(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) **1-0041915**

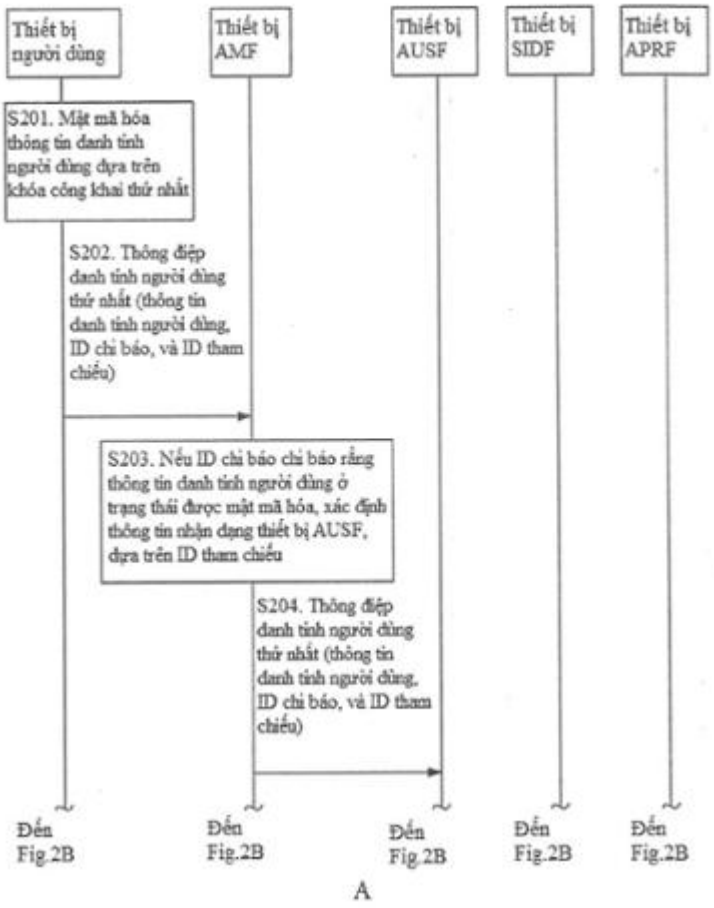
(51)[2020.01] **H04L 9/32**; H04L 9/08

(13) **B**

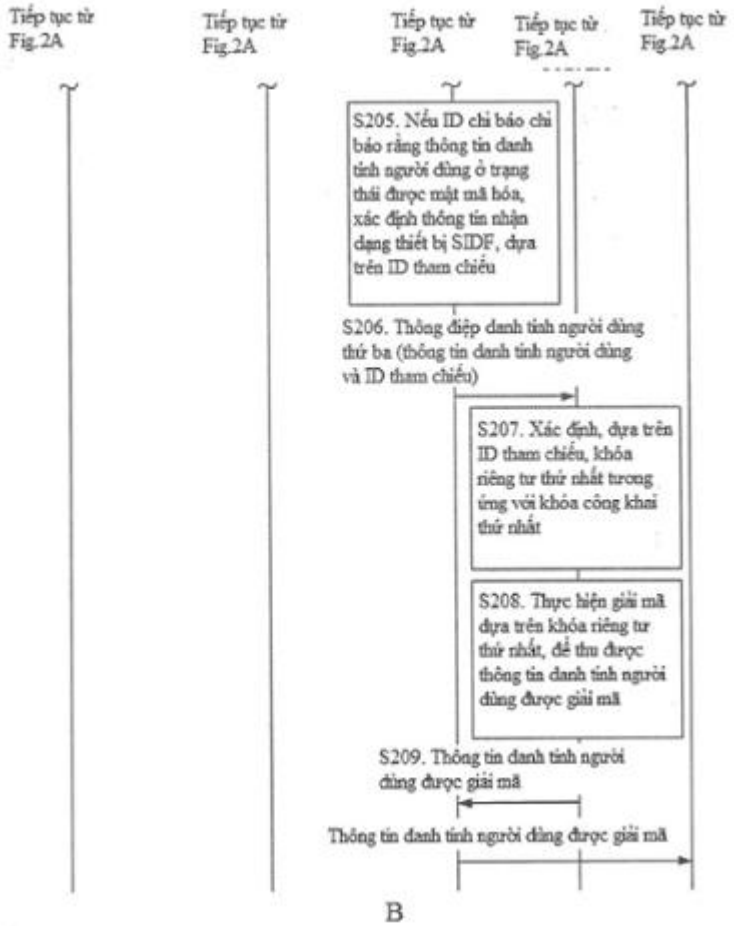
(21) 1-2020-02322
(22) 29/09/2017
(86) PCT/SG2017/050492 29/09/2017
(87) WO2019/066720 04/04/2019
(45) 25/12/2024 441
(43) 27/07/2020 388
(73) HUAWEI INTERNATIONAL PTE. LTD. (SG)
51, Changi Business Park Central 2, #07-08, The Signature, Singapore 486066, Singapore
(72) WANG, Haiguang (CN); KANG, Xin (CN); LEI, Zhongding (SG); LIU, Fei (CN).
(74) Công ty Luật TNHH Phạm và Liên danh (PHAM & ASSOCIATES)

(54) PHƯƠNG PHÁP VÀ THIẾT BỊ QUẢN LÝ KHÓA

(57) Sáng chế đề xuất phương pháp và thiết bị quản lý khóa, và phương pháp quản lý khóa bao gồm: mật mã hóa, bởi thiết bị người dùng (user equipment, UE), thông tin danh tính người dùng dựa trên khóa công khai thứ nhất; gửi, bởi UE, thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, bộ nhận dạng (Identifier, ID) chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và gửi, bởi thiết bị mạng thứ nhất đến thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông điệp danh tính người dùng thứ ba, thiết bị mạng thứ hai có thể xác định, theo bảng ánh xạ được lưu trữ trước giữa cặp khóa công khai - riêng tư và ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.


Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
Thiết bị APRF
S201. Mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất
S202. Thông điệp danh tính người dùng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S203. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị AUSF, dựa trên ID tham chiếu
S204. Thông điệp danh tính người dùng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B

A


Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
S205. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị SIDF, dựa trên ID tham chiếu
S206. Thông điệp danh tính người dùng thứ ba (thông tin danh tính người dùng và ID tham chiếu)
S207. Xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất
S208. Thực hiện giải mã dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã
S209. Thông tin danh tính người dùng được giải mã
Thông tin danh tính người dùng được giải mã

B

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến lĩnh vực công nghệ truyền thông, và cụ thể là, đến phương pháp và thiết bị quản lý khóa.

Tình trạng kỹ thuật của sáng chế

Để cải thiện bảo mật của thông tin danh tính người dùng, trước khi thông tin danh tính người dùng được gửi, thông tin danh tính người dùng thường được mật mã hóa bằng cách sử dụng khóa công khai của mạng tại nhà, sao cho thông tin danh tính người dùng được mật mã hóa được gửi.

Hệ thống mật mã hóa khóa công khai hiện tại có thể bao gồm thiết bị người dùng (user equipment, UE), bộ phận chức năng truy nhập và quản lý di động (Access and Mobility Function, AMF), bộ phận chức năng khối xác thực (Authentication Unit Function, AUSF), và bộ phận chức năng kho chứa xác thực (Authentication Repository Function, ARPF). Trước khi gửi thông tin danh tính người thuê bao lâu dài (subscriber permanent identity information, SUPI), UE mật mã hóa thông tin danh tính người dùng bằng cách sử dụng khóa công khai, và gửi thông tin danh tính người dùng được mật mã hóa đến thiết bị AMF mà lưu trữ khóa riêng tư tương ứng với khóa công khai. Sau khi nhận thông tin danh tính người dùng được mật mã hóa, thiết bị AMF gửi thông tin danh tính người dùng được mật mã hóa đến thiết bị AUSF, sao cho thiết bị AUSF hoặc bộ phận giải mã khác giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư tương ứng với khóa công khai, để thu được thông tin danh tính người dùng được giải mã, và gửi thông tin danh tính người dùng thu được đến bộ phận ARPF, để thực hiện xác thực trên thông tin danh tính người dùng.

Tuy nhiên, trong hệ thống mạng hiện tại, cặp khóa công khai - riêng tư bất kỳ được sử dụng để mật mã hóa và giải mã có vòng đời, và trước khi kết thúc vòng đời của cặp khóa công khai - riêng tư, cặp khóa công khai - riêng tư mới cần quá trình phân phối. Do vậy, trong hệ thống mật mã hóa khóa công khai hiện tại, ít nhất một tập hợp cặp khóa công khai - riêng tư được phép mật mã hóa và giải

mã thông tin danh tính người dùng. Khi có ít nhất một tập hợp cặp khóa công khai - riêng tư trong hệ thống mật mã hóa khóa công khai, thiết bị AUSF không thể xác định cặp khóa công khai - riêng tư mà có khóa công khai được sử dụng bởi UE để mật mã hóa thông tin danh tính người dùng, và kết quả là, không thể xác định cặp khóa công khai - riêng tư mà khóa riêng tư của nó được sử dụng để giải mã thông tin danh tính người dùng được mật mã hóa, dẫn đến hiệu suất giải mã dữ liệu bị giảm.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp và thiết bị quản lý khóa, để cải thiện hiệu suất giải mã dữ liệu.

Theo khía cạnh thứ nhất, phương án thực hiện sáng chế đề xuất phương pháp quản lý khóa, và phương pháp quản lý khóa có thể bao gồm các bước:

mật mã hóa, bởi UE, thông tin danh tính người dùng dựa trên khóa công khai thứ nhất; và

gửi, bởi UE, thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người sử dụng thứ nhất dựa trên ID chỉ báo và ID tham chiếu.

Có thể hiểu rằng khóa công khai thứ nhất có thể được lưu trữ trước, hoặc có thể tạm thời thu được để sử dụng.

Có thể hiểu rằng các khóa công khai được lưu trữ trong UE, và ID tham chiếu cần được sử dụng để chỉ báo khóa công khai được sử dụng để mật mã hóa. Nói theo cách khác, các khóa công khai tương ứng một - một với các ID tham chiếu. Chẳng hạn, nếu có 100 khóa công khai, khoảng giá trị của các ID tham chiếu là từ 0 đến 99. Chắc chắn là, ID tham chiếu cũng có thể là một phần bị chặn từ khóa công khai, hoặc tổ hợp của các giá trị hoặc một số bit của khóa công khai. Chẳng hạn, nếu khóa công khai có độ dài 50 bit, ID tham chiếu có thể là tổ hợp của các giá trị trên bit thứ nhất, thứ hai, thứ tư, thứ tám, thứ mười sau, và thứ ba mươi

hai.

Nên lưu ý rằng mặc dù thông điệp danh tính người sử dụng thứ nhất bao gồm ba tham số, thông điệp danh tính người sử dụng thứ nhất có thể được biểu diễn bằng hai giá trị: Giá trị thứ nhất là thông tin danh tính người dùng, và giá trị thứ hai có thể chỉ báo ID tham chiếu, hoặc có thể chỉ báo ID chỉ báo.

Chẳng hạn, ID chỉ báo bằng 0, chỉ báo rằng thông tin danh tính người dùng không được mật mã hóa, và ID tham chiếu cũng bằng 0 ở thời điểm này, chỉ báo rằng ID khóa công khai là trống. Chẳng hạn, ID chỉ báo là giá trị khác 0 (Chẳng hạn, a value greater than 0), giá trị khác 0 chỉ báo rằng thông tin danh tính người dùng được mật mã hóa, và giá trị khác 0 có thể chỉ báo chỉ mục của khóa công khai được sử dụng để mật mã hóa. Chẳng hạn, nếu giá trị khác 0 bằng 100, và được sử dụng để chỉ báo rằng danh tính người dùng được mật mã hóa, khóa công khai được sử dụng để mật mã hóa có ID tham chiếu 100.

Ngoài ra, nên lưu ý rằng thông điệp danh tính người sử dụng thứ nhất bao gồm ba tham số, và có thể được biểu diễn bằng ba giá trị: Giá trị thứ nhất là thông tin danh tính người dùng, ID thứ hai chỉ báo ID chỉ báo, và giá trị thứ ba có thể chỉ báo ID tham chiếu. Điều này không bị giới hạn theo sáng chế.

Có thể nhận biết rằng theo phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế, UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và gửi, đến thiết bị mạng thứ hai bằng cách sử dụng thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng được mật mã hóa và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông điệp danh tính người dùng thứ ba, thiết bị mạng thứ hai có thể xác định, theo bảng ánh xạ được lưu trữ trước giữa cặp khóa riêng tư-công khai và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi, trước khi mật mã hóa, bởi UE, thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, phương pháp có thể còn bao gồm các bước:

xác định, bởi UE, liệu mật mã hóa thông tin danh tính người dùng; và

khi xác định không mật mã hóa thông tin danh tính người dùng, gửi, bởi UE, thông điệp danh tính người dùng thứ hai đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ hai bao gồm thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo.

Theo triển khai khả thi, trước khi mật mã hóa, bởi UE, thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, phương pháp có thể còn bao gồm bước:

xác định, bởi UE, liệu khóa công khai thứ nhất trong chu kỳ hợp lệ; và

việc mật mã hóa, bởi UE, thông tin danh tính người dùng dựa trên khóa công khai thứ nhất bao gồm bước:

khi khóa công khai thứ nhất trong chu kỳ hợp lệ, mật mã hóa, bởi UE, thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, nhờ đó cải thiện bảo mật của thông tin danh tính người dùng.

Có thể hiểu rằng mỗi khóa công khai có ngày tạo và ngày hết hạn tương ứng, và ngày hiện tại có thể được so sánh với ngày hết hạn, để xác định liệu khóa công khai trong chu kỳ hợp lệ.

Theo triển khai khả thi, khi bằng 0, ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa.

Một cách tùy chọn, ID chỉ báo có thể được biểu diễn dưới dạng số hoặc dưới dạng chuỗi ký tự. Các số hoặc các chuỗi ký tự khác nhau được sử dụng để phân biệt liệu thông tin danh tính người dùng ở trạng thái được mật mã hóa. Chẳng hạn, 0 chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, và 1 chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa; và ngược lại.

Theo khía cạnh thứ hai, phương án thực hiện sáng chế đề xuất phương pháp quản lý khóa, và phương pháp có thể bao gồm các bước:

nhận, bởi thiết bị mạng thứ nhất, thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để

đánh chỉ mục khóa công khai thứ nhất; và

nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, gửi, bởi thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên ID tham chiếu, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu, sao cho thiết bị mạng thứ hai xử lý thông tin danh tính người dùng dựa trên ID tham chiếu.

Có thể nhận biết rằng sau khi nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, thiết bị mạng thứ nhất gửi, đến thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng được mật mã hóa và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông điệp danh tính người dùng thứ ba, thiết bị mạng thứ hai có thể xác định, theo bảng ánh xạ được lưu trữ trước giữa cặp khóa riêng tư-công khai và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi, việc gửi, bởi thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên ID tham chiếu có thể bao gồm:

gửi, bởi thiết bị mạng thứ nhất, thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ ba dựa trên ID tham chiếu, sao cho thiết bị mạng thứ ba gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai khi ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa.

Theo triển khai khả thi, việc gửi, bởi thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên ID tham chiếu có thể bao gồm:

xác định, bởi thiết bị mạng thứ nhất dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất; và

gửi, bởi thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ ba to thiết bị mạng thứ hai dựa trên thông tin nhận dạng của thiết bị mạng thứ hai.

Theo triển khai khả thi, phương pháp có thể còn bao gồm các bước:

nhận, bởi thiết bị mạng thứ nhất, thông điệp danh tính thứ tư được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất;

mật mã hóa, bởi thiết bị mạng thứ nhất, thông tin danh tính người dùng được giải mã bằng cách sử dụng khóa công khai thứ nhất, để tạo thông tin danh tính người dùng cần được kiểm chứng;

so sánh, bởi thiết bị mạng thứ nhất, thông tin danh tính người dùng cần được kiểm chứng and thông tin danh tính người dùng; và

nếu thông tin danh tính người dùng cần được kiểm chứng giống như thông tin danh tính người dùng, gửi, bởi thiết bị mạng thứ nhất, thông tin lệnh đến thiết bị mạng thứ ba, trong đó thông điệp lệnh bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Có thể nhận biết rằng thiết bị mạng thứ nhất so sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng được mật mã hóa, để xác định, dựa trên kết quả so sánh, liệu có thực hiện đăng ký và xác thực trên thông tin danh tính người dùng, nhờ đó thỏa mãn điều kiện ngăn chặn hợp pháp việc kiểm chứng danh tính được mật mã hóa.

Theo triển khai khả thi, việc nhận, bởi thiết bị mạng thứ nhất, thông tin danh tính người dùng thứ tư được gửi bởi thiết bị mạng thứ hai có thể bao gồm bước:

nhận, bởi thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ tư được chuyển tiếp bởi thiết bị mạng thứ ba.

Theo triển khai khả thi, trước khi xác định, bởi thiết bị mạng thứ nhất dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất, phương pháp có thể còn bao gồm các bước:

nhận, bởi thiết bị mạng thứ nhất, bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

việc xác định, bởi thiết bị mạng thứ nhất dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất bao gồm bước:

xác định, bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất.

Theo khía cạnh thứ ba, phương án thực hiện sáng chế đề xuất phương pháp quản lý khóa, và phương pháp có thể bao gồm các bước:

nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất;

xác định, bởi thiết bị mạng thứ hai dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, trong đó khóa công khai thứ nhất và khóa riêng tư thứ nhất là cặp khóa riêng tư-công khai thứ nhất;

giải mã, bởi thiết bị mạng thứ hai, thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã; và

gửi, bởi thiết bị mạng thứ hai, thông tin danh tính người dùng được giải mã đến thiết bị mạng thứ ba, sao cho thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Có thể nhận biết rằng sau khi nhận thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng được mật mã hóa và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, thiết bị mạng thứ hai có thể xác định, theo bảng ánh xạ được lưu trữ trước giữa cặp khóa riêng tư-công khai và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi, việc nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất có thể bao gồm bước:

nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được

chuyển tiếp bởi thiết bị mạng thứ ba.

Theo triển khai khả thi, trước khi xác định, bởi thiết bị mạng thứ hai dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, phương pháp có thể còn bao gồm bước:

xác định, bởi thiết bị mạng thứ hai, liệu khóa công khai thứ nhất trong chu kỳ hợp lệ; và

việc xác định, bởi thiết bị mạng thứ hai dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất bao gồm bước:

khi khóa công khai thứ nhất trong chu kỳ hợp lệ, xác định, bởi thiết bị mạng thứ hai dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất.

Có thể nhận biết rằng, liệu khóa công khai thứ nhất trong chu kỳ hợp lệ được xác định, và khi khóa công khai thứ nhất trong chu kỳ hợp lệ, thiết bị mạng thứ hai xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi, trước khi nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất, phương pháp có thể còn bao gồm bước:

thu thập, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai và N ID tham chiếu, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N cặp khóa riêng tư-công khai, cặp khóa riêng tư-công khai thứ nhất là một trong N cặp khóa riêng tư-công khai, và N là số nguyên lớn hơn 0.

Theo triển khai khả thi, việc thu thập, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai và N ID tham chiếus có thể bao gồm các bước:

tạo, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai; và

phân phối, bởi thiết bị mạng thứ hai, các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Theo triển khai khả thi, việc thu thập, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai và N ID tham chiếu có thể bao gồm các bước:

tạo, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai; và

gửi, bởi thiết bị mạng thứ hai, thông điệp yêu cầu ID tham chiếu đến thiết bị

mạng thứ tư, trong đó thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết bị mạng thứ tư phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai; và

nhận, bởi thiết bị mạng thứ hai, các khóa công khai trong N cặp khóa riêng tư-công khai và N ID tham chiếu mà được gửi bởi thiết bị mạng thứ tư.

Theo triển khai khả thi, việc thu thập, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai và N ID tham chiếus có thể bao gồm:

nhận, bởi thiết bị mạng thứ hai, N cặp khóa riêng tư-công khai và N ID tham chiếu mà được gửi bởi thiết bị mạng thứ tư.

Theo triển khai khả thi, trước khi nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất, phương pháp có thể còn bao gồm các bước:

thu thập, bởi thiết bị mạng thứ hai, khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai, và thu thập ID tham chiếu từ N ID tham chiếu; và

gửi, bởi thiết bị mạng thứ hai, khóa công khai thứ nhất và ID tham chiếu đến UE.

Theo triển khai khả thi, sau khi giải mã, bởi thiết bị mạng thứ hai, thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã, phương pháp có thể còn bao gồm bước:

gửi, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người dùng thứ tư dựa trên khóa công khai thứ nhất.

Theo triển khai khả thi, việc gửi, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất có thể bao gồm bước:

chuyển tiếp, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất bằng cách sử dụng thiết bị mạng thứ ba.

Theo triển khai khả thi, phương pháp có thể còn bao gồm:

khi khóa công khai thứ nhất không nằm trong chu kỳ hợp lệ, gửi, bởi thiết bị

mạng thứ hai, thông điệp yêu cầu cập nhật khóa công khai đến UE, trong đó thông điệp yêu cầu cập nhật khóa công khai được sử dụng để ra lệnh UE cập nhật khóa công khai thứ nhất, mật mã hóa thông tin danh tính người dùng bằng cách sử dụng khóa công khai hợp lệ, nhờ đó cải thiện bảo mật dữ liệu.

Theo triển khai khả thi, trước khi nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất, phương pháp có thể còn bao gồm các bước:

gửi, bởi thiết bị mạng thứ hai, bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu đến thiết bị mạng thứ nhất, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

việc nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất có thể bao gồm bước:

nhận, bởi thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu.

Theo khía cạnh thứ tư, phương án thực hiện sáng chế đề xuất phương pháp quản lý khóa, và phương pháp có thể bao gồm bước:

nhận, bởi thiết bị mạng thứ ba, thông điệp danh tính người sử dụng thứ nhất được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất;

nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định, bởi thiết bị mạng thứ ba dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu; và

gửi, bởi thiết bị mạng thứ ba, thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên thông tin nhận dạng của thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ

nhất, sao cho thiết bị mạng thứ hai xử lý thông điệp danh tính người dùng thứ ba dựa trên ID tham chiếu.

Có thể nhận biết rằng sau khi nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, thiết bị mạng thứ ba gửi, đến thiết bị mạng thứ hai, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng được mật mã hóa và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông điệp danh tính người dùng thứ ba, thiết bị mạng thứ hai có thể xác định, theo bảng ánh xạ được lưu trữ trước giữa cặp khóa riêng tư-công khai và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi, phương pháp còn bao gồm các bước:

nhận, bởi thiết bị mạng thứ ba, thông điệp danh tính người dùng thứ tư được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất; và

gửi, bởi thiết bị mạng thứ ba, thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người dùng thứ tư dựa trên khóa công khai thứ nhất.

Theo triển khai khả thi, sau khi gửi, bởi thiết bị mạng thứ ba, thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, phương pháp còn bao gồm bước:

nhận, bởi thiết bị mạng thứ ba, thông tin lệnh được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp lệnh bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Theo triển khai khả thi, trước khi xác định, bởi thiết bị mạng thứ ba dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu, phương pháp có thể còn bao gồm bước:

nhận, bởi thiết bị mạng thứ ba, bảng ánh xạ giữa thông tin nhận dạng của

thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất lafmoojt trong N khóa công khai, và N là số nguyên lớn hơn 0; và

việc xác định, bởi thiết bị mạng thứ ba dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu bao gồm các bước:

xác định, bởi thiết bị mạng thứ ba theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu.

Theo triển khai khả thi, sau khi nhận, bởi thiết bị mạng thứ ba, bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, phương pháp có thể còn bao gồm các bước:

gửi, bởi thiết bị mạng thứ ba, bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ ba và N ID tham chiếu đến thiết bị mạng thứ nhất; và

việc nhận, bởi thiết bị mạng thứ ba, thông điệp danh tính người sử dụng thứ nhất được gửi bởi thiết bị mạng thứ nhất bao gồm bước:

nhận, bởi thiết bị mạng thứ ba, thông điệp danh tính người sử dụng thứ nhất của UE được chuyển tiếp bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ ba và N ID tham chiếu.

Theo khía cạnh thứ năm, phương án thực hiện sáng chế đề xuất phương pháp quản lý khóa, và phương pháp có thể bao gồm các bước:

thu thập, bởi thiết bị mạng thứ tư, N khóa công khai, trong đó N là số nguyên lớn hơn 0;

phân phối, bởi thiết bị mạng thứ tư, N ID tham chiếu đến N khóa công khai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai; và

gửi, bởi thiết bị mạng thứ tư, N khóa công khai và N ID tham chiếu đến thiết bị mạng thứ hai, sao cho thiết bị mạng thứ hai thu được N khóa công khai và N ID tham chiếu.

Có thể nhận biết rằng thiết bị mạng thứ tư gửi N khóa công khai và N ID tham chiếu đến thiết bị mạng thứ hai, sao cho khi nhận thông điệp danh tính

người dùng thứ ba, thiết bị mạng thứ hai có thể xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi, việc thu thập, bởi thiết bị mạng thứ tư, N khóa công khai có thể bao gồm bước:

tạo, bởi thiết bị mạng thứ tư, N cặp khóa riêng tư-công khai, trong đó each cặp khóa công khai - riêng tư bao gồm khóa công khai và khóa riêng tư, và N khóa công khai là khóa công khai trong N cặp khóa riêng tư-công khai; và

việc gửi, bởi thiết bị mạng thứ tư, N khóa công khai và N ID tham chiếu đến thiết bị mạng thứ hai bao gồm bước:

gửi, bởi thiết bị mạng thứ tư, N cặp khóa riêng tư-công khai và N ID tham chiếu đến thiết bị mạng thứ hai.

Theo triển khai khả thi, việc thu thập, bởi thiết bị mạng thứ tư, N khóa công khai có thể bao gồm bước:

nhận, bởi thiết bị mạng thứ tư, thông điệp yêu cầu ID tham chiếu được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết bị mạng thứ tư phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Theo triển khai khả thi, phương pháp có thể còn bao gồm các bước:

thu thập, bởi thiết bị mạng thứ tư, khóa công khai thứ nhất từ N khóa công khai, và thu thập, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và

gửi, bởi thiết bị mạng thứ tư, khóa công khai thứ nhất và ID tham chiếu đến UE.

Theo khía cạnh thứ sáu, phương án thực hiện sáng chế đề xuất thiết bị quản lý khóa, và thiết bị có thể bao gồm:

khối mật mã hóa, được tạo cấu hình để mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất; và

khối gửi, được tạo cấu hình để gửi thông điệp danh tính người sử dụng thứ

nhất đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người sử dụng thứ nhất dựa trên ID chỉ báo và ID tham chiếu.

Theo triển khai khả thi, khối mật mã hóa còn được tạo cấu hình để xác định liệu mật mã hóa thông tin danh tính người dùng; và

khối gửi còn được tạo cấu hình để: khi được xác định rằng thông tin danh tính người dùng sẽ không được mật mã hóa, gửi, bởi UE, thông điệp danh tính người dùng thứ hai đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ hai bao gồm thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo.

Theo triển khai khả thi, thiết bị có thể còn bao gồm:

khối đánh giá, được tạo cấu hình để xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ, trong đó

khối mật mã hóa được tạo cấu hình cụ thể để: khi khóa công khai thứ nhất trong chu kỳ hợp lệ, mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất.

Đối với các nguyên lý triển khai và các hiệu quả có lợi của các khối trong thiết bị quản lý khóa theo phương án thực hiện, tham khảo phương án thực hiện của phương pháp quản lý khóa theo khía cạnh thứ nhất. Các chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ bảy, phương án thực hiện sáng chế đề xuất thiết bị quản lý khóa, và thiết bị có thể bao gồm:

khối nhận, được tạo cấu hình để nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và

khối gửi, được tạo cấu hình để: nếu ID chỉ báo chỉ báo rằng thông tin danh

tính người dùng ở trạng thái được mật mã hóa, gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên ID tham chiếu, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu, sao cho thiết bị mạng thứ hai xử lý thông tin danh tính người dùng dựa trên ID tham chiếu.

Theo triển khai khả thi, khối gửi được tạo cấu hình cụ thể để gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ ba dựa trên ID tham chiếu, sao cho thiết bị mạng thứ ba gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai khi ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa.

Theo triển khai khả thi, khối gửi được tạo cấu hình cụ thể để xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất, và gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên thông tin nhận dạng của thiết bị mạng thứ hai.

Theo triển khai khả thi, thiết bị có thể còn bao gồm khối mật mã hóa và khối so sánh, trong đó

khối nhận còn được tạo cấu hình để nhận thông điệp danh tính thứ tư được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất;

khối mật mã hóa được tạo cấu hình để mật mã hóa thông tin danh tính người dùng được giải mã bằng cách sử dụng khóa công khai thứ nhất, để tạo thông tin danh tính người dùng cần được kiểm chứng;

khối so sánh được tạo cấu hình để so sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng; và

khối gửi còn được tạo cấu hình để: nếu thông tin danh tính người dùng cần được kiểm chứng giống như thông tin danh tính người dùng, gửi thông tin lệnh đến thiết bị mạng thứ ba, trong đó thông điệp lệnh bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Theo triển khai khả thi, khối nhận được tạo cấu hình cụ thể để nhận thông

điệp danh tính người dùng thứ tư được chuyển tiếp bởi thiết bị mạng thứ ba.

Theo triển khai khả thi, thiết bị có thể còn bao gồm khối xác định, trong đó

khối nhận còn được tạo cấu hình để nhận bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

việc khối xác định được tạo cấu hình để xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất bao gồm:

khối xác định còn được tạo cấu hình để xác định, theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất.

Đối với các nguyên lý triển khai và các hiệu quả có lợi của các khối trong thiết bị quản lý khóa theo phương án thực hiện, tham khảo phương án thực hiện của phương pháp quản lý khóa theo khía cạnh thứ hai. Các chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ tám, phương án thực hiện sáng chế đề xuất thiết bị quản lý khóa, và thiết bị có thể bao gồm:

khối nhận, được tạo cấu hình để nhận thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất;

khối xác định, được tạo cấu hình để xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, trong đó khóa công khai thứ nhất và khóa riêng tư thứ nhất là cặp khóa riêng tư-công khai thứ nhất;

khối giải mã, được tạo cấu hình để giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã; và

khối gửi, được tạo cấu hình để gửi thông tin danh tính người dùng được giải mã đến thiết bị mạng thứ ba, sao cho thiết bị mạng thứ ba xử lý thông tin danh

tính người dùng được giải mã.

Theo triển khai khả thi, khối nhận được tạo cấu hình cụ thể để nhận thông điệp danh tính người dùng thứ ba được chuyển tiếp bởi thiết bị mạng thứ ba.

Theo triển khai khả thi, thiết bị có thể còn bao gồm:

khối đánh giá, được tạo cấu hình để xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ, trong đó

khối xác định được tạo cấu hình cụ thể để: khi khóa công khai thứ nhất trong chu kỳ hợp lệ, xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất.

Theo triển khai khả thi, thiết bị có thể còn bao gồm:

khối thu thập, được tạo cấu hình để thu được N cặp khóa riêng tư-công khai và N ID tham chiếu, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N cặp khóa riêng tư-công khai, cặp khóa riêng tư-công khai thứ nhất là một trong N cặp khóa riêng tư-công khai, và N là số nguyên lớn hơn 0.

Theo triển khai khả thi, khối thu thập được tạo cấu hình cụ thể để tạo N cặp khóa riêng tư-công khai và phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Theo triển khai khả thi, khối thu thập được tạo cấu hình cụ thể để tạo N cặp khóa riêng tư-công khai; và khối gửi còn được tạo cấu hình để gửi thông điệp yêu cầu ID tham chiếu đến thiết bị mạng thứ tư, trong đó thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết bị mạng thứ tư phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai; và

khối nhận còn được tạo cấu hình để nhận các khóa công khai trong N cặp khóa riêng tư-công khai và N ID tham chiếu được gửi bởi thiết bị mạng thứ tư.

Theo triển khai khả thi, khối nhận còn được tạo cấu hình để nhận N cặp khóa riêng tư-công khai và N ID tham chiếu được gửi bởi thiết bị mạng thứ tư.

Theo triển khai khả thi, khối thu thập còn được tạo cấu hình để thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai và thu được ID tham chiếu

từ N ID tham chiếu; và

khối gửi còn được tạo cấu hình để gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Theo triển khai khả thi, khối gửi còn được tạo cấu hình để gửi thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người dùng thứ tư dựa trên khóa công khai thứ nhất.

Theo triển khai khả thi, khối gửi còn được tạo cấu hình để chuyển tiếp thông điệp danh tính người dùng thứ tư to thiết bị mạng thứ nhất bằng cách sử dụng thiết bị mạng thứ ba.

Theo triển khai khả thi, khối gửi còn được tạo cấu hình để gửi thông điệp yêu cầu cập nhật khóa công khai đến UE khi khóa công khai thứ nhất không nằm trong chu kỳ hợp lệ, trong đó thông điệp yêu cầu cập nhật khóa công khai được sử dụng để ra lệnh UE cập nhật khóa công khai thứ nhất.

Theo triển khai khả thi, khối nhận còn được tạo cấu hình để gửi bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu đến thiết bị mạng thứ nhất, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

khối nhận được tạo cấu hình cụ thể để nhận thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu.

Đối với các nguyên lý triển khai và các hiệu quả có lợi của các khối in thiết bị quản lý khóa theo phương án thực hiện, tham khảo phương án thực hiện của phương pháp quản lý khóa theo khía cạnh thứ ba. Các chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ chín, phương án thực hiện sáng chế đề xuất thiết bị quản lý khóa, và thiết bị có thể bao gồm:

khối nhận, được tạo cấu hình để nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử

dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất;

khối xác định, được tạo cấu hình để: nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu; và

khối gửi, được tạo cấu hình để gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên thông tin nhận dạng của thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho thiết bị mạng thứ hai xử lý thông điệp danh tính người dùng thứ ba dựa trên ID tham chiếu.

Theo triển khai khả thi, khối nhận còn được tạo cấu hình để nhận thông điệp danh tính người dùng thứ tư được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã and khóa công khai thứ nhất; và

khối gửi còn được tạo cấu hình để gửi thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người dùng thứ tư dựa trên khóa công khai thứ nhất.

Theo triển khai khả thi, khối nhận còn được tạo cấu hình để nhận thông tin lệnh được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp lệnh bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Theo triển khai khả thi, khối nhận còn được tạo cấu hình để nhận bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

khối xác định được tạo cấu hình cụ thể để xác định, theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu, thông tin nhận

dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu.

Theo triển khai khả thi, khối gửi còn được tạo cấu hình để gửi bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ ba và N ID tham chiếu đến thiết bị mạng thứ nhất; và

khối nhận được tạo cấu hình cụ thể để nhận thông điệp danh tính người sử dụng thứ nhất của UE được chuyển tiếp bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ ba và N ID tham chiếu.

Đối với các nguyên lý triển khai và các hiệu quả có lợi của các khối ở thiết bị quản lý khóa theo phương án thực hiện, tham khảo phương án thực hiện của phương pháp quản lý khóa theo khía cạnh thứ tư. Các chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ mười, phương án thực hiện sáng chế đề xuất thiết bị quản lý khóa, và thiết bị có thể bao gồm:

khối thu thập, được tạo cấu hình để thu được N khóa công khai, trong đó N là số nguyên lớn hơn 0;

khối phân phối, được tạo cấu hình để phân phối N ID tham chiếu đến N khóa công khai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai; và

khối gửi, được tạo cấu hình để gửi N khóa công khai và N ID tham chiếu đến thiết bị mạng thứ hai, sao cho thiết bị mạng thứ hai thu được N khóa công khai và N ID tham chiếu.

Theo triển khai khả thi, khối thu thập được tạo cấu hình cụ thể để tạo N cặp khóa riêng tư-công khai, trong đó mỗi cặp khóa công khai - riêng tư bao gồm khóa công khai và khóa riêng tư, và N khóa công khai là các khóa công khai trong N cặp khóa riêng tư-công khai; và

khối gửi còn được tạo cấu hình để gửi N cặp khóa riêng tư-công khai và N ID tham chiếu đến thiết bị mạng thứ hai.

Theo triển khai khả thi, khối nhận còn được tạo cấu hình để nhận thông điệp yêu cầu ID tham chiếu được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết

bị mạng thứ tư phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Theo triển khai khả thi, khối thu thập còn được tạo cấu hình để thu được khóa công khai thứ nhất từ N khóa công khai, và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa thứ nhất; và

khối gửi còn được tạo cấu hình để gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Đối với các nguyên lý triển khai và các hiệu quả có lợi của các khối trong thiết bị quản lý khóa theo phương án thực hiện, tham khảo phương án thực hiện của phương pháp quản lý khóa theo khía cạnh thứ nhất. Các chi tiết không được mô tả lại ở đây.

Theo khía cạnh thứ mười một, phương án thực hiện sáng chế còn đề xuất thiết bị, bao gồm bộ xử lý và bộ nhớ.

Bộ nhớ được tạo cấu hình để lưu trữ lệnh, và bộ xử lý được tạo cấu hình để thực thi lệnh được lưu trữ trong bộ nhớ. Khi bộ xử lý thực thi lệnh được lưu trữ trong bộ nhớ, bộ phận này thực hiện phương pháp theo phương án thực hiện bất kỳ ở khía cạnh thứ nhất đến khía cạnh thứ năm.

Theo khía cạnh thứ mười hai, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính đọc được, và vật lưu trữ máy tính đọc được lưu trữ lệnh.

Khi ít nhất một bộ xử lý của UE thực thi lệnh, UE thực hiện phương pháp quản lý khóa theo các phương án thực hiện phương pháp theo khía cạnh thứ nhất đến khía cạnh thứ năm.

Theo khía cạnh thứ mười ba, phương án thực hiện sáng chế đề xuất vật lưu trữ máy tính đọc được, và vật lưu trữ máy tính đọc được lưu trữ lệnh. Khi ít nhất một bộ xử lý của thiết bị mạng thực thi lệnh, thiết bị mạng thực hiện phương pháp quản lý khóa theo các phương án thực hiện phương pháp theo khía cạnh thứ nhất đến khía cạnh thứ năm.

Theo phương pháp và thiết bị quản lý khóa theo các phương án thực hiện sáng chế, khi xác định mật mã hóa thông tin danh tính người dùng, UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ nhất, trong

đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông tin danh tính người dùng thứ nhất, thiết bị mạng thứ nhất xác định, dựa trên ID chỉ báo, liệu thông tin danh tính người dùng ở trạng thái được mật mã hóa, và nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, thiết bị mạng thứ nhất xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất, và gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai. Do vậy, khi nhận thông điệp danh tính người dùng thứ ba của UE, thiết bị mạng thứ hai giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã, và thực hiện xác thực trên thông tin danh tính người dùng bằng cách sử dụng bộ phận ARPF. Có thể nhận biết rằng theo phương pháp và thiết bị quản lý khóa công khai theo các phương án thực hiện sáng chế, UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và gửi, đến thiết bị mạng thứ hai bằng cách sử dụng thiết bị mạng thứ nhất, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng được mật mã hóa và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông điệp danh tính người dùng thứ ba, thiết bị mạng thứ hai có thể xác định, dựa trên bảng ánh xạ được lưu trữ trước giữa các cặp khóa công khai - riêng tư và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ của kiến trúc hệ thống theo phương án thực hiện sáng chế;

Fig.2A và Fig.2B là sơ đồ 1 của phương pháp quản lý khóa theo sáng chế;

Fig.3A và Fig.3B là sơ đồ 2 của phương pháp quản lý khóa công khai theo sáng chế;

Fig.4A và Fig.4B là sơ đồ 3 của phương pháp quản lý khóa công khai theo

sáng chế;

Fig.5A và Fig.5B là sơ đồ 4 của phương pháp quản lý khóa công khai theo sáng chế;

Fig.6 là sơ đồ 5 của phương pháp quản lý khóa công khai theo sáng chế;

Fig.7 là sơ đồ 6 của phương pháp quản lý khóa công khai theo sáng chế;

Fig.8 là sơ đồ 7 của phương pháp quản lý khóa công khai theo sáng chế;

Fig.9 là sơ đồ 8 của phương pháp quản lý khóa công khai theo sáng chế;

Fig.10 là sơ đồ 1 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.11 là sơ đồ 2 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.12 là sơ đồ 3 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.13 là sơ đồ 4 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.14 là sơ đồ 5 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.15 là sơ đồ 6 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.16 là sơ đồ 7 của thiết bị quản lý khóa công khai theo sáng chế;

Fig.17 là sơ đồ 8 của thiết bị quản lý khóa công khai theo sáng chế; và

Fig.18 là sơ đồ khối của thiết bị theo sáng chế.

Mô tả chi tiết sáng chế

Fig.1 là sơ đồ kiến trúc của hệ thống theo phương án thực hiện sáng chế. Dựa vào Fig.1, trong hệ thống truyền thông, thiết bị mạng thứ nhất là thiết bị chức năng truy nhập và quản lý di động (Access and Mobility Management Function, AMF), thiết bị mạng thứ hai là thiết bị chức năng bộc lộ bộ nhân dạng thuê bao (Subscription Identifier De-concealing Function, SIDF), thiết bị mạng thứ ba là thiết bị chức năng khối nhận dạng (Authentication Unit Function, AUSF), và thiết bị mạng thứ tư là thiết bị chức năng quản lý khóa công khai trong đó chức năng quản lý khóa công khai được tích hợp. Hệ thống truyền thông bao gồm UE, thiết bị AMF, thiết bị AUSF, thiết bị SIDF, thiết bị chức năng quản lý khóa công khai, và máy chủ xác thực vốn là thiết bị chức năng kho chứa xác thực (Authentication Repository Function, ARPF). Trong kiến trúc hệ thống được thể hiện trên Fig.1, UE có thể tương tác với thiết bị SIDF bằng cách sử dụng thiết bị AMF và thiết bị AUSF, hoặc tương tác với thiết bị SIDF bằng cách sử dụng chỉ

thiết bị AMF.

UE có thể là điện thoại di động (hoặc được gọi là điện thoại "tế bào") hoặc máy tính có thiết bị đầu cuối di động, chẳng hạn, thiết bị mang đi được, bỏ túi, cầm tay, cài sẵn trong máy tính, hoặc di động trong xe. UE cũng có thể được gọi là thiết bị đầu cuối, trạm di động (mobile station, MS) hoặc thiết bị đầu cuối, hoặc UE có thể còn bao gồm khối người thuê bao, điện thoại di động, điện thoại thông minh, thẻ dữ liệu không dây, máy tính hỗ trợ số cá nhân (personal digital assistant, PDA), máy tính tablet, modem không dây, thiết bị cầm tay, máy tính xách tay, điện thoại không dây, trạm vòng cục bộ không dây, thiết bị đầu cuối truyền thông loại máy (machine type communication, MTC), hoặc tương tự.

Thiết bị AMF được sử dụng để chuyển tiếp các thông điệp được trao đổi giữa UE và thiết bị AUSF, và còn chịu trách nhiệm quản lý di động trong mạng di động, chẳng hạn cập nhật vị trí người dùng, đăng ký mạng người dùng, và chuyển đổi người dùng.

Thiết bị AUSF được sử dụng để chuyển tiếp các thông điệp được trao đổi giữa thiết bị AMF và thiết bị SIDF, và còn chịu trách nhiệm tương tác với bộ phận ARPF, và thực hiện xác thực trên thông tin danh tính người dùng bằng cách sử dụng bộ phận ARPF.

Thiết bị SIDF được sử dụng để tạo cặp khóa công khai - riêng tư, phân phối ID tham chiếu đến cặp khóa công khai - riêng tư, giải mã thông tin danh tính người dùng bằng cách sử dụng khóa riêng tư được lưu trữ trong thiết bị SIDF, và tương tác với thiết bị AUSF và thiết bị chức năng quản lý khóa công khai.

Thiết bị chức năng quản lý khóa công khai được sử dụng để tạo cặp khóa công khai - riêng tư, phân phối ID tham chiếu đến cặp khóa công khai - riêng tư, và gửi cặp khóa công khai - riêng tư và ID tham chiếu được tạo đến thiết bị SIDF, sao cho thiết bị SIDF giải mã thông tin danh tính người dùng bằng cách sử dụng khóa riêng tư.

Bộ phận ARPF chủ yếu được sử dụng để tương tác với thiết bị AUSF và chịu trách nhiệm chính để thực hiện xác thực trên thông tin danh tính người dùng.

Trong hệ thống mật mã hóa khóa công khai hiện tại, ít nhất một một cặp khóa công khai - riêng tư được phép mật mã hóa và giải mã thông tin danh tính người

dùng. Khi có ít nhất một tập cặp khóa công khai - riêng tư trong hệ thống mật mã hóa khóa công khai, thiết bị AUSF không thể xác định cặp khóa công khai - riêng tư mà khóa công khai của nó được sử dụng bởi UE mật mã hóa thông tin danh tính người dùng, và kết quả là, không thể xác định cặp khóa công khai - riêng tư mà khóa riêng tư của nó được sử dụng để giải mã thông tin danh tính người dùng được mật mã hóa, dẫn đến hiệu suất giải mã dữ liệu được giảm. Để cải thiện hiệu suất giải mãi dữ liệu, phương pháp quản lý khóa công khai được đề xuất theo sáng chế. Khi xác định mật mã hóa thông tin danh tính người dùng, UE mật mã hóa thông tin danh tính người dùng bằng cách sử dụng khóa công khai thứ nhất, và gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AMF. Thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho thiết bị AMF gửi thông tin danh tính người dùng được mật mã hóa và ID tham chiếu đến thiết bị SIDF dựa trên ID chỉ báo và ID tham chiếu. Một cách tương ứng, thiết bị SIDF cũng có thể tìm kiếm, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất được đánh chỉ mục bởi ID tham chiếu, và giải mã thông tin danh tính người dùng bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Nên lưu ý rằng ở phương pháp quản lý khóa công khai theo sáng chế, khi gửi thông tin danh tính người dùng và ID tham chiếu (tức là, thông điệp danh tính người dùng thứ ba theo sáng chế) đến thiết bị SIDF dựa trên ID tham chiếu, thiết bị AMF có thể trực tiếp gửi thông điệp danh tính người dùng thứ ba đến thiết bị SIDF dựa trên ID tham chiếu, hoặc có thể chuyển tiếp thông điệp danh tính người dùng thứ ba đến thiết bị SIDF bằng cách sử dụng AUSF dựa trên ID tham chiếu. Các phương án thực hiện cụ thể được sử dụng dưới đây để mô tả chi tiết các giải pháp kỹ thuật của sáng chế. Nên lưu ý rằng các phương án thực hiện cụ thể sau có thể được kết hợp với nhau, và nội dung tương tự hoặc giống nhau không được mô tả lặp lại theo các phương án thực hiện khác nhau.

Nên lưu ý rằng phương pháp quản lý khóa công khai theo sáng chế có thể

được phân chia thành hai quá trình chính: quá trình giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng quá trình tạo và chuyển phát khóa công khaivà khóa công khai. Cụ thể là, đối với quá trình giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa công khai, tham khảo các phương án thực hiện được thể hiện trên Fig.2A đến Fig.6. Đối với quá trình tạo và chuyển phát khóa công khai, tham khảo các phương án thực hiện được thể hiện trên Fig.7 đến Fig.9.

Fig.2A và Fig.2B là sơ đồ 1 của phương pháp quản lý khóa theo sáng chế. Theo phương án thực hiện được thể hiện trên Fig.2A và Fig.2B, thiết bị AMF chuyển tiếp thông điệp danh tính người dùng thứ ba đến thiết bị SIDF bằng cách sử dụng thiết bị AUSF. Dựa vào Fig.2A và Fig.2B, phương pháp quản lý khóa có thể bao gồm các bước sau.

S201. UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất.

Chẳng hạn, trước khi mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, UE có thể trước hết nhận khóa công khai thứ nhất và ID tham chiếu that được sử dụng để đánh chỉ mục khóa công khai thứ nhất mà được gửi bởi thiết bị SIDF hoặc thiết bị chức năng quản lý khóa công khai, để thu được khóa công khai thứ nhất được sử dụng để mật mã hóa thông tin danh tính người dùng và ID tham chiếu tương ứng.

Sau khi thu thập khóa công khai thứ nhất, UE có thể mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất. Chẳng hạn, khi thông tin danh tính người dùng được mật mã hóa dựa trên khóa công khai thứ nhất, thông tin danh tính người dùng có thể được mật mã hóa ngay bằng cách sử dụng khóa công khai thứ nhất; hoặc thông tin danh tính người dùng có thể được mật mã hóa trước hết bằng cách sử dụng khóa công khai tạm thời, và sau đó thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa công khai tạm thời được mật mã hóa bằng cách sử dụng khóa công khai thứ nhất. Một cách tùy chọn, trước khi mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, UE có thể trước hết xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ. Khi khóa công khai thứ nhất trong chu kỳ hợp lệ, UE mật

mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất. Nên lưu ý rằng khi UE xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ, UE còn cần nhân chu kỳ sử dụng khóa công khai thứ nhất được gửi bởi thiết bị SIDF hoặc thiết bị chức năng quản lý khóa công khai, sao cho UE xác định, dựa trên chu kỳ sử dụng của khóa công khai thứ nhất, liệu khóa công khai thứ nhất trong chu kỳ hợp lệ. Chẳng hạn, chu kỳ sử dụng của khóa công khai thứ nhất có thể được biểu diễn bởi ngày tạo và ngày hết hạn của khóa công khai thứ nhất, hoặc có thể được biểu diễn bởi ngày tạo và chu kỳ hữu dụng của khóa công khai thứ nhất.

S202. UE gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AMF.

Thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng (tức là, thông tin danh tính người dùng được mật mã hóa), ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất. Một cách tùy chọn, thông điệp danh tính người sử dụng thứ nhất có thể còn bao gồm giao thức mật mã hóa được hỗ trợ bởi khóa công khai thứ nhất. Chẳng hạn, thông điệp danh tính người sử dụng thứ nhất có thể được mang trong gói tầng không truy nhập (Non-Access Stratum, NAS) và được gửi đến thiết bị AMF. Cụ thể là, thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất có thể được mang trong gói NAS.

Nên lưu ý rằng ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất có thể là số được phân phối trước, có thể là thông ti địa lý ám chỉ thiết bị mạng quản lý danh tính, hoặc có thể là khóa công khai thứ nhất. Khi ID chỉ báo chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, khi là số lớn hơn 0, ID chỉ báo có thể chỉ báo rằng danh tính người dùng ở trạng thái được mật mã hóa, hoặc khi là 0, ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa. Một cách tùy chọn, khi bằng 0, ID tham chiếu cũng có thể chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa.

S203. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng

thái được mật mã hóa, thiết bị AMF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị AUSF tương ứng với khóa công khai thứ nhất.

S204. Thiết bị AMF chuyển tiếp thông điệp danh tính người sử dụng thứ nhất đến thiết bị AUSF dựa trên thông tin nhận dạng thiết bị AUSF.

Khi nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, thiết bị AMF xác định, dựa trên ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa và được bao gồm trong thông điệp danh tính người sử dụng thứ nhất, liệu danh tính người dùng được mật mã hóa, và khi xác định rằng thông tin danh tính người dùng được mật mã hóa, xác định, dựa trên ID tham chiếu, nhận dạng thiết bị AUSF tương ứng với khóa công khai thứ nhất, để chuyển tiếp thông điệp danh tính người sử dụng thứ nhất đến thiết bị AUSF dựa trên thông tin nhận dạng thiết bị AUSF.

Một cách tùy chọn, theo phương án thực hiện sáng chế, ở các bước S203 và S204, việc thiết bị AMF xác định, dựa trên ID tham chiếu, nhận dạng thiết bị AUSF tương ứng với khóa công khai thứ nhất, và chuyển tiếp thông điệp danh tính người dùng đến thiết bị AUSF dựa trên thông tin nhận dạng thiết bị AUSF có thể bao gồm: Thiết bị AMF nhận và lưu trữ trước bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu và được gửi bởi thiết bị AUSF, sao cho sau khi nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, thiết bị AMF có thể xác định, theo bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu, thông tin nhận dạng thiết bị AUSF tương ứng với khóa công khai thứ nhất, để gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AUSF. N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một rong N khóa công khai, và N là số nguyên lớn hơn 0.

S205. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, thiết bị AUSF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với ID tham chiếu.

S206. Thiết bị AUSF gửi thông điệp danh tính người dùng thứ ba đến thiết bị SIDF dựa trên thông tin nhận dạng thiết bị SIDF.

Thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người

dùng (cụ thể là, thông tin danh tính người dùng được mật mã hóa) và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất. Sau khi nhận thông điệp danh tính người sử dụng thứ nhất của UE, thiết bị AUSF xác định, dựa trên ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa và trong thông điệp danh tính người sử dụng thứ nhất, liệu danh tính người dùng ở trạng thái có được mật mã hóa không. Khi xác định rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AUSF gửi ngay thông tin danh tính người dùng đến bộ phận ARPF để xác thực. Khi xác định rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, thiết bị AUSF chỉ cần gửi, đến thiết bị SIDF, thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa công khai thứ nhất và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho SIDF tìm kiếm ngay, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, và ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa không cần được gửi. Một cách tùy chọn, thông điệp danh tính người dùng thứ ba có thể còn bao gồm giao thức mật mã hóa được hỗ trợ bởi khóa công khai thứ nhất.

Sau khi nhận thông điệp danh tính người sử dụng thứ nhất được chuyển tiếp bởi thiết bị AMF, thiết bị AUSF xác định, dựa trên ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa và được bao gồm trong thông điệp danh tính người sử dụng thứ nhất, liệu danh tính người dùng ở trạng thái được mật mã hóa, và khi xác định rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với ID tham chiếu, chuyển tiếp thông điệp danh tính người dùng thứ ba đến thiết bị SIDF dựa trên thông tin nhận dạng thiết bị SIDF.

Một cách tùy chọn, theo phương án thực hiện sáng chế, ở bước S205 và S206, việc thiết bị AUSF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với ID tham chiếu, và gửi thông điệp danh tính người dùng thứ ba đến thiết bị SIDF dựa trên thông tin nhận dạng thiết bị SIDF có thể bao

gồm: Thiết bị AUSF nhận và lưu trữ trước bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu và được gửi bởi thiết bị SIDF, sao cho sau khi nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, thiết bị AUSF có thể xác định, theo bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với ID tham chiếu, để gửi thông điệp danh tính người dùng thứ ba đến thiết bị SIDF.

S207. Thiết bị SIDF xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất.

Khóa công khai thứ nhất và khóa riêng tư thứ nhất là cặp khóa riêng tư-công khai thứ nhất.

Theo phương án thực hiện sáng chế, thiết bị SIDF có thể lưu trữ trước bảng ánh xạ giữa N cặp khóa riêng tư-công khai và N ID tham chiếu, sao cho sau khi nhận thông điệp danh tính người dùng thứ ba, SIDF có thể tìm kiếm, dựa trên ID tham chiếu được bao gồm trong thông điệp danh tính người dùng thứ ba, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa dựa trên khóa riêng tư thứ nhất.

S208. Thiết bị SIDF giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã.

S209. Thiết bị SIDF gửi thông tin danh tính người dùng được giải mã đến thiết bị AUSF, sao cho thiết bị AUSF xử lý thông tin danh tính người dùng được giải mã.

Chẳng hạn, theo phương án thực hiện sáng chế, thiết bị SIDF gửi thông tin danh tính người dùng được giải mã đến thiết bị AUSF, và thiết bị AUSF gửi thông tin danh tính người dùng được giải mã đến bộ phận ARPF, sao cho bộ phận ARPF thực hiện xác thực trên thông tin danh tính người dùng.

Nên lưu ý rằng theo phương án thực hiện được thể hiện trên Fig.2A và Fig.2B, S203 đến S206 cũng có thể được thay bằng bước S211 và S212 sau. Cụ thể là, thiết bị AMF gửi ngay thông điệp danh tính người dùng thứ ba đến thiết bị SIDF dựa trên ID tham chiếu. Để biết chi tiết, tham khảo Fig.3A và Fig.3B. Fig.3A and Fig.3B là sơ đồ 2 của phương pháp quản lý khóa theo sáng chế.

S210. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng

thái được mật mã hóa, thiết bị AMF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với khóa công khai thứ nhất.

Một cách tùy chọn, trước khi S210 trong đó thiết bị AMF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với khóa công khai thứ nhất, phương pháp có thể còn bao gồm:

Thiết bị AMF nhận bảng ánh xạ giữa thông tin nhận dạng SIDF và N ID tham chiếu và được gửi bởi thiết bị SIDF. N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0. Thiết bị AMF xác định, theo bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với khóa công khai thứ nhất. Nên lưu ý rằng bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu cũng có thể được tạo bởi thiết bị AMF dựa trên thông tin cấu hình hệ thống.

S211. Thiết bị AMF chuyển tiếp thông điệp danh tính người dùng thứ ba đến thiết bị SIDF dựa trên thông tin nhận dạng thiết bị SIDF.

Theo phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế, khi xác định mật mã hóa thông tin danh tính người dùng, UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AMF, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông tin danh tính người dùng thứ nhất, thiết bị AMF xác định, dựa trên ID chỉ báo, liệu thông tin danh tính người dùng ở trạng thái được mật mã hóa. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, thiết bị AMF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị AUSF tương ứng với khóa công khai thứ nhất, và gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AUSF. Một cách tương tự, khi nhận thông tin danh tính người dùng thứ nhất, thiết bị AUSF xác định, dựa trên ID chỉ báo, liệu thông tin danh tính người dùng ở trạng thái được mật mã hóa. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được

mật mã hóa, thiết bị AUSF xác định, dựa trên ID tham chiếu, thông tin nhận dạng thiết bị SIDF tương ứng với ID tham chiếu, và gửi thông điệp danh tính người dùng thứ ba đến thiết bị SIDF, sao cho khi nhận thông điệp danh tính người dùng thứ ba của UE, thiết bị SIDF giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, thu được thông tin danh tính người dùng được giải mã, và gửi thông tin danh tính người dùng được giải mã đến bộ phận ARPF. Do vậy, bộ phận ARPF thực hiện xác thực trên thông tin danh tính người dùng. Có thể nhận biết rằng theo phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế, UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và gửi, đến thiết bị SIDF, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng được mật mã hóa và ID tham chiếu mà được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho khi nhận thông điệp danh tính người dùng thứ ba, thiết bị SIDF có thể xác định, dựa trên bảng ánh xạ được lưu trữ trước giữa các cặp khóa công khai - riêng tư và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Dựa trên các phương án thực hiện được thể hiện trên Fig.2A đến Fig.3B, Một cách tùy chọn, theo phương án thực hiện sáng chế, trước khi S208 trong đó thiết bị SIDF xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, phương pháp còn bao gồm:

Thiết bị SIDF xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ. Khi khóa công khai thứ nhất trong chu kỳ hợp lệ, S208 được thực hiện, cụ thể là, thiết bị SIDF xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất.

Ngược lại, khi khóa công khai thứ nhất không nằm trong chu kỳ hợp lệ, S210 được thực hiện ngay. Để biết chi tiết, tham khảo Fig.4A và Fig.4B. Fig.4A và Fig.4B là sơ đồ 3 của phương pháp quản lý khóa công khai theo sáng chế.

S212. Thiết bị SIDF gửi thông điệp yêu cầu cập nhật khóa công khai đến UE.

Thông điệp yêu cầu cập nhật khóa công khai được sử dụng để ra lệnh UE cập nhật khóa công khai thứ nhất.

Có thể nhận biết rằng theo sáng chế, trước bước S208 trong đó thiết bị SID xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, thiết bị SIDF trước hết xác định liệu khóa công khai thứ nhất hợp lệ. Nếu khóa công khai thứ nhất hợp lệ, thiết bị SIDF xác định ngay khóa riêng tư thứ nhất tương ứng dựa trên khóa công khai thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa dựa trên khóa riêng tư thứ nhất. Nếu khóa công khai thứ nhất không hợp lệ, thiết bị SIDF gửi thông điệp yêu cầu cập nhật khóa công khai đến UE, sao cho UE cập nhật khóa công khai thứ nhất, nhờ đó cải thiện bảo mật của thông tin danh tính người dùng.

Ngoài ra, dựa trên các phương án thực hiện được thể hiện trên Fig.2A đến Fig.3B, để thỏa mãn yêu cầu ngăn chặn hợp pháp (Law for Interception) để kiểm chứng danh tính được mật mã hóa, một cách tùy chọn, sau khi giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất để thu được thông tin danh tính người dùng được giải mã, bước S208 thiết bị SIDF có thể còn gửi thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất đến thiết bị AMF, sao cho thiết bị AMF xác định liệu đăng ký và xác định sẽ được thực hiện trên thông tin danh tính người dùng. Để biết chi tiết, tham khảo Fig.5A và Fig.5B. Fig.5A và Fig.5B là sơ đồ 4 của phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế. Phương pháp quản lý khóa công khai có thể còn bao gồm các bước sau.

S213. Thiết bị SIDF gửi thông điệp danh tính người dùng thứ tư đến thiết bị AMF.

Thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất. Một cách tùy chọn, thông tin danh tính người dùng thứ tư có thể còn bao gồm giao thức mật mã hóa của khóa công khai thứ nhất, tham số khác được sử dụng để mật mã hóa, và tương tự.

Một cách tùy chọn, khi thiết bị SIDF gửi thông điệp danh tính người dùng thứ tư đến thiết bị AMF, thiết bị SIDF có thể trực tiếp gửi thông điệp danh tính người dùng thứ tư đến thiết bị AMF, hoặc có thể chuyển tiếp thông điệp danh tính người dùng thứ tư bằng cách sử dụng thiết bị AUSF. Cụ thể là, thiết bị SIDF có thể trước hết gửi thông điệp danh tính người dùng thứ tư đến thiết bị AUSF,

và sau đó thiết bị AUSF chuyển tiếp thông điệp danh tính người dùng thứ tư đến thiết bị AMF. Nói theo cách khác, thiết bị AMF có thể trực tiếp nhận thông tin danh tính người dùng thứ tư được gửi bởi thiết bị SIDF, hoặc có thể nhận thông tin danh tính người dùng thứ tư bằng cách sử dụng thiết bị AUSF.

S214. Thiết bị AMF mật mã hóa thông tin danh tính người dùng được giải mã bằng cách sử dụng khóa công khai thứ nhất, để tạo thông tin danh tính người dùng cần được kiểm chứng.

S215. Thiết bị AMF so sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng.

Dựa vào các phương án thực hiện được thể hiện trên Fig.2A đến Fig.3B, UE gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AMF ở bước S202. Thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất. Thiết bị AMF thu được trước thông tin danh tính người dùng, và sau khi tạo thông tin danh tính người dùng cần được kiểm chứng, thiết bị AMF có thể so sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng, để xác định liệu có thực hiện đăng ký và xác thực trên thông tin danh tính người dùng.

S216. Nếu thông tin danh tính người dùng cần được kiểm chứng giống như thông tin danh tính người dùng, thiết bị AMF gửi thông tin lệnh đến thiết bị AUSF.

Thông tin lệnh có thể bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

S217. Thiết bị AUSF xử lý thông tin danh tính người dùng được giải mã.

Chẳng hạn, theo phương án thực hiện sáng chế, việc thiết bị AUSF xử lý thông tin danh tính người dùng được giải mã nghĩa là thiết bị AUSF gửi thông tin danh tính người dùng được giải mã đến bộ phận ARPF, sao cho bộ phận ARPF thực hiện xác thực trên thông tin danh tính người dùng.

Một cách tùy chọn, sau bước S215, phương pháp có thể còn bao gồm: nếu

thông tin danh tính người dùng cần được kiểm chứng khác với thông tin danh tính người dùng, chỉ báo rằng thông tin danh tính người dùng là không hợp pháp. Thiết bị AMF có thể gửi thông điệp gián đoạn quá trình đăng ký đến thiết bị AUSF, sao cho thiết bị AUSF dừng đăng ký và xác thực trên thông tin danh tính người dùng dựa trên thông điệp gián đoạn quá trình đăng ký, và không cần thực hiện S217.

Có thể nhận biết rằng theo phương án thực hiện sáng chế, after thu thập thông tin danh tính người dùng được giải mã, thiết bị SIDF gửi thông tin danh tính người dùng to thiết bị AMF, sao cho thiết bị AMF mật mã hóa thông tin danh tính người dùng được giải mã dựa trên khóa công khai thứ nhất, để tạo thông tin danh tính người dùng cần được kiểm chứng, và so sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng, để xác định, dựa trên kết quả so sánh, liệu đăng ký và xác thực có được thực hiện trên thông tin danh tính người dùng, nhờ đó thỏa mãn yêu cầu ngăn chặn hợp pháp để kiểm chứng danh tính được mật mã hóa.

Các phương án thực hiện được thể hiện trên Fig.2A đến Fig.5B mô tả chi tiết quá trình trong đó khi UE xác định mật mã hóa thông tin danh tính người dùng, thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa công khai được giải mã. Nếu UE không mật mã hóa thông tin danh tính người dùng, Fig.6 là sơ đồ 5 của phương pháp quản lý khóa công khai theo sáng chế. Phương pháp quản lý khóa công khai có thể bao gồm các bước sau.

S601. UE xác định liệu mật mã hóa thông tin danh tính người dùng.

Trước khi gửi thông tin danh tính người dùng, UE trước hết xác định liệu mật mã hóa thông tin danh tính người dùng. Nếu được xác định mật mã hóa thông tin danh tính người dùng, bước S201 được thực hiện. Nếu xác định không mật mã hóa thông tin danh tính người dùng, bước S602 được thực hiện.

S602. Khi xác định không mật mã hóa thông tin danh tính người dùng, UE gửi thông điệp danh tính người dùng thứ hai đến thiết bị AMF.

Thông điệp danh tính người dùng thứ hai bao gồm thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa. Nên lưu ý rằng khi ID chỉ báo bằng

0, chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa. Chẳng hạn, thông điệp danh tính người dùng thứ hai có thể được mang trong gói NAS và được gửi đến thiết bị AMF. Cụ thể là, thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa có thể được mang trong gói NAS.

S603. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AMF xác định thông tin nhận dạng thiết bị AUSF tương ứng dựa trên thông tin danh tính người dùng.

S604. Thiết bị AMF chuyển tiếp thông điệp danh tính người dùng thứ hai đến thiết bị AUSF dựa trên thông tin nhận dạng thiết bị AUSF.

Khi nhận thông điệp danh tính người dùng thứ hai được gửi bởi UE, thiết bị AMF xác định, dựa trên ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa và được bao gồm trong thông điệp danh tính người dùng thứ hai, liệu thông tin danh tính người dùng ở trạng thái không được mật mã hóa, và khi xác định rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AMF xác định thông tin nhận dạng thiết bị AUSF tương ứng dựa trên thông tin danh tính người dùng.

S605. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AUSF gửi thông tin danh tính người dùng đến bộ phận ARPF.

Khi nhận thông điệp danh tính người dùng thứ hai được chuyển tiếp bởi thiết bị AMF, thiết bị AUSF xác định, dựa trên ID chỉ báo that được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa và được bao gồm trong thông điệp danh tính người dùng thứ hai, liệu thông tin danh tính người dùng ở trạng thái không được mật mã hóa. Khi xác định rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AUSF trực tiếp gửi thông tin danh tính người dùng đến bộ phận ARPF, sao cho bộ phận ARPF thực hiện xác thực trên thông tin danh tính người dùng.

Theo phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế, UE xác định liệu mật mã hóa thông tin danh tính người dùng, khi xác định không mật mã hóa thông tin danh tính người dùng, UE gửi thông điệp danh tính

người dùng thứ hai đến thiết bị AMF, trong đó thông điệp danh tính người dùng thứ hai bao gồm thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, sao cho khi thiết bị AMF nhận thông tin danh tính người dùng thứ hai, nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AMF xác định thông tin nhận dạng thiết bị AUSF tương ứng dựa trên thông tin danh tính người dùng, và chuyển tiếp thông điệp danh tính người dùng thứ hai đến thiết bị AUSF. Do vậy, khi nhận thông điệp danh tính người dùng thứ hai được chuyển tiếp bởi thiết bị AMF, thiết bị AUSF gửi thông tin danh tính người dùng đến bộ phận ARPF nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa. Có thể nhận biết rằng theo phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế, khi UE gửi thông điệp danh tính người dùng thứ hai đến thiết bị AUSF, do thông điệp danh tính người dùng thứ hai bao gồm ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, khi thiết bị AUSF nhận thông điệp danh tính người dùng thứ hai, thiết bị AUSF có thể xác định, dựa trên ID chỉ báo, liệu thông tin danh tính người dùng ở trạng thái không được mật mã hóa. Khi xác định rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, thiết bị AUSF gửi ngay thông tin danh tính người dùng đến bộ phận ARPF, sao cho bộ phận ARPF thực hiện xác thực trên thông tin danh tính người dùng, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Dựa trên các phương án thực hiện được thể hiện trên Fig.2A đến Fig.3B, khi UE gửi thông tin danh tính người dùng được mật mã hóa đến thiết bị SIDF để giải mãi, thiết bị SIDF cần lưu trữ trước N cặp khóa riêng tư-công khai và N ID tham chiếu, thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai, thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, và sau đó chuyển phát khóa công khai thứ nhất và chỉ mục thứ nhất đến UE, tức là, quá trình tạo và chuyển phát khóa công khai. Quá trình này có thể được triển khai cụ thể bằng cách sử dụng ba phương pháp triển khai khả thi dưới đây, như được thể hiện trên Fig.7 đến Fig.9.

Theo triển khai khả thi thứ nhất, Fig.7 là sơ đồ 6 của phương pháp quản lý

khóa công khai theo sáng chế. Phương pháp quản lý khóa công khai có thể bao gồm các bước sau.

S701. Thiết bị SIDF tạo N cặp khóa riêng tư-công khai.

Cặp khóa riêng tư-công khai thứ nhất theo các phương án thực hiện nêu trên là một trong N cặp khóa riêng tư-công khai, và N là số nguyên lớn hơn 0. Mỗi cặp trong N cặp khóa riêng tư-công khai bao gồm khóa công khai và khóa riêng tư tương ứng. Khóa công khai có thể được sử dụng để mật mã hóa thông tin danh tính người dùng, và khóa riêng tư có thể được sử dụng để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa công khai.

S702. Thiết bị SIDF phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Nên lưu ý rằng ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai có thể là số được phân phối trước, có thể là thông tin địa lý ngầm chỉ báo thiết bị mạng quản lý danh tính, hoặc có thể là khóa công khai. Khi ID chỉ báo chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, khi bằng số lớn hơn 0, ID chỉ báo có thể chỉ báo việc danh tính người dùng ở trạng thái được mật mã hóa, hoặc khi bằng 0, ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa.

Thiết bị SIDF phân phối ID tham chiếu đến mỗi khóa công khai trong N cặp khóa riêng tư-công khai. Một cách tương ứng, có N ID tham chiếu, và N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N cặp khóa riêng tư-công khai.

Để tránh việc khóa riêng tư từ cặp khóa công khai - riêng tư trong các cặp khóa công khai - riêng tư không thể được xác định để giải mã thông tin danh tính người dùng được mật mã hóa, theo phương án thực hiện sáng chế, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai được phân phối đến khóa công khai trong mỗi cặp của N cặp khóa riêng tư-công khai, sao cho khi nhận thông tin danh tính người dùng và ID tham chiếu, thiết bị SIDF có thể xác định, theo bảng ánh xạ được lưu trữ trước giữa cặp khóa riêng tư-công khai và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, giải mã thông tin danh tính người dùng bằng cách sử dụng khóa riêng tư thứ nhất, nhờ

đó cải thiện hiệu suất giải mã dữ liệu.

S703. Thiết bị SIDF thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai và ID tham chiếu từ N ID tham chiếu.

ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất.

S904. Thiết bị SIDF gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Chẳng hạn, thiết bị SIDF có thể gửi khóa công khai thứ nhất và ID tham chiếu đến môi trường lưu trữ tin cậy trên UE theo cách ngoại tuyến hoặc trực tuyến (OTP). Nên lưu ý rằng khi ID tham chiếu là khóa công khai thứ nhất, thiết bị SIDF có thể gửi chỉ khóa công khai thứ nhất đến UE.

Một cách tùy chọn, thiết bị SIDF có thể còn gửi giao thức mật mã hóa được hỗ trợ bởi khóa công khai thứ nhất đến UE, sao cho UE mật mã hóa thông tin UE theo giao thức mật mã hóa dựa trên khóa công khai thứ nhất.

Ngoài ra, khi gửi, đến UE, khóa công khai thứ nhất và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, thiết bị SIDF có thể cũng gửi chu kỳ sử dụng của khóa công khai thứ nhất đến UE, sao cho UE có thể xác định, dựa trên chu kỳ sử dụng của khóa công khai thứ nhất, liệu khóa công khai thứ nhất trong chu kỳ hợp lệ. Chẳng hạn, chu kỳ sử dụng có thể được biểu diễn bằng ngày tạo và ngày hết hạn của khóa công khai thứ nhất, hoặc có thể được biểu diễn bằng ngày tạo và chu kỳ sử dụng của khóa công khai thứ nhất.

Có thể nhận biết rằng theo phương án thực hiện sáng chế, sau khi tạo N cặp khóa riêng tư-công khai và phân phối, đến khóa công khai trong mỗi cặp của N cặp khóa riêng tư-công khai, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai, thiết bị SIDF thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai và ID tham chiếu từ N ID tham chiếu, và gửi khóa công khai thứ nhất và ID tham chiếu đến UE, sao cho UE có thể mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và gửi, đến thiết bị SIDF bằng cách sử dụng thiết bị AMF và thiết bị AUSF, thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu. Khi nhận thông điệp danh tính người dùng thứ ba, thiết bị SIDF có thể xác định, dựa trên bảng ánh xạ được lưu trữ trước giữa cặp khóa riêng tư-công khai và các ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, giải mã thông tin

danh tính người dùng bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi thứ hai, Fig.8 là sơ đồ 7 của phương pháp quản lý khóa công khai theo sáng chế. Phương pháp quản lý khóa công khai có thể bao gồm các bước sau.

S801. Thiết bị SIDF tạo N cặp khóa riêng tư-công khai.

Cặp khóa riêng tư-công khai thứ nhất theo các phương án thực hiện nêu trên là một trong N cặp khóa riêng tư-công khai, và N là số nguyên lớn hơn 0.

S802. Thiết bị SIDF gửi thông điệp yêu cầu ID tham chiếu đến thiết bị chức năng quản lý khóa công khai.

Thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết bị chức năng quản lý khóa công khai phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Sau khi tạo N cặp khóa riêng tư-công khai, thiết bị SIDF gửi thông điệp yêu cầu ID tham chiếu đến thiết bị chức năng quản lý khóa công khai, sao cho thiết bị chức năng quản lý khóa công khai phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

S803. Thiết bị chức năng quản lý khóa công khai phân phối N ID tham chiếu đến N khóa công khai.

N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai. Nên lưu ý rằng ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai có thể là số được phân phối trước, có thể là thông tin địa lý ngầm chỉ thiết bị mạng quản lý danh tính, hoặc có thể là khóa công khai. Khi ID chỉ báo chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, khi bằng số lớn hơn 0, ID chỉ báo có thể chỉ báo rằng danh tính người dùng ở trạng thái được mật mã hóa, hoặc khi bằng 0, ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa.

S804. Thiết bị chức năng quản lý khóa công khai gửi N khóa công khai và N ID tham chiếu đến thiết bị SIDF.

Sau khi phân phối N ID tham chiếu đến N khóa công khai, thiết bị chức năng

quản lý khóa công khai gửi N khóa công khai và N ID tham chiếu đến thiết bị SIDF, sao cho thiết bị SIDF thu được N khóa công khai và N ID tham chiếu, và lưu trữ bảng ánh xạ giữa N cặp khóa riêng tư-công khai và N ID tham chiếu. Do vậy, sau khi nhận thông điệp danh tính người sử dụng thứ nhất, thiết bị SIDF tìm thấy khóa riêng tư thứ nhất tương ứng dựa trên ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất và được bao gồm trong thông điệp danh tính người sử dụng thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất.

S805. Thiết bị chức năng quản lý khóa công khai thu được khóa công khai thứ nhất từ N khóa công khai và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất.

S806. Thiết bị chức năng quản lý khóa công khai gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Chẳng hạn, thiết bị chức năng quản lý khóa công khai có thể gửi khóa công khai thứ nhất và ID tham chiếu đến môi trường lưu trữ tin cậy trên UE theo cách trực tuyến hoặc ngoại tuyến (OTP). Nên lưu ý rằng khi ID tham chiếu là khóa công khai thứ nhất, thiết bị SIDF có thể gửi chỉ khóa công khai thứ nhất đến UE.

Một cách tùy chọn, thiết bị chức năng quản lý khóa công khai có thể còn gửi giao thức mật mã hóa được hỗ trợ bởi khóa công khai thứ nhất đến UE, sao cho UE mật mã hóa thông tin UE theo giao thức mật mã hóa dựa trên khóa công khai thứ nhất.

Sau khi phân phối N ID tham chiếu đến N khóa công khai, thiết bị chức năng quản lý khóa công khai có thể thu được khóa công khai thứ nhất từ N khóa công khai, và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và gửi khóa công khai thứ nhất và ID tham chiếu đến UE, sao cho khi xác định mật mã hóa thông tin danh tính người dùng, UE có thể mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và chỉ báo, bằng cách sử dụng ID tham chiếu, khóa công khai thứ nhất được sử dụng để mật mã hóa thông tin danh tính người dùng.

Nên lưu ý rằng theo phương án thực hiện sáng chế, không có chuỗi giữa S804 và S805.

Có thể nhận biết rằng theo phương án thực hiện sáng chế, thiết bị SIDF tạo N cặp khóa riêng tư-công khai và gửi thông điệp yêu cầu ID tham chiếu đến thiết bị chức năng quản lý khóa công khai, sao cho thiết bị chức năng quản lý khóa công khai phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai. Sau khi phân phối N ID tham chiếu đến N khóa công khai, thiết bị chức năng quản lý khóa công khai có thể thu được khóa công khai thứ nhất từ N khóa công khai và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và gửi khóa công khai thứ nhất và ID tham chiếu đến UE, sao cho khi xác định mật mã hóa thông tin danh tính người dùng, UE có thể mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất. Ngoài ra, thiết bị chức năng quản lý khóa công khai gửi N khóa công khai và N ID tham chiếu đến thiết bị SIDF, sao cho thiết bị SIDF thu được N khóa công khai và N ID tham chiếu, và lưu trữ bảng ánh xạ giữa N cặp khóa riêng tư-công khai và N ID tham chiếu. Do vậy, sau khi nhận thông điệp danh tính người dùng thứ ba, thiết bị SIDF tìm thấy khóa riêng tư thứ nhất tương ứng dựa trên ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất và được bao gồm trong thông điệp danh tính người dùng thứ ba, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Theo triển khai khả thi thứ ba, Fig.9 là sơ đồ 8 của phương pháp quản lý khóa công khai theo sáng chế. Phương pháp quản lý khóa công khai có thể bao gồm các bước sau.

S901. Thiết bị chức năng quản lý khóa công khai tạo N cặp khóa riêng tư-công khai và phân phối N ID tham chiếu đến N khóa công khai.

Mỗi cặp khóa công khai - riêng tư bao gồm khóa công khai và khóa riêng tư, và N khóa công khai là các khóa công khai trong N cặp khóa riêng tư-công khai. Cặp khóa riêng tư-công khai thứ nhất theo các phương án thực hiện là một trong N cặp khóa riêng tư-công khai, và N là số nguyên lớn hơn 0. N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai. Có thể hiểu rằng các ID tham chiếu có thể là các chuỗi ký tự, các số, hoặc tương tự. Chẳng hạn, nếu có 100 cặp khóa công khai - riêng tư, các ID được phân phối đến

các khóa công khai có thể bằng từ 0 đến 99. Chắc chắn là, độ dài của ID tham chiếu có thể bị giới hạn theo cách khác, chẳng hạn, độ dài bằng 6 bit, 8 bit, 15 bit, hoặc 100 bit, và có thể được xác định chắc chắn dựa trên thang tỷ lệ dịch vụ.

S902. Thiết bị chức năng quản lý khóa công khai gửi các khóa công khai trong N cặp khóa riêng tư-công khai và N ID tham chiếu đến thiết bị SIDF.

Nên lưu ý rằng ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai có thể là số được phân phối trước, có thể là thông tin địa lý ngầm chỉ thiết bị mạng quản lý danh tính, hoặc có thể là khóa công khai.

Chẳng hạn, khi bằng số lớn hơn 0, ID chỉ báo có thể chỉ báo rằng danh tính người dùng ở trạng thái được mật mã hóa, và khi bằng 0, ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa. Chẳng hạn, ID chỉ báo bằng 1, chỉ báo rằng danh tính người dùng ở trạng thái được mật mã hóa. ID chỉ báo bằng 0, chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa.

Chẳng hạn, ID chỉ báo có thể là chuỗi ký tự định trước. Chẳng hạn, chuỗi ký tự định trước thứ nhất chỉ báo rằng danh tính người dùng ở trạng thái được mật mã hóa, và chuỗi ký tự định trước thứ hai chỉ báo rằng danh tính người dùng ở trạng thái không được mật mã hóa. Có thể hiểu rằng chuỗi ký tự định trước thứ nhất khác với chuỗi ký tự định trước thứ hai, và định dạng của chuỗi ký tự không bị giới hạn ở đây theo sáng chế.

Sau khi phân phối N ID tham chiếu đến N khóa công khai, thiết bị chức năng quản lý khóa công khai gửi N khóa công khai và N ID tham chiếu đến thiết bị SIDF, sao cho thiết bị SIDF thu được N khóa công khai và N ID tham chiếu, và lưu trữ bảng ánh xạ giữa N cặp khóa riêng tư-công khai và N ID tham chiếu. Do vậy, sau khi nhận thông điệp danh tính người sử dụng thứ nhất, thiết bị SIDF tìm ra khóa riêng tư thứ nhất tương ứng dựa trên ID tham chiếu that được sử dụng để đánh chỉ mục khóa công khai thứ nhất và được bao gồm trong thông điệp danh tính người sử dụng thứ nhất, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất.

S903. Thiết bị chức năng quản lý khóa công khai thu được khóa công khai thứ nhất từ N khóa công khai và thu được, từ N ID tham chiếu, ID tham chiếu

được sử dụng để đánh chỉ mục khóa công khai thứ nhất.

S904. Thiết bị chức năng quản lý khóa công khai gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Chẳng hạn, thiết bị chức năng quản lý khóa công khai có thể gửi khóa công khai thứ nhất và ID tham chiếu đến môi trường lưu trữ tin cậy trên UE theo cách trực tuyến hoặc ngoại tuyến (OTP). Nên lưu ý rằng khi ID tham chiếu là khóa công khai thứ nhất, thiết bị SIDF có thể gửi khóa công khai thứ nhất đến UE.

Một cách tùy chọn, thiết bị chức năng quản lý khóa công khai có thể còn gửi giao thức mật mã hóa được hỗ trợ bởi khóa công khai thứ nhất đến UE, sao cho UE mật mã hóa thông tin UE theo giao thức mật mã hóa dựa trên khóa công khai thứ nhất.

Sau khi phân phối N ID tham chiếu đến N khóa công khai, thiết bị chức năng quản lý khóa công khai may thu được khóa công khai thứ nhất từ N khóa công khai, và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và gửi khóa công khai thứ nhất và ID tham chiếu đến UE, sao cho khi xác định mật mã hóa thông tin danh tính người dùng, UE có thể mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất, và chỉ báo, bằng cách sử dụng ID tham chiếu, khóa công khai thứ nhất được sử dụng để mật mã hóa thông tin danh tính người dùng.

Nên lưu ý rằng theo phương án thực hiện sáng chế, không có chuỗi giữa S902 và S903.

Có thể nhận biết rằng theo phương án thực hiện sáng chế, thiết bị chức năng quản lý khóa công khai tạo N cặp khóa riêng tư-công khai và phân phối N ID tham chiếu đến N khóa công khai. Sau khi phân phối N ID tham chiếu đến N khóa công khai, thiết bị chức năng quản lý khóa công khai may thu được khóa công khai thứ nhất từ N khóa công khai và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và gửi khóa công khai thứ nhất và ID tham chiếu đến UE, sao cho khi xác định mật mã hóa thông tin danh tính người dùng, UE có thể mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất. Ngoài ra, thiết bị chức năng quản lý khóa công khai gửi các khóa công khai trong N cặp khóa riêng tư-công khai và N ID

tham chiếu đến thiết bị SIDF, sao cho thiết bị SIDF thu được các khóa công khai trong N cặp khóa riêng tư-công khai và N ID tham chiếu, và lưu trữ bảng ánh xạ giữa N cặp khóa riêng tư-công khai và N ID tham chiếu. Do vậy, sau khi nhận thông điệp danh tính người dùng thứ ba, thiết bị SIDF tìm thấy khóa riêng tư thứ nhất tương ứng dựa trên ID tham chiếu that được sử dụng để đánh chỉ mục khóa công khai thứ nhất và được bao gồm trong thông điệp danh tính người dùng thứ ba, để giải mã thông tin danh tính người dùng được mật mã hóa bằng cách sử dụng khóa riêng tư thứ nhất, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Dựa trên các phương án thực hiện được thể hiện trên hình vẽ đi kèm trên Fig.7 đến Fig.9, sau khi thiết bị SIDF hoặc thiết bị chức năng quản lý khóa công khai thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai và ID tham chiếu, để thiết bị AUSF có thể tìm ra thiết bị SIDF của khóa riêng tư thứ nhất được sử dụng để giải mãi, và để thiết bị AMF có thể tìm thấy thiết bị AUSF tương ứng với khóa công khai thứ nhất trong quá trình giải mãi tiếp theo (phương án thực hiện được thể hiện trên Fig.2A và Fig.2B), S905 và S906 có thể được thực hiện.

S905. Thiết bị SIDF gửi bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu đến thiết bị AUSF.

Thông tin nhận dạng thiết bị SIDF có thể là thông tin địa lý của thiết bị SIDF, hoặc có thể là thông tin tên của thiết bị SIDF, giả sử rằng thiết bị SIDF có thể được tìm thấy dựa trên thông tin nhận dạng thiết bị SIDF.

Thiết bị SIDF gửi bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu đến thiết bị AUSF, sao cho thiết bị AUSF thu được và lưu trữ bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu. Do vậy, sau khi nhận thông tin danh tính người dùng thứ hai của UE, thiết bị AUSF gửi thông tin danh tính người dùng thứ hai của UE đến thiết bị SIDF dựa trên bảng ánh xạ được lưu trữ trước giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu, sao cho thiết bị SIDF giải mã thông tin danh tính người dùng được mật mã hóa.

Nên lưu ý rằng khi hệ thống truyền thông bao gồm một thiết bị SIDF, thiết bị SIDF cần gửi chỉ N ID tham chiếu đến thiết bị AUSF, và không cần gửi thông tin nhận dạng thiết bị SIDF. Theo cách khác, khi ID tham chiếu là thông tin địa

lý của thiết bị SIDF và thiết bị SIDF, thiết bị SIDF cần gửi chỉ N ID tham chiếu đến thiết bị AUSF, và không cần gửi thông tin nhận dạng thiết bị SIDF. Thiết bị AUSF có thể tìm thấy thiết bị SIDF dựa trên thông tin địa lý của thiết bị SIDF.

S906. Thiết bị AUSF gửi bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu đến thiết bị AMF.

Thông tin nhận dạng thiết bị AUSF có thể là thông tin địa lý của thiết bị AUSF, hoặc có thể là thông tin tên của thiết bị AUSF, giả sử rằng thiết bị AUSF có thể được tìm thấy dựa trên thông tin nhận dạng thiết bị AUSF.

Thiết bị AUSF gửi bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu đến thiết bị AMF, sao cho thiết bị AMF thu được và lưu trữ bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu. Do vậy, sau khi nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, thiết bị AMF gửi thông tin danh tính người dùng thứ nhất của UE đến thiết bị AUSF dựa trên bảng ánh xạ được lưu trữ trước giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu.

Nên lưu ý rằng khi hệ thống truyền thông bao gồm một thiết bị AUSF, thiết bị AUSF cần gửi chỉ N ID tham chiếu đến thiết bị AMF, và không cần gửi thông tin nhận dạng thiết bị AUSF. Theo cách khác, khi ID tham chiếu là thông tin địa lý của thiết bị AUSF và thiết bị AUSF, thiết bị AUSF cần gửi chỉ N ID tham chiếu đến thiết bị AMF, và không cần gửi thông tin nhận dạng thiết bị AUSF. Thiết bị AMF có thể tìm ra thiết bị AUSF dựa trên thông tin địa lý của thiết bị AUSF.

Nên lưu ý rằng theo phương án thực hiện được thể hiện trên Fig.7, không có chuỗi giữa S704, và S905 và S906. Phương án thực hiện được thể hiện trên Fig.7 mô tả chỉ bằng cách sử dụng ví dụ trong đó bước S905 và S906 được thực hiện trước, và sau đó bước S704 được thực hiện. Một cách tương tự, theo phương án thực hiện được thể hiện trên Fig.8, không có chuỗi giữa bước S806, và S905 và S906. Phương án thực hiện được thể hiện trên Fig.8 mô tả chỉ bằng cách sử dụng ví dụ trong đó S905 và S906 được thực hiện trước, và sau đó S806 được thực hiện. Một cách tương tự, theo phương án thực hiện được thể hiện trên Fig.9, không có chuỗi giữa bước S904, và S905 và S906. Phương án thực hiện được

thể hiện trên Fig.9 mô tả chỉ bằng cách sử dụng ví dụ trong đó các bước S905 và S906 được thực hiện trước, và sau đó bước S904 được thực hiện.

Theo phương pháp quản lý khóa công khai theo phương án thực hiện sáng chế, bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu được gửi đến thiết bị AUSF, và thiết bị AUSF gửi bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu đến thiết bị AMF, sao cho sau khi UE mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất và gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị AMF, thiết bị AMF có thể gửi thông tin danh tính người dùng thứ nhất của UE đến thiết bị AUSF dựa trên bảng ánh xạ được lưu trữ trước giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu. Do vậy, thiết bị AUSF có thể gửi thông tin danh tính người dùng thứ hai của UE đến thiết bị SIDF dựa trên bảng ánh xạ được lưu trữ trước giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu, và thiết bị SIDF giải mã thông tin danh tính người dùng được mật mã hóa, nhờ đó cải thiện hiệu suất giải mã dữ liệu.

Fig.10 là sơ đồ 1 của thiết bị quản lý khóa công khai 100 theo sáng chế. Thiết bị quản lý khóa công khai 100 có thể bao gồm:

khối mật mã hóa 1001, được tạo cấu hình để mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất; và

khối gửi 1002, được tạo cấu hình để gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người sử dụng thứ nhất dựa trên ID chỉ báo và ID tham chiếu.

Một cách tùy chọn, khối mật mã hóa 1001 còn được tạo cấu hình để xác định liệu mật mã hóa thông tin danh tính người dùng; và

khối gửi 1002 còn được tạo cấu hình để: khi được xác định rằng thông tin danh tính người dùng sẽ không được mật mã hóa, gửi, bởi UE, thông điệp danh tính người dùng thứ hai đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính

người dùng thứ hai bao gồm thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo.

Một cách tùy chọn, thiết bị quản lý khóa công khai 100 có thể còn bao gồm khối đánh giá 1003. Fig.11 là sơ đồ 2 của thiết bị quản lý khóa công khai 100 theo sáng chế.

Khối đánh giá 1003 được tạo cấu hình để xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ.

Khối mật mã hóa 1001 được tạo cấu hình cụ thể để: khi khóa công khai thứ nhất trong chu kỳ hợp lệ, mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất.

Phương pháp quản lý khóa và các ví dụ cụ thể của thiết bị quản lý khóa theo các phương án thực hiện được thể hiện trên Fig.2A đến Fig.9 cũng áp dụng được cho thiết bị quản lý khóa theo phương án thực hiện. Từ các phần mô tả chi tiết về phương pháp quản lý khóa, người có hiểu biết trung bình trong lĩnh vực có thể biết rõ phương pháp triển khai của thiết bị quản lý khóa theo phương án thực hiện. Do vậy, để bản mô tả ngắn gọn, các chi tiết không được mô tả lại ở đây.

Fig.12 là sơ đồ 3 của thiết bị quản lý khóa công khai 120 theo sáng chế. Thiết bị quản lý khóa công khai 120 có thể bao gồm:

khối nhận 1201, được tạo cấu hình để nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi UE, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất; và

khối gửi 1202, được tạo cấu hình để: nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên ID tham chiếu, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu, sao cho thiết bị mạng thứ hai xử lý thông tin danh tính người dùng dựa trên ID tham chiếu.

Một cách tùy chọn, khối gửi 1202 được tạo cấu hình cụ thể để gửi thông điệp danh tính người sử dụng thứ nhất đến thiết bị mạng thứ ba dựa trên ID tham

chiếu, sao cho thiết bị mạng thứ ba gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai khi ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa.

Một cách tùy chọn, khối gửi 1202 được tạo cấu hình cụ thể để xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất, và gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên thông tin nhận dạng của thiết bị mạng thứ hai.

Một cách tùy chọn, thiết bị quản lý khóa 120 có thể còn bao gồm khối mật mã hóa 1203 và khối so sánh 1204. Fig.13 là sơ đồ 4 của thiết bị quản lý khóa công khai 120 theo sáng chế. Thiết bị quản lý khóa công khai 120 có thể bao gồm khối nhận 1201, khối mật mã hóa 1203, khối so sánh 1204, và khối gửi 1202.

Khối nhận 1201 còn được tạo cấu hình để nhận thông điệp danh tính thứ tư được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất.

Khối mật mã hóa 1203 được tạo cấu hình để mật mã hóa thông tin danh tính người dùng được giải mã bằng cách sử dụng khóa công khai thứ nhất, để tạo thông tin danh tính người dùng cần được kiểm chứng.

Khối so sánh 1204 được tạo cấu hình để so sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng.

Khối gửi 1202 còn được tạo cấu hình để: nếu thông tin danh tính người dùng cần được kiểm chứng giống như thông tin danh tính người dùng, gửi thông tin lệnh đến thiết bị mạng thứ ba, trong đó thông điệp lệnh bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Một cách tùy chọn, khối nhận 1201 được tạo cấu hình cụ thể để nhận thông điệp danh tính người dùng thứ tư được chuyển tiếp bởi thiết bị mạng thứ ba.

Một cách tùy chọn, thiết bị quản lý khóa 120 có thể còn bao gồm khối xác định 1205.

Khối nhận 1201 còn được tạo cấu hình để nhận bảng ánh xạ giữa thông tin

nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0.

Việc khối xác định 1205 được tạo cấu hình để xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất bao gồm:

khối xác định 1205 còn được tạo cấu hình để xác định, theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với khóa công khai thứ nhất.

Phương pháp quản lý khóa và các ví dụ cụ thể của thiết bị quản lý khóa theo các phương án thực hiện được thể hiện trên Fig.2A đến Fig.9 cũng áp dụng được cho thiết bị quản lý khóa theo phương án thực hiện. Từ các phần mô tả chi tiết về phương pháp quản lý khóa, người có hiểu biết trung bình trong lĩnh vực có thể biết rõ phương pháp triển khai của thiết bị quản lý khóa theo phương án thực hiện. Do vậy, để bản mô tả ngắn gọn, các chi tiết không được mô tả lại ở đây.

Fig.14 là sơ đồ 5 của thiết bị quản lý khóa công khai 140 theo sáng chế. Thiết bị quản lý khóa công khai 140 có thể bao gồm:

khối nhận 1401, được tạo cấu hình để nhận thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất;

khối xác định 1402, được tạo cấu hình để xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất, trong đó khóa công khai thứ nhất và khóa riêng tư thứ nhất là cặp khóa riêng tư-công khai thứ nhất;

khối giải mã 1403, được tạo cấu hình để giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã; và

khối gửi 1404, được tạo cấu hình để gửi thông tin danh tính người dùng được giải mã đến thiết bị mạng thứ ba, sao cho thiết bị mạng thứ ba xử lý thông tin

danh tính người dùng được giải mã.

Một cách tùy chọn, khối nhận 1401 được tạo cấu hình cụ thể để nhận thông điệp danh tính người dùng thứ ba được chuyển tiếp bởi thiết bị mạng thứ ba.

Một cách tùy chọn, thiết bị quản lý khóa 140 có thể còn bao gồm khối đánh giá 1405. Fig.15 là sơ đồ 6 của thiết bị quản lý khóa công khai 140 theo sáng chế.

Khối đánh giá 1405 được tạo cấu hình để xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ, trong đó

khối xác định 1402 được tạo cấu hình cụ thể để: khi khóa công khai thứ nhất trong chu kỳ hợp lệ, xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất.

Một cách tùy chọn, thiết bị quản lý khóa 140 có thể còn bao gồm:

khối thu thập 1406, được tạo cấu hình để thu được N cặp khóa riêng tư-công khai và N ID tham chiếu, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N cặp khóa riêng tư-công khai, cặp khóa riêng tư-công khai thứ nhất là một trong N cặp khóa riêng tư-công khai, và N là số nguyên lớn hơn 0.

Một cách tùy chọn, khối thu thập 1406 được tạo cấu hình cụ thể để tạo N cặp khóa riêng tư-công khai và phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Một cách tùy chọn, khối thu thập 1406 được tạo cấu hình cụ thể để tạo N cặp khóa riêng tư-công khai; và khối gửi 1404 còn được tạo cấu hình để gửi thông điệp yêu cầu ID tham chiếu đến thiết bị mạng thứ tư, trong đó thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết bị mạng thứ tư phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai; và

khối nhận 1401 còn được tạo cấu hình để nhận các khóa công khai trong N cặp khóa riêng tư-công khai và N ID tham chiếu được gửi bởi thiết bị mạng thứ tư.

Một cách tùy chọn, khối nhận 1401 còn được tạo cấu hình để nhận N cặp khóa riêng tư-công khai và N ID tham chiếu được gửi bởi thiết bị mạng thứ tư.

Một cách tùy chọn, khối thu thập 1406 còn được tạo cấu hình để thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai và thu được ID tham chiếu từ N ID tham chiếu; và

khối gửi 1404 còn được tạo cấu hình để gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Một cách tùy chọn, khối gửi 1404 còn được tạo cấu hình để gửi thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người dùng thứ tư dựa trên khóa công khai thứ nhất.

Một cách tùy chọn, khối gửi 1404 còn được tạo cấu hình để chuyển tiếp thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất bằng cách sử dụng thiết bị mạng thứ ba.

Một cách tùy chọn, khối gửi 1404 còn được tạo cấu hình để gửi thông điệp yêu cầu cập nhật khóa công khai đến UE khi khóa công khai thứ nhất không nằm trong chu kỳ hợp lệ, trong đó thông điệp yêu cầu cập nhật khóa công khai được sử dụng để ra lệnh UE cập nhật khóa công khai thứ nhất.

Một cách tùy chọn, khối nhận 1404 còn được tạo cấu hình để gửi bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu đến thiết bị mạng thứ nhất, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

khối nhận 1401 được tạo cấu hình cụ thể để nhận thông điệp danh tính người dùng thứ ba được gửi bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu.

Phương pháp quản lý khóa và các ví dụ cụ thể của thiết bị quản lý khóa theo các phương án thực hiện được thể hiện trên Fig.2A đến Fig.9 cũng áp dụng được cho thiết bị quản lý khóa theo phương án thực hiện. Từ các phần mô tả chi tiết về phương pháp quản lý khóa, người có hiểu biết trung bình trong lĩnh vực có thể biết rõ phương pháp triển khai của thiết bị quản lý khóa theo phương án thực hiện. Do vậy, để mô tả ngắn gọn, các chi tiết không được mô tả lại ở đây.

Fig.16 là sơ đồ 7 của thiết bị quản lý khóa công khai 160 theo sáng chế. Thiết bị quản lý khóa công khai 160 có thể bao gồm:

khối nhận 1601, được tạo cấu hình để nhận thông điệp danh tính người sử dụng thứ nhất được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp danh tính người sử dụng thứ nhất bao gồm thông tin danh tính người dùng, ID chỉ báo được sử dụng để chỉ báo liệu thông tin danh tính người dùng được mật mã hóa, và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất;

khối xác định 1602, được tạo cấu hình để: nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định, dựa trên ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu; và

khối gửi 1603, được tạo cấu hình để gửi thông điệp danh tính người dùng thứ ba đến thiết bị mạng thứ hai dựa trên thông tin nhận dạng của thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ ba bao gồm thông tin danh tính người dùng và ID tham chiếu được sử dụng để đánh chỉ mục khóa công khai thứ nhất, sao cho thiết bị mạng thứ hai xử lý thông điệp danh tính người dùng thứ ba dựa trên ID tham chiếu.

Một cách tùy chọn, khối nhận 1601 còn được tạo cấu hình để nhận thông điệp danh tính người dùng thứ tư được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp danh tính người dùng thứ tư bao gồm thông tin danh tính người dùng được giải mã và khóa công khai thứ nhất; và

khối gửi 1603 còn được tạo cấu hình để gửi thông điệp danh tính người dùng thứ tư đến thiết bị mạng thứ nhất, sao cho thiết bị mạng thứ nhất xử lý thông điệp danh tính người dùng thứ tư dựa trên khóa công khai thứ nhất.

Một cách tùy chọn, khối nhận 1601 còn được tạo cấu hình để nhận thông tin lệnh được gửi bởi thiết bị mạng thứ nhất, trong đó thông điệp lệnh bao gồm thông tin danh tính người dùng được giải mã, và thông tin lệnh được sử dụng để ra lệnh thiết bị mạng thứ ba xử lý thông tin danh tính người dùng được giải mã.

Một cách tùy chọn, khối nhận 1601 còn được tạo cấu hình để nhận bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu và được gửi bởi thiết bị mạng thứ hai, trong đó N ID tham chiếu được sử dụng để

đánh chỉ mục tương ứng một - một N khóa công khai, khóa công khai thứ nhất là một trong N khóa công khai, và N là số nguyên lớn hơn 0; và

khối xác định 1602 được tạo cấu hình cụ thể để xác định, theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ hai và N ID tham chiếu, thông tin nhận dạng của thiết bị mạng thứ hai tương ứng với ID tham chiếu.

Một cách tùy chọn, khối gửi 1603 còn được tạo cấu hình để gửi bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ ba và N ID tham chiếu đến thiết bị mạng thứ nhất; và

khối nhận 1601 được tạo cấu hình cụ thể để nhận thông điệp danh tính người sử dụng thứ nhất của UE được chuyển tiếp bởi thiết bị mạng thứ nhất theo bảng ánh xạ giữa thông tin nhận dạng của thiết bị mạng thứ ba và N ID tham chiếu.

Phương pháp quản lý khóa và các ví dụ cụ thể của thiết bị quản lý khóa theo các phương án thực hiện được thể hiện trên các hình vẽ từ Fig.2A đến Fig.9 cũng áp dụng được cho thiết bị quản lý khóa theo phương án thực hiện. Từ các phần mô tả chi tiết về phương pháp quản lý khóa, người có hiểu biết trung bình trong lĩnh vực có thể biết rõ phương pháp triển khai của thiết bị quản lý khóa theo phương án thực hiện. Do vậy, để bản mô tả ngắn gọn, các chi tiết không được mô tả lại ở đây.

Fig.17 là sơ đồ 8 của thiết bị quản lý khóa công khai 170 theo sáng chế. Thiết bị quản lý khóa công khai 170 có thể bao gồm:

khối thu thập 1701, được tạo cấu hình để thu được N khóa công khai, trong đó N là số nguyên lớn hơn 0;

khối phân phối 1702, được tạo cấu hình để phân phối N ID tham chiếu đến N khóa công khai, trong đó N ID tham chiếu được sử dụng để đánh chỉ mục tương ứng một - một N khóa công khai; và

khối gửi 1703, được tạo cấu hình để gửi N khóa công khai và N ID tham chiếu đến thiết bị mạng thứ hai, sao cho thiết bị mạng thứ hai thu được N khóa công khai và N ID tham chiếu.

Một cách tùy chọn, khối thu thập 1701 được tạo cấu hình cụ thể để tạo N cặp khóa riêng tư-công khai, trong đó mỗi cặp khóa công khai - riêng tư bao gồm khóa công khai và khóa riêng tư, và N khóa công khai là các khóa công khai

trong N cặp khóa riêng tư-công khai; và

khối gửi 1703 còn được tạo cấu hình để gửi N cặp khóa riêng tư-công khai và N ID tham chiếu đến thiết bị mạng thứ hai.

Một cách tùy chọn, khối nhận còn được tạo cấu hình để nhận thông điệp yêu cầu ID tham chiếu được gửi bởi thiết bị mạng thứ hai, trong đó thông điệp yêu cầu ID tham chiếu bao gồm các khóa công khai trong N cặp khóa riêng tư-công khai, và thông điệp yêu cầu ID tham chiếu được sử dụng để yêu cầu thiết bị mạng thứ tư phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai.

Một cách tùy chọn, khối thu thập 1701 còn được tạo cấu hình để thu được khóa công khai thứ nhất từ N khóa công khai, và thu được, từ N ID tham chiếu, ID tham chiếu được sử dụng để đánh chỉ mục khóa thứ nhất; và

khối gửi 1703 còn được tạo cấu hình để gửi khóa công khai thứ nhất và ID tham chiếu đến UE.

Phương pháp quản lý khóa và các ví dụ cụ thể của thiết bị quản lý khóa theo các phương án thực hiện được thể hiện trên Fig.2A đến Fig.9 cũng áp dụng được cho thiết bị quản lý khóa theo phương án thực hiện. Từ các phần mô tả chi tiết về phương pháp quản lý khóa, người có hiểu biết trung bình trong lĩnh vực có thể biết rõ phương pháp triển khai của thiết bị quản lý khóa theo phương án thực hiện. Do vậy, để mô tả ngắn gọn, các chi tiết không được mô tả lại ở đây.

Fig.18 là sơ đồ khối của thiết bị 180 theo sáng chế. Dựa vào Fig.18, thiết bị 180 bao gồm bộ xử lý 1801 và bộ nhớ 1802.

Bộ nhớ 1802 được tạo cấu hình để lưu trữ lệnh, và bộ xử lý 1801 được tạo cấu hình để thực thi lệnh được lưu trữ trong bộ nhớ 1802. Khi bộ xử lý 1801 thực thi lệnh được lưu trữ trong bộ nhớ 1802, thiết bị 180 thực hiện phương pháp theo phương án thực hiện bất kỳ trên Fig.2A đến Fig.9.

Nên hiểu rằng bộ xử lý 1801 có thể là khối xử lý trung tâm (Central Processing Unit, CPU), hoặc có thể là bộ xử lý đa năng 1801 khác, bộ xử lý tín hiệu số 1801 (Digital Signal Processor, DSP), mạch tích hợp ứng dụng cụ thể (Application Specific Integrated Circuit, ASIC), hoặc tương tự. Bộ xử lý đa năng 1801 có thể là bộ vi xử lý 1801, hoặc bộ xử lý 1801 có thể là bộ xử lý 1801

truyền thống bất kỳ hoặc tương tự. Các bước của các phương pháp được bộc lộ dựa vào sáng chế có thể được triển khai ngay bằng bộ xử lý phần cứng 1801, hoặc có thể được triển khai bằng tổ hợp của phần cứng và môđun phần mềm trong bộ xử lý 1801.

Tất cả hoặc một số bước của phương pháp nêu trên theo các phương án thực hiện có thể được triển khai bằng cách sử dụng phần cứng liên quan đến lệnh chương trình. Chương trình nêu trên có thể được lưu trữ trong bộ nhớ máy tính đọc được 1802. Khi chương trình được thực thi, các bước của các phương pháp theo các phương án thực hiện được thực hiện. Bộ nhớ 1802 (vật lưu trữ) bao gồm: bộ nhớ chỉ đọc (read-only memory, ROM) 1802, bộ nhớ truy nhập ngẫu nhiên (Random access memory, RAM), bộ nhớ nhanh 1802, đĩa cứng, ổ trạng thái rắn (solid state disk, SS), băng từ, đĩa mềm, đĩa quang, và tổ hợp bất kỳ của nó.

Sáng chế còn đề xuất vật lưu trữ máy tính đọc được, và vật lưu trữ máy tính đọc được lưu trữ lệnh.

Khi ít nhất một bộ xử lý của UE thực thi lệnh, UE thực hiện phương pháp quản lý khóa theo phương pháp các phương án thực hiện trên Fig.2A đến Fig.9.

Sáng chế còn đề xuất vật lưu trữ máy tính đọc được, và vật lưu trữ máy tính đọc được lưu trữ lệnh. Khi ít nhất một bộ xử lý của thiết bị mạng thực hiện lệnh, thiết bị mạng thực hiện phương pháp quản lý khóa theo phương pháp các phương án thực hiện trên Fig.2A đến Fig.9.

Các phần mô tả nêu trên chỉ là các triển khai cụ thể của sáng chế, nhưng không nhằm giới hạn phạm vi bảo hộ của sáng chế. Biến thể hoặc thay thế bất kỳ mà người có hiểu biết trung bình trong lĩnh vực đoán ra được trong phạm vi kỹ thuật được bộc lộ theo sáng chế sẽ nằm trong phạm vi bảo hộ của sáng chế. Do vậy, phạm vi bảo hộ của sáng chế sẽ phụ thuộc vào phạm vi bảo hộ của các điểm yêu cầu bảo hộ.

YÊU CẦU BẢO HỘ

1. Phương pháp quản lý khóa được thực hiện bởi thiết bị người dùng (user equipment, UE), trong đó phương pháp bao gồm các bước:

xác định liệu có mật mã hóa thông tin định danh người dùng không được mật mã hóa; và

thực hiện, dựa trên xác định này, một trong nhóm bao gồm:

thu được, theo xác định mật mã hóa thông tin định danh người dùng, thông tin định danh người dùng được mật mã hóa bằng cách:

mật mã hóa thông tin định danh người dùng không được mật mã hóa dựa trên khóa công khai thứ nhất; và

gửi thông tin định danh người dùng thứ nhất đến thiết bị thực hiện chức năng quản lý và truy nhập (access and management function, AMF), trong đó thông tin định danh người dùng thứ nhất bao gồm thông tin định danh người dùng được mật mã hóa, định danh chỉ báo thứ nhất, và định danh tham chiếu, trong đó định danh chỉ báo thứ nhất là giá trị khác 0 để chỉ báo rằng thông tin định danh người dùng ở trạng thái được mật mã hóa, và trong đó định danh tham chiếu là giá trị khác 0 để đánh chỉ số khóa công khai thứ nhất; và

gửi, theo xác định không mật mã hóa thông tin định danh người dùng, thông điệp định danh người dùng thứ hai đến thiết bị AMF, trong đó thông điệp định danh người dùng thứ hai bao gồm thông tin định danh người dùng không được mật mã hóa, định danh chỉ báo thứ hai, và định danh khóa công khai, trong đó giá trị của định danh chỉ báo thứ hai bằng 0 để chỉ báo rằng thông tin định danh người dùng ở trạng thái không được mật mã hóa, và giá trị của định danh khóa công khai bằng 0.

2. Phương pháp theo điểm 1, trong đó trước khi mật mã hóa thông tin định danh người dùng không được mật mã hóa dựa trên khóa công khai thứ nhất, phương pháp còn bao gồm bước:

xác định, bởi UE, liệu khóa công khai thứ nhất trong chu kỳ hợp lệ; và

bước mật mã hóa, bởi UE, thông tin định danh người dùng dựa trên khóa công khai thứ nhất bao gồm bước:

khi khóa công khai thứ nhất trong chu kỳ hợp lệ, mật mã hóa, bởi UE, thông

tin định danh người dùng dựa trên khóa công khai thứ nhất.

3. Phương pháp theo điểm 1, trong đó khóa công khai là rỗng (null) khi giá trị của định danh khóa công khai bằng 0.

4. Thiết bị quản lý khóa, trong đó thiết bị bao gồm:

bộ xử lý; và

vật ghi máy tính đọc được bất biến bao gồm các lệnh máy tính thực thi được mà, khi được thực thi bởi bộ xử lý, tạo thuận tiện thiết bị quản lý khóa thực hiện phương pháp bao gồm các bước:

xác định liệu có mật mã hóa thông tin định danh người dùng không được mật mã hóa; và

thực hiện, dựa trên xác định này, một trong nhóm bao gồm:

thu được, theo xác định mật mã hóa thông tin định danh người dùng, thông tin định danh người dùng được mật mã hóa bằng cách:

mật mã hóa thông tin định danh người dùng không được mật mã hóa dựa trên khóa công khai thứ nhất; và

gửi thông tin định danh người dùng thứ nhất đến thiết bị AMF, trong đó thông tin định danh người dùng thứ nhất bao gồm thông tin định danh người dùng được mật mã hóa, định danh chỉ báo thứ nhất, và định danh tham chiếu, trong đó định danh chỉ báo thứ nhất là giá trị khác 0 để chỉ báo rằng thông tin định danh người dùng ở trạng thái được mật mã hóa, và trong đó định danh tham chiếu là giá trị khác 0 để đánh chỉ số khóa công khai thứ nhất; và

gửi, theo xác định không mật mã hóa thông tin định danh người dùng, thông điệp định danh người dùng thứ hai đến thiết bị AMF, trong đó thông điệp định danh người dùng thứ hai bao gồm thông tin định danh người dùng không được mật mã hóa, định danh chỉ báo thứ hai, và định danh khóa công khai, trong đó giá trị của định danh chỉ báo thứ hai bằng 0 để chỉ báo rằng thông tin định danh người dùng ở trạng thái không được mật mã hóa, và giá trị của định danh khóa công khai bằng 0.

5. Thiết bị theo điểm 4, trong đó khi được thực thi bằng bộ xử lý, tạo thuận tiện cho thiết bị quản lý khóa thực hiện phương pháp còn bao gồm bước:

xác định liệu khóa công khai thứ nhất trong chu kỳ hợp lệ; và

khi khóa công khai thứ nhất trong chu kỳ hợp lệ, mật mã hóa, bởi UE, thông tin định danh người dùng dựa trên khóa công khai thứ nhất.

6. Thiết bị theo điểm 4, trong đó khóa công khai là null khi giá trị của định danh khóa công khai bằng 0.

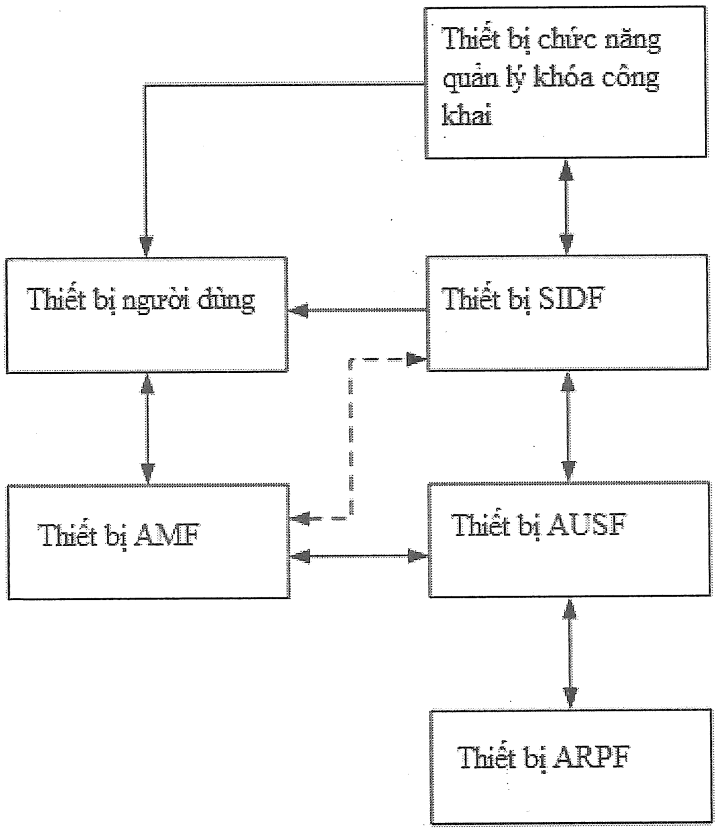

Thiết bị chức năng quản lý khóa công khai
Thiết bị người dùng
Thiết bị SIDF
Thiết bị AMF
Thiết bị AUSF
Thiết bị ARPF

Fig.1

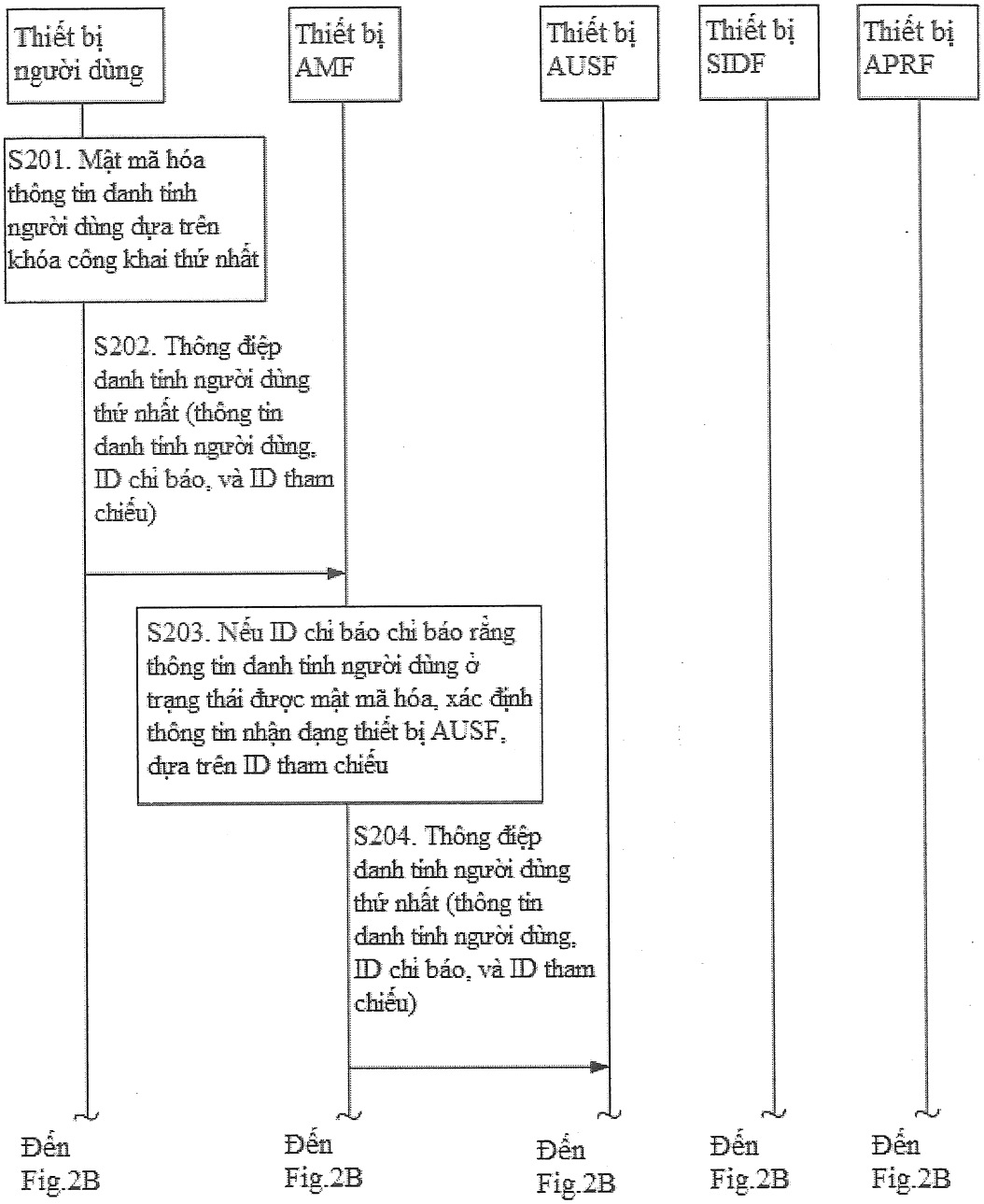

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
Thiết bị APRF
S201. Mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất
S202. Thông điệp danh tính người dùng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S203. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị AUSF, dựa trên ID tham chiếu
S204. Thông điệp danh tính người dùng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B
Đến Fig.2B

Fig.2A

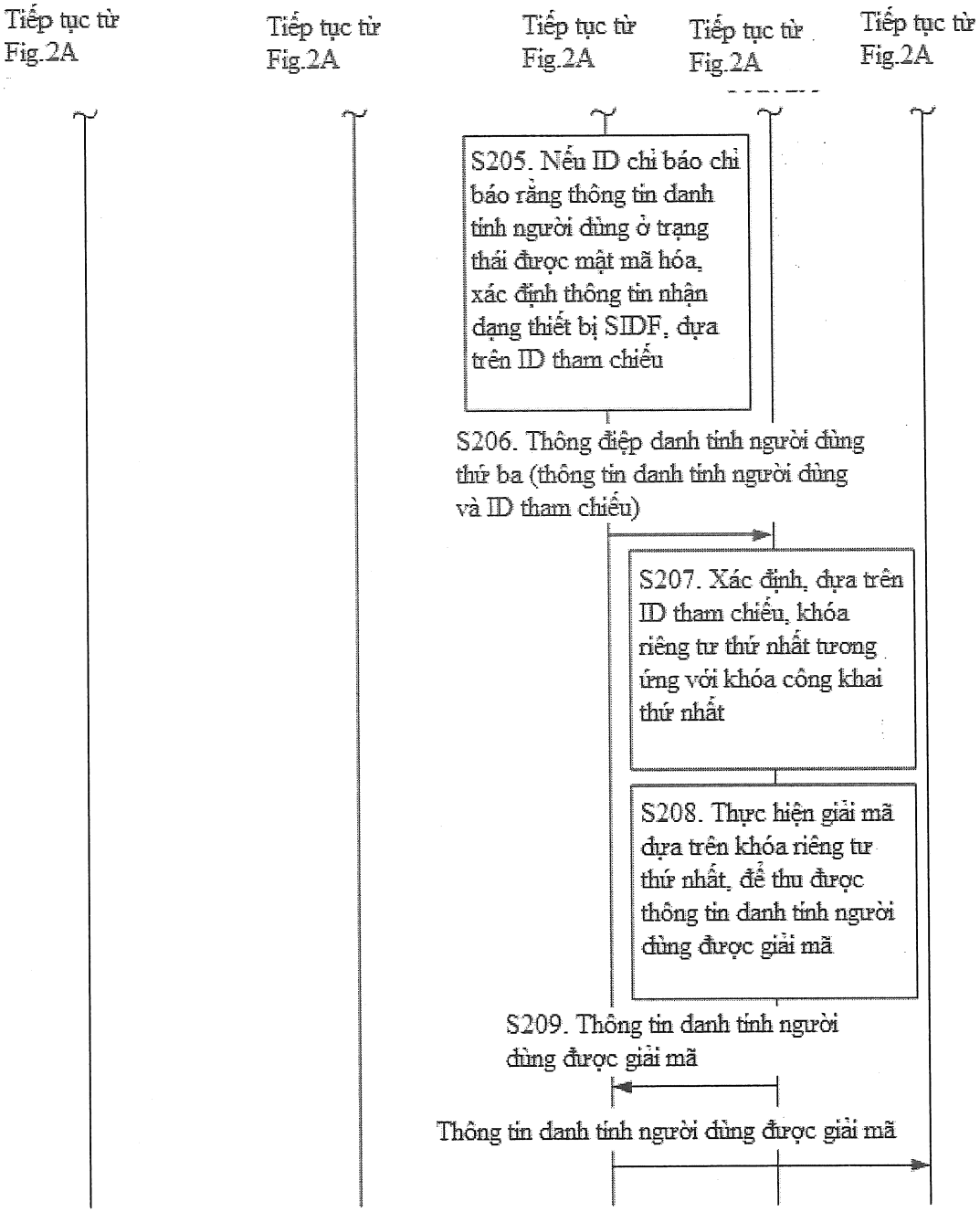

Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
Tiếp tục từ Fig.2A
S205. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị SIDF, dựa trên ID tham chiếu
S206. Thông điệp danh tính người dùng thứ ba (thông tin danh tính người dùng và ID tham chiếu)
S207. Xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất
S208. Thực hiện giải mã dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã
S209. Thông tin danh tính người dùng được giải mã
Thông tin danh tính người dùng được giải mã

Fig.2B

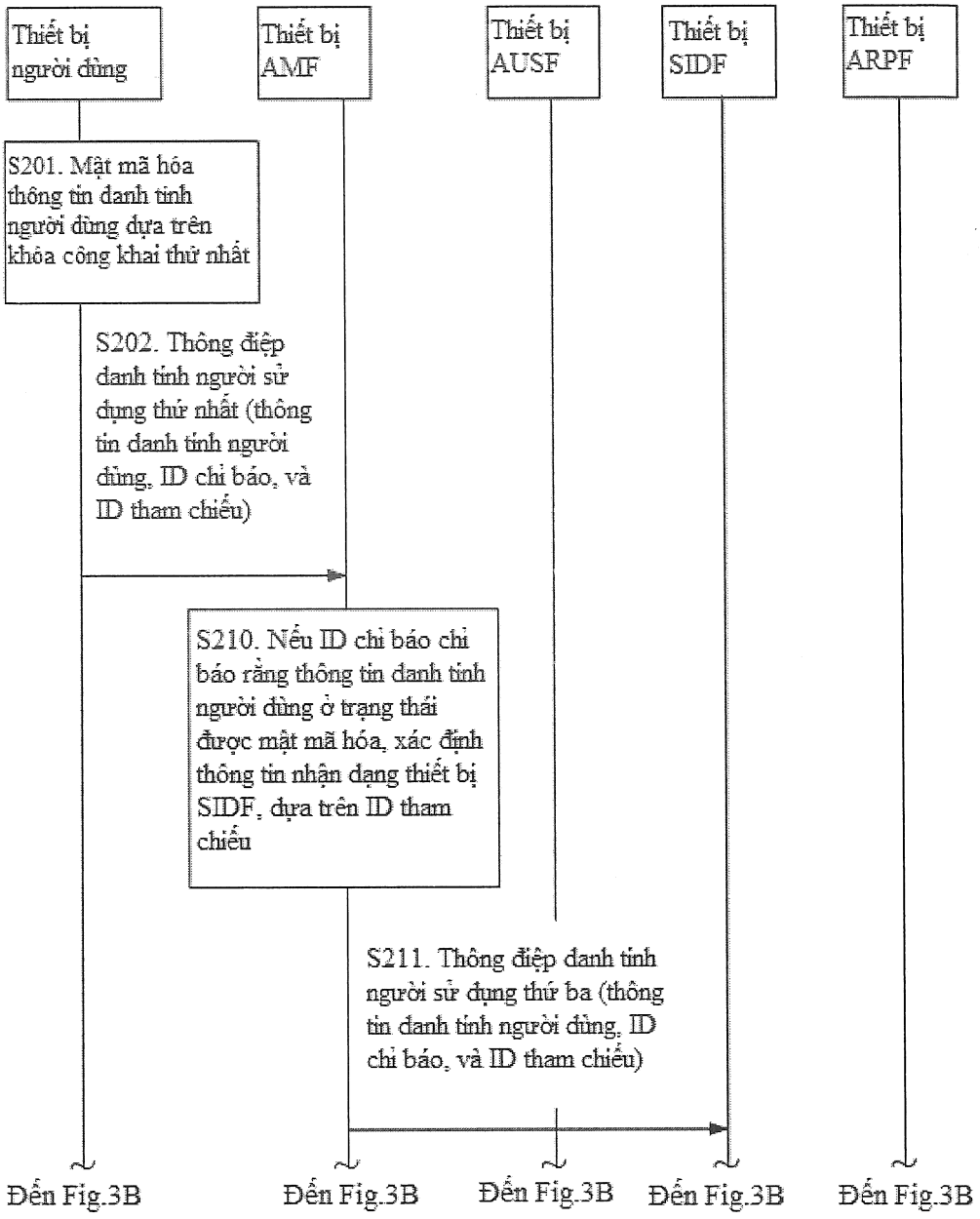

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
Thiết bị ARPF
S201. Mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất
S202. Thông điệp danh tính người sử dụng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S210. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị SIDF, dựa trên ID tham chiếu
S211. Thông điệp danh tính người sử dụng thứ ba (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
Đến Fig.3B
Đến Fig.3B
Đến Fig.3B
Đến Fig.3B
Đến Fig.3B

Fig.3A

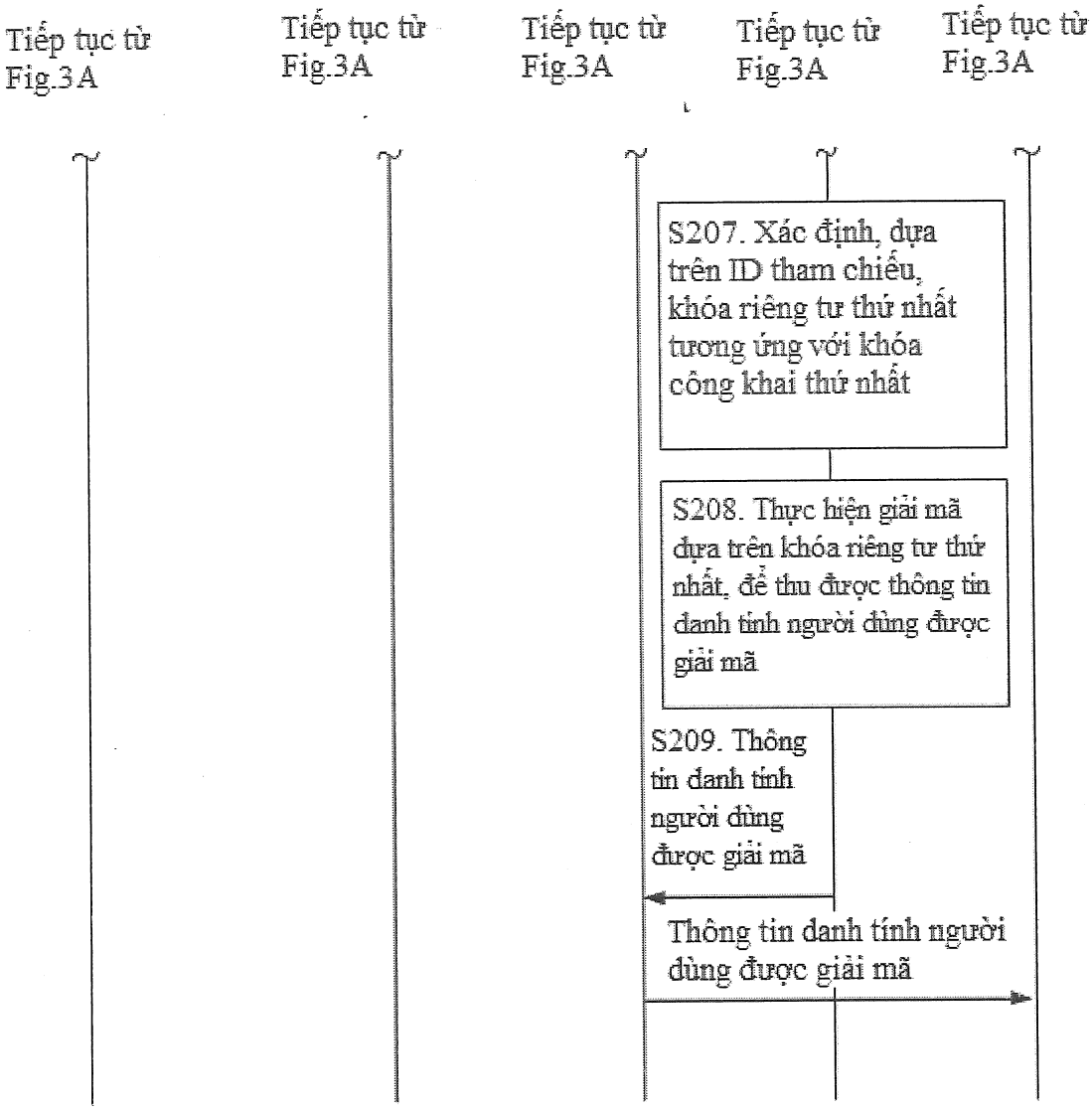

Tiếp tục từ Fig.3A
Tiếp tục từ Fig.3A
Tiếp tục từ Fig.3A
Tiếp tục từ Fig.3A
Tiếp tục từ Fig.3A
S207. Xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất
S208. Thực hiện giải mã dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã
S209. Thông tin danh tính người dùng được giải mã
Thông tin danh tính người dùng được giải mã

Fig.3B

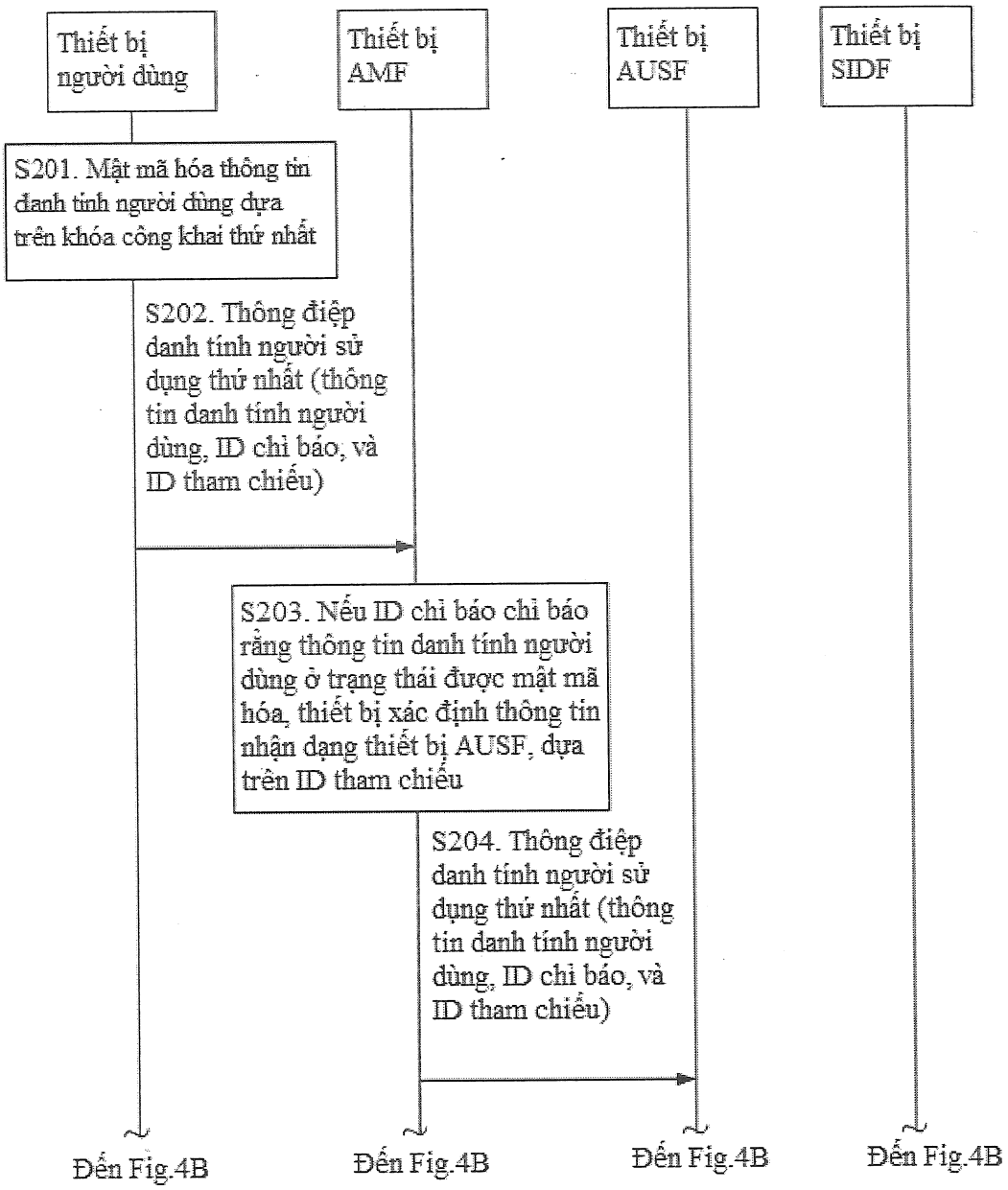

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
S201. Mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất
S202. Thông điệp danh tính người sử dụng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S203. Nếu ID chỉ báo chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, thiết bị xác định thông tin nhận dạng thiết bị AUSF, dựa trên ID tham chiếu
S204. Thông điệp danh tính người sử dụng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
Đến Fig.4B
Đến Fig.4B
Đến Fig.4B
Đến Fig.4B

Fig.4A

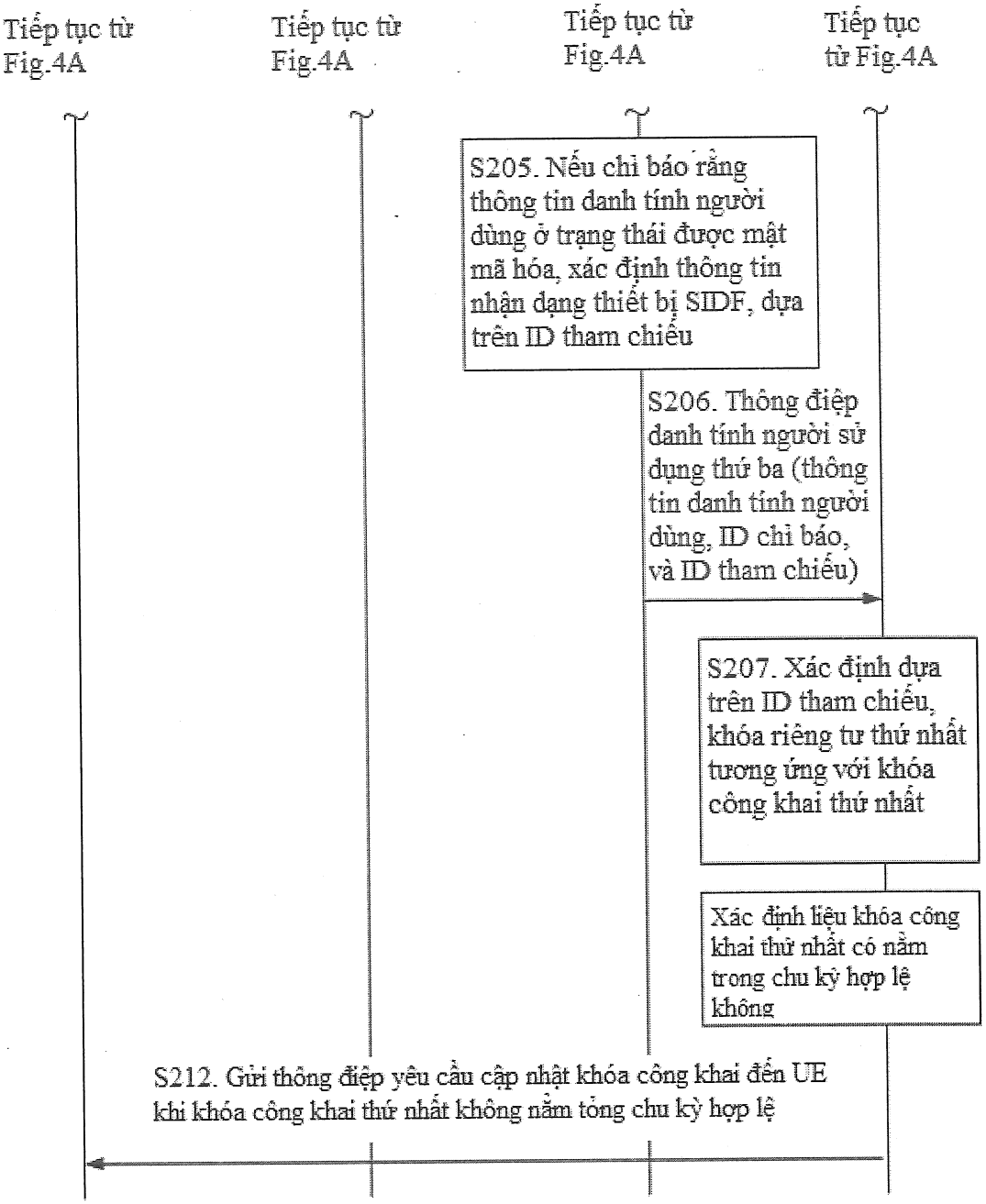

Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
Tiếp tục từ Fig.4A
S205. Nếu chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị SIDF, dựa trên ID tham chiếu
S206. Thông điệp danh tính người sử dụng thứ ba (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S207. Xác định dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất
Xác định liệu khóa công khai thứ nhất có nằm trong chu kỳ hợp lệ không
S212. Gửi thông điệp yêu cầu cập nhật khóa công khai đến UE khi khóa công khai thứ nhất không nằm tòng chu kỳ hợp lệ

Fig.4B

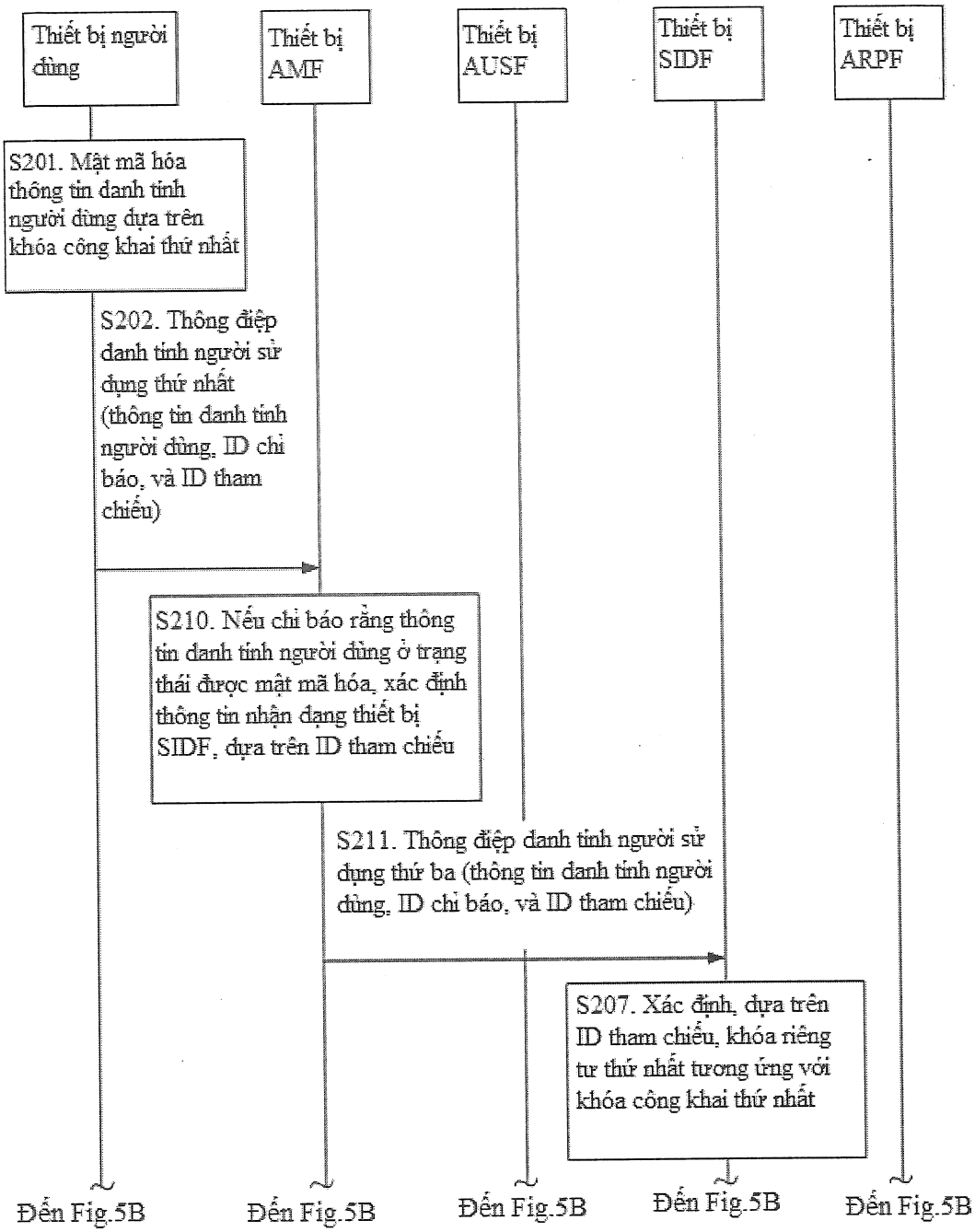

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
Thiết bị ARPF
S201. Mật mã hóa thông tin danh tính người dùng dựa trên khóa công khai thứ nhất
S202. Thông điệp danh tính người sử dụng thứ nhất (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S210. Nếu chỉ báo rằng thông tin danh tính người dùng ở trạng thái được mật mã hóa, xác định thông tin nhận dạng thiết bị SIDF, dựa trên ID tham chiếu
S211. Thông điệp danh tính người sử dụng thứ ba (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S207. Xác định, dựa trên ID tham chiếu, khóa riêng tư thứ nhất tương ứng với khóa công khai thứ nhất
Đến Fig.5B
Đến Fig.5B
Đến Fig.5B
Đến Fig.5B
Đến Fig.5B

Fig.5A

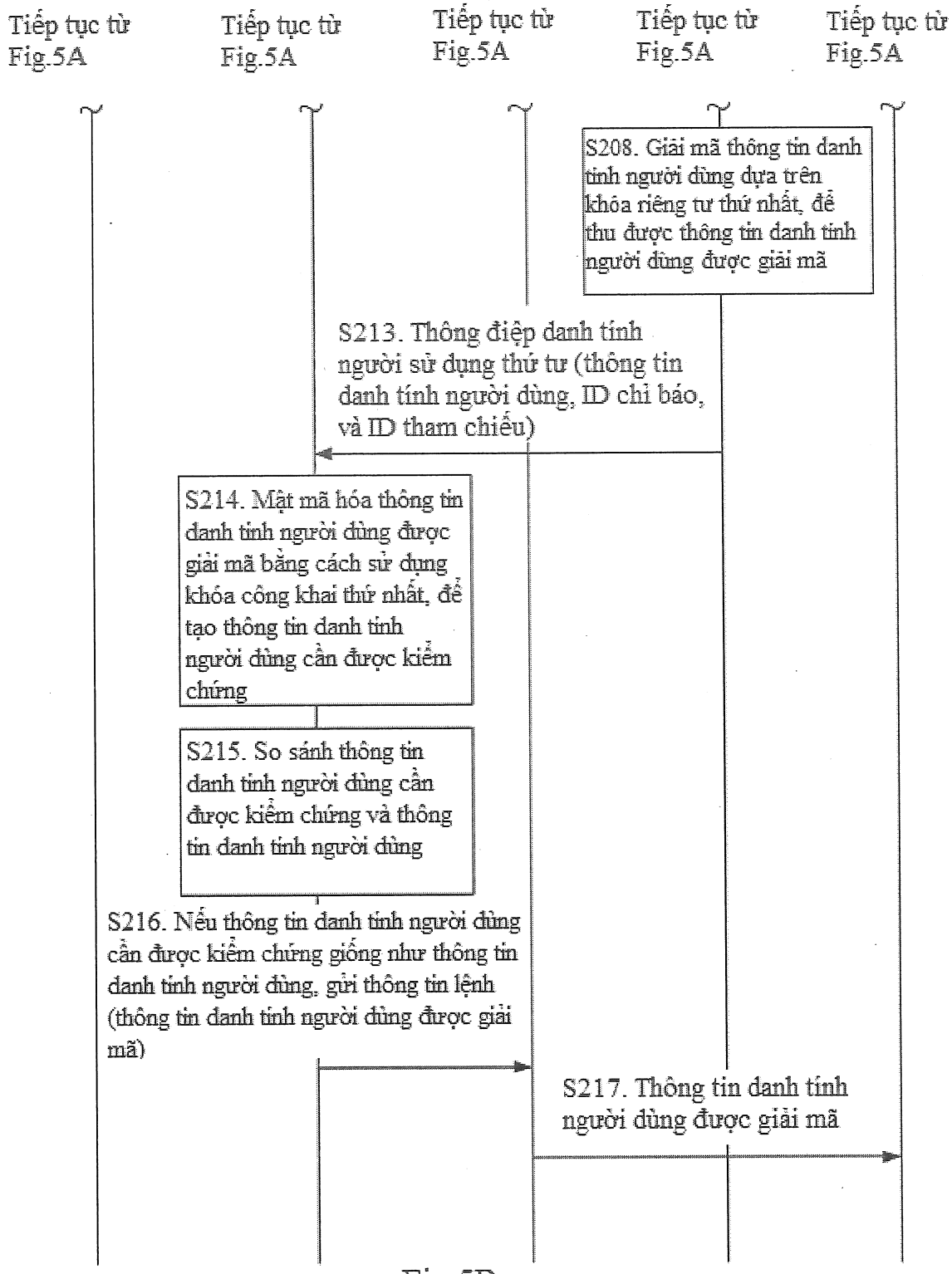

Tiếp tục từ Fig.5A
Tiếp tục từ Fig.5A
Tiếp tục từ Fig.5A
Tiếp tục từ Fig.5A
Tiếp tục từ Fig.5A
S208. Giải mã thông tin danh tính người dùng dựa trên khóa riêng tư thứ nhất, để thu được thông tin danh tính người dùng được giải mã
S213. Thông điệp danh tính người sử dụng thứ tư (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S214. Mật mã hóa thông tin danh tính người dùng được giải mã bằng cách sử dụng khóa công khai thứ nhất, để tạo thông tin danh tính người dùng cần được kiểm chứng
S215. So sánh thông tin danh tính người dùng cần được kiểm chứng và thông tin danh tính người dùng
S216. Nếu thông tin danh tính người dùng cần được kiểm chứng giống như thông tin danh tính người dùng, gửi thông tin lệnh (thông tin danh tính người dùng được giải mã)
S217. Thông tin danh tính người dùng được giải mã

Fig.5B

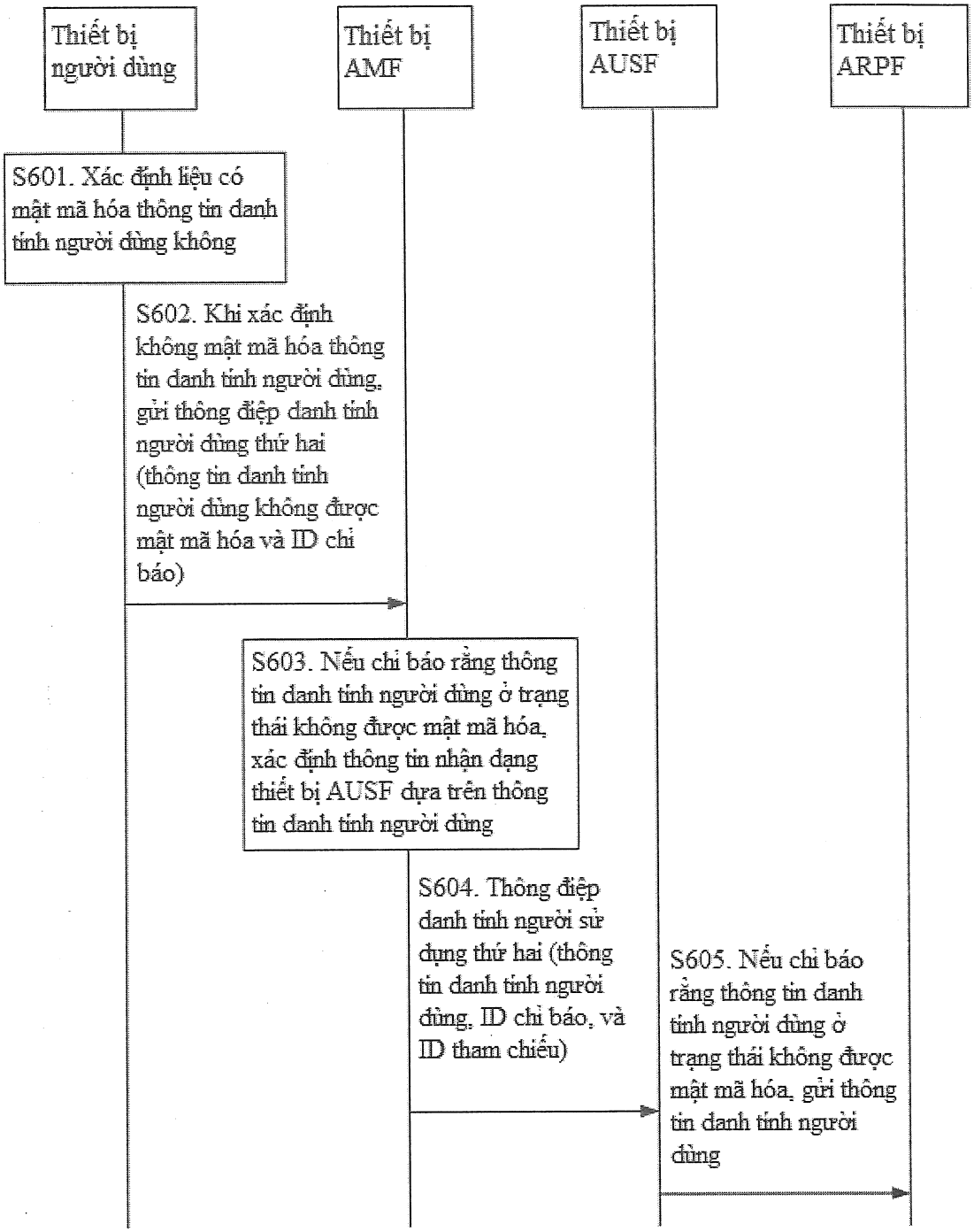

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị ARPF
S601. Xác định liệu có mật mã hóa thông tin danh tính người dùng không
S602. Khi xác định không mật mã hóa thông tin danh tính người dùng, gửi thông điệp danh tính người dùng thứ hai (thông tin danh tính người dùng không được mật mã hóa và ID chỉ báo)
S603. Nếu chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, xác định thông tin nhận dạng thiết bị AUSF dựa trên thông tin danh tính người dùng
S604. Thông điệp danh tính người sử dụng thứ hai (thông tin danh tính người dùng, ID chỉ báo, và ID tham chiếu)
S605. Nếu chỉ báo rằng thông tin danh tính người dùng ở trạng thái không được mật mã hóa, gửi thông tin danh tính người dùng

Fig.6

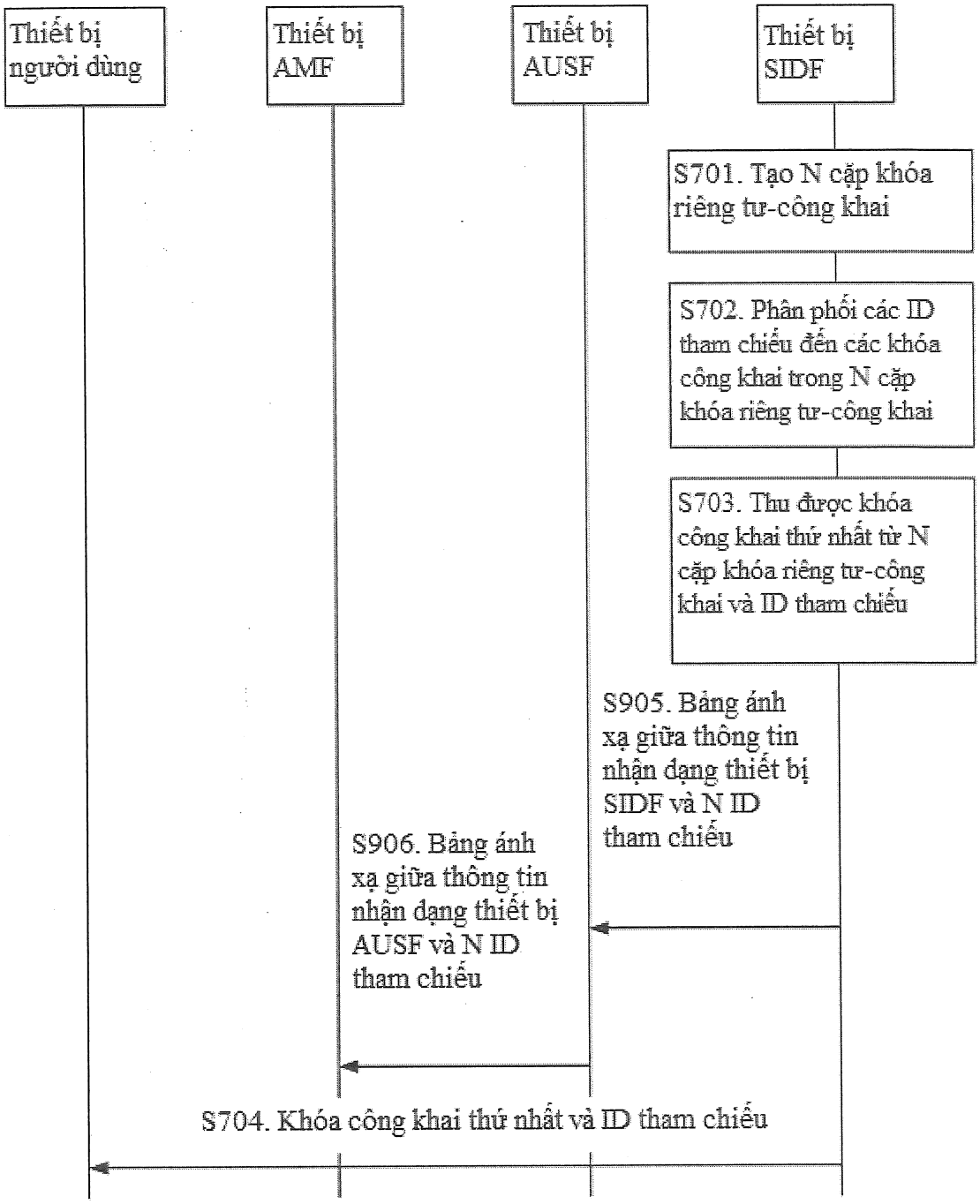

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
S701. Tạo N cặp khóa riêng tư-công khai
S702. Phân phối các ID tham chiếu đến các khóa công khai trong N cặp khóa riêng tư-công khai
S703. Thu được khóa công khai thứ nhất từ N cặp khóa riêng tư-công khai và ID tham chiếu
S905. Bảng ánh xạ giữa thông tin nhận dạng thiết bị SIDF và N ID tham chiếu
S906. Bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu
S704. Khóa công khai thứ nhất và ID tham chiếu

Fig.7

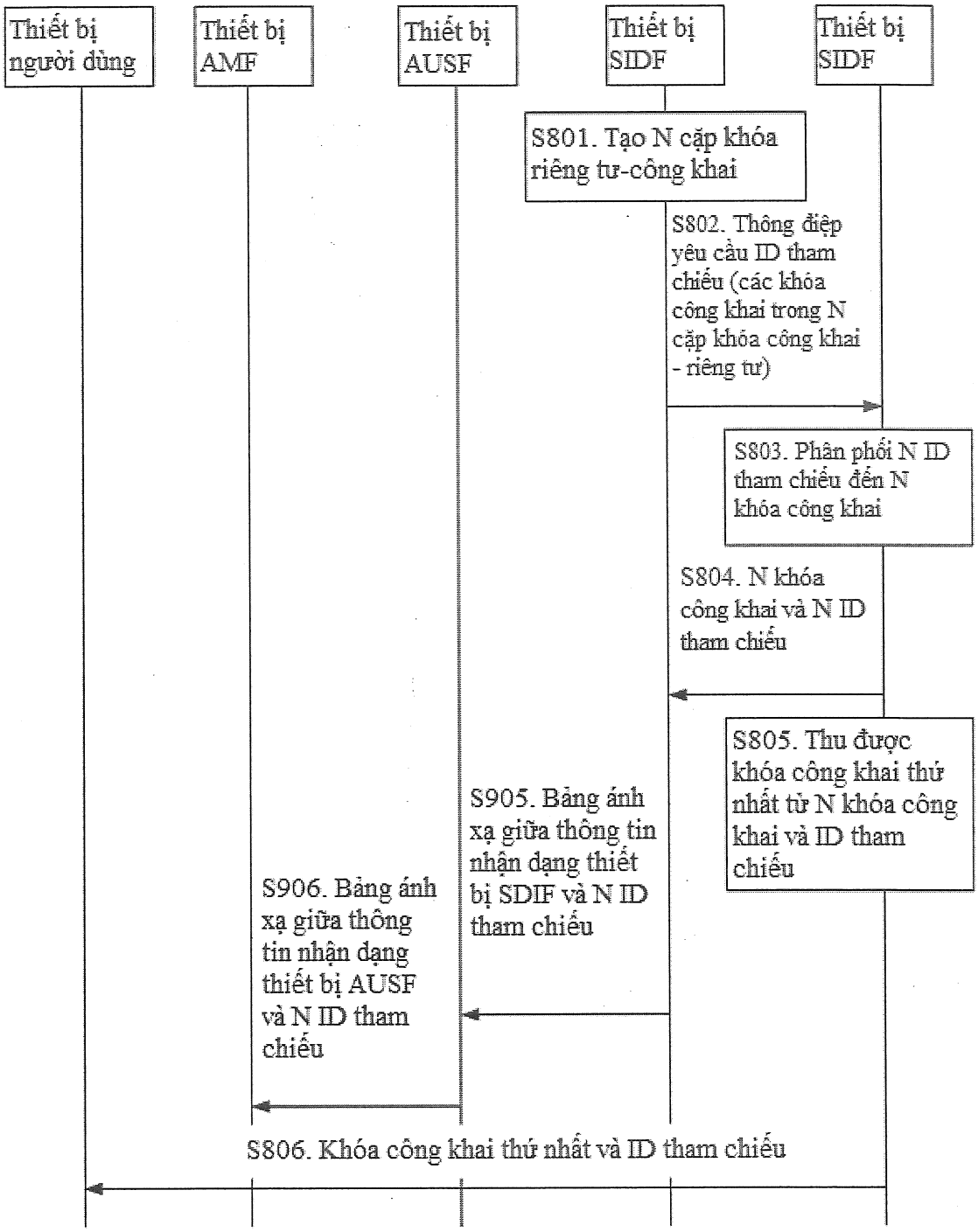

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
Thiết bị SIDF
S801. Tạo N cặp khóa riêng tư-công khai
S802. Thông điệp yêu cầu ID tham chiếu (các khóa công khai trong N cặp khóa công khai - riêng tư)
S803. Phân phối N ID tham chiếu đến N khóa công khai
S804. N khóa công khai và N ID tham chiếu
S805. Thu được khóa công khai thứ nhất từ N khóa công khai và ID tham chiếu
S905. Bảng ánh xạ giữa thông tin nhận dạng thiết bị SDIF và N ID tham chiếu
S906. Bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu
S806. Khóa công khai thứ nhất và ID tham chiếu

Fig.8

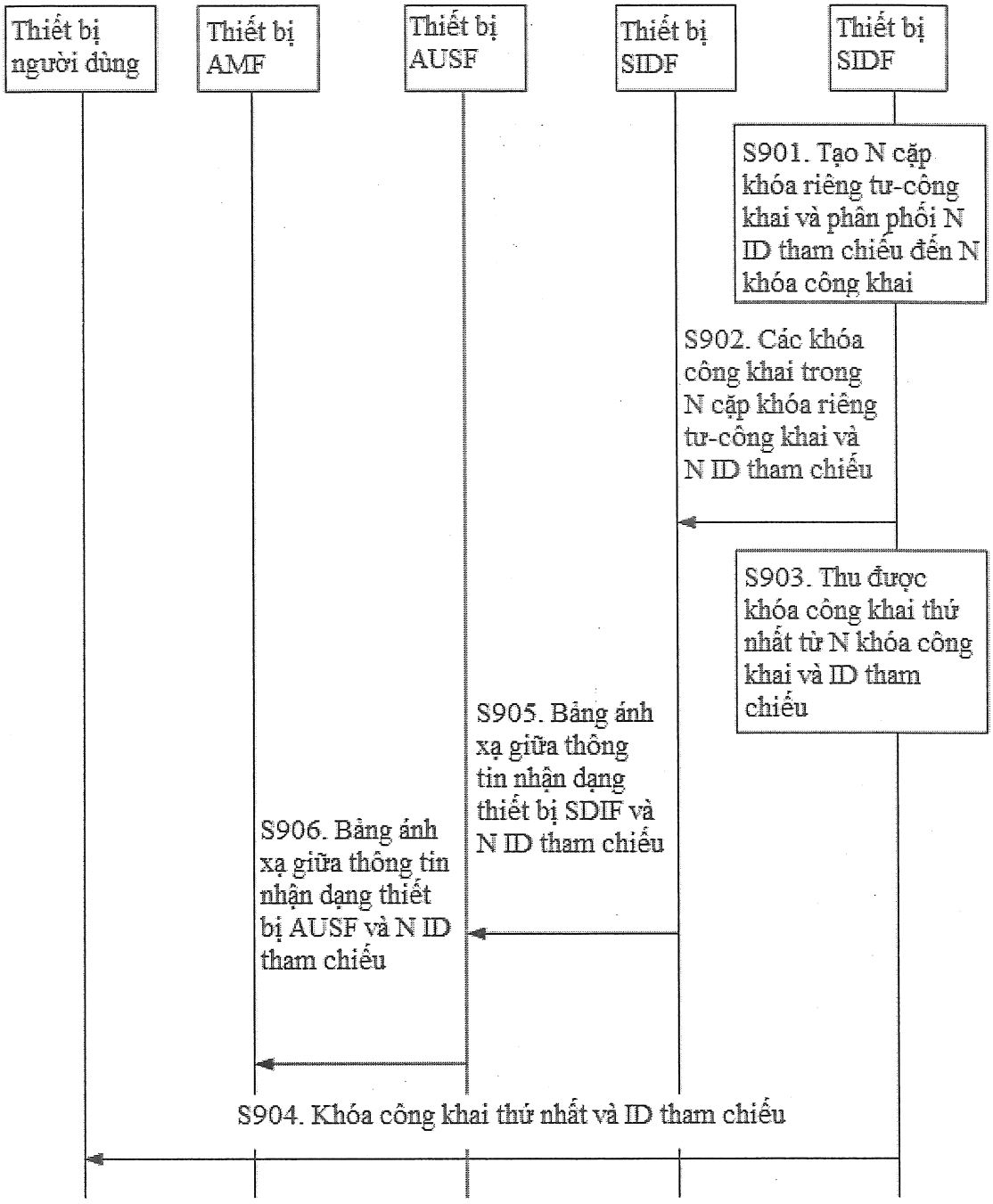

Thiết bị người dùng
Thiết bị AMF
Thiết bị AUSF
Thiết bị SIDF
Thiết bị SIDF
S901. Tạo N cặp khóa riêng tư-công khai và phân phối N ID tham chiếu đến N khóa công khai
S902. Các khóa công khai trong N cặp khóa riêng tư-công khai và N ID tham chiếu
S903. Thu được khóa công khai thứ nhất từ N khóa công khai và ID tham chiếu
S905. Bảng ánh xạ giữa thông tin nhận dạng thiết bị SDIF và N ID tham chiếu
S906. Bảng ánh xạ giữa thông tin nhận dạng thiết bị AUSF và N ID tham chiếu
S904. Khóa công khai thứ nhất và ID tham chiếu

Fig.9

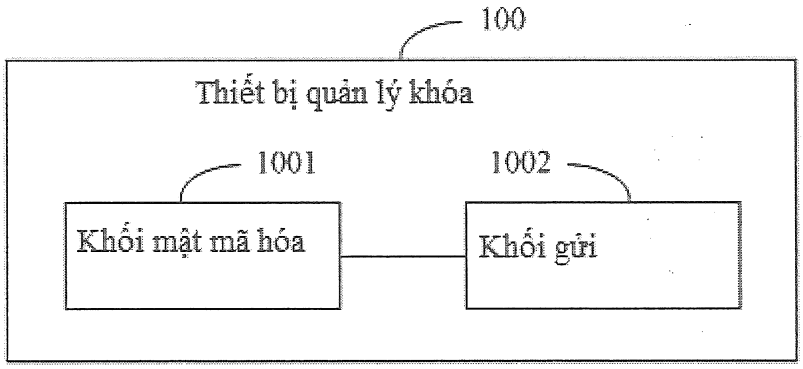

100
Thiết bị quản lý khóa
1001
1002
Khối mật mã hóa
Khối gửi

Fig.10

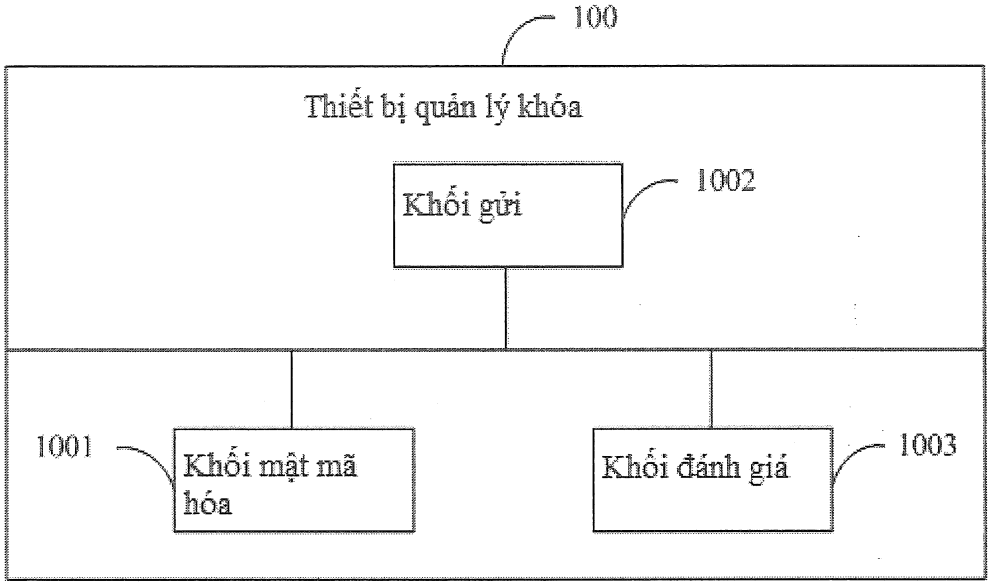

100
Thiết bị quản lý khóa
Khối gửi
1002
1001
Khối mật mã hóa
Khối đánh giá
1003

Fig.11

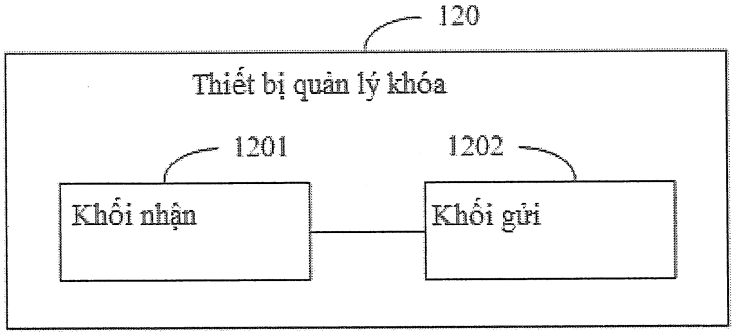

120
Thiết bị quản lý khóa
1201
1202
Khối nhận
Khối gửi

Fig.12

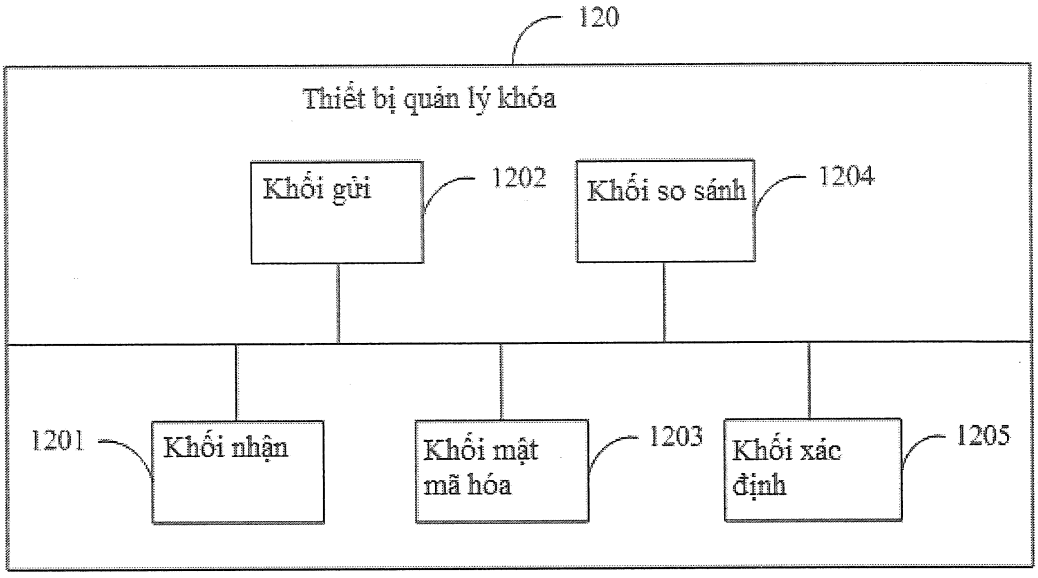

120
Thiết bị quản lý khóa
Khối gửi
1202
Khối so sánh
1204
1201
Khối nhận
Khối mật mã hóa
1203
Khối xác định
1205

Fig.13

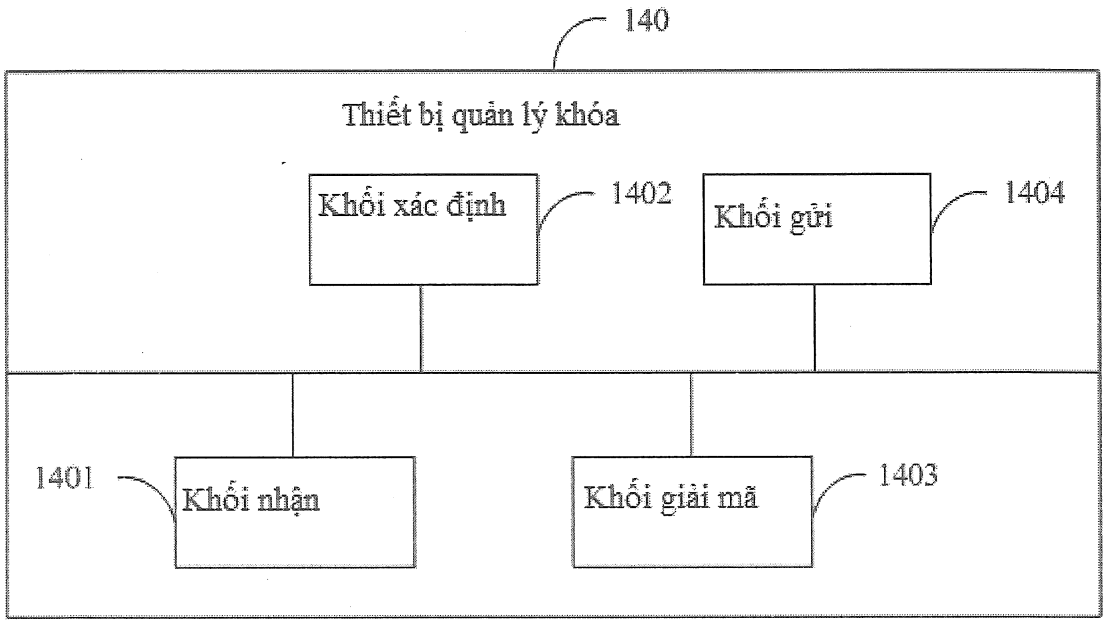

140
Thiết bị quản lý khóa
Khối xác định
1402
Khối gửi
1404
1401
Khối nhận
Khối giải mã
1403

Fig.14

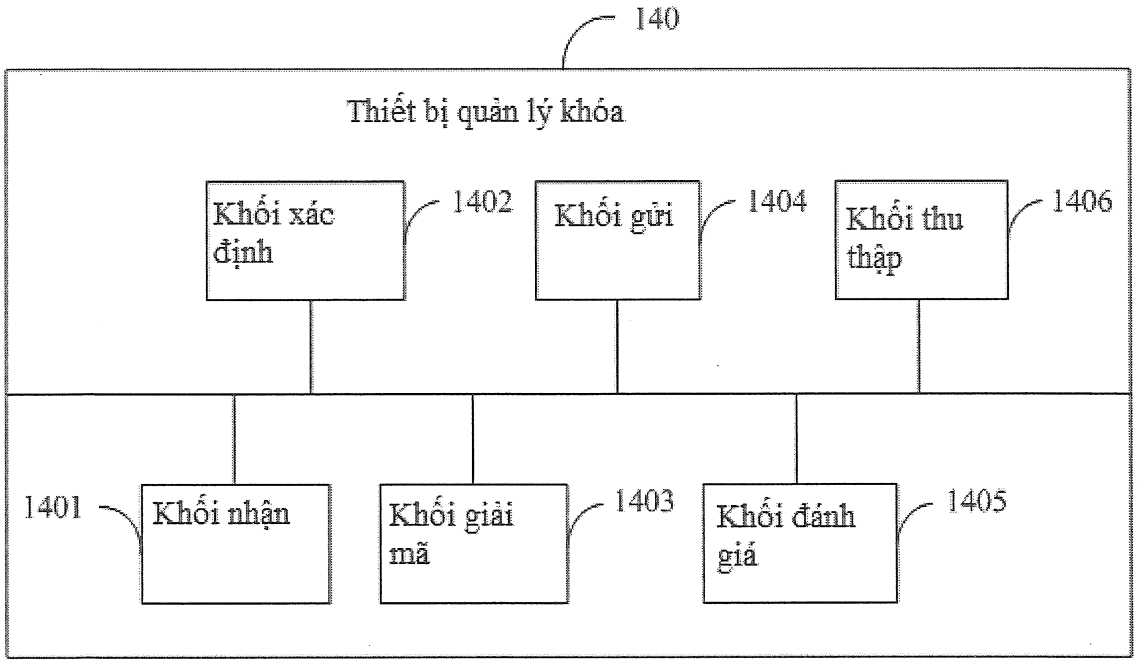

140
Thiết bị quản lý khóa
Khối xác định
1402
Khối gửi
1404
Khối thu thập
1406
1401
Khối nhận
Khối giải mã
1403
Khối đánh giá
1405

Fig.15

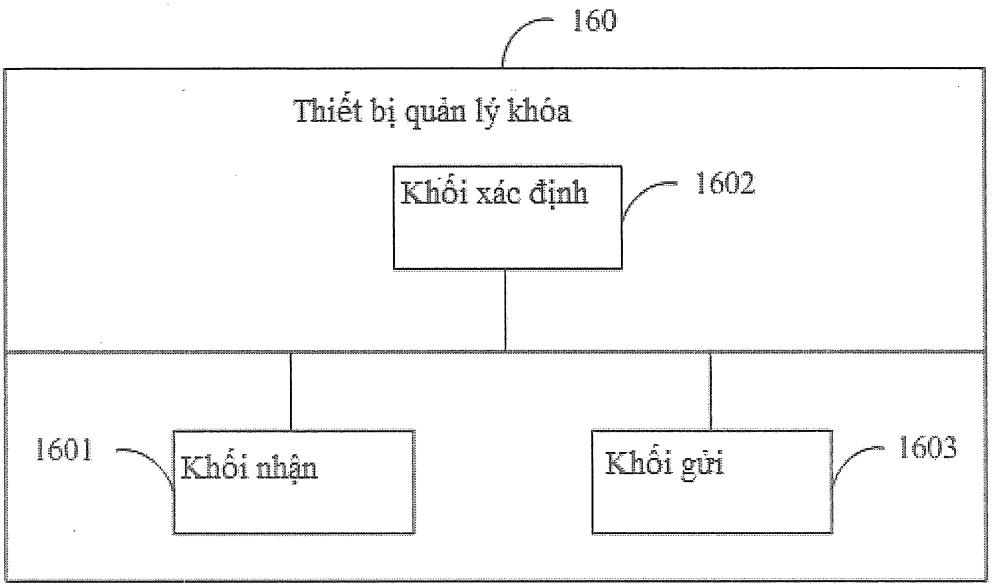

160
Thiết bị quản lý khóa
Khối xác định
1602
1601
Khối nhận
Khối gửi
1603

Fig.16

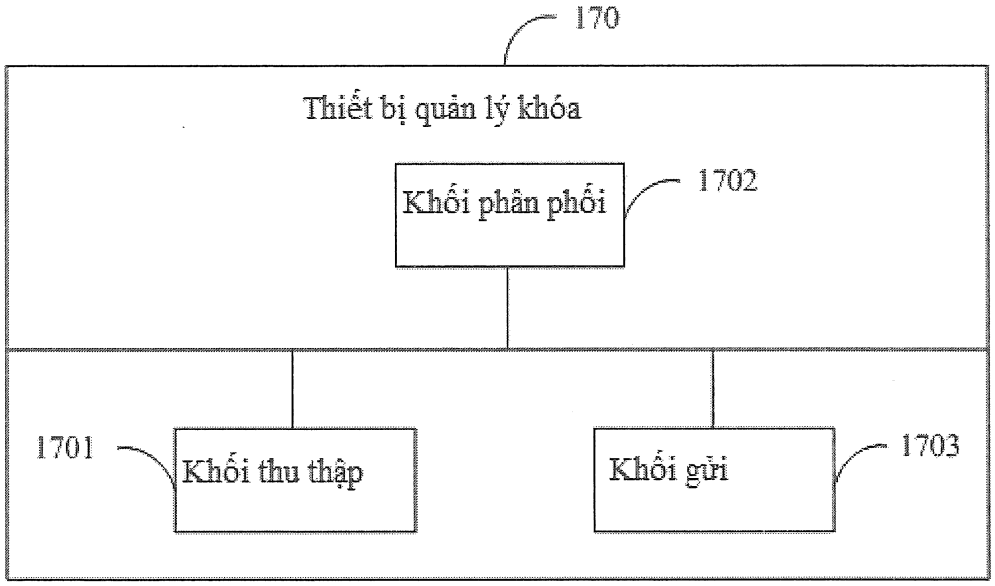

170
Thiết bị quản lý khóa
Khối phân phối
1702
1701
Khối thu thập
Khối gửi
1703

Fig.17

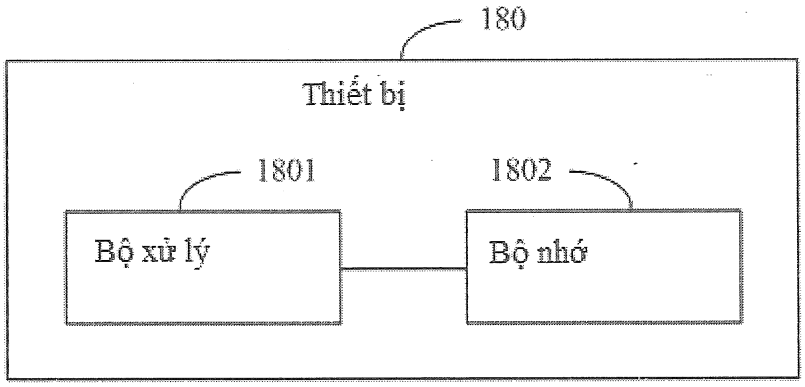


Fig.18