD), hoặc ổ đĩa thể rắn (solid-state drive, SSD); hoặc bộ nhớ này có thể bao gồm sự kết hợp các loại bộ nhớ nêu trên.

Yêu cầu bảo hộ

1. Phương pháp thỏa thuận bảo mật, phương pháp này bao gồm các bước:

nhận, bởi thiết bị đầu cuối, thông tin thỏa thuận bảo mật được gửi bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

2. Phương pháp theo điểm 1, trong đó thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa, và phương pháp này còn bao gồm bước:

tạo ra, bởi thiết bị đầu cuối, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa, trong đó tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

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

gửi, bởi thiết bị đầu cuối, yêu cầu thiết lập phiên thứ nhất đến thực thể chức năng quản lý phiên SMF; và

bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên của thiết bị đầu cuối.

4. Phương pháp theo điểm 1 hoặc 2, trong đó bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm bước:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

5. Phương pháp theo điểm 4, trong đó sau bước xác định, bởi thiết bị đầu cuối, để cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, tham số bảo vệ trạng thái nguyên vẹn đến CU-CP.

6. Phương pháp theo điểm 1, trong đó bước xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối hay không bao gồm bước:

xác định, bởi thiết bị đầu cuối khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là không được phép, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối.

7. Phương pháp theo điểm 6, trong đó sau bước xác định, bởi thiết bị đầu cuối, để không cho phép bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, phản hồi thỏa thuận bảo mật đến CU-CP, trong đó phản hồi thỏa thuận bảo mật này bao gồm tham số bảo vệ trạng thái nguyên vẹn và mã định danh chỉ báo được sử dụng để chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối là được phép.

8. Phương pháp theo điểm bất kỳ trong số các điểm 5 đến 7, trong đó thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và phương pháp này còn bao gồm bước:

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không.

9. Phương pháp theo điểm bất kỳ trong số các điểm 5 đến 7, trong đó thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP, và phương pháp này còn bao gồm các bước:

gửi, bởi thiết bị đầu cuối, yêu cầu thiết lập phiên thứ nhất đến SMF; và

xác định, bởi thiết bị đầu cuối dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa dựa vào phiên đối với thiết bị đầu cuối hay không.

10. Phương pháp thỏa thuận bảo mật bao gồm các bước:

gửi, bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, lệnh bảo mật đến bộ phận tập trung mặt phẳng người dùng CU-UP đích, trong đó lệnh bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ nhất của CU-UP;

nhận, bởi CU-CP, phản hồi bảo mật từ CU-UP đích, trong đó phản hồi bảo mật này mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP chỉ báo xem CU-UP có cho phép bảo vệ trạng thái nguyên vẹn hay không;

ghi lại, bởi CU-CP, mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP; và

gửi, bởi CU-CP, thông tin thỏa thuận bảo mật đến thiết bị đầu cuối, trong đó thông tin thỏa thuận bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba chỉ báo xem thiết bị đầu cuối có cho phép bảo vệ trạng thái nguyên vẹn hay không.

11. Phương pháp theo điểm 10, trong đó thông tin thỏa thuận bảo mật còn bao gồm tham

số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

12. Phương pháp theo điểm 10, trong đó phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

13. Phương pháp theo điểm 11 hoặc 12, trong đó phương pháp này còn bao gồm bước:

tạo ra, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

14. Phương pháp theo điểm 13, trong đó sau bước tạo ra, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa vào tham số tạo khóa, phương pháp này còn bao gồm

bước:

gửi, bởi CU-CP, khóa bảo vệ trạng thái nguyên vẹn của CU-UP đến CU-UP này.

15. Phương pháp theo điểm 11 hoặc 12, trong đó thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

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

tạo ra, bởi CU-CP, khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa.

17. Phương pháp theo điểm 16, trong đó phương pháp này còn bao gồm bước:

gửi, bởi CU-CP, khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP đến CU-UP này.

18. Phương pháp theo điểm 10, trong đó phương pháp này còn bao gồm các bước:

tạo ra, bởi CU-CP, khóa cơ sở; và

gửi, bởi CU-CP, khóa cơ sở này đến CU-UP.

19. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 18, trong đó phương pháp này còn bao gồm các bước:

nhận, bởi CU-CP, yêu cầu thiết lập phiên thứ hai được gửi bởi thực thể chức năng quản lý phiên SMF sau khi SMF nhận yêu cầu thiết lập phiên thứ nhất được gửi bởi thiết bị đầu cuối; và

gửi, bởi CU-CP, phản hồi thiết lập phiên đến SMF.

20. Phương pháp theo điểm bất kỳ trong số các điểm từ 16 đến 18, trong đó thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

21. Phương pháp thỏa thuận bảo mật bao gồm các bước:

nhận, bởi bộ phận tập trung mặt phẳng người dùng CU-UP đích, lệnh bảo mật từ

bộ phận tập trung mặt phẳng điều khiển CU-CP, trong đó lệnh bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ nhất của CU-UP;

gửi, bởi CU-UP đích, phản hồi bảo mật đến CU-CP, trong đó phản hồi bảo mật mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP chỉ báo xem CU-UP có cho phép bảo vệ trạng thái nguyên vẹn hay không.

22. Phương pháp theo điểm 21, trong đó phản hồi bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

23. Phương pháp theo điểm 21, trong đó phản hồi bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

24. Thiết bị thỏa thuận bảo mật bao gồm:

môđun nhận, được tạo cấu hình để nhận thông tin thỏa thuận bảo mật được gửi bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, trong đó thông tin thỏa thuận bảo mật này bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP; và

môđun xác định, được tạo cấu hình để xác định, dựa vào mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP, xem có cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối hay không.

25. Thiết bị theo điểm 24, trong đó thông tin thỏa thuận bảo mật còn bao gồm tham số

tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

26. Thiết bị theo điểm 24 hoặc 25, trong đó thiết bị này còn bao gồm:

môđun gửi, được tạo cấu hình để gửi yêu cầu thiết lập phiên thứ nhất đến thực thể chức năng quản lý phiên SMF, trong đó

môđun xác định được tạo cấu hình cụ thể để xác định, khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng dựa vào phiên của thiết bị đầu cuối.

27. Thiết bị theo điểm 24 hoặc 25, trong đó môđun xác định được tạo cấu hình cụ thể để xác định, khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là được phép, để cho phép bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của thiết bị đầu cuối.

28. Thiết bị theo điểm 27, trong đó thiết bị này còn bao gồm:

môđun gửi, được tạo cấu hình để gửi tham số bảo vệ trạng thái nguyên vẹn đến CU-CP.

29. Thiết bị theo điểm 24, trong đó môđun xác định được tạo cấu hình cụ thể để xác định, khi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn của CU-UP chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của CU-UP là không được phép, để không cho phép

bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối.

30. Thiết bị theo điểm 29, trong đó thiết bị này còn bao gồm:

môđun gửi, được tạo cấu hình để gửi phản hồi thỏa thuận bảo mật đến CU-CP, trong đó phản hồi thỏa thuận bảo mật này bao gồm tham số bảo vệ trạng thái nguyên vẹn và mã định danh chỉ báo được sử dụng để chỉ báo rằng việc bảo vệ trạng thái nguyên vẹn của thiết bị đầu cuối là được phép.

31. Thiết bị theo điểm bất kỳ trong số các điểm từ 28 đến 30, trong đó thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP; và

môđun xác định còn được tạo cấu hình để xác định, dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa đối với thiết bị đầu cuối hay không.

32. Thiết bị theo điểm bất kỳ trong số các điểm từ 28 đến 31, trong đó thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP;

thiết bị này còn bao gồm:

môđun gửi, được tạo cấu hình để gửi yêu cầu thiết lập phiên thứ nhất đến SMF; và

môđun xác định được tạo cấu hình cụ thể để xác định, sau khi yêu cầu thiết lập phiên thứ nhất được gửi đến SMF, dựa vào mã định danh chỉ báo bảo vệ mã hóa của CU-UP, xem có cho phép bảo vệ mã hóa dựa vào phiên đối với thiết bị đầu cuối hay không.

33. Thiết bị thỏa thuận bảo mật bao gồm:

môđun gửi, được tạo cấu hình để gửi lệnh bảo mật đến bộ phận tập trung mặt phẳng người dùng CU-UP đích, trong đó lệnh bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ nhất của CU-UP;

môđun nhận, được tạo cấu hình để nhận phản hồi bảo mật từ CU-UP đích, trong đó phản hồi bảo mật mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP chỉ báo xem CU-UP có cho phép bảo vệ trạng thái nguyên vẹn hay không;

môđun xác định, được tạo cấu hình để ghi lại mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP; và

môđun gửi, được tạo cấu hình để gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối, trong đó thông tin thỏa thuận bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba chỉ báo xem thiết bị đầu cuối có cho phép bảo vệ trạng thái nguyên vẹn hay không.

34. Thiết bị theo điểm 33, trong đó thông tin thỏa thuận bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

35. Thiết bị theo điểm 34, trong đó môđun gửi còn được tạo cấu hình để gửi thông tin giao diện không gian đến thiết bị đầu cuối, trong đó thông tin giao diện không gian này bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ

dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

36. Thiết bị theo điểm 34 hoặc 35, trong đó thiết bị này còn bao gồm:

môđun tạo khóa, được tạo cấu hình để tạo ra khóa bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP dựa vào tham số tạo khóa.

37. Thiết bị theo điểm 36, trong đó môđun gửi còn được tạo cấu hình để gửi khóa bảo vệ trạng thái nguyên vẹn của CU-UP đến CU-UP.

38. Thiết bị theo điểm 34 hoặc 35, trong đó thông tin thỏa thuận bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

39. Thiết bị theo điểm 38, trong đó thiết bị này còn bao gồm:

môđun tạo khóa, được tạo cấu hình để tạo ra khóa bảo vệ mã hóa của CU-UP dựa vào tham số tạo khóa.

40. Thiết bị theo điểm 39, trong đó môđun gửi còn được tạo cấu hình để gửi khóa bảo vệ mã hóa mặt phẳng người dùng của CU-UP đến CU-UP.

41. Thiết bị theo điểm 34, trong đó thiết bị này còn bao gồm:

môđun tạo khóa, được tạo cấu hình để tạo ra khóa cơ sở, trong đó:

môđun gửi còn được tạo cấu hình để gửi khóa cơ sở đến CU-UP.

42. Thiết bị theo điểm bất kỳ trong số các điểm từ 39 đến 41, trong đó thiết bị này còn bao gồm:

môđun nhận, được tạo cấu hình để nhận yêu cầu thiết lập phiên thứ hai được gửi bởi thực thể chức năng quản lý phiên SMF sau khi SMF nhận yêu cầu thiết lập phiên thứ nhất được gửi bởi thiết bị đầu cuối, trong đó:

môđun gửi còn được tạo cấu hình để gửi phản hồi thiết lập phiên đến SMF.

43. Thiết bị theo điểm bất kỳ trong số các điểm từ 39 đến 41, trong đó thông tin thỏa thuận bảo mật còn bao gồm một hoặc nhiều dấu hiệu sau: mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-CP, mã định danh thuật toán bảo vệ mã hóa của CU-CP, mã định danh thuật toán bảo vệ trạng thái nguyên vẹn của CU-UP, mã định danh

thuật toán bảo vệ mã hóa của CU-UP, và mã kiểm tra trạng thái nguyên vẹn tin nhắn.

44. Thiết bị thỏa thuận bảo mật bao gồm:

môđun xác định, được tạo cấu hình để nhận lệnh bảo mật từ bộ phận tập trung mặt phẳng điều khiển CU-CP, trong đó lệnh bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ nhất của CU-UP; và

môđun gửi, được tạo cấu hình để gửi phản hồi bảo mật đến CU-CP, trong đó phản hồi bảo mật mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP chỉ báo xem CU-UP có cho phép bảo vệ trạng thái nguyên vẹn hay không.

45. Thiết bị theo điểm 44, trong đó phản hồi bảo mật còn bao gồm tham số tạo khóa; và

tham số tạo khóa này bao gồm một hoặc nhiều dấu hiệu sau: mã định danh mẫu, mã định danh CU-UP, mã định danh DU, mã định danh bearer dữ liệu, mã định danh bearer, mã định danh dòng, mã định danh phiên, mã định danh lát, mã định danh lớp điều khiển truy cập môi trường MAC, bộ đếm báo hiệu điều khiển tài nguyên vô tuyến RRC, mã định danh tần số, mã định danh ô, tham số làm mới, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-UP, độ dài mã định danh kiểu thuật toán bảo vệ trạng thái nguyên vẹn mặt phẳng người dùng của CU-CP, độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-UP, và độ dài mã định danh kiểu bảo vệ mã hóa mặt phẳng người dùng của CU-CP.

46. Thiết bị theo điểm 45, trong đó phản hồi bảo mật còn bao gồm mã định danh chỉ báo bảo vệ mã hóa của CU-UP.

47. Phương pháp thỏa thuận bảo mật, bao gồm các bước:

gửi, bởi bộ phận tập trung mặt phẳng điều khiển CU-CP, lệnh bảo mật đến bộ phận tập trung mặt phẳng người dùng CU-UP đích, trong đó lệnh bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ nhất của CU-UP;

gửi, bởi CU-UP đích, phản hồi bảo mật đến CU-CP, trong đó phản hồi bảo mật mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP, trong đó

mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP chỉ báo xem CU-UP có cho phép bảo vệ trạng thái nguyên vẹn hay không;

ghi lại, bởi CU-CP, mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP; và

gửi, bởi CU-CP, thông tin thỏa thuận bảo mật đến thiết bị đầu cuối, trong đó thông tin thỏa thuận bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba chỉ báo xem thiết bị đầu cuối có cho phép bảo vệ trạng thái nguyên vẹn hay không.

48. Phương pháp theo điểm 47, trong đó lệnh bảo mật còn bao gồm mã định danh chỉ báo mã hóa thứ nhất của CU-UP.

49. Phương pháp theo điểm 47 hoặc 48, trong đó lệnh bảo mật còn bao gồm khóa bảo vệ mã hóa và khóa bảo vệ trạng thái nguyên vẹn.

50. Hệ thống thỏa thuận bảo mật, bao gồm:

bộ phận tập trung mặt phẳng điều khiển CU-CP, được tạo cấu hình để gửi lệnh bảo mật đến bộ phận tập trung mặt phẳng người dùng CU-UP đích, trong đó lệnh bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ nhất của CU-UP;

CU-UP đích, được tạo cấu hình để gửi phản hồi bảo mật đến CU-CP, trong đó phản hồi bảo mật mang mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP chỉ báo xem CU-UP có cho phép bảo vệ trạng thái nguyên vẹn hay không;

trong đó CU-CP còn được tạo cấu hình để ghi lại bởi mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ hai của CU-UP; và gửi thông tin thỏa thuận bảo mật đến thiết bị đầu cuối, trong đó thông tin thỏa thuận bảo mật bao gồm mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba, trong đó mã định danh chỉ báo bảo vệ trạng thái nguyên vẹn thứ ba chỉ báo xem thiết bị đầu cuối có cho phép bảo vệ trạng thái nguyên vẹn hay không.

51. Hệ thống theo điểm 50, trong đó lệnh bảo mật còn bao gồm mã định danh chỉ báo

mã hóa thứ nhất của CU-UP.

52. Hệ thống theo điểm 50 hoặc 51, trong đó lệnh bảo mật còn bao gồm khóa bảo vệ mã hóa và khóa bảo vệ trạng thái nguyên vẹn.

1/11

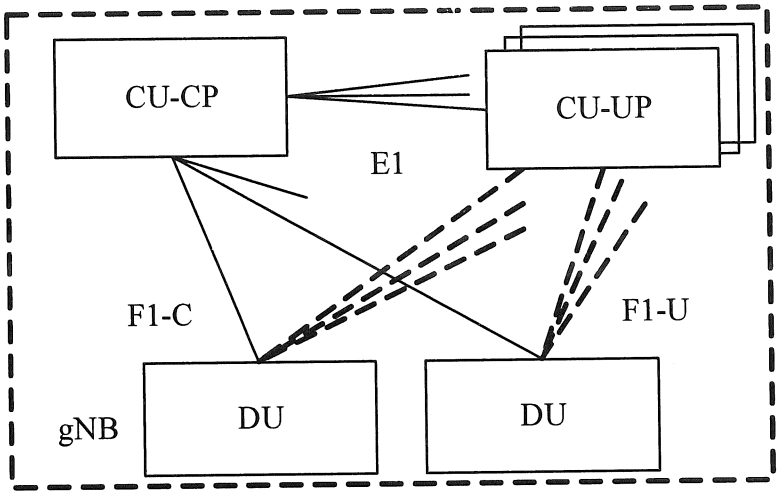

FIG.1

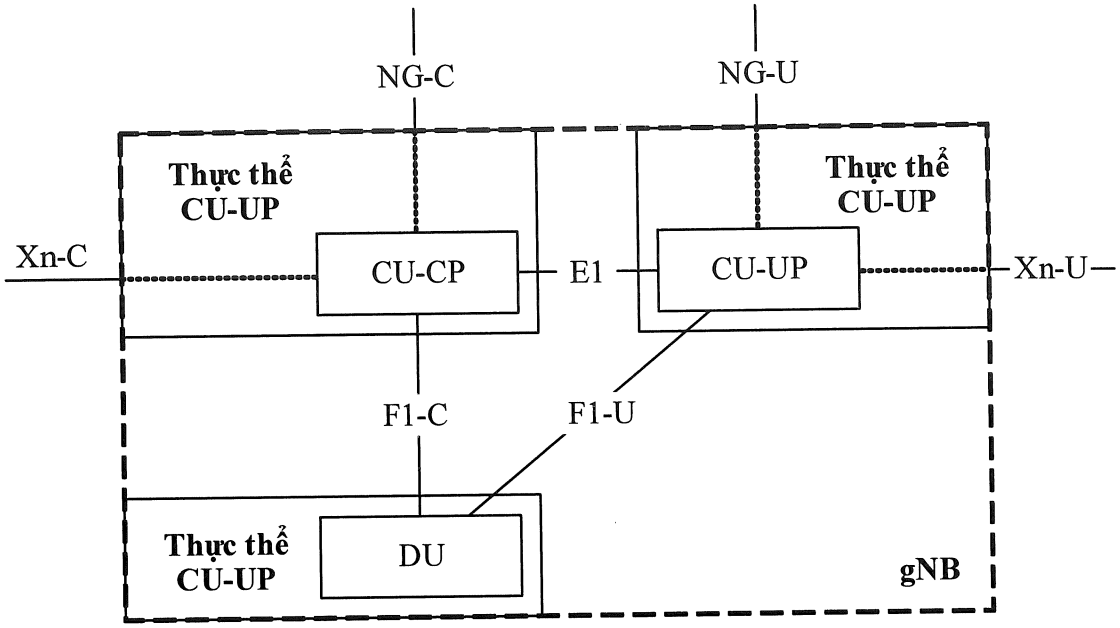

FIG.2

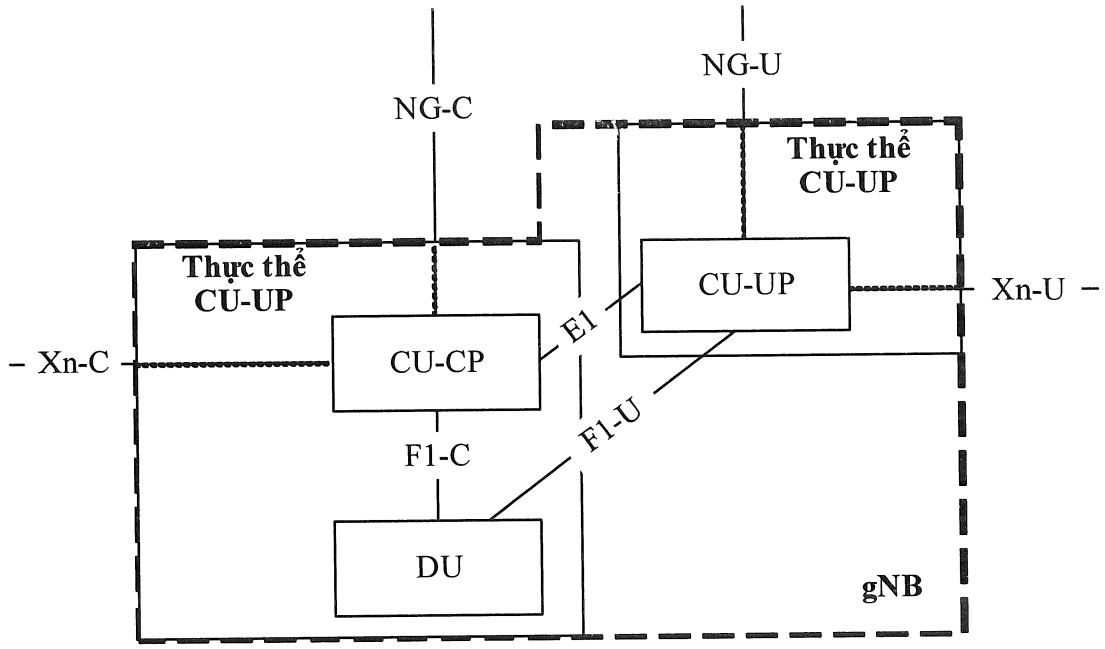
NG-C
NG-U
Thực thể CU-UP
Thực thể CU-UP
CU-UP
Xn-U
Xn-C
CU-CP
E1
F1-U
F1-C
DU
gNB

FIG.3

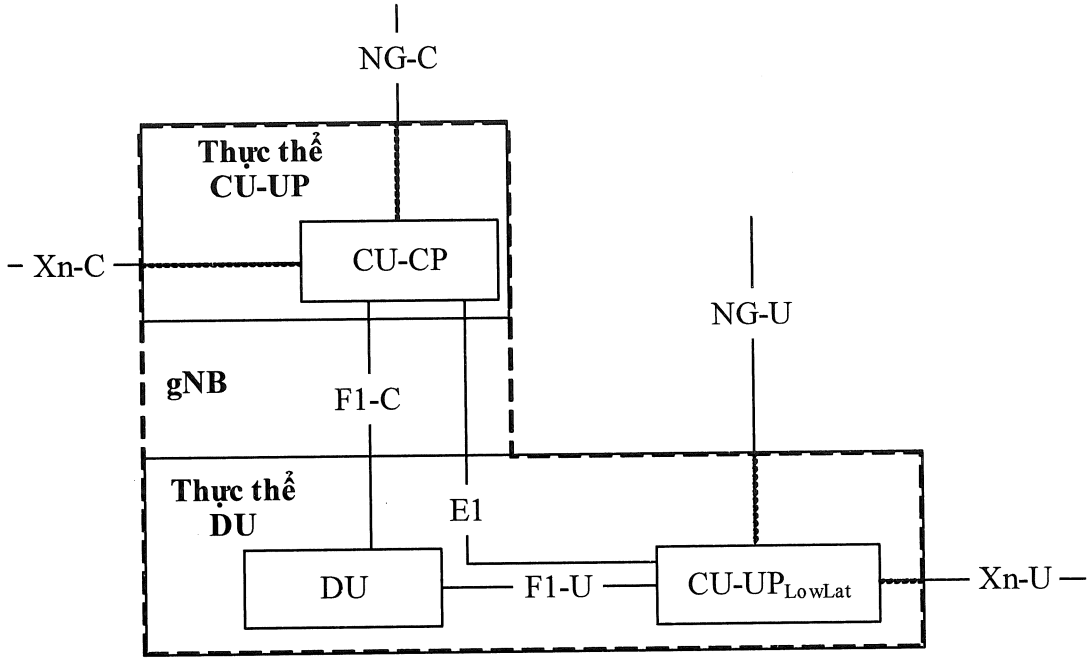
NG-C
Thực thể CU-UP
Xn-C
CU-CP
NG-U
gNB
F1-C
Thực thể DU
E1
DU
F1-U
CU-UP LowLat
Xn-U

FIG.4

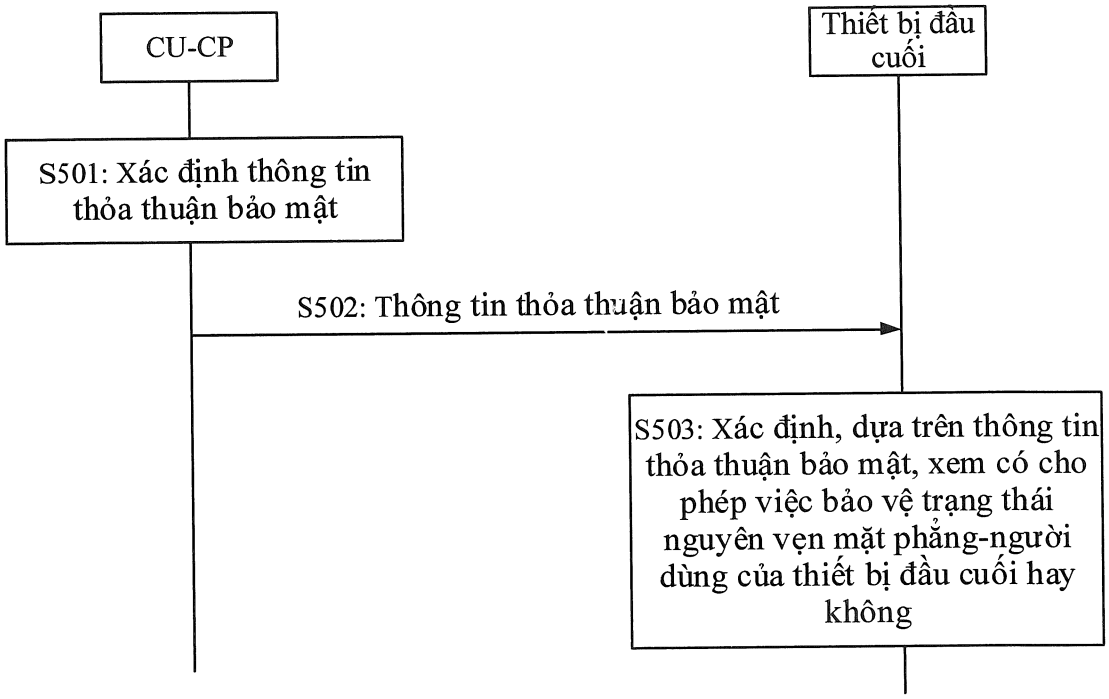
CU-CP
Thiết bị đầu cuối
S501: Xác định thông tin thỏa thuận bảo mật
S502: Thông tin thỏa thuận bảo mật
S503: Xác định, dựa trên thông tin thỏa thuận bảo mật, xem có cho phép việc bảo vệ trạng thái nguyên vẹn mặt phẳng-người dùng của thiết bị đầu cuối hay không

FIG.5

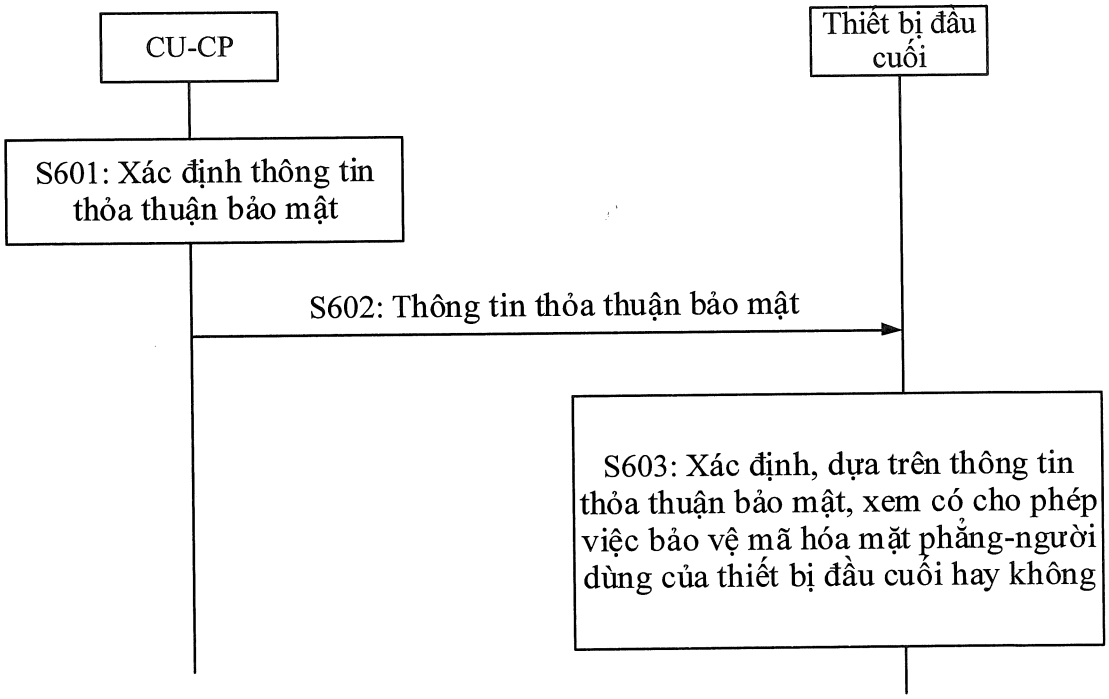
CU-CP
Thiết bị đầu cuối
S601: Xác định thông tin thỏa thuận bảo mật
S602: Thông tin thỏa thuận bảo mật
S603: Xác định, dựa trên thông tin thỏa thuận bảo mật, xem có cho phép việc bảo vệ mã hóa mặt phẳng-người dùng của thiết bị đầu cuối hay không

FIG.6

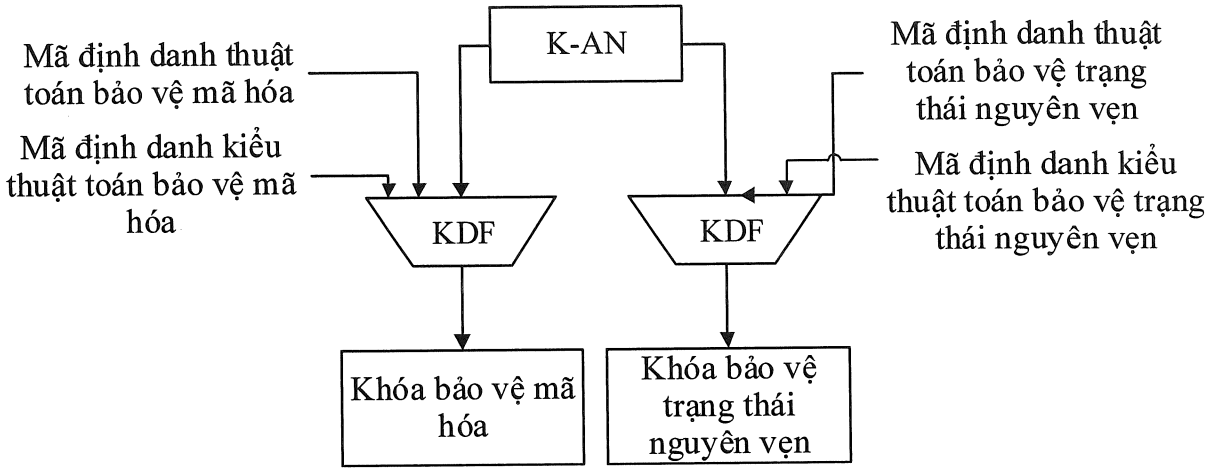

FIG.7

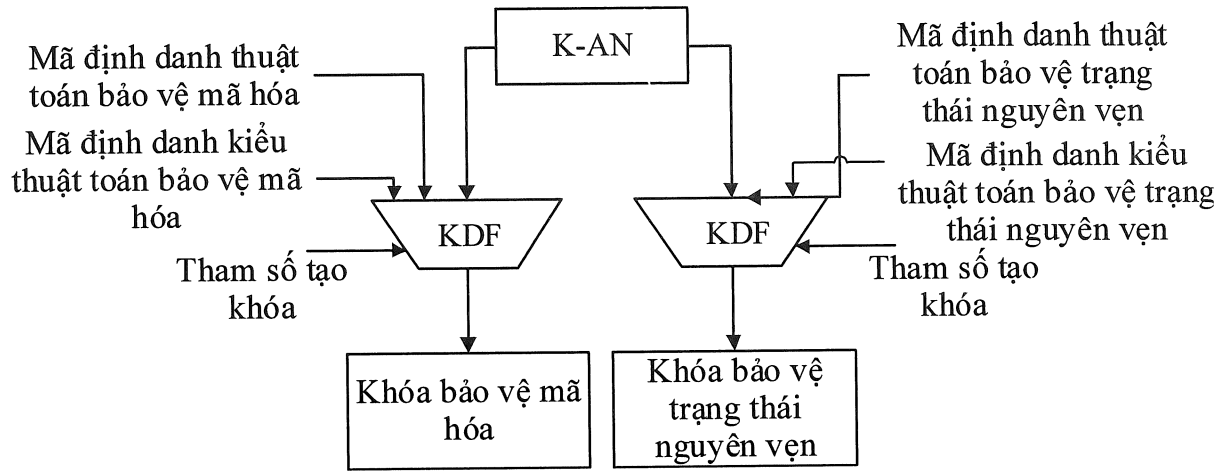

FIG.8

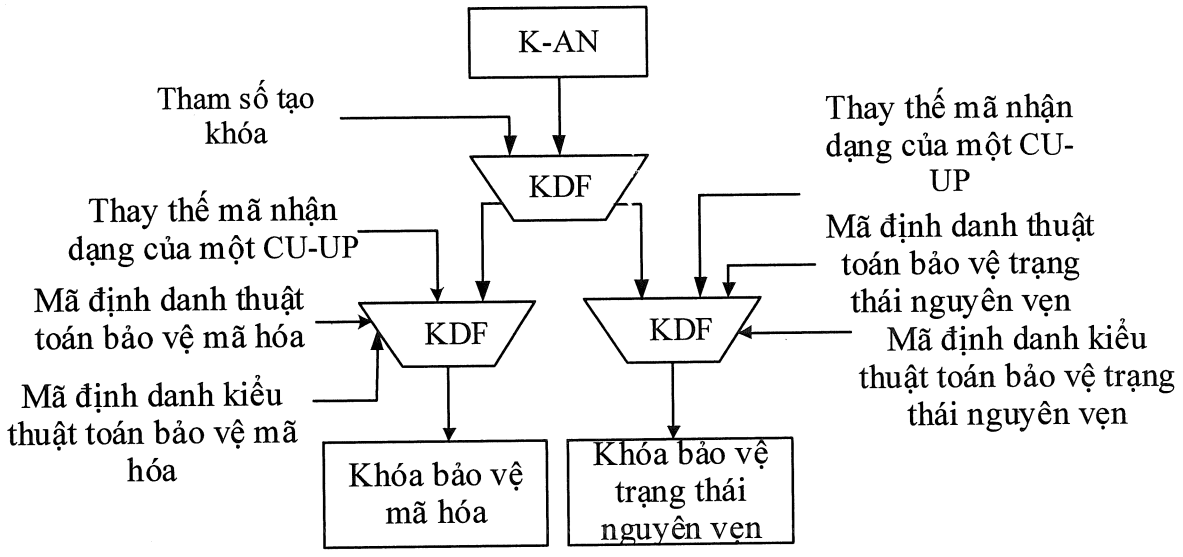

FIG.9

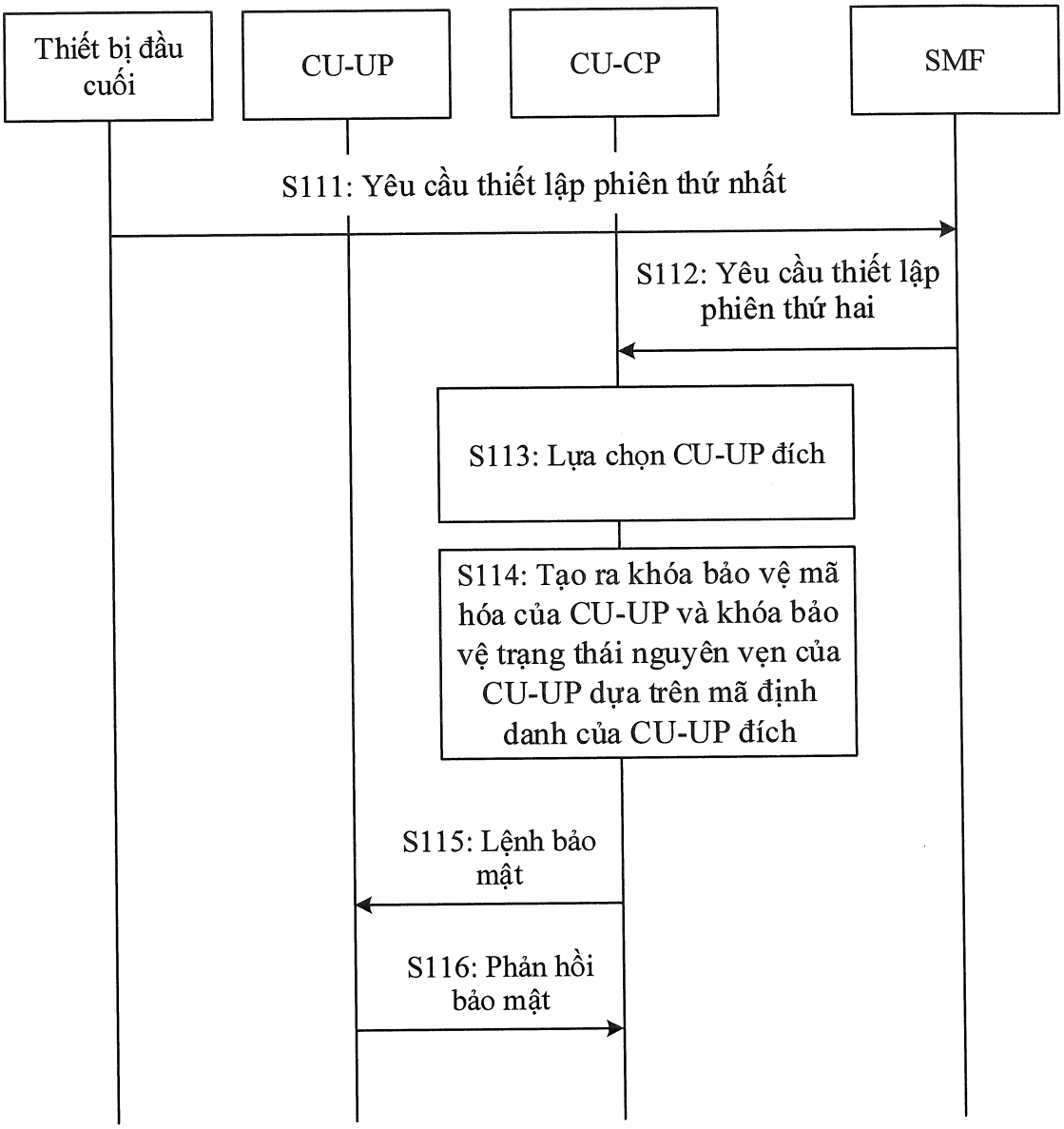
Thiết bị đầu cuối
CU-UP
CU-CP
SMF
S111: Yêu cầu thiết lập phiên thứ nhất
S112: Yêu cầu thiết lập phiên thứ hai
S113: Lựa chọn CU-UP đích
S114: Tạo ra khóa bảo vệ mã hóa của CU-UP và khóa bảo vệ trạng thái nguyên vẹn của CU-UP dựa trên mã định danh của CU-UP đích
S115: Lệnh bảo mật
S116: Phản hồi bảo mật

FIG.10

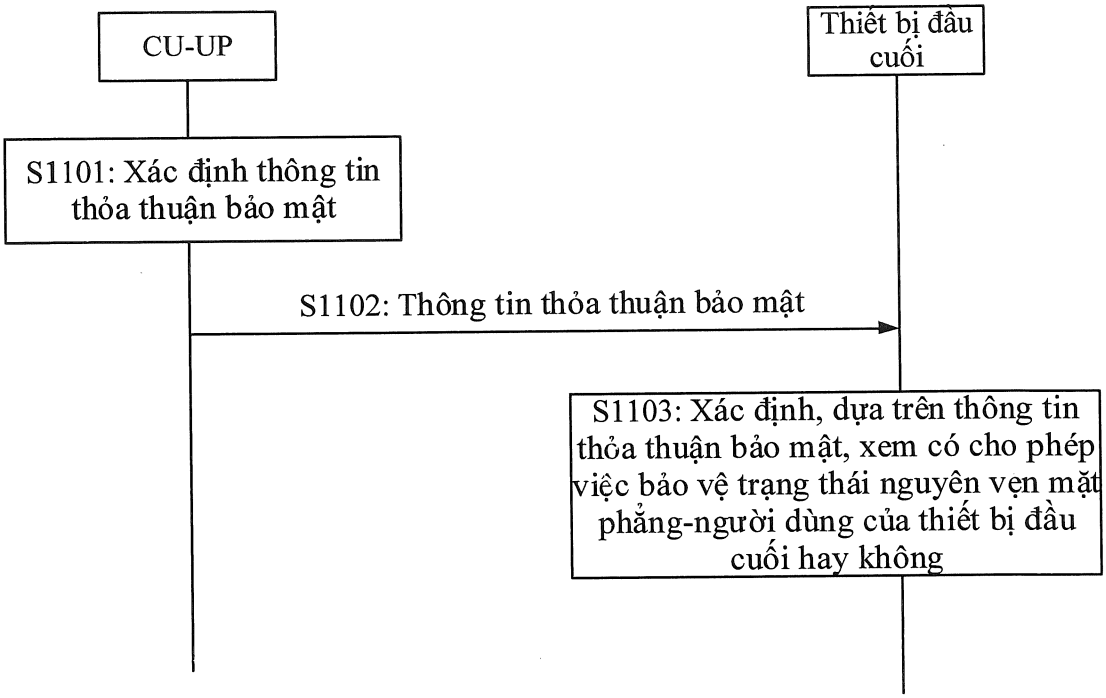
CU-UP
Thiết bị đầu cuối
S1101: Xác định thông tin thỏa thuận bảo mật
S1102: Thông tin thỏa thuận bảo mật
S1103: Xác định, dựa trên thông tin thỏa thuận bảo mật, xem có cho phép việc bảo vệ trạng thái nguyên vẹn mặt phẳng-người dùng của thiết bị đầu cuối hay không

FIG.11

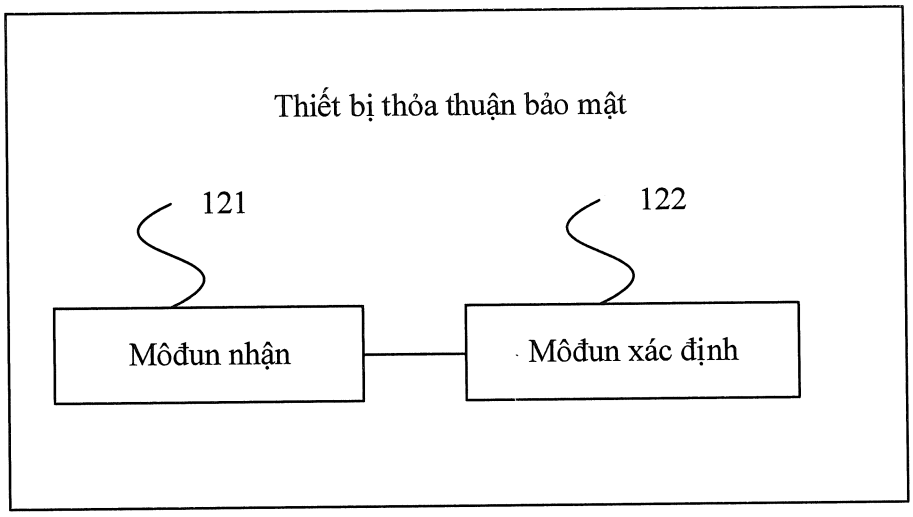
Thiết bị thỏa thuận bảo mật
121
122
Môđun nhận
Môđun xác định

FIG.12

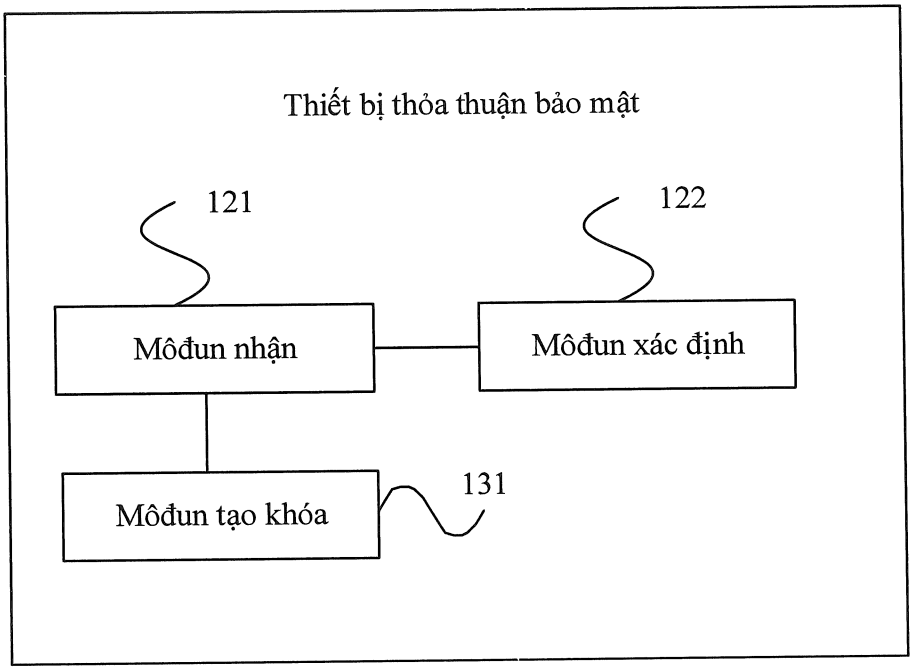
Thiết bị thỏa thuận bảo mật
121
122
Môđun nhận
Môđun xác định
Môđun tạo khóa
131

FIG.13

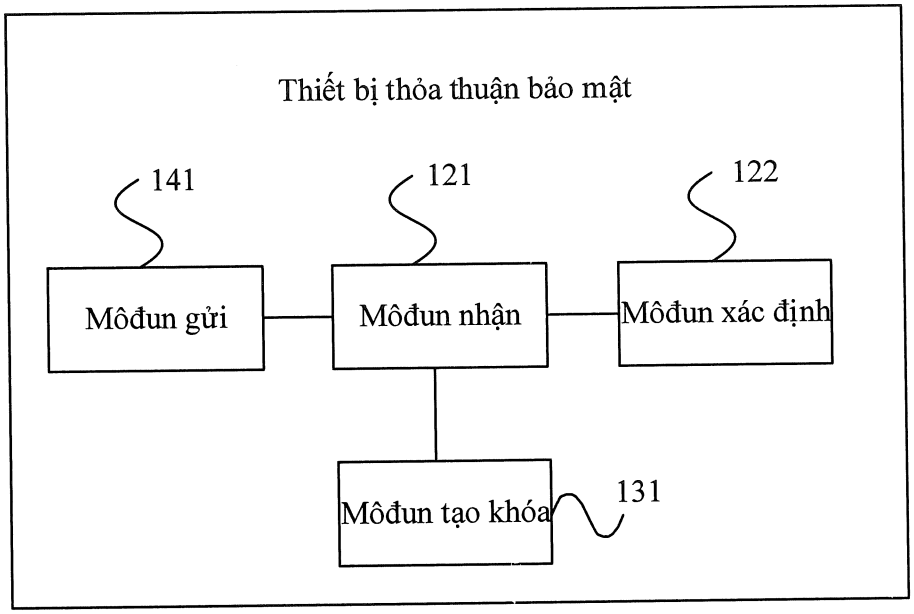
Thiết bị thỏa thuận bảo mật
141
121
122
Môđun gửi
Môđun nhận
Môđun xác định
Môđun tạo khóa
131

FIG.14

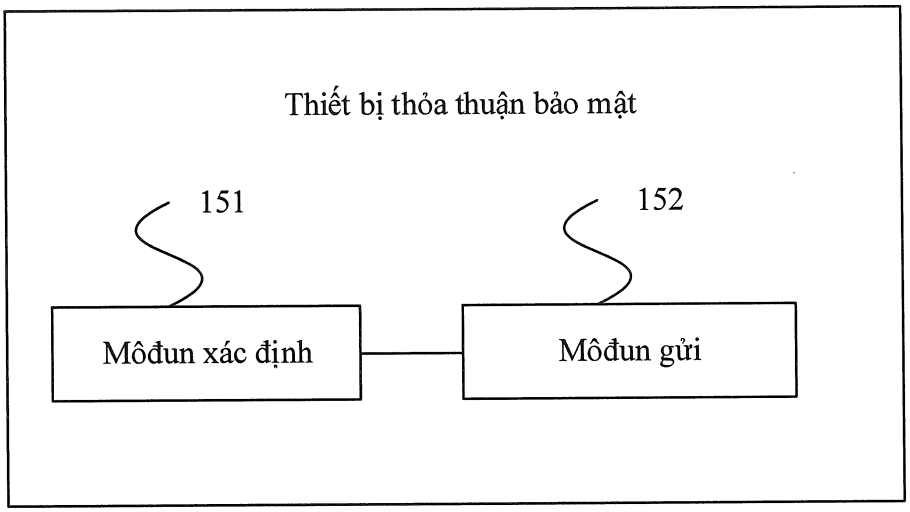
Thiết bị thỏa thuận bảo mật
151
152
Môđun xác định
Môđun gửi

FIG.15

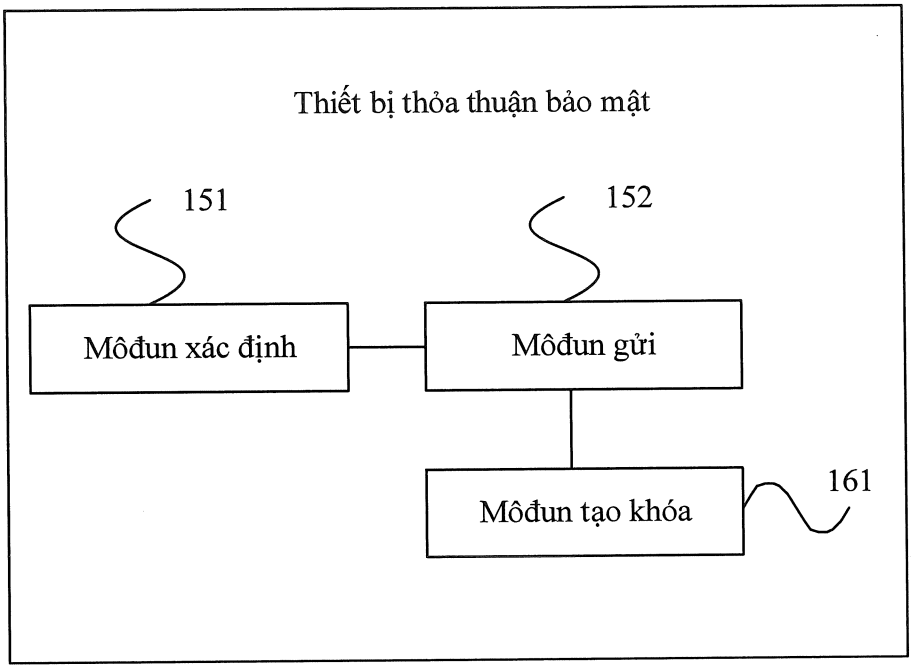
Thiết bị thỏa thuận bảo mật
151
152
Môđun xác định
Môđun gửi
161
Môđun tạo khóa

FIG.16

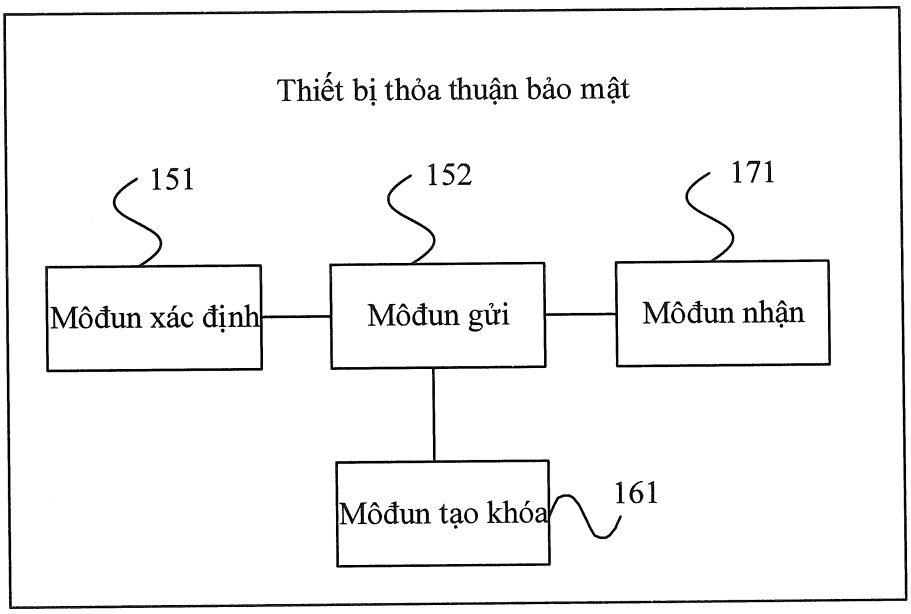
Thiết bị thỏa thuận bảo mật
151
152
171
Môđun xác định
Môđun gửi
Môđun nhận
Môđun tạo khóa
161

FIG.17

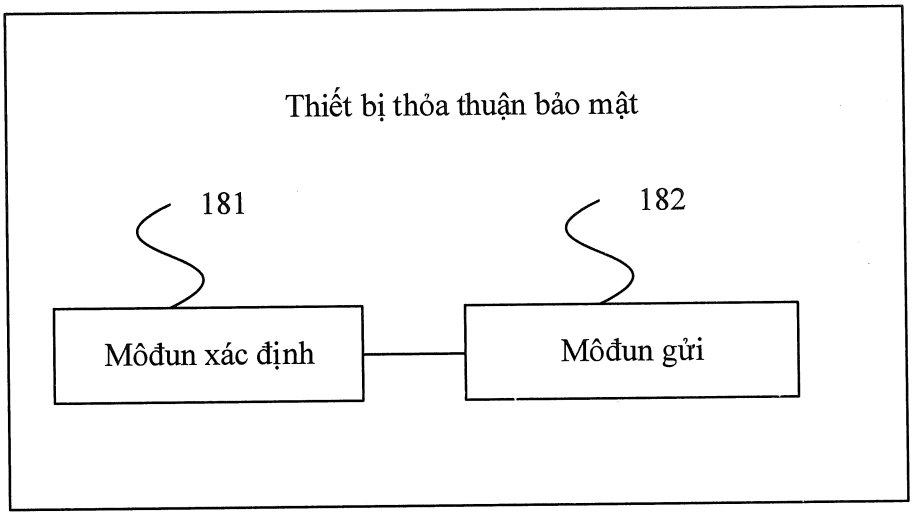
Thiết bị thỏa thuận bảo mật
181
182
Môđun xác định
Môđun gửi

FIG.18

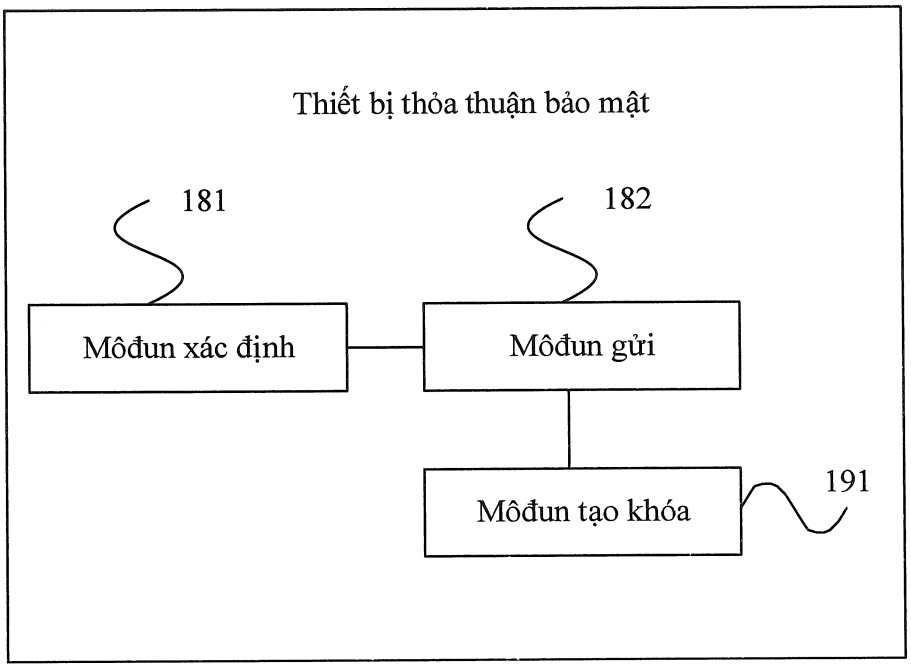
Thiết bị thỏa thuận bảo mật
181
182
Môđun xác định
Môđun gửi
Môđun tạo khóa
191

FIG.19

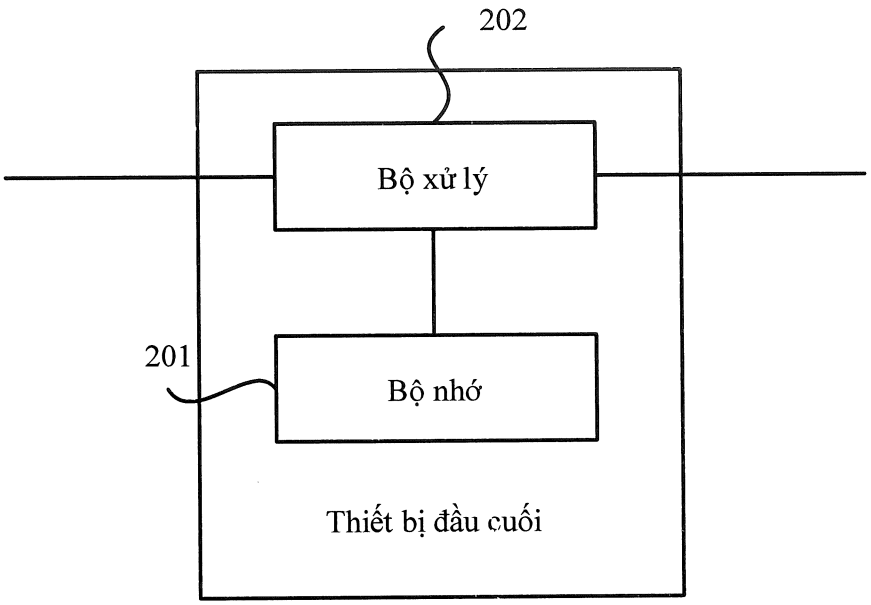
202
Bộ xử lý
201
Bộ nhớ
Thiết bị đầu cuối

FIG.20

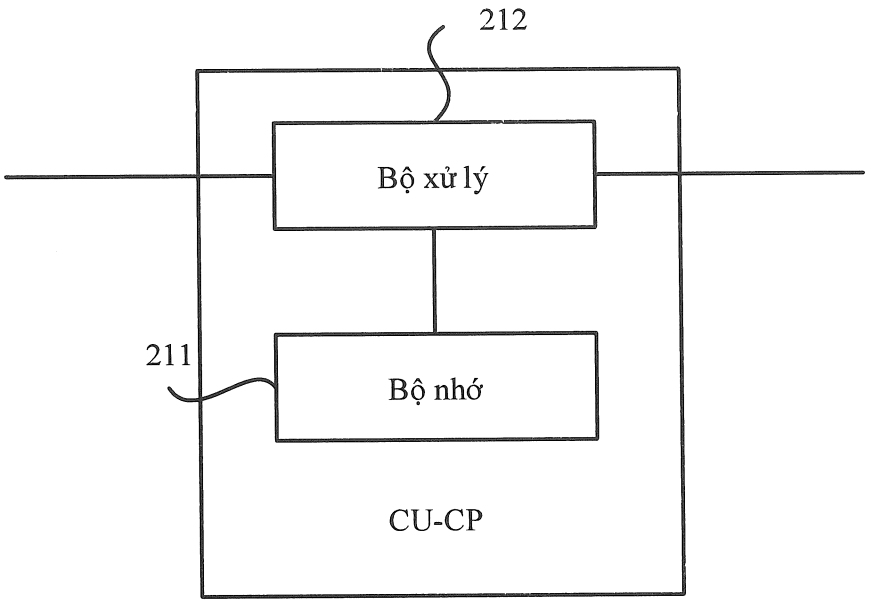

FIG.21

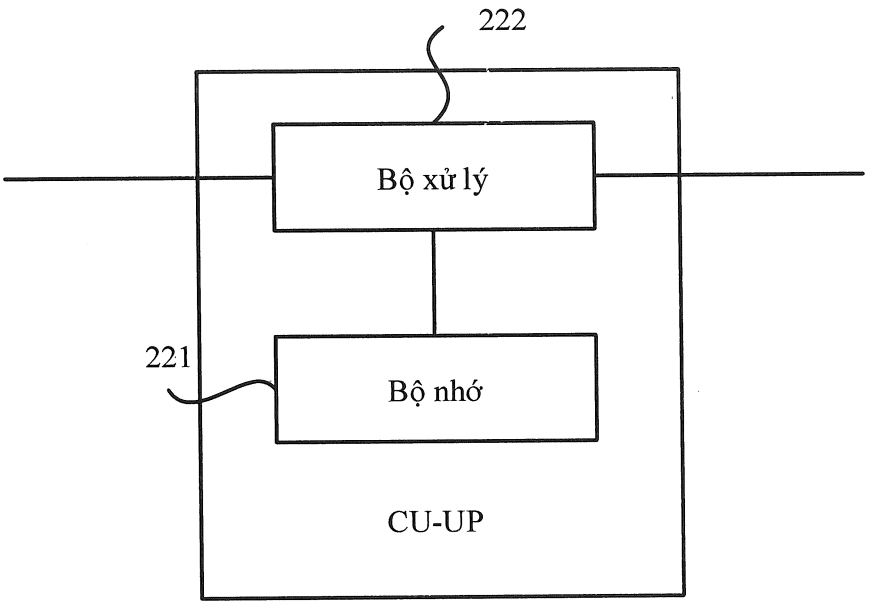

FIG.22