(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) **1-0037436**

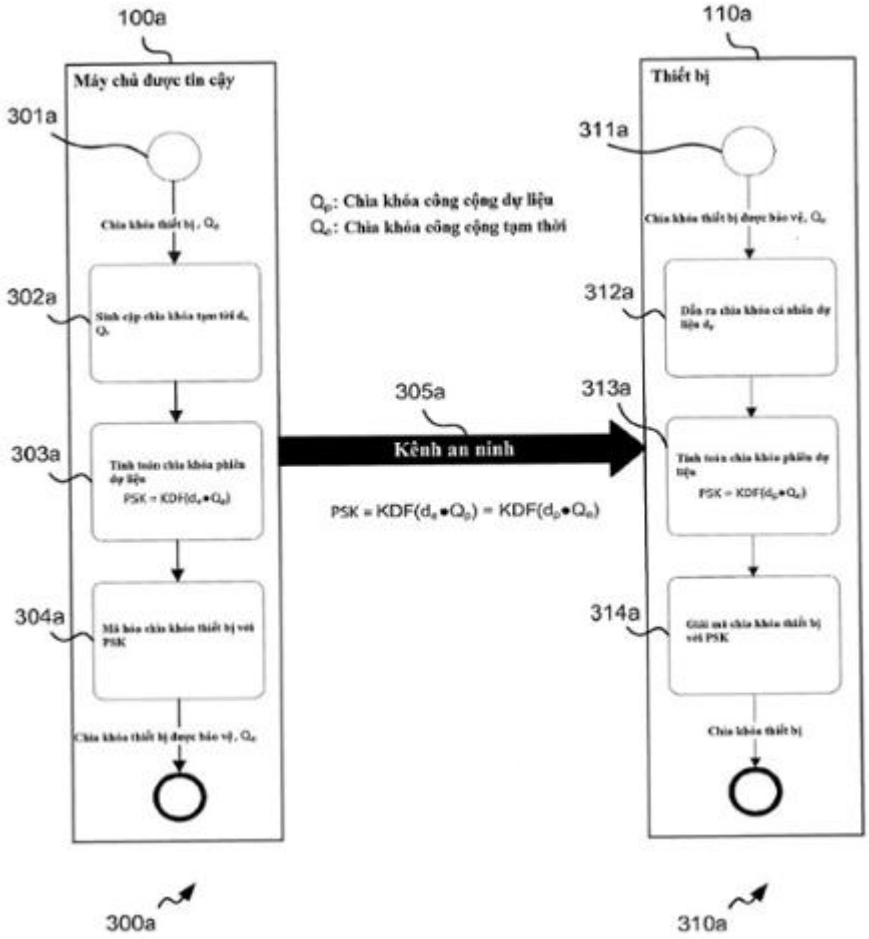
(51)[2020.01] **H04L 9/30**; H04L 9/08

(13) **B**

(21) 1-2020-03501
(22) 01/12/2017
(86) PCT/EP2017/081203 01/12/2017
(87) WO2019/105571 06/06/2019
(45) 27/11/2023 428
(43) 25/09/2020 390A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, P. R. China
(72) SOVIO, Sampo (FI); LI, Qiming (SG); LAITINEN, Pekka (FI); LIAN, Gang (CN); XIE, Meilun (CN); FANG, Xiwen (CN); SHAN, Zhihua (CN).
(74) Công ty Luật TNHH T&G (TGVN)

(54) THIẾT BỊ MÁY CHỦ AN NINH, THIẾT BỊ MÁY KHÁCH, PHƯƠNG PHÁP TRUYỀN THÔNG VÀ VẬT GHI ĐỌC ĐƯỢC BẰNG MÁY TÍNH

(57) Sáng chế đề cập tới thiết bị và phương pháp để cung cấp theo cách an ninh dữ liệu tới thiết bị máy khách. Cơ sở sản xuất không được tin cậy được trang bị thiết bị máy chủ an ninh để thiết lập kênh cung cấp dữ liệu an ninh từ thiết bị máy chủ an ninh tới phần cứng tin cậy trong các thiết bị khách mà không có việc thiết bị máy chủ an ninh và các thiết bị khách cần phải có bí mật được chia sẻ. Cụ thể hơn, sáng chế đề cập tới thiết bị máy chủ an ninh, thiết bị máy khách, các bộ xử lý được sử dụng trong các thiết bị này, phương pháp truyền thông và vật ghi đọc được bằng máy tính.


100a
Máy chủ được tin cậy
301a
Chìa khóa thiết bị, Q_d
302a
Sinh cặp chìa khóa tạm thời d_s, Q_s
303a
Tính toán chìa khóa phiên dự liệu
PSK = KDF(d_s•Q_d)
304a
Mã hóa chìa khóa thiết bị với PSK
Chìa khóa thiết bị được bảo vệ, Q_d
300a
Q_d: Chìa khóa công cộng dự liệu
Q_s: Chìa khóa công cộng tạm thời
305a
Kênh an ninh
PSK = KDF(d_s•Q_d) = KDF(d_d•Q_s)
110a
Thiết bị
311a
Chìa khóa thiết bị được bảo vệ, Q_d
312a
Dẫn ra chìa khóa cá nhân dự liệu d_d
313a
Tính toán chìa khóa phiên dự liệu
PSK = KDF(d_d•Q_s)
314a
Giải mã chìa khóa thiết bị với PSK
Chìa khóa thiết bị
310a

Lĩnh vực kỹ thuật được đề cập

Sáng chế này đề cập tới lĩnh vực mã hóa, và cụ thể hơn là để cung cấp dữ liệu tới thiết bị máy khách theo cách an ninh, và các thiết bị, phương pháp và các chương trình máy tính liên quan.

Tình trạng kỹ thuật của sáng chế

Dữ liệu có thể cần được cung cấp tới các thiết bị di động và đeo được trong quá trình sản xuất thiết bị. Dữ liệu này có thể chứa dữ liệu tài sản khác nhau, bao gồm, nhưng không giới hạn ở: các cặp chìa khóa thiết bị, vật liệu chìa khóa mã hóa khác, các chứng thư dạng số, các chính sách an ninh, các bộ phận nhận diện thiết bị và các thư ủy nhiệm. Các cặp chìa khóa thiết bị thường được yêu cầu, ví dụ là để cho phép các dịch vụ an ninh khác nhau được đề xuất bởi thiết bị di động/đeo được. Theo cách bổ sung/theo cách khác, dữ liệu này có thể chứa mã thực thi được, ví dụ ứng dụng được tin cậy (Trusted Application - TA). Dữ liệu được cung cấp thường được bảo vệ theo một số cách, bởi phần cứng an ninh của thiết bị di động/đeo được.

Như là một ví dụ, trong suốt quá trình sản xuất thiết bị tại nhà máy, cặp chìa khóa thiết bị có thể được sinh ra và chìa khóa công cộng của nó được chứng thực bởi việc kết nạp chứng thư thiết bị cho nó. Cả cặp chìa khóa thiết bị và chứng thư thiết bị đều có thể được đặt trong vị trí an ninh trong thiết bị để cho phép việc sử dụng của chìa khóa cá nhân được điều khiển một cách chặt chẽ. Thông thường, cặp chìa khóa thiết bị có thể được sử dụng chỉ cho các trường hợp sử dụng được xác định từ trước khi thiết bị là với người sử dụng cuối cùng. Các trường hợp sử dụng này bao gồm, ví dụ việc chứng nhận thiết bị mà trong đó thiết bị có thể ký chứng nhận để chứng minh rằng các thuộc tính cụ thể là hợp lệ cho thiết bị. Ví dụ khác là việc chứng nhận chìa khóa mà trong đó cặp chìa khóa được sinh ra bởi môi trường an ninh trong thiết bị, và cặp chìa khóa thiết bị sau đó được sử dụng để chứng nhận rằng cặp chìa khóa được xem xét thực sự được sinh ra trong và được bảo vệ bởi môi trường an ninh của thiết bị.

Tuy nhiên, việc cung cấp của dữ liệu (như các chìa khóa thiết bị hoặc các cặp chìa khóa thiết bị và dạng tương tự) trong thiết bị máy khách trong suốt quá trình sản xuất thiết bị có thể có các vấn đề an ninh, như cách để mã hóa dữ liệu cần được cung cấp sao chỉ thiết bị máy khách đích là có khả năng giải mã dữ liệu.

Bản chất kỹ thuật của sáng chế

Phần bản chất kỹ thuật của sáng chế được cung cấp nhằm giới thiệu sự lựa chọn các khái niệm ở dạng được đơn giản hóa mà sẽ được mô tả tiếp sau đây, trong phần mô tả chi tiết sáng chế. Phần bản chất kỹ thuật của sáng chế này không được dự tính để nhận biết các dấu hiệu chính hay các dấu hiệu cơ bản của đối tượng được yêu cầu bảo hộ, cũng không được dự tính để được sử dụng để hạn chế phạm vi bảo hộ của đối tượng được yêu cầu bảo hộ.

Mục đích của sáng chế này là để đề xuất việc cung cấp an ninh, được cải tiến của dữ liệu tới thiết bị máy khách. Mục đích nêu trên cũng như các mục đích khác đạt được bởi các dấu hiệu của các yêu cầu bảo hộ độc lập. Các dạng áp dụng khác là rõ ràng từ các yêu cầu bảo hộ phụ thuộc, phần mô tả và các hình vẽ.

Theo khía cạnh thứ nhất, thiết bị máy chủ an ninh được đề xuất. Thiết bị máy chủ an ninh bao gồm giao diện được đặt cấu hình để thu được chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách. Thiết bị máy chủ an ninh còn bao gồm bộ xử lý được đặt cấu hình để tận dụng chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa của dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại. Giao diện còn được đặt cấu hình để gửi dữ liệu được mã hóa để được cung cấp tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại nêu trên. Phương án thực hiện cho phép cơ sở sản xuất không tin cậy được trang bị thiết bị máy chủ an ninh để thiết lập kênh cung cấp dữ liệu an ninh từ thiết bị máy chủ an ninh tới phần cứng được tin cậy trong các thiết bị khách, nhờ đó

loại bỏ các vấn đề về an ninh được kết hợp với việc cung cấp của dữ liệu trong thiết bị máy khách trong suốt quá trình sản xuất thiết bị.

Theo dạng áp dụng khác của khía cạnh thứ nhất, bộ xử lý còn được đặt cấu hình để sinh ra cặp chìa khóa mật mã không đối xứng tạm thời, và để sinh ra chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, và giao diện còn được đặt cấu hình để gửi chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại. Việc sử dụng chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời cùng với chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu cho phép thực hiện cách an toàn để thiết lập bí mật được chia sẻ (tức là chìa khóa mật mã đối xứng thứ hai) giữa thiết bị máy chủ an ninh và thiết bị máy khách.

Theo dạng áp dụng khác của khía cạnh thứ nhất, dữ liệu cần được cung cấp bao gồm ít nhất một thành phần trong số vật liệu chìa khóa mã hóa hoặc mã thực thi được.

Theo dạng áp dụng khác của khía cạnh thứ nhất, cặp chìa khóa mật mã không đối xứng dự liệu bao gồm cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman. Việc sử dụng cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman làm cặp chìa khóa mật mã không đối xứng dự liệu cho phép thực hiện các cải tiến khác trong an ninh cho việc sinh ra của chìa khóa mật mã đối xứng thứ hai.

Theo dạng áp dụng khác của khía cạnh thứ nhất, giao thức thỏa thuận chìa khóa được xác định từ trước bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman. Việc sử dụng giao thức thỏa thuận chìa khóa như giao thức thỏa thuận chìa khóa Diffie-Hellman cho phép thực hiện các cải tiến khác trong an ninh cho việc sinh ra của chìa khóa mật mã đối xứng thứ hai.

Theo dạng áp dụng khác của khía cạnh thứ nhất, giao thức thỏa thuận chìa khóa Diffie-Hellman bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic. Việc sử dụng giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic

cho phép thực hiện các cải tiến khác trong an ninh cho việc sinh ra của chìa khóa mật mã đối xứng thứ hai.

Theo dạng áp dụng khác của khía cạnh thứ nhất, thiết bị máy chủ an ninh còn bao gồm môđun an ninh phần cứng. Việc sử dụng môđun an ninh phần cứng trong thiết bị máy chủ an ninh cho phép thực hiện môi trường an ninh và được chứng thực chống lại các tấn công vật lý và logic.

Theo khía cạnh thứ hai, thiết bị máy chủ an ninh được tạo ra. Thiết bị máy chủ an ninh bao gồm giao diện được đặt cấu hình để thu được chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách. Thiết bị máy chủ an ninh còn bao gồm bộ xử lý được đặt cấu hình để tận dụng chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, sinh ra theo cách ngẫu nhiên chìa khóa mã hóa đối xứng thứ ba, mã hóa dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại với chìa khóa mã hóa đối xứng thứ ba được sinh ra ngẫu nhiên, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa của chìa khóa mã hóa đối xứng thứ ba. Giao diện còn được đặt cấu hình để gửi dữ liệu được mã hóa cần được cung cấp và chìa khóa mã hóa đối xứng thứ ba được mã hóa tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại. Phương án thực hiện cho phép cơ sở sản xuất không tin cậy được trang bị thiết bị máy chủ an ninh để thiết lập kênh cung cấp dữ liệu an ninh từ thiết bị máy chủ an ninh tới phần cứng được tin cậy trong các thiết bị khách, nhờ đó loại bỏ các vấn đề về an ninh được kết hợp với việc cung cấp của dữ liệu trong thiết bị máy khách trong suốt quá trình sản xuất thiết bị.

Theo dạng áp dụng khác của khía cạnh thứ hai, bộ xử lý còn được đặt cấu hình để sinh ra cặp chìa khóa mật mã không đối xứng tạm thời, và để sinh ra chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, và giao diện còn được đặt cấu hình để gửi chìa khóa công cộng của cặp chìa

khóa mật mã không đối xứng tạm thời được sinh ra tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại. Việc sử dụng chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời cùng với chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu cho phép thực hiện cách an toàn để thiết lập bí mật được chia sẻ (tức là chìa khóa mật mã đối xứng thứ hai) giữa thiết bị máy chủ an ninh và thiết bị máy khách.

Theo dạng áp dụng khác của khía cạnh thứ hai, bộ xử lý còn được đặt cấu hình để tận dụng kỹ thuật mã hóa hộp trắng trong việc mã hóa của chìa khóa mã hóa đối xứng thứ ba được sinh ra. Nói cách khác, phương án thực hiện có thể được áp dụng cùng với các phương pháp bảo vệ hiện tồn tại, như việc mã hóa hộp trắng.

Theo dạng áp dụng khác của khía cạnh thứ hai, dữ liệu cần được cung cấp bao gồm ít nhất một thành phần trong số vật liệu chìa khóa mã hóa hoặc mã thực thi được.

Theo dạng áp dụng khác của khía cạnh thứ hai, cặp chìa khóa mật mã không đối xứng dự liệu bao gồm cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman. Việc sử dụng cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman làm cặp chìa khóa mật mã không đối xứng dự liệu cho phép thực hiện các cải tiến khác trong an ninh cho việc sinh ra của chìa khóa mật mã đối xứng thứ hai.

Theo dạng áp dụng khác của khía cạnh thứ hai, giao thức thỏa thuận chìa khóa được xác định từ trước bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman. Việc sử dụng giao thức thỏa thuận chìa khóa như giao thức thỏa thuận chìa khóa Diffie-Hellman cho phép thực hiện các cải tiến khác trong an ninh cho việc sinh ra của chìa khóa mật mã đối xứng thứ hai.

Theo dạng áp dụng khác của khía cạnh thứ hai, giao thức thỏa thuận chìa khóa Diffie-Hellman bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic. Việc sử dụng giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic cho phép thực hiện các cải tiến khác trong an ninh cho việc sinh ra của chìa khóa mật mã đối xứng thứ hai.

Theo dạng áp dụng khác của khía cạnh thứ hai, thiết bị máy chủ an ninh còn bao gồm môđun an ninh phần cứng. Việc sử dụng môđun an ninh phần cứng trong thiết bị

máy chủ an ninh cho phép thực hiện môi trường an ninh và được chứng thực chống lại các tấn công vật lý và logic.

Theo khía cạnh thứ ba, thiết bị máy khách được đề xuất. Thiết bị máy khách bao gồm phần lưu giữ an ninh được đặt cấu hình để lưu chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách. Thiết bị máy khách còn bao gồm bộ thu phát được đặt cấu hình để nhận từ thiết bị máy chủ an ninh dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách. Thiết bị máy khách còn bao gồm bộ xử lý được đặt cấu hình để thu được chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra tại thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất được lưu, tận dụng chìa khóa cá nhân thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc giải mã của dữ liệu được mã hóa cần được cung cấp. Phương án thực hiện cho phép kênh cung cấp dữ liệu an ninh được thiết lập giữa phần cứng được tin cậy trong thiết bị máy khách và cơ sở sản xuất không được tin cậy được trang bị thiết bị máy chủ an ninh, nhờ đó loại bỏ được các vấn đề an ninh được kết hợp với việc cung cấp của dữ liệu trong thiết bị máy khách trong suốt quá trình sản xuất của thiết bị máy khách.

Theo dạng áp dụng khác của khía cạnh thứ ba, bộ thu phát còn được đặt cấu hình để nhận từ thiết bị máy chủ an ninh chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời, và bộ xử lý còn được đặt cấu hình để sinh ra chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra và chìa khóa công cộng nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước. Việc sử dụng chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời cùng với chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu cho phép thực hiện cách an toàn để thiết lập bí mật được chia sẻ (tức là chìa khóa mật mã đối xứng thứ hai) giữa thiết bị máy khách và thiết bị máy chủ an ninh.

Theo dạng áp dụng khác của khía cạnh thứ ba, thiết bị máy khách còn bao gồm môi trường thực thi được tin cậy được đặt cấu hình để thực hiện các thao tác mã hóa.

Việc sử dụng của môi trường thực thi được tin cậy cho phép bí mật phân loại và việc cung cấp dẫn xuất của chìa khóa được bảo vệ trong các thiết bị khách.

Theo khía cạnh thứ tư, thiết bị máy khách được đề xuất. Thiết bị máy khách bao gồm phần lưu giữ an ninh được đặt cấu hình để lưu chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách. Thiết bị máy khách còn bao gồm bộ thu phát được đặt cấu hình để nhận từ thiết bị máy chủ an ninh dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách. Thiết bị máy khách còn bao gồm bộ xử lý được đặt cấu hình để thu được chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra tại thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất được lưu, tận dụng chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu được thu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa, và tận dụng chìa khóa mã hóa đối xứng thứ ba được giải mã trong việc giải mã của dữ liệu cần được cung cấp, chìa khóa mã hóa đối xứng thứ ba được mã hóa đã được nhận từ thiết bị máy chủ an ninh bởi bộ thu phát. Phương án thực hiện cho phép kênh cung cấp dữ liệu an ninh được thiết lập giữa phần cứng được tin cậy trong thiết bị máy khách và cơ sở sản xuất không được tin cậy được trang bị với thiết bị máy chủ an ninh, nhờ đó loại bỏ được các vấn đề an ninh được kết hợp với việc cung cấp của dữ liệu trong thiết bị máy khách trong suốt quá trình sản xuất của thiết bị máy khách.

Theo dạng áp dụng khác của khía cạnh thứ tư, bộ thu phát còn được đặt cấu hình để nhận từ thiết bị máy chủ an ninh chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời, và bộ xử lý còn được đặt cấu hình để sinh ra chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra và chìa khóa công cộng nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước. Việc sử dụng chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời cùng với chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu cho phép thực hiện cách an toàn để thiết lập bí mật được chia sẻ (tức là chìa khóa mật mã đối xứng thứ hai) giữa thiết bị máy khách và thiết bị máy chủ an ninh.

Theo dạng áp dụng khác của khía cạnh thứ tư, bộ xử lý còn được đặt cấu hình để tận dụng kỹ thuật mã hóa hộp trắng trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa nhận được. Nói cách khác, phương án thực hiện có thể được áp dụng cùng với các phương pháp bảo vệ hiện tồn tại, như việc mã hóa hộp trắng.

Theo dạng áp dụng khác của khía cạnh thứ tư, thiết bị máy khách còn bao gồm môi trường thực thi được tin cậy được đặt cấu hình để thực hiện các thao tác mã hóa. Việc sử dụng của môi trường thực thi được tin cậy cho phép bí mật phân loại và việc cung cấp dẫn xuất của chìa khóa được bảo vệ trong các thiết bị khách.

Theo khía cạnh thứ năm, bộ xử lý được sử dụng trong thiết bị máy chủ an ninh bao gồm giao diện được ghép nối vào bộ xử lý sẽ được tạo ra. Bộ xử lý được đặt cấu hình để làm cho giao diện thu được chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách. Bộ xử lý còn được đặt cấu hình để tận dụng chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa của dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại. Bộ xử lý còn được đặt cấu hình để làm cho giao diện gửi dữ liệu được mã hóa để được cung cấp tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại.

Theo khía cạnh thứ sáu, bộ xử lý được sử dụng trong thiết bị máy chủ an ninh bao gồm giao diện được ghép nối vào bộ xử lý được đề xuất. Bộ xử lý được đặt cấu hình để làm cho giao diện thu được chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách. Bộ xử lý còn được đặt cấu hình để tận dụng chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, sinh ra theo cách ngẫu nhiên chìa khóa mã hóa đối xứng thứ ba, mã hóa dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại với chìa khóa mã hóa đối xứng thứ ba được sinh ra ngẫu nhiên, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa

của chìa khóa mã hóa đối xứng thứ ba. Bộ xử lý còn được đặt cấu hình để làm cho giao diện gửi dữ liệu được mã hóa cần được cung cấp và chìa khóa mã hóa đối xứng thứ ba được mã hóa tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại.

Theo khía cạnh thứ bảy, bộ xử lý được sử dụng trong thiết bị máy khách bao gồm bộ thu phát được ghép nối vào bộ xử lý được đề xuất. Bộ xử lý được đặt cấu hình để làm cho bộ thu phát nhận từ thiết bị máy chủ an ninh dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách. Bộ xử lý còn được đặt cấu hình để thu được chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra tại thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất được lưu trong phần lưu giữ an ninh của thiết bị máy khách. Bộ xử lý còn được đặt cấu hình để tận dụng chìa khóa cá nhân thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai. Bộ xử lý còn được đặt cấu hình để tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc giải mã của dữ liệu được mã hóa cần được cung cấp.

Theo khía cạnh thứ tám, bộ xử lý được sử dụng trong thiết bị máy khách bao gồm bộ thu phát được ghép nối vào bộ xử lý được đề xuất. Bộ xử lý được đặt cấu hình để làm cho bộ thu phát nhận từ thiết bị máy chủ an ninh dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách. Bộ xử lý còn được đặt cấu hình để thu được chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra tại thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất được lưu trong phần lưu giữ an ninh của thiết bị máy khách. Bộ xử lý còn được đặt cấu hình để tận dụng chìa khóa cá nhân thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai. Bộ xử lý còn được đặt cấu hình để tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa, và tận dụng chìa khóa mã hóa đối xứng thứ ba đã

được giải mã trong việc giải mã của dữ liệu cần được cung cấp, chìa khóa mã hóa đối xứng thứ ba được mã hóa đã được nhận từ thiết bị máy chủ an ninh bởi bộ thu phát.

Theo khía cạnh thứ chín, phương pháp được đề xuất. Phương pháp bao gồm bước thu, bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa của dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại. Phương pháp còn bao gồm bước gửi dữ liệu được mã hóa cần được cung cấp từ thiết bị máy chủ an ninh tới một hoặc nhiều thiết bị trong các thiết bị khách được kết hợp với bộ phận nhận diện phân loại.

Theo dạng áp dụng khác của khía cạnh thứ chín, phương pháp còn bao gồm bước sinh ra cặp chìa khóa mật mã không đối xứng tạm thời bởi thiết bị máy chủ an ninh. Chìa khóa mật mã đối xứng thứ hai được sinh ra trên cơ sở chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước. Phương pháp còn bao gồm bước gửi, bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại.

Theo dạng áp dụng khác của khía cạnh thứ chín, dữ liệu cần được cung cấp bao gồm ít nhất một thành phần trong số vật liệu chìa khóa mã hóa hoặc mã thực thi được.

Theo dạng áp dụng khác của khía cạnh thứ chín, cặp chìa khóa mật mã không đối xứng dự liệu bao gồm cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman.

Theo dạng áp dụng khác của khía cạnh thứ chín, giao thức thỏa thuận chìa khóa được xác định từ trước bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman.

Theo dạng áp dụng khác của khía cạnh thứ chín, giao thức thỏa thuận chìa khóa Diffie-Hellman bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic.

Theo dạng áp dụng khác của khía cạnh thứ chín, thiết bị máy chủ an ninh còn bao gồm môđun an ninh phần cứng.

Theo khía cạnh thứ mười, chương trình máy tính được đề xuất. Chương trình máy tính bao gồm mã chương trình được đặt cấu hình để thực hiện phương pháp khía cạnh thứ chín, khi chương trình máy tính được thực thi trên thiết bị tính toán.

Theo khía cạnh thứ mười một, phương pháp được đề xuất. Phương pháp bao gồm bước thu, bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai. Phương pháp còn bao gồm bước sinh ra theo cách ngẫu nhiên chìa khóa mã hóa đối xứng thứ ba bởi thiết bị máy chủ an ninh. Phương pháp còn bao gồm bước mã hóa, bởi thiết bị máy chủ an ninh, dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại với chìa khóa mã hóa đối xứng thứ ba được sinh ra ngẫu nhiên. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa của chìa khóa mã hóa đối xứng thứ ba. Phương pháp còn bao gồm bước gửi dữ liệu được mã hóa cần được cung cấp và chìa khóa mã hóa đối xứng thứ ba được mã hóa từ thiết bị máy chủ an ninh tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại.

Theo dạng áp dụng khác của khía cạnh thứ mười một, phương pháp còn bao gồm bước sinh ra cặp chìa khóa mật mã không đối xứng tạm thời bởi thiết bị máy chủ an ninh. Chìa khóa mật mã đối xứng thứ hai được sinh ra trên cơ sở chìa khóa công cộng thu được của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước. Phương pháp còn bao gồm bước gửi, bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng

tạm thời được sinh ra tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại.

Theo dạng áp dụng khác của khía cạnh thứ mười một, phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, kỹ thuật mã hóa hộp trắng trong việc mã hóa của chìa khóa mã hóa đối xứng thứ ba được sinh ra.

Theo dạng áp dụng khác của khía cạnh thứ mười một, dữ liệu cần được cung cấp bao gồm ít nhất một thành phần trong số vật liệu chìa khóa mã hóa hoặc mã thực thi được.

Theo dạng áp dụng khác của khía cạnh thứ mười một, cặp chìa khóa mật mã không đối xứng dự liệu bao gồm cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman.

Theo dạng áp dụng khác của khía cạnh thứ mười một, giao thức thỏa thuận chìa khóa được xác định từ trước bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman.

Theo dạng áp dụng khác của khía cạnh thứ mười một, giao thức thỏa thuận chìa khóa Diffie-Hellman bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic.

Theo dạng áp dụng khác của khía cạnh thứ mười một, thiết bị máy chủ an ninh còn bao gồm môđun an ninh phần cứng.

Theo khía cạnh thứ mười hai, chương trình máy tính được đề xuất. Chương trình máy tính bao gồm mã chương trình được đặt cấu hình để thực hiện phương pháp khía cạnh thứ mười một, khi chương trình máy tính được thực thi trên thiết bị tính toán.

Theo khía cạnh thứ mười ba, phương pháp được đề xuất. Phương pháp bao gồm bước nhận, tại thiết bị máy khách từ thiết bị máy chủ an ninh, dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách. Phương pháp còn bao gồm bước thu, bởi thiết bị máy khách, chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra bởi thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất được lưu tại phần lưu giữ an ninh của thiết bị máy khách. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy khách, chìa khóa cá nhân thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ

hai. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc giải mã của dữ liệu được mã hóa cần được cung cấp.

Theo dạng áp dụng khác của khía cạnh thứ mười ba, phương pháp còn bao gồm bước nhận chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời tại thiết bị máy khách từ thiết bị máy chủ an ninh. Phương pháp còn bao gồm bước sinh ra, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra và chìa khóa công cộng nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước.

Theo dạng áp dụng khác của khía cạnh thứ mười ba, thiết bị máy khách còn bao gồm môi trường thực thi được tin cậy để thực thi các thao tác mã hóa.

Theo khía cạnh thứ mười bốn, chương trình máy tính được đề xuất. Chương trình máy tính bao gồm mã chương trình được đặt cấu hình để thực hiện phương pháp theo khía cạnh thứ mười ba, khi chương trình máy tính được thực thi trên thiết bị tính toán.

Theo khía cạnh thứ mười lăm, phương pháp được đề xuất. Phương pháp bao gồm bước nhận, tại thiết bị máy khách từ thiết bị máy chủ an ninh, dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách. Phương pháp còn bao gồm bước thu, bởi thiết bị máy khách, chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra bởi thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất được lưu tại phần lưu giữ an ninh của thiết bị máy khách. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy khách, chìa khóa cá nhân thu được của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai. Phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa, chìa khóa mã hóa đối xứng thứ ba được mã hóa đã được nhận tại thiết bị máy khách từ thiết bị máy chủ an ninh. Phương pháp còn bao gồm bước tận dụng chìa khóa mã hóa đối xứng thứ ba đã được giải mã trong việc giải mã của dữ liệu cần được cung cấp.

Theo dạng áp dụng khác của khía cạnh thứ mười lăm, phương pháp còn bao gồm bước nhận chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời của thiết bị máy khách từ thiết bị máy chủ an ninh. Phương pháp còn bao gồm bước sinh ra, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra và chìa khóa công cộng nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước.

Theo dạng áp dụng khác của khía cạnh thứ mười lăm, phương pháp còn bao gồm bước tận dụng, bởi thiết bị máy khách, kỹ thuật mã hóa hộp trắng trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa nhận được.

Theo dạng áp dụng khác của khía cạnh thứ mười lăm, thiết bị máy khách còn bao gồm môi trường thực thi được tin cậy để thực thi các thao tác mã hóa.

Theo khía cạnh thứ mười sáu, chương trình máy tính được đề xuất. Chương trình máy tính bao gồm mã chương trình được đặt cấu hình để thực hiện phương pháp theo khía cạnh thứ mười lăm, khi chương trình máy tính được thực thi trên thiết bị tính toán.

Nhiều dấu hiệu trong các dấu hiệu có mặt sẽ được xem xét rõ ràng hơn khi chúng trở nên dễ hiểu hơn bởi việc tham chiếu tới phần mô tả chi tiết dưới đây trong kết hợp với các hình vẽ kèm theo.

Mô tả vắn tắt các hình vẽ

Trong phần dưới đây, các phương án thực hiện làm ví dụ sẽ được mô tả chi tiết hơn với tham khảo tới các hình vẽ và các hình kèm theo, trong đó:

Fig.1A là giản đồ khối minh họa thiết bị máy chủ an ninh theo một phương án thực hiện;

Fig.1B là giản đồ khối minh họa thiết bị máy chủ an ninh theo phương án thực hiện khác;

Fig.1C là giản đồ khối minh họa thiết bị máy khách theo một phương án thực hiện;

Fig.1D là giản đồ khối minh họa thiết bị máy khách theo phương án thực hiện khác;

Fig.2 là giản đồ minh họa hệ thống theo một phương án thực hiện;

Fig.3A là giản đồ minh họa các phương pháp theo một phương án thực hiện;

Fig.3B là giản đồ minh họa phương pháp theo phương án thực hiện khác; và

Fig.3C là lưu đồ minh họa phương pháp khác theo phương án thực hiện khác nữa.

Trong phần sau, các ký hiệu tham chiếu giống nhau đề cập tới các dấu hiệu chức năng giống nhau hoặc ít nhất là tương đương.

Mô tả chi tiết sáng chế

Trong phần mô tả sau, tham khảo được dẫn tới các hình vẽ kèm theo, tạo thành một phần của bản mô tả này, và trong đó, được thể hiện, theo cách minh họa, các khía cạnh đặc biệt của sáng chế có thể được thể hiện. Cần hiểu rằng các khía cạnh khác cũng có thể được tận dụng, và những thay đổi về cấu trúc hoặc logic có thể được tạo ra mà không tách khỏi phạm vi bảo hộ của sáng chế. Do đó, phần mô tả chi tiết sau đây không được xem là nghĩa giới hạn, và phạm vi của sáng chế sẽ được xác định bởi các điểm yêu cầu bảo hộ kèm theo.

Ví dụ, cần hiểu rằng phần mô tả này, cùng với phương pháp được mô tả ở đây cũng đúng cho thiết bị hoặc hệ thống tương ứng được đặt cấu hình để thực hiện phương pháp và ngược lại. Ví dụ, nếu bước của phương pháp cụ thể được mô tả, thì thiết bị tương ứng có thể chứa đơn vị để thực hiện bước của phương pháp đã được mô tả, thậm chí nếu đơn vị này không được mô tả hoặc được minh họa một cách rõ ràng trên các hình vẽ. Mặt khác, ví dụ, nếu thiết bị cụ thể được mô tả trên cơ sở của các đơn vị chức năng thì phương pháp tương ứng có thể chứa bước thực hiện chức năng được mô tả, thậm chí nếu bước không được mô tả hoặc được minh họa rõ ràng trên các hình vẽ. Thêm nữa, cần hiểu rằng các dấu hiệu của các khía cạnh làm ví dụ khác nhau, được mô tả ở đây có thể được kết hợp với nhau, trừ khi được chỉ ra theo cách khác.

Mã hóa phi đối xứng (còn được biết tới như là mã hóa chìa khóa công cộng) đề cập tới kỹ thuật mã hóa chứa cặp các chìa khóa được liên kết với nhau, tức là chìa khóa công cộng và chìa khóa cá nhân. Chìa khóa công cộng có thể được phân tán rộng rãi, trong đó chìa khóa cá nhân chỉ được biết bởi chủ của nó. Người bất kỳ có thể mã hóa tin nhắn sử dụng chìa khóa công cộng của người chủ (tức là người nhận của tin nhắn), nhưng tin nhắn được mã hóa này chỉ có thể được giải mã với chìa khóa cá nhân của người nhận. Thêm nữa, chìa khóa công cộng có thể được sử dụng cho việc xác thực,

tức là để xác thực bởi bất kỳ ai mà người chỉ của chìa khóa cá nhân tương ứng đã gửi tin nhắn.

Mã hóa đối xứng đề cập tới kỹ thuật mã hóa bao gồm việc sử dụng của cùng một chìa khóa mã hóa cho cả việc mã hóa của văn bản gốc và việc giải mã của văn bản mã hóa. Nói cách khác, chìa khóa mã hóa của việc mã hóa đối xứng thể hiện rằng bí mật được chia sẻ giữa hai hoặc nhiều bên.

Như được mô tả chi tiết bên dưới, các thiết bị máy chủ an ninh 100a, 100b sẽ được tận dụng trong việc cung cấp dữ liệu tới các thiết bị khách 110a, 110b trong suốt quá trình sản xuất thiết bị. Dữ liệu này có thể chứa dữ liệu tài sản khác nhau, bao gồm, nhưng không giới hạn ở: các chìa khóa thiết bị hoặc các cặp chìa khóa thiết bị, vật liệu chìa khóa mã hóa khác, các chứng thư dạng số, các chính sách an ninh, các bộ phận nhận diện thiết bị và các thư ủy nhiệm. Các chìa khóa/cặp chìa khóa thiết bị này thường được yêu cầu ví dụ để cho phép các dịch vụ an ninh khác nhau được đề xuất bởi thiết bị di động/đeo được. Theo cách bổ sung/theo cách khác, dữ liệu cần được cung cấp này có thể chứa mã thực thi được, ví dụ ứng dụng được tin cậy (Trusted Application - TA). Các chìa khóa/cặp chìa khóa thiết bị này (hoặc dữ liệu cần được cung cấp khác) có thể được sinh ra sử dụng ví dụ là giao diện lập trình mã hóa, như phần được tạo ra bởi môđun an ninh phần cứng 103a, 103b.

Trong phần sau, các phương án thực hiện làm ví dụ của các thiết bị máy chủ an ninh 100a và 100b và các thiết bị khách 110a và 110b được mô tả trên các hình vẽ Fig. 1A, Fig.1B, Fig.1C và Fig.1D.

Fig.1A thể hiện thiết bị máy chủ an ninh 100a bao gồm giao diện 101a, bộ xử lý 102a, và tùy chọn là môđun an ninh phần cứng (HSM) 103a.

Thiết bị máy chủ an ninh 100a có thể bao gồm, ví dụ là máy chủ sản xuất được sử dụng trong việc sản xuất các thiết bị khách, như các thiết bị di động và/hoặc các thiết bị đeo được. Nói cách khác, thiết bị máy chủ an ninh 100a có thể được triển khai tại dây chuyền sản xuất cho các thiết bị khách. Ở đây, thuật ngữ "an ninh" đề cập tới thiết bị máy chủ được tin cậy 100a bao gồm thành phần hoặc đơn vị cho phép xử lý một cách an ninh cho dữ liệu nhạy cảm hoặc riêng tư. Thiết bị máy chủ an ninh 100a có thể được áp dụng, ví dụ bởi việc chứa của môđun an ninh phần cứng 103a. Thông thường, thuật ngữ "môđun an ninh phần cứng" đề cập tới thiết bị tính toán vật lý bảo

vệ và quản lý các chìa khóa số và cung cấp việc xử lý mã hóa. Môđun này có thể cung cấp môi trường an ninh và được chứng nhận chống lại các tấn công vật lý và logic và có thể bao gồm, ví dụ là thẻ cắm vào hoặc thiết bị bên ngoài gắn một cách trực tiếp vào thiết bị máy chủ an ninh 100a.

Ở đây, mỗi thiết bị máy khách thuộc về một loại của các thiết bị khách. Ví dụ, các thiết bị khách với cùng các bản mô tả phần cứng có thể chia sẻ cùng một phân loại. Tuy nhiên, theo một số phương án thực hiện là khả thi với các bản mô tả khác nhau cũng có cùng một bộ phận nhận diện phân loại. Phân loại thiết bị máy khách được nhận diện duy nhất bởi bộ phận nhận diện phân loại thiết bị khách được kết hợp. Hơn nữa, mỗi bộ phận nhận diện phân loại thiết bị khách được gán chìa khóa phân loại (K) của riêng nó. Chìa khóa K là chìa khóa mã hóa đối xứng là giống nhau cho tất cả các phần cứng với cùng một bộ phận nhận diện phân loại. Nói cách khác, chìa khóa phân loại là chìa khóa mã hóa bí mật được chia sẻ bởi tất cả phần cứng với cùng một phân loại được sản xuất bởi người bán phần cứng. Chìa khóa K thường được viết vào trong vùng nhớ an ninh của thiết bị máy khách (như phần lưu giữ an ninh 113a, 113b của các hình vẽ Fig. 1C và Fig.1D) là có thể truy cập được bởi phần cứng an ninh (như môi trường thực thi được tin cậy 114a, 114b của các hình vẽ Fig. 1C và Fig.1D) của thiết bị máy khách. Mã ứng dụng thông thường không thể truy cập chìa khóa K. Việc sinh ra của chìa khóa K và việc lập trình của nó vào trong các thiết bị khách 110a, 110b có thể được thực hiện, ví dụ bởi máy chủ 120 trên Fig.2.

Giao diện 101a được đặt cấu hình để thu được (ví dụ truy hồi hoặc nhận) chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu (PKP). Cặp chìa khóa mật mã không đối xứng dự liệu PKP bao gồm chìa khóa cá nhân (d_p) và chìa khóa công cộng (Q_p).

Cặp chìa khóa mật mã không đối xứng dự liệu PKP có thể được dẫn ra từ chìa khóa phân loại K sử dụng phương pháp thích hợp. Ví dụ, theo một phương án thực hiện, chìa khóa phân loại K có thể được sử dụng để dẫn ra cặp chìa khóa đường cong eliptic (elliptic curve - EC). Theo phương án thực hiện khác, chìa khóa K có thể được sử dụng để dẫn ra cặp chìa khóa Rivest-Shamir-Adleman (RSA). Nói cách khác, cặp chìa khóa mật mã không đối xứng dự liệu có thể bao gồm, ví dụ là cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman.

Việc dẫn ra của cặp chìa khóa mật mã không đối xứng dự liệu PKP có thể được thực hiện, ví dụ bởi nhà sản xuất chip (ví dụ máy chủ 120), hoặc bởi nhà sản xuất thiết bị máy khách (ví dụ thiết bị máy chủ an ninh 100a). Việc dẫn ra hoặc sinh ra của cặp chìa khóa mật mã không đối xứng dự liệu sẽ được mô tả chi tiết cùng với Fig.2. Nói cách khác, cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách.

Bộ xử lý 102a tùy chọn còn có thể được đặt cấu hình để sinh ra cặp chìa khóa mật mã không đối xứng tạm thời. Cặp chìa khóa mật mã không đối xứng tạm thời bao gồm chìa khóa cá nhân (d_e) và chìa khóa công cộng (Q_e). Bộ xử lý 102a có thể chứa ví dụ một hoặc nhiều thiết bị trong số các thiết bị xử lý khác nhau, như bộ đồng xử lý, bộ vi xử lý, bộ điều khiển, bộ xử lý tín hiệu số (digital signal processor - DSP), mạch xử lý có hoặc không có DSP kèm theo, hoặc các thiết bị xử lý khác chứa các mạch tích hợp như, ví dụ, mạch tích hợp ứng dụng cụ thể (application specific integrated circuit - ASIC), mảng cổng lập trình được bằng trường (field programmable gate array - FPGA), đơn vị vi xử lý (microcontroller unit - MCU), bộ tăng tốc phần cứng, chip máy tính mục đích đặc biệt, hoặc dạng tương tự.

Bộ xử lý 102a còn được đặt cấu hình để thiết lập bí mật được chia sẻ, tức là chìa khóa phiên dự liệu (provisioning session key - PSK) giữa thiết bị máy chủ an ninh 100a và thiết bị máy khách 110a. Nói cách khác, bộ xử lý 102a còn được đặt cấu hình để tận dụng chìa khóa công cộng thu được Q_p của cặp chìa khóa mật mã không đối xứng dự liệu trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai (tức là chìa khóa phiên dự liệu (provisioning session key - PSK)).

Ví dụ, khi cặp chìa khóa mật mã không đối xứng tạm thời đã được sinh ra, nó có thể được áp dụng sao cho bộ xử lý 102a sinh ra chìa khóa mật mã đối xứng thứ hai PSK trên cơ sở chìa khóa công cộng thu được Q_p của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân d_e của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra, ví dụ bằng cách sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước. Giao thức thỏa thuận chìa khóa có thể bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman, như giao thức thỏa thuận chìa khóa Diffie–Hellman (ECDH) đường cong eliptic. Nói cách khác, cặp chìa khóa tạm thời có thể được sử dụng cùng

với cặp chìa khóa dự liệu (provisioning key pair - PKP) để đồng ý trên bí mật được chia sẻ PSK sử dụng ví dụ như thỏa thuận chìa khóa Diffie-Hellman, như ECDH.

Bộ xử lý 102a còn được đặt cấu hình để tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra PSK trong việc mã hóa của dữ liệu để được cung cấp tới thiết bị máy khách 110a. Ví dụ, bộ xử lý 102a có thể tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra PSK để bao bọc một cách an ninh dữ liệu cần được cung cấp. Sau việc mã hóa, giao diện 101a còn được đặt cấu hình để gửi dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách 110a. Khi cặp chìa khóa mật mã không đối xứng tạm thời đã được sinh ra, giao diện 101a tùy chọn có thể được đặt cấu hình để cũng gửi chìa khóa công cộng Q_e của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra tới thiết bị máy khách 110a.

Fig.1B thể hiện thiết bị máy chủ an ninh 100b bao gồm an giao diện 101b, bộ xử lý 102b, và tùy chọn là môđun an ninh phần cứng (hardware security module - HSM) 103b.

Tương tự như phương án thực hiện của Fig.1A, bộ xử lý 102b được đặt cấu hình để tận dụng chìa khóa công cộng thu được Q_p của cặp chìa khóa mật mã không đối xứng dự liệu (PKP) trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai (chìa khóa phiên dự liệu (provisioning session key - PSK)), tùy chọn là tận dụng cặp chìa khóa mật mã không đối xứng tạm thời và giao thức thỏa thuận chìa khóa thích hợp theo phương án thực hiện của Fig.1A.

Tuy nhiên, trái với phương án thực hiện trên Fig.1A, bộ xử lý 102b được đặt cấu hình để sinh ra một cách ngẫu nhiên chìa khóa mã hóa đối xứng thứ ba (hoặc nói cách khác, là chìa khóa mã hóa được chia sẻ (shared key encryption key - KEK)).

Còn trái với phương án thực hiện của Fig.1A, bộ xử lý 102b được đặt cấu hình để mã hóa dữ liệu để được cung cấp tới thiết bị máy khách 110b với chìa khóa mã hóa đối xứng thứ ba được sinh ra ngẫu nhiên KEK. Như được mô tả ở trên, trong phương án thực hiện trên Fig.1A, dữ liệu cần được cung cấp được thay cho việc được mã hóa hoặc được bao bọc với chìa khóa mật mã đối xứng thứ hai PSK.

Còn trái với phương án thực hiện trên Fig.1A, bộ xử lý 102b được đặt cấu hình để sử dụng chìa khóa mật mã đối xứng thứ hai PSK để mã hóa chìa khóa mã hóa đối xứng thứ ba KEK sau việc sử dụng của nó để mã hóa dữ liệu cần được cung cấp. Do

đó, chìa khóa mã hóa đối xứng thứ ba được mã hóa KEK (hoặc nói cách khác, chìa khóa dự liệu được mã hóa (encrypted provisioning key - PEK) có thể vẫn được mã hóa bởi bộ xử lý 102b với kỹ thuật mã hóa hộp trắng.

Còn trái với phương án thực hiện trên Fig.1A, giao diện 101b còn được đặt cấu hình để cũng gửi chìa khóa mã hóa đối xứng thứ ba được mã hóa PEK tới thiết bị máy khách 110b.

Trái lại, các thành phần, các dấu hiệu và các thông số (như các chìa khóa mã hóa, các bộ phận nhận diện, và dữ liệu cần được cung cấp) của thiết bị máy chủ an ninh 100a và thiết bị máy chủ an ninh 100b là giống nhau hoặc ít nhất là tương đương về mặt chức năng do đó các phần mô tả của chúng không được lặp lại chi tiết.

Fig.1C thể hiện thiết bị máy khách 110a bao gồm bộ thu phát 111a, bộ xử lý 112a, phần lưu giữ an ninh 113a, và tùy chọn là phần cứng an ninh, như môi trường thực thi được tin cậy (TEE) 114a.

Thiết bị máy khách 110a có thể là loại bất kỳ trong số các loại khác nhau của các thiết bị di động và/hoặc đeo được, được sử dụng một cách trực tiếp bởi thực thể người sử dụng cuối cùng và có khả năng liên lạc qua mạng không dây, như thiết bị người sử dụng (user equipment - UE). Các thiết bị này bao gồm, nhưng không giới hạn ở các điện thoại thông minh, các máy tính bảng, các đồng hồ thông minh, các máy tính xách tay, các thiết bị Internet vạn vật (Internet of things - IoT), v.v.

Thêm nữa, thiết bị máy khách 110a có thể bao gồm phần cứng an ninh, như môi trường thực thi được tin cậy (trusted execution environment - TEE) 114a để thực hiện các thao tác mã hóa, như các thao tác liên quan tới việc mã hóa và/hoặc việc giải mã. Thông thường, môi trường thực thi được tin cậy đề cập tới vùng an ninh trong bộ xử lý (như bộ xử lý 112a), hoặc bộ xử lý (như bộ xử lý 112a) đang thực thi trong chế độ an ninh, hoặc dạng tương tự. Nó có thể được sử dụng, ví dụ để đảm bảo rằng mã và dữ liệu được tải bên trong và được cách ly khỏi các ứng dụng khác và được bảo vệ liên quan tới tính bí mật và toàn vẹn. Môi trường thực thi được tin cậy 114a có thể được tích hợp với phần lưu giữ an ninh 113a, tức là chỉ TEE có thể được phép để truy cập phần lưu giữ an ninh 113a chứa các bí mật thiết bị.

Phần lưu giữ an ninh 113a được đặt cấu hình để lưu chìa khóa mật mã đối xứng thứ nhất (tức là chìa khóa phân loại K được mô tả chi tiết hơn ở trên) của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách 110a.

Cần chú ý rằng các chìa khóa mã hóa khác nhau, các bộ phận nhận diện, và dữ liệu cần được cung cấp được sử dụng bởi thiết bị máy khách 110a là giống nhau hoặc ít nhất là có chức năng tương đương với các thành phần được sử dụng bởi thiết bị máy chủ an ninh 100a do đó các phần mô tả của chúng không được lặp lại chi tiết ở đây.

Bộ thu phát 111a được đặt cấu hình để nhận từ thiết bị máy chủ an ninh 100a dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách 110a.

Bộ xử lý 112a được đặt cấu hình để thu được chìa khóa cá nhân d_p của cặp chìa khóa mật mã không đối xứng dự liệu PKP. Cặp chìa khóa mật mã không đối xứng dự liệu PKP được sinh ra hoặc đã được sinh ra từ trước tại thiết bị máy khách 110a trên cơ sở chìa khóa mật mã đối xứng thứ nhất K được lưu trong phần lưu giữ an ninh 113a. Nếu việc cung cấp dữ liệu đã được thực hiện trước cho thiết bị máy khách 110a, thì sau đó cặp chìa khóa mật mã không đối xứng dự liệu PKP đã được sinh ra trong suốt việc cung cấp thứ nhất. Theo ví dụ, thiết bị máy khách 110a có thể lưu cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra PKP ví dụ vào phần lưu giữ an ninh 113a tại việc cung cấp dữ liệu thứ nhất, và trong suốt các việc cung cấp dữ liệu tiếp theo, cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra PKP có thể được thu từ phần lưu giữ an ninh 113a. Nói cách khác, việc sinh ra của cặp chìa khóa mật mã không đối xứng dự liệu PKP có thể được thực hiện chỉ một lần cho mỗi thiết bị máy khách 110a.

Bộ xử lý 112a còn được đặt cấu hình để tận dụng chìa khóa cá nhân d_p thu được của cặp chìa khóa mật mã không đối xứng dự liệu PKP trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai PSK. Ví dụ, nó có thể được áp dụng sao cho bộ thu phát 111a nhận chìa khóa công cộng Q_e của cặp chìa khóa mật mã không đối xứng tạm thời từ thiết bị máy chủ an ninh 100a, và bộ xử lý 112a sinh ra chìa khóa mật mã đối xứng thứ hai PSK trên cơ sở chìa khóa cá nhân d_p của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra PKP và chìa khóa công cộng Q_e nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước. Như ở trên, giao thức thỏa thuận chìa khóa có thể bao gồm giao thức thỏa thuận

chìa khóa Diffie-Hellman, như giao thức thỏa thuận chìa khóa Diffie–Hellman (ECDH) đường cong eliptic.

Bộ xử lý 112a còn được đặt cấu hình để tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra PSK trong việc giải mã của dữ liệu được mã hóa cần được cung cấp được nhận từ thiết bị máy chủ an ninh 100a.

Fig.1D thể hiện thiết bị máy khách 110b bao gồm bộ thu phát 111b, bộ xử lý 112b, phần lưu giữ an ninh 113b, và tùy chọn là phần cứng an ninh, như môi trường thực thi được tin cậy (trusted execution environment - TEE) 114b.

Trái với phương án thực hiện trên Fig.1C, bộ thu phát 111b cũng được đặt cấu hình để nhận chìa khóa mã hóa đối xứng thứ ba được mã hóa PEK từ thiết bị máy chủ an ninh 100b. Trái với phương án thực hiện trên Fig.1C, bộ xử lý 112b được đặt cấu hình để tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra PSK trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa (PEK) để nhờ đó thu được chìa khóa mã hóa đối xứng thứ ba (KEK) được giải mã, trong đó, theo phương án thực hiện trên Fig.1C, PSK được sử dụng để giải mã dữ liệu được mã hóa cần được cung cấp.

Còn trái với phương án thực hiện trên Fig.1C, bộ xử lý 112b được đặt cấu hình để tận dụng chìa khóa mã hóa đối xứng thứ ba KEK được giải mã trong việc giải mã của dữ liệu cần được cung cấp.

Trái lại, các thành phần, các dấu hiệu và các thông số (như các chìa khóa mã hóa, các bộ phận nhận diện, và dữ liệu cần được cung cấp) của thiết bị máy khách 110a và thiết bị máy khách 110b là giống nhau hoặc ít nhất là tương đương về mặt chức năng do đó các phần mô tả của chúng không được lặp lại chi tiết.

Fig.2 thể hiện giản đồ minh họa hệ thống 200 theo một phương án thực hiện; Hệ thống 200 bao gồm máy chủ 120 (ví dụ máy chủ nhà sản xuất chip), thiết bị máy chủ an ninh 100, thiết bị máy khách 110_0, và các thiết bị khách 110_1-110_n.

Theo một phương án thực hiện, các thành phần, các dấu hiệu và các thông số (như các chìa khóa mã hóa, các bộ phận nhận diện, và dữ liệu cần được cung cấp khác nhau) của thiết bị máy chủ an ninh 100 là giống nhau hoặc ít nhất là tương tự về mặt chức năng với các thành phần của thiết bị máy chủ an ninh 100a, và các thành phần, các dấu hiệu và các thông số của các thiết bị khách 110_1-110_n là giống hoặc ít nhất là tương đương về mặt chức năng với các thành phần của các thiết bị khách 110a. Theo

một phương án thực hiện khác, các thành phần, các dấu hiệu và các thông số của thiết bị máy chủ an ninh 100 là giống nhau hoặc ít nhất là tương tự về mặt chức năng với các thành phần của thiết bị máy chủ an ninh 100b, và các thành phần, các dấu hiệu và các thông số của các thiết bị khách 110_1-110_n là giống hoặc ít nhất là tương đương về mặt chức năng với các thành phần của thiết bị khách 110b. Do đó, các phần mô tả chi tiết của chúng sẽ không được lặp lại chi tiết.

Như được thể hiện trên Fig.2, giai đoạn sản xuất an ninh 210 bao gồm chìa khóa phân loại K đang được lập trình theo cách an ninh tới các thiết bị khách 110_1-110_n trong các thao tác 211_1 đến 211_n. Giai đoạn sản xuất an ninh 210 cần phải được thực hiện một lần cho mỗi phân loại thiết bị máy khách. Như được thảo luận ở trên, chìa khóa phân loại K thường được viết vào trong các vùng bộ nhớ an ninh của các thiết bị khách 110_1-110_n (như phần lưu giữ an ninh 113_1-113_n) là có thể truy cập được bởi phần cứng an ninh (như môi trường thực thi được tin cậy) của các thiết bị khách 110_1-110_n. Mã ứng dụng bình thường không thể truy cập được chìa khóa phân loại K.

Các giai đoạn 220 và 230 bao gồm việc truyền của các tài sản/dữ liệu cần được cung cấp từ thiết bị máy chủ an ninh 100 tới các thiết bị khách 110_1-110_n. Các giai đoạn 220 và 230 cần phải được thực hiện một lần cho mỗi thiết bị máy khách.

Phần dẫn ra của PKP có thể được thực hiện, ví dụ bởi nhà sản xuất chip, hoặc bởi nhà sản xuất thiết bị máy khách sử dụng thiết bị máy khách đơn 113_0 đang thuộc về phân loại cụ thể. Trong trường hợp sau, nhà sản xuất chip dẫn ra PKP trong môi trường an ninh (ví dụ máy chủ 120) mà chìa khóa phân loại K là có sẵn ở trong đó. Trong trường hợp sau, nhà sản xuất thiết bị máy khách có thể tải ứng dụng sinh PKP được tin cậy đặc biệt tới thiết bị máy khách 113_0 đơn. Ứng dụng được tin cậy này truy cập tới chìa khóa phân loại K và dẫn ra PKP trong thiết bị máy khách 113_0 này. Trong cả hai trường hợp, việc dẫn ra chìa khóa cần phải được thực hiện một lần cho mỗi phân loại thiết bị. Phần chìa khóa công cộng mà PKP được truyền theo cách an ninh (thao tác 212 hoặc 221) tới máy chủ được tin cậy (tức là thiết bị máy chủ an ninh 100) thực hiện việc sử dụng của nó theo cách tương ứng.

PKP sau đó được sử dụng để bao bọc/mã hóa (thao tác 222) tài sản trong máy chủ được tin cậy 100, tài sản được bao bọc/mã hóa được truyền (các thao tác 231_1 đến 231_n) tới các thiết bị khách 110_1-110_n, và các thiết bị khách 110_1-110_n tháo/giải mã tài

sản với PKP. Bên cạnh việc truyền tài sản được bao bọc/mã hóa, các thông số an ninh bổ sung cũng cần phải được truyền, chứa chìa khóa công cộng Q_e của cặp chìa khóa tam thời, các vectơ khởi tạo (initialization vector - IV) tiềm năng được sử dụng trong suốt quá trình bao bọc/mã hóa các tài sản, và/hoặc dữ liệu thuần (như chuỗi chứng thư thiết bị).

Fig.3A thể hiện giản đồ 300a của phương pháp làm ví dụ theo một phương án thực hiện.

Phương pháp 300a bao gồm bước thu, bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu PKP, cặp chìa khóa mật mã không đối xứng dự liệu PKP đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất K của bộ phận nhận diện phân loại thiết bị khách, bước 301a.

Phương pháp 300a còn bao gồm bước sinh ra cặp chìa khóa mật mã không đối xứng tạm thời bởi thiết bị máy chủ an ninh, bước 302a.

Phương pháp 300a còn bao gồm bước sinh ra chìa khóa mật mã đối xứng thứ hai PSK trên cơ sở chìa khóa công cộng thu được Q_p của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân d_e của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, bước 303a.

Phương pháp 300a còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, chìa khóa mật mã đối xứng thứ hai được sinh ra trong việc mã hóa của dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại, bước 304a.

Phương pháp 300a còn bao gồm bước gửi dữ liệu được mã hóa cần được cung cấp và chìa khóa công cộng Q_e của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra từ thiết bị máy chủ an ninh tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại, bước 305a.

Phương pháp 300a có thể được thực hiện bởi thiết bị máy chủ an ninh 100a. Các dấu hiệu khác của phương pháp 300a là kết quả trực tiếp từ các chức năng của thiết bị máy chủ an ninh 100a. Phương pháp 300a có thể được thực hiện bởi chương trình máy tính.

Fig.3A còn thể hiện giản đồ 310a của phương pháp làm ví dụ khác theo cùng một phương án thực hiện.

Phương pháp 310a bao gồm bước nhận, tại thiết bị máy khách từ thiết bị máy chủ an ninh, chìa khóa công cộng Q_e của cặp chìa khóa mật mã không đối xứng tạm thời và dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách, bước 311a.

Phương pháp 310a còn bao gồm bước thu, bởi thiết bị máy khách, chìa khóa cá nhân d_p của cặp chìa khóa mật mã không đối xứng dự liệu, bước 312a. Cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra bởi thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất (chìa khóa phân loại K) của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất nào được lưu tại phần lưu giữ an ninh của thiết bị máy khách.

Phương pháp 310a còn bao gồm bước sinh ra, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai PSK trên cơ sở chìa khóa cá nhân d_p của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra và chìa khóa công cộng Q_e nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, bước 313a.

Phương pháp 310a còn bao gồm bước tận dụng, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai được sinh ra PSK trong việc giải mã của dữ liệu được mã hóa cần được cung cấp, bước 314a.

Phương pháp 310a có thể được thực hiện bởi thiết bị máy khách 110a. Các dấu hiệu khác của phương pháp 310a là kết quả trực tiếp từ các chức năng của thiết bị máy khách 110a. Phương pháp 310a có thể được thực hiện bởi chương trình máy tính.

Fig.3B thể hiện giản đồ của phương pháp làm ví dụ 300b theo một phương án thực hiện khác.

Phương pháp 300b bao gồm bước thu, bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu PKP, cặp chìa khóa mật mã không đối xứng dự liệu PKP đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất K của bộ phận nhận diện phân loại thiết bị khách, bước 301b.

Phương pháp 300b còn bao gồm bước sinh ra cặp chìa khóa mật mã không đối xứng tạm thời bởi thiết bị máy chủ an ninh, bước 302b.

Phương pháp 300b còn bao gồm bước sinh ra chìa khóa mật mã đối xứng thứ hai PSK trên cơ sở chìa khóa công cộng thu được Q_p của cặp chìa khóa mật mã không đối xứng dự liệu và chìa khóa cá nhân d_e của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, bước 303b.

Phương pháp 300b còn bao gồm bước thu (sinh ra hoặc truy hồi) dữ liệu cần được cung cấp (chìa khóa thiết bị cá nhân K_{priv}) cho một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại, bước 304b.

Phương pháp 300b còn bao gồm bước sinh ra chìa khóa mã hóa đối xứng thứ ba KEK theo cách ngẫu nhiên bởi thiết bị máy chủ an ninh, bước 305b.

Phương pháp 300b còn bao gồm bước mã hóa, bởi thiết bị máy chủ an ninh, dữ liệu cần được cung cấp với chìa khóa mã hóa đối xứng thứ ba được sinh ra ngẫu nhiên KEK, bước 306b.

Phương pháp 300b còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, chìa khóa mật mã đối xứng thứ hai được sinh ra PSK trong việc mã hóa của chìa khóa mã hóa đối xứng thứ ba (KEK), nhờ đó thu được chìa khóa mã hóa đối xứng thứ ba được mã hóa (PEK), bước $307b_1$.

Tùy chọn là, phương pháp 300b còn bao gồm bước tận dụng, bởi thiết bị máy chủ an ninh, kỹ thuật mã hóa hộp trắng trong việc mã hóa của chìa khóa mã hóa đối xứng thứ ba được sinh ra, bước $307b_2$.

Tùy chọn là, phương pháp 300b còn bao gồm bước tạo yêu cầu ký chứng thư (certificate signing request - CSR), bước 308b.

Phương pháp 300b còn bao gồm bước gửi dữ liệu được mã hóa cần được cung cấp và chìa khóa mã hóa đối xứng thứ ba được mã hóa từ thiết bị máy chủ an ninh tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại, bước 309b.

Phương pháp 300b có thể được thực hiện bởi thiết bị máy chủ an ninh 100b. Các dấu hiệu khác của phương pháp 300b là kết quả trực tiếp từ các chức năng của thiết bị máy chủ an ninh 100b. Phương pháp 300b có thể được thực hiện bởi chương trình máy tính.

Fig.3C thể hiện lưu đồ 310b của phương pháp làm ví dụ theo phương án thực hiện khác nữa.

Phương pháp 310b bao gồm bước nhận, tại thiết bị máy khách từ thiết bị máy chủ an ninh, chìa khóa công cộng Q_e của cặp chìa khóa mật mã không đối xứng tạm thời, chìa khóa mã hóa đối xứng thứ ba được mã hóa (PEK), và dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách, bước 311b.

Phương pháp 310b còn bao gồm bước thu, bởi thiết bị máy khách, chìa khóa cá nhân d_p của cặp chìa khóa mật mã không đối xứng dự liệu, bước 312b. Cặp chìa khóa mật mã không đối xứng dự liệu đã được sinh ra bởi thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất (chìa khóa phân loại K) của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất nào được lưu tại phần lưu giữ an ninh của thiết bị máy khách.

Phương pháp 310b còn bao gồm bước sinh ra, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai PSK trên cơ sở chìa khóa cá nhân d_p của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra và chìa khóa công cộng Q_e nhận được của cặp chìa khóa mật mã không đối xứng tạm thời sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, bước 313b.

Phương pháp 310b còn bao gồm bước tận dụng, bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai được sinh ra PSK (và tùy chọn là kỹ thuật mã hóa hộp trắng) trong việc giải mã của chìa khóa mã hóa đối xứng thứ ba được mã hóa (PEK) để thu được chìa khóa mã hóa đối xứng thứ ba (KEK) được giải mã, bước 314b.

Phương pháp 310b còn bao gồm bước tận dụng chìa khóa mã hóa đối xứng thứ ba (KEK) đã được giải mã trong việc giải mã của dữ liệu cần được cung cấp, bước 315b.

Phương pháp 310b có thể được thực hiện bởi thiết bị máy khách 110b. Các dấu hiệu khác của phương pháp 310b là kết quả trực tiếp từ các chức năng của thiết bị máy khách 110b. Phương pháp 310b có thể được thực hiện bởi chương trình máy tính.

Nói cách khác, quy trình của các hình vẽ Fig. 3B và Fig.3C có thể bắt đầu với việc sinh ra (hoặc truy hồi) của cặp chìa khóa thiết bị, việc sinh ra của chìa khóa mã hóa chìa khóa (key encryption key - KEK) được chia sẻ, và việc sinh ra của cặp chìa khóa tạm thời (ephemeral key pair - EKP) là để được sử dụng với ECHD. Đầu tiên,

cặp chìa khóa thiết bị có thể được sử dụng sinh ra yêu cầu ký chứng thư (certificate signing request - CSR) có thể, ví dụ ở định dạng PKCS#10. CSR có thể được sử dụng để đăng ký chứng thư thiết bị từ hệ thống cơ sở hạ tầng chìa khóa công cộng (public key infrastructure - PKI) (tức là, từ bên có thẩm quyền cấp chứng thư). Sau đó, KEK được sử dụng để bao bọc/mã hóa chìa khóa thiết bị cá nhân. Sau đó, chìa khóa cá nhân của cặp chìa khóa tạm thời Q_e được sử dụng cùng với chìa khóa công cộng của PKP d_p để dẫn ra PSK (ví dụ bằng cách sử dụng thỏa thuận chìa khóa ECDH). PSK sau đó được sử dụng để bao bọc/mã hóa KEK tạo thành chìa khóa dự liệu được mã hóa (encrypted provisioning key - PEK). Hàm loại trừ hoặc (exclusive or - XOR) có thể được sử dụng cho nó (tức là OneTimePad, OTP), nhưng các mẫu mã hóa khác cũng có thể được sử dụng. Cuối cùng, PEK được mã hóa sử dụng việc mã hóa hộp trắng. Chứng thư thiết bị (với chuỗi chứng thư toàn thể), chìa khóa cá nhân được mã hóa, và KEK được mã hóa (với PSK và việc mã hóa hộp trắng) tạo thành cục dữ liệu sẽ được sử dụng cho việc cung cấp cặp chìa khóa thiết bị với chuỗi chứng thư cho thiết bị máy khách. Cục dữ liệu (tức là đầu ra) cũng có thể chứa các trường dữ liệu bổ sung, như các vectơ khởi tạo (initialization vector - IV) được sử dụng trong các bước bao bọc/mã hóa khác nhau, và chìa khóa công cộng Q_e của EPK tạm thời.

Sau khi giải mã dữ liệu cần được cung cấp (ví dụ chìa khóa thiết bị cá nhân), thiết bị máy khách có thể lưu dữ liệu cần được cung cấp và tùy chọn là chứng thư thiết bị (chuỗi) vào trong vị trí an ninh và hạn chế nó sử dụng khi thích hợp.

Phần bộc lộ này cho phép cơ sở sản xuất không được tin cậy được trang bị với thiết bị máy chủ an ninh để thiết lập kênh cung cấp dữ liệu an ninh từ thiết bị máy chủ an ninh tới phần cứng được tin cậy trong các thiết bị khách, nhờ đó loại bỏ các vấn đề về an ninh được kết hợp với việc cung cấp của dữ liệu trong thiết bị máy khách trong suốt quá trình sản xuất thiết bị, như cách để mã hóa dữ liệu cần được cung cấp sao cho chỉ thiết bị máy khách đích là có khả năng giải mã dữ liệu, và cách để xác thực thiết bị máy khách đích.

Trong phần mô tả này, chìa khóa K được sử dụng để sinh ra cặp chìa khóa dự liệu (provisioning key pair - PKP), trong đó phần chìa khóa cá nhân chỉ được biết bởi thiết bị máy khách, và phần chìa khóa công cộng được truyền tới thiết bị máy chủ an ninh. PKP sau đó sử dụng, ví dụ là với phương pháp Diffie-Hellman đường cong eliptic

(Elliptic Curve Diffie-Hellman - ECDH) để dẫn ra bí mật được chia sẻ dự liệu (provisioning shared secret - PSK), vốn có thể được sử dụng để đảm bảo an ninh cho việc truyền của dữ liệu cần được cung cấp từ thiết bị máy chủ an ninh tới thiết bị máy khách. Do chỉ thiết bị máy khách truy cập vào phần chìa khóa cá nhân của PKP, nên chỉ nó có thể thu được tài sản ở dạng văn bản gốc. Quy trình này cũng xác thực một cách hoàn toàn thiết bị máy khách khi thiết bị máy chủ an ninh biết rằng chìa khóa cá nhân tương ứng chỉ có sẵn trong các thiết bị khách đã được xác thực.

Thêm nữa, chìa khóa công cộng đơn cho mỗi phân loại thiết bị cần phải được dẫn ra và/hoặc được thu, vốn sẽ được nhập vào trong thiết bị máy chủ an ninh. Thêm nữa, phần bộc lộ này là có thể triển khai được một cách sẵn sàng do các nhà sản xuất chip thường lập trình từ trước các bí mật phân loại trong các chip của họ. Thêm nữa, việc dẫn ra của chìa khóa có thể được làm đa dạng hóa để cho phép nhiều chìa khóa dự liệu cho nhiều trường hợp sử dụng. Thêm nữa, thậm chí nếu một chìa khóa phiên dự liệu được dàn xếp, thì nó không cho phép truy cập tới các chìa khóa thiết bị bất kỳ khác.

Chức năng được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều thành phần sản phẩm chương trình máy tính như các thành phần phần mềm. Theo phương án thực hiện này, các thiết bị khách 110a, 110b và/hoặc các thiết bị máy chủ an ninh 100a, 100b chứa bộ xử lý được đặt cấu hình bởi mã chương trình thi được thực thi để thực thi các phương án thực hiện của các hoạt động và chức năng được mô tả. Theo cách khác, hoặc bổ sung là, chức năng được mô tả ở đây có thể được thực hiện, ít nhất một phần, bởi một hoặc nhiều thành phần logic phần cứng. Ví dụ, và không bị hạn chế, các loại minh họa của các thành phần logic phần cứng có thể được sử dụng bao gồm các mạng cổng lập trình được bằng trường (Field-programmable Gate Array - FPGA), các mạch tích hợp chương trình cụ thể (Program-specific Integrated Circuit - ASIC), các sản phẩm tiêu chuẩn chương trình cụ thể (Program-specific Standard Product - ASSP), các hệ thống hệ thống trên chip (System-on-a-chip system - SOC), các thiết bị logic lập trình được phức tạp (Complex Programmable Logic Device - CPLD), và các đơn vị xử lý đồ họa (Graphics Processing Unit - GPU).

Khoảng giới hạn hoặc trị số thiết bị bất kỳ được cho ở đây có thể được mở rộng hoặc được thay đổi mà không làm mất tác dụng của nó. Phương án thực hiện bất kỳ

nào cũng có thể được kết hợp với phương án thực hiện khác, trừ khi không được cho phép một cách rõ ràng.

Mặc dù đối tượng đã được mô tả theo ngôn ngữ cụ thể hóa cho các dấu hiệu cấu trúc và/hoặc các hành động, nhưng cần hiểu rằng đối tượng được xác định trong các yêu cầu bảo hộ kèm theo không nhất thiết bị hạn chế vào các dấu hiệu và các hành động cụ thể nêu trên. Thay vào đó, các dấu hiệu và các hành động được mô tả ở trên được bộc lộ như là các ví dụ của việc áp dụng của các yêu cầu bảo hộ và các dấu hiệu và các hành động tương đương được tính đến để nằm trong phạm vi bảo hộ của các yêu cầu bảo hộ.

Cần hiểu rằng các lợi ích và các ưu điểm đã được mô tả ở trên có thể liên quan tới một hoặc nhiều phương án thực hiện hoặc có thể liên quan tới nhiều phương án thực hiện. Các phương án thực hiện không bị hạn chế vào các phương án giải quyết vấn đề bất kỳ hoặc tất cả các vấn đề trong số các vấn đề nêu trên hoặc các phương án có lợi ích và ưu điểm bất kỳ hoặc tất các các lợi ích và ưu điểm trong số các lợi ích và các ưu điểm nêu trên. Cần hiểu rằng tham khảo tới một mục có thể đề cập tới một hoặc nhiều mục này.

Các bước của phương pháp được mô tả ở đây có thể được thực hiện theo thứ tự thích hợp bất kỳ, hoặc là đồng thời, khi thích hợp. Thêm vào đó, các khối riêng rẽ có thể được xóa khỏi phương pháp bất kỳ trong số các phương pháp mà không tách khỏi tinh thần và phạm vi bảo hộ của đối tượng được mô tả ở đây. Các khía cạnh của phương án thực hiện bất kỳ trong số các phương án thực hiện được mô tả ở trên có thể được kết hợp với các khía cạnh của phương án thực hiện bất kỳ trong số các phương án thực hiện khác được mô tả để tạo thành các phương án thực hiện khác nữa mà không mất tác dụng của nó.

Thuật ngữ 'bao gồm' được sử dụng ở đây để có nghĩa là chứa phương pháp, các khối hoặc các thành phần được nhận diện, nhưng không phải là các khối hoặc các thành phần không chứa danh sách loại trừ và phương pháp hoặc thiết bị có thể chứa các khối hoặc các thành phần bổ sung.

Cần hiểu rằng phần mô tả nêu trên chỉ được cho theo cách làm ví dụ và các biến đổi khác cũng có thể được tạo ra bởi người có hiểu biết trung bình trong lĩnh vực kỹ thuật. Phần mô tả, phần ví dụ và các dữ liệu trên cung cấp bản mô tả hoàn chỉnh về cấu

trúc và việc sử dụng các phương án thực hiện làm ví dụ. Mặc dù các phương án thực hiện khác đã được mô tả trên với mức độ cụ thể nhất định, hoặc tham chiếu đến một hoặc nhiều phương án thực hiện riêng lẻ, nhưng người có hiểu biết trung bình trong lĩnh vực này có thể thực hiện nhiều biến đổi với các phương án thực hiện được bộc lộ mà không trệch khỏi ý tưởng hoặc phạm vi bảo hộ của sáng chế.

YÊU CẦU BẢO HỘ

1. Thiết bị máy chủ an ninh (100a), bao gồm:

giao diện (101a) được đặt cấu hình để thu được chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu nêu trên đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách, trong đó chìa khóa mật mã đối xứng thứ nhất là cùng chìa khóa mật mã đối xứng thứ nhất cho tất cả các thiết bị khách với cùng bộ phận nhận diện phân loại; và

bộ xử lý (102a) được đặt cấu hình để tận dụng chìa khóa công cộng thu được nêu trên của cặp chìa khóa mật mã không đối xứng dự liệu nêu trên trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra nêu trên trong việc mã hóa của dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại nêu trên,

trong đó giao diện (101a) còn được đặt cấu hình để gửi dữ liệu được mã hóa để được cung cấp tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại nêu trên.

2. Thiết bị máy chủ an ninh (100a) theo điểm 1, trong đó bộ xử lý (102a) còn được đặt cấu hình để sinh ra cặp chìa khóa mật mã không đối xứng tạm thời, và để sinh ra chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa công cộng thu được nêu trên của cặp chìa khóa mật mã không đối xứng dự liệu nêu trên và chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra nêu trên sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước, và giao diện (101a) còn được đặt cấu hình để gửi chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời được sinh ra nêu trên tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại nêu trên.

3. Thiết bị máy chủ an ninh (100a) theo điểm 1 hoặc 2, trong đó dữ liệu cần được cung cấp bao gồm ít nhất một phần trong số vật liệu chìa khóa mã hóa hoặc mã thực thi được.

4. Thiết bị máy chủ an ninh (100a) theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó cặp chìa khóa mật mã không đối xứng dự liệu bao gồm cặp chìa khóa đường cong eliptic hoặc cặp chìa khóa Rivest-Shamir-Adleman.

5. Thiết bị máy chủ an ninh (100a) theo điểm bất kỳ trong số các điểm từ 2 đến 4, trong đó giao thức thỏa thuận chìa khóa được xác định từ trước bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman.

6. Thiết bị máy chủ an ninh (100a) theo điểm 5, trong đó giao thức thỏa thuận chìa khóa Diffie-Hellman bao gồm giao thức thỏa thuận chìa khóa Diffie-Hellman đường cong eliptic.

7. Thiết bị máy chủ an ninh (100a) theo điểm bất kỳ trong số các điểm từ 1 đến 6, còn bao gồm môđun an ninh phần cứng (103a).

8. Thiết bị máy khách (110a), bao gồm:

phần lưu giữ an ninh (113a) được đặt cấu hình để lưu chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách (110a), trong đó chìa khóa mật mã đối xứng thứ nhất là cùng chìa khóa mật mã đối xứng thứ nhất cho tất cả các thiết bị khách với cùng bộ phận nhận diện phân loại;

bộ thu phát (111a) được đặt cấu hình để nhận từ thiết bị máy chủ an ninh dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách (110a); và

bộ xử lý (112a) được đặt cấu hình để thu được chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu nêu trên đã được sinh ra tại thiết bị máy khách (110a) trên cơ sở chìa khóa mật mã đối xứng thứ nhất đã được lưu, tận dụng chìa khóa cá nhân thu được nêu trên của cặp chìa khóa mật mã không đối xứng dự liệu nêu trên trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai, và tận dụng chìa khóa mật mã đối xứng thứ hai được sinh ra nêu trên trong việc giải mã của dữ liệu được mã hóa cần được cung cấp.

9. Thiết bị máy khách (110a) theo điểm 8, trong đó bộ thu phát (111a) còn được đặt cấu hình để nhận từ thiết bị máy chủ an ninh chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng tạm thời, và bộ xử lý (112a) còn được đặt cấu hình để sinh ra

chìa khóa mật mã đối xứng thứ hai trên cơ sở chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu được sinh ra nêu trên và chìa khóa công cộng nhận được của cặp chìa khóa mật mã không đối xứng tạm thời nêu trên sử dụng giao thức thỏa thuận chìa khóa được xác định từ trước.

10. Thiết bị máy khách (110a) theo điểm 8 hoặc 9, còn bao gồm môi trường thực thi được tin cậy (114a) được đặt cấu hình để thực hiện các thao tác mã hóa.

11. Phương pháp truyền thông (300a) bao gồm các bước:

thu (301a), bởi thiết bị máy chủ an ninh, chìa khóa công cộng của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu nêu trên đã được sinh ra trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách, trong đó chìa khóa mật mã đối xứng thứ nhất là cùng chìa khóa mật mã đối xứng thứ nhất cho tất cả các thiết bị khách với cùng bộ phận nhận diện phân loại;

tận dụng (303a), bởi thiết bị máy chủ an ninh, chìa khóa công cộng thu được nêu trên của cặp chìa khóa mật mã không đối xứng dự liệu nêu trên trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai;

tận dụng (304a), bởi thiết bị máy chủ an ninh, chìa khóa mật mã đối xứng thứ hai được sinh ra nêu trên trong việc mã hóa của dữ liệu để được cung cấp tới một hoặc nhiều thiết bị khách được kết hợp với bộ phận nhận diện phân loại nêu trên; và

gửi (305a) dữ liệu được mã hóa cần được cung cấp từ thiết bị máy chủ an ninh tới một hoặc nhiều thiết bị trong số các thiết bị khách được kết hợp với bộ phận nhận diện phân loại nêu trên.

12. Vật ghi đọc được bằng máy tính lưu giữ chương trình máy tính bao gồm mã chương trình được đặt cấu hình để thực hiện phương pháp theo điểm 11, khi chương trình máy tính được thực thi trên thiết bị tính toán.

13. Phương pháp truyền thông (310a) bao gồm các bước:

nhận (311a), tại thiết bị máy khách từ thiết bị máy chủ an ninh, dữ liệu được mã hóa để được cung cấp tới thiết bị máy khách;

thu được (312a), bởi thiết bị máy khách, chìa khóa cá nhân của cặp chìa khóa mật mã không đối xứng dự liệu, cặp chìa khóa mật mã không đối xứng dự liệu nêu trên đã được sinh ra bởi thiết bị máy khách trên cơ sở chìa khóa mật mã đối xứng thứ nhất của bộ phận nhận diện phân loại thiết bị khách được kết hợp với thiết bị máy khách, chìa khóa mật mã đối xứng thứ nhất nêu trên được lưu tại phần lưu giữ an ninh của thiết bị máy khách, trong đó chìa khóa mật mã đối xứng thứ nhất là cùng chìa khóa mật mã đối xứng thứ nhất cho tất cả các thiết bị khách với cùng bộ phận nhận diện phân loại;

tận dụng (313a), bởi thiết bị máy khách, chìa khóa cá nhân thu được nêu trên của cặp chìa khóa mật mã không đối xứng dự liệu nêu trên trong việc sinh ra của chìa khóa mật mã đối xứng thứ hai; và

tận dụng (314a), bởi thiết bị máy khách, chìa khóa mật mã đối xứng thứ hai được sinh ra nêu trên trong việc giải mã của dữ liệu được mã hóa cần được cung cấp.

14. Vật ghi đọc được bằng máy tính lưu giữ chương trình máy tính bao gồm mã chương trình được đặt cấu hình để thực hiện phương pháp theo điểm 13, khi chương trình máy tính được thực thi trên thiết bị tính toán.

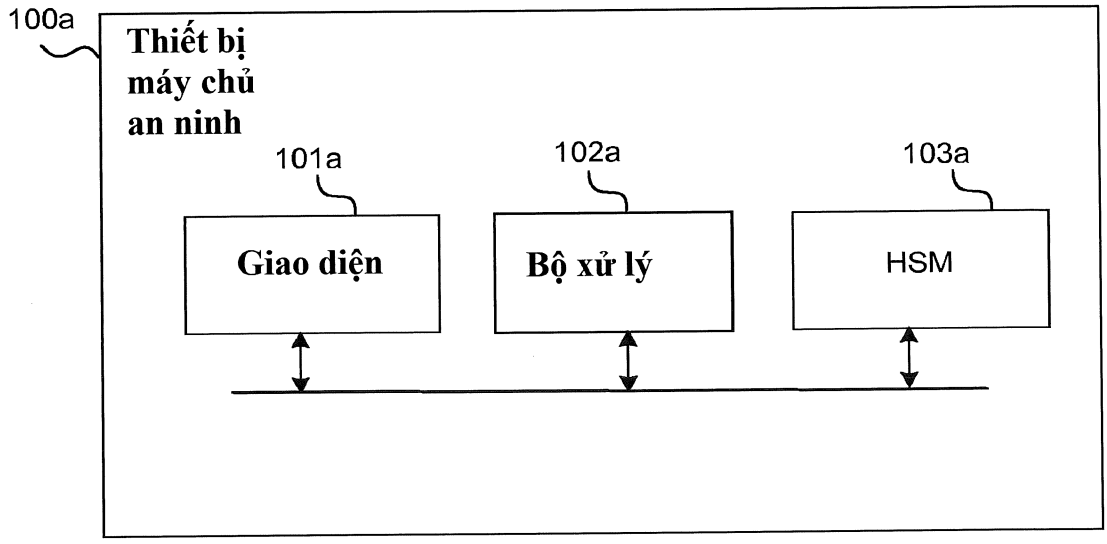

100a
Thiết bị máy chủ an ninh
101a
102a
103a
Giao diện
Bộ xử lý
HSM

FIG. 1A

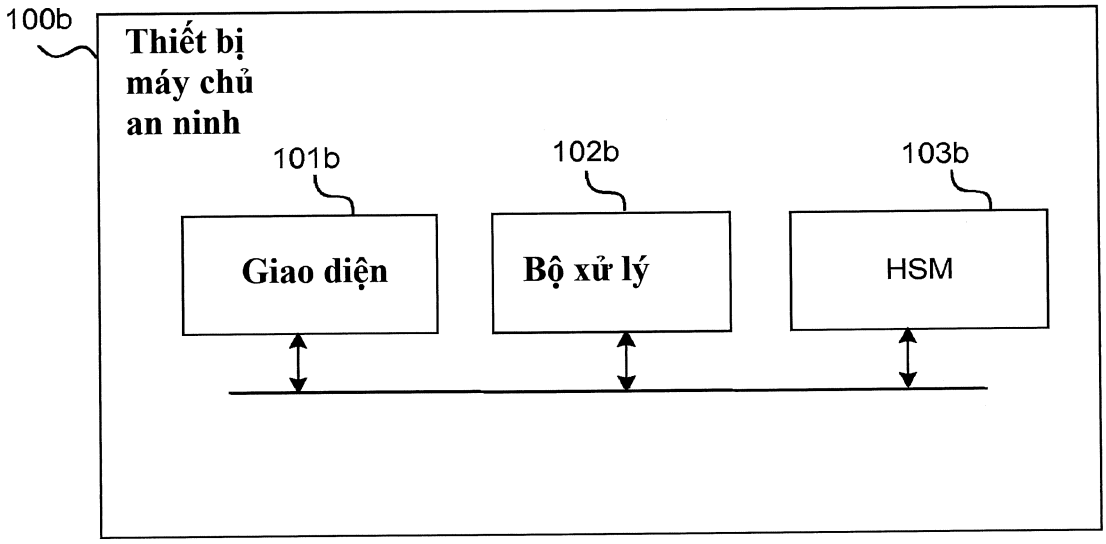

100b
Thiết bị máy chủ an ninh
101b
102b
103b
Giao diện
Bộ xử lý
HSM

FIG. 1B

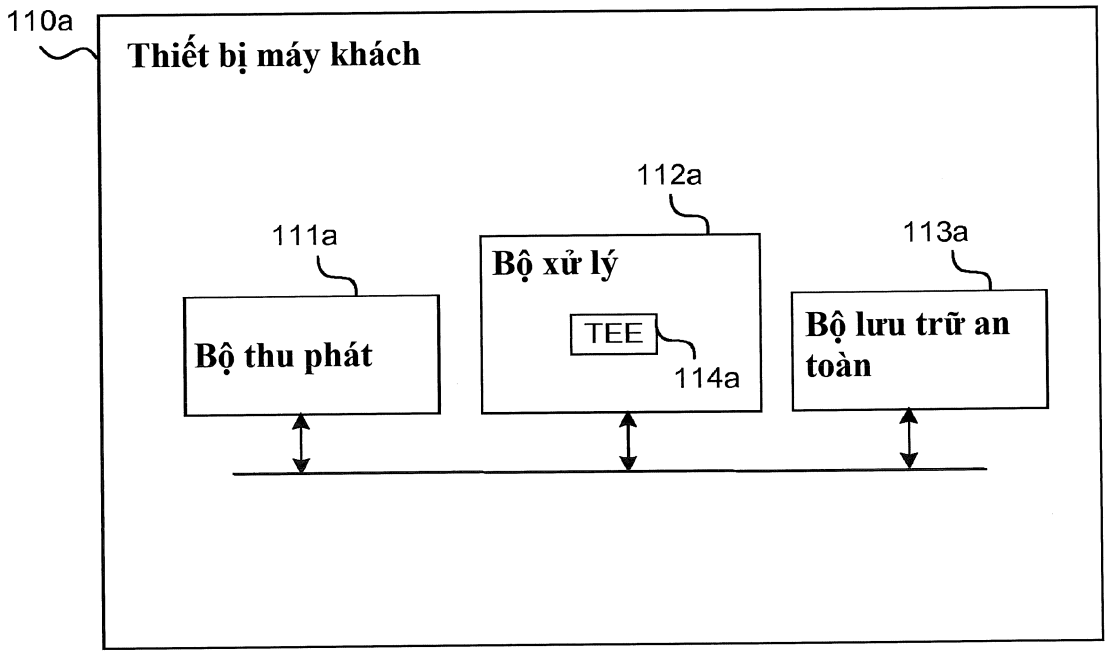

110a
Thiết bị máy khách
112a
111a
Bộ xử lý
113a
Bộ thu phát
TEE
114a
Bộ lưu trữ an toàn

FIG. 1C

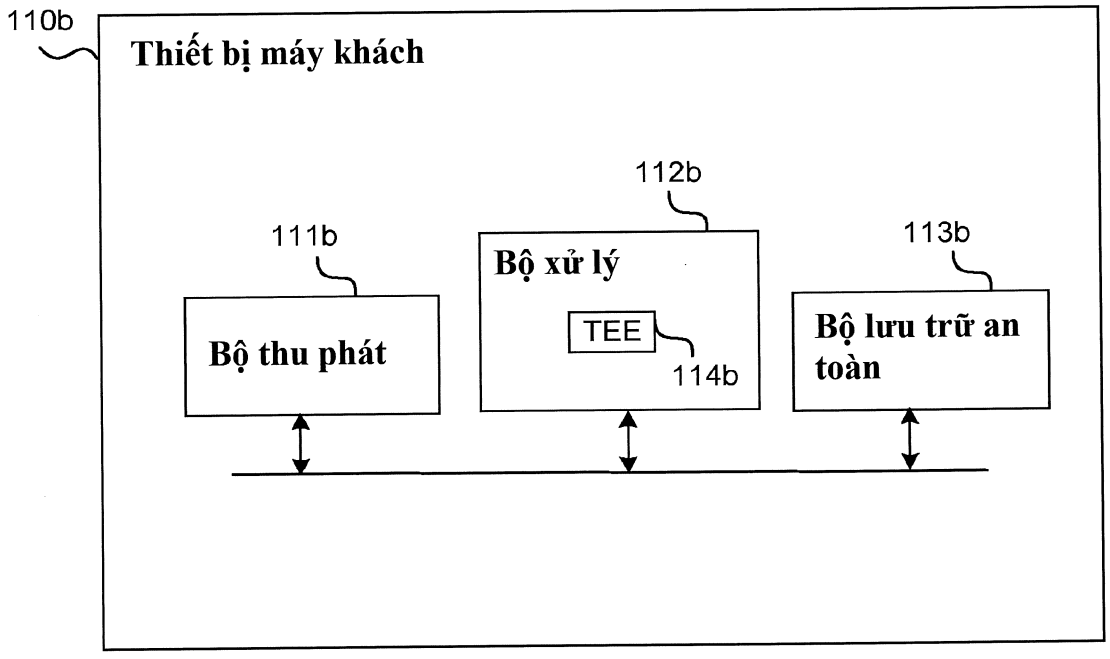

110b
Thiết bị máy khách
112b
111b
Bộ xử lý
113b
Bộ thu phát
TEE
114b
Bộ lưu trữ an toàn

FIG. 1D

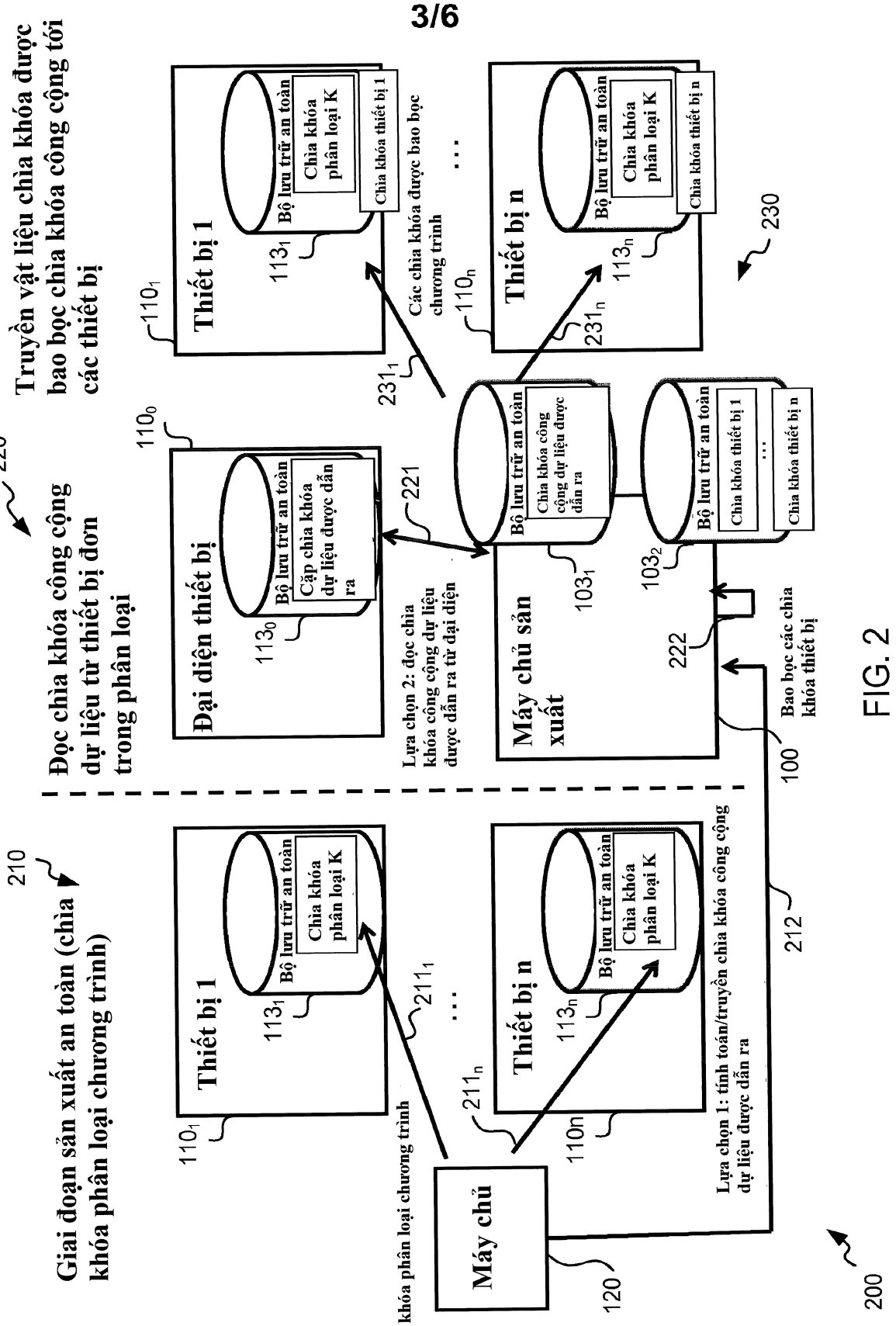

Truyền vật liệu chìa khóa được bao bọc chìa khóa công cộng tới các thiết bị
Đọc chìa khóa công cộng dự liệu từ thiết bị đơn trong phân loại
Giai đoạn sản xuất an toàn (chìa khóa phân loại chương trình)
220
210
Đại diện thiết bị
Bộ lưu trữ an toàn
Cặp chia khóa dự liệu được dẫn ra
Thiết bị 1
Chìa khóa phân loại K
Chìa khóa thiết bị 1
Các chìa khóa được bao bọc chương trình
Thiết bị n
Chìa khóa thiết bị n
Máy chủ sản xuất
Chìa khóa công cộng dự liệu được dẫn ra
Lựa chọn 2: đọc chìa khóa công cộng dự liệu được dẫn ra từ đại diện
Máy chủ
Chìa khóa phân loại chương trình
Lựa chọn 1: tính toán/truyền chìa khóa công cộng dự liệu được dẫn ra
Bao bọc các chìa khóa thiết bị
100
120
200
212
221
222
230

FIG. 2

4/6

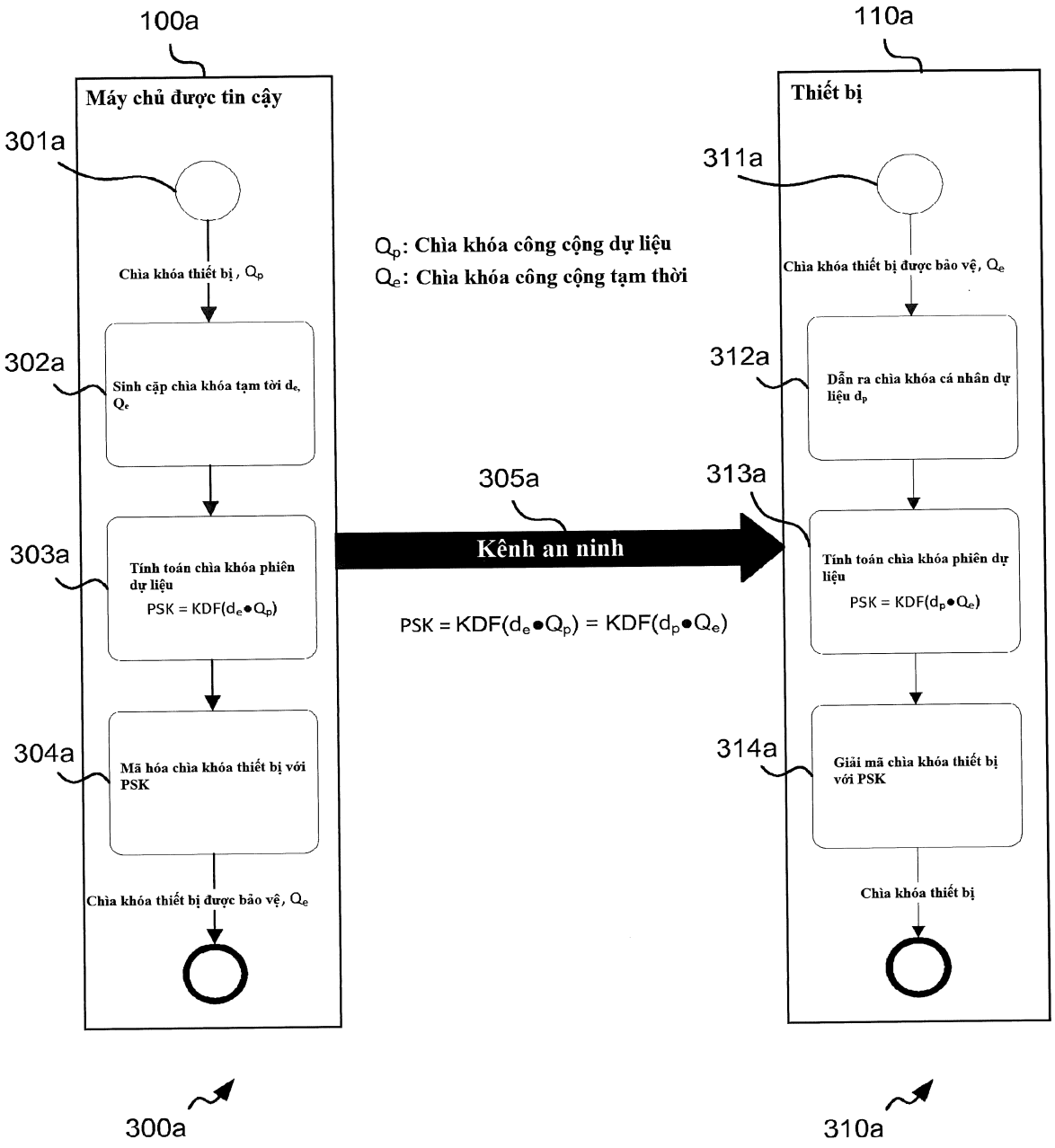

100a
Máy chủ được tin cậy
301a
Chìa khóa thiết bị , Q_p
302a
Sinh cặp chìa khóa tạm tời d_e, Q_e
303a
Tính toán chìa khóa phiên dự liệu
PSK = KDF(d_e•Q_p)
304a
Mã hóa chìa khóa thiết bị với PSK
Chìa khóa thiết bị được bảo vệ, Q_e
300a
Q_p: Chìa khóa công cộng dự liệu
Q_e: Chìa khóa công cộng tạm thời
305a
Kênh an ninh
PSK = KDF(d_e•Q_p) = KDF(d_p•Q_e)
110a
Thiết bị
311a
Chìa khóa thiết bị được bảo vệ, Q_e
312a
Dẫn ra chìa khóa cá nhân dự liệu d_p
313a
Tính toán chìa khóa phiên dự liệu
PSK = KDF(d_p•Q_e)
314a
Giải mã chìa khóa thiết bị với PSK
Chìa khóa thiết bị
310a

FIG. 3A

5/6

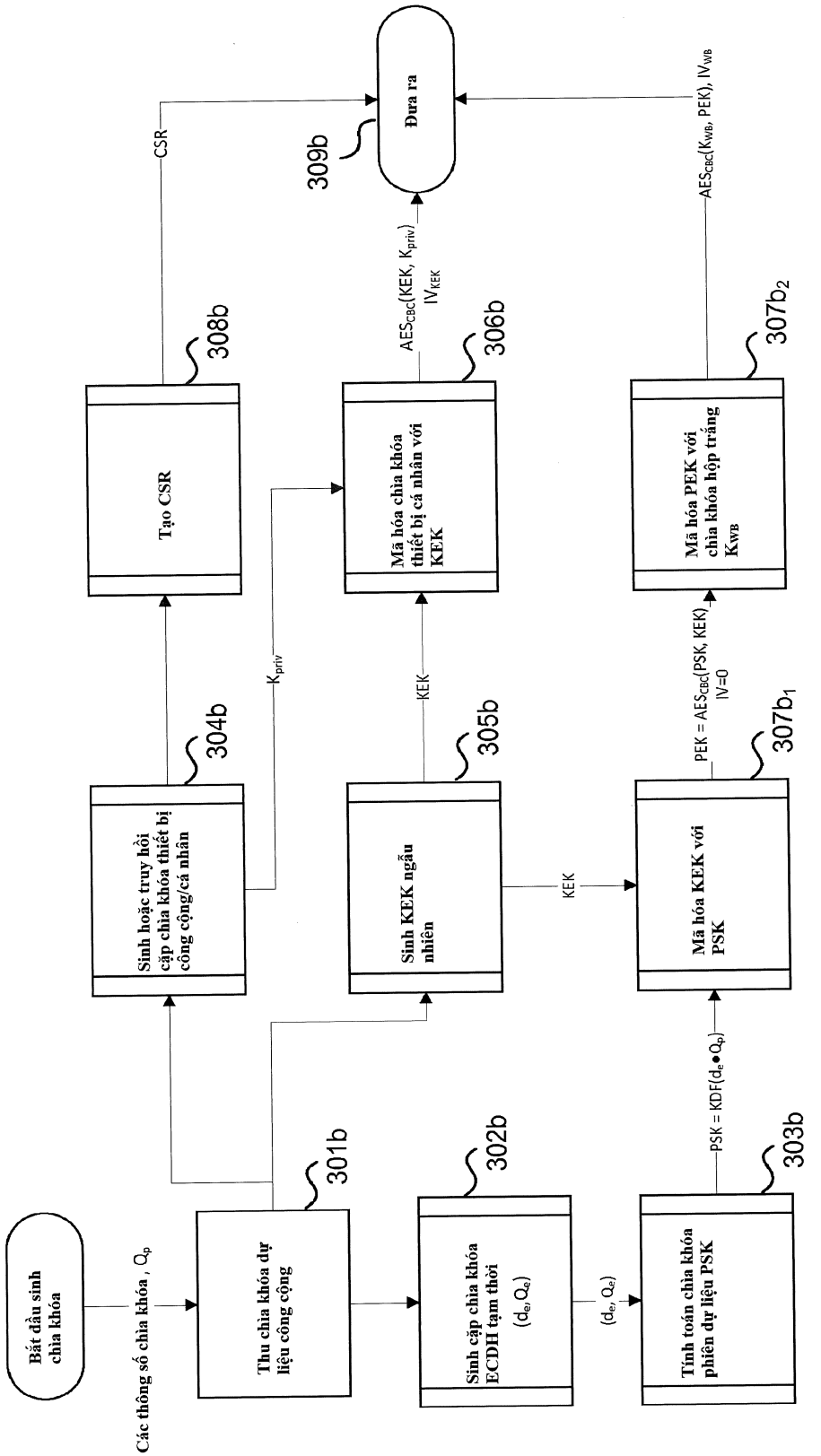

Bắt đầu sinh chia khóa
Các thông số chia khóa , Q_p
Thu chia khóa dự liệu công cộng
301b
Sinh cặp chia khóa ECDH tạm thời (d_e, Q_e)
302b
(d_e, Q_e)
Tính toán chia khóa phiên dự liệu PSK
303b
PSK = KDF($d_e \bullet Q_p$)
Sinh hoặc truy hồi cặp chia khóa thiết bị công cộng/cá nhân
304b
K_{priv}
Sinh KEK ngẫu nhiên
305b
KEK
Mã hóa KEK với PSK
307b1
PEK = AES_{CBC}(PSK, KEK)
IV=0
Mã hóa PEK với chìa khóa hộp trắng K_{WB}
307b2
$AES_{CBC}(K_{WB}, PEK), IV_{WB}$
Tạo CSR
308b
CSR
Mã hóa chìa khóa thiết bị cá nhân với KEK
306b
$AES_{CBC}(KEK, K_{priv})$
IV_{KEK}
Đưa ra
309b
300b

FIG. 3B

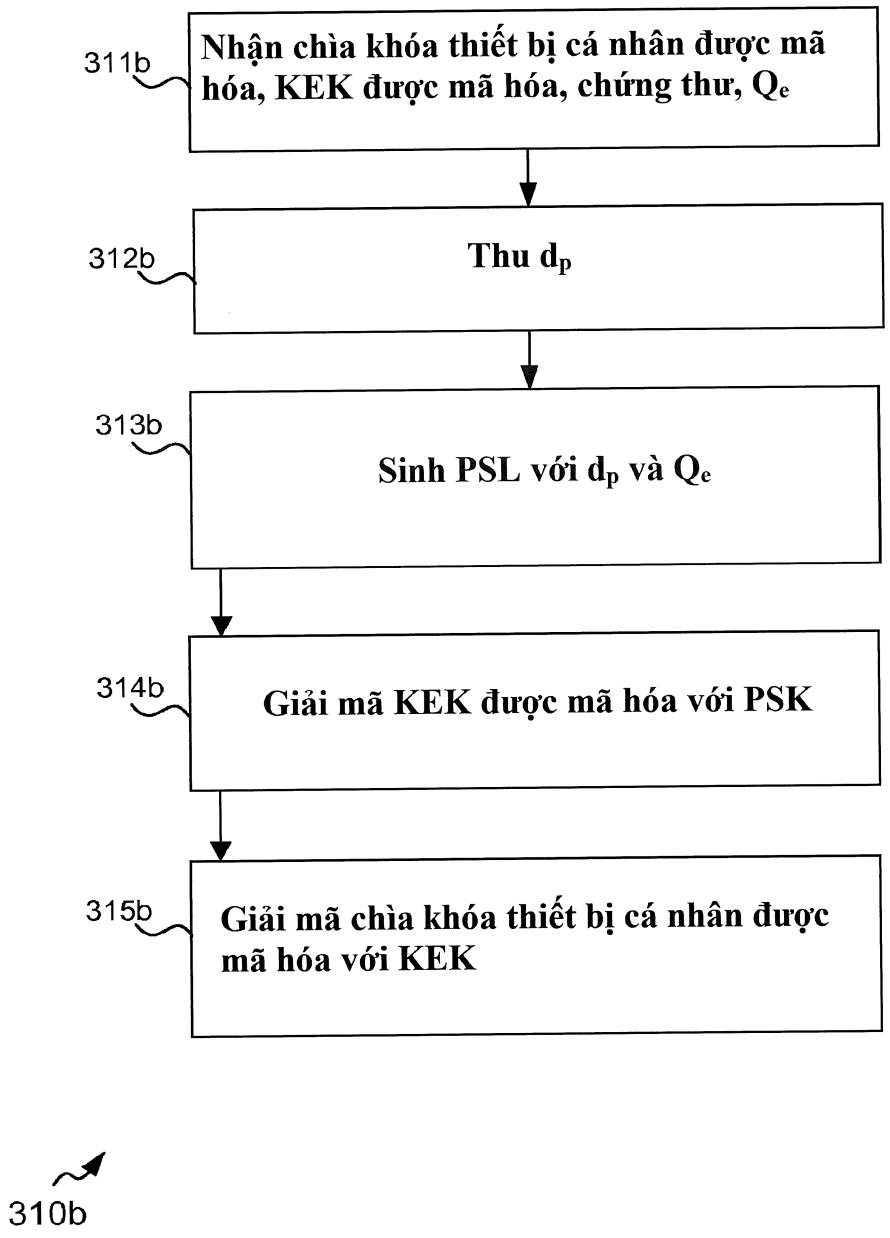

311b
Nhận chìa khóa thiết bị cá nhân được mã hóa, KEK được mã hóa, chứng thư, Q_e
312b
Thu d_p
313b
Sinh PSL với d_p và Q_e
314b
Giải mã KEK được mã hóa với PSK
315b
Giải mã chìa khóa thiết bị cá nhân được mã hóa với KEK
310b

FIG. 3C