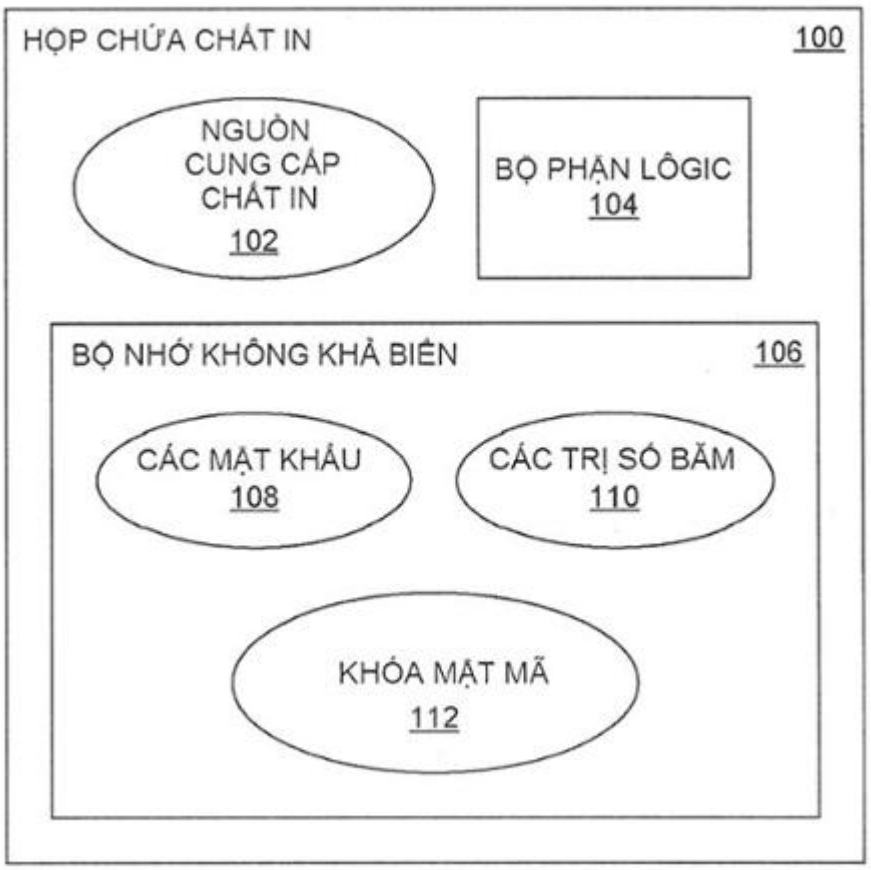
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0031263**
(51)[7] **B41J 2/175**
(13) **B**

(21) 1-2017-01061
(22) 17/06/2016
(86) PCT/US2016/038211 17/06/2016
(87) WO 2017/218016 A1 21/12/2017
(45) 25/03/2022 408
(43) 26/03/2018 360A
(73) HEWLETT-PACKARD DEVELOPMENT COMPANY, L.P. (US)
11445 Compaq Center Drive West, Houston, Texas 77070, United States of America
(72) NESS, Erik D. (US); PANSHIN, Stephen D. (US); WARD, Jefferson P. (US).
(74) Công ty Luật TNHH T&G (TGVN)

(54) HỘP CHỨA CHẤT IN CHO THIẾT BỊ IN VÀ VẬT GHI DỮ LIỆU KHÔNG CHUYỂN TIẾP ĐỌC ĐƯỢC BỞI MÁY TÍNH TRONG THIẾT BỊ IN NÀY

(57) Sáng chế đề xuất phần tử thay thế được cho thiết bị chủ bao gồm bộ nhớ không khả biến và bộ phận lôgic. Bộ nhớ không khả biến lưu trữ các mật khẩu hoặc các trị số xác thực, và/hoặc khóa mật mã. Bộ phận lôgic cho phép lấy ra số lượng lớn nhất định trước của các mật khẩu từ bộ nhớ không khả biến để xác thực phần tử thay thế được trong thiết bị chủ. Số lượng lớn nhất định trước của các mật khẩu nhỏ hơn tổng số lượng các mật khẩu.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến hộp chứa chất in cho thiết bị in, và vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính trong thiết bị in.

Tình trạng kỹ thuật của sáng chế

Các thiết bị mà sử dụng các phần tử thay thế được bao gồm các thiết bị in, bao gồm các máy in độc lập, máy sao chép, và các thiết bị AIO (all-in-one - tất cả trong một) mà có thể thực hiện nhiều chức năng, như in, sao chép, quét, và/hoặc gửi fax. Các phần tử thay thế được ví dụ cho các thiết bị in này bao gồm mực, mực toner (toner), và/hoặc các loại thuốc nhuộm màu khác, bao gồm thuốc nhuộm màu 2D (two-dimensional - hai chiều). Các phần tử thay thế ví dụ khác, cụ thể là cho các thiết bị in 3D (three-dimensional - ba chiều), bao gồm tác nhân in 3D và vật liệu xây dựng in 3D.

Bản chất kỹ thuật của sáng chế

Như được lưu ý trong phần tình trạng kỹ thuật, các thiết bị mà sử dụng các phần tử thay thế được bao gồm các thiết bị in. Nguồn cung cấp của chất in, như thuốc nhuộm màu hoặc một loại chất in khác, được lưu trữ trong hộp chứa (cartridge) mà có thể được lồng vào trong thiết bị in. Khi nguồn cung cấp trở thành đã dùng hết, hộp chứa có thể được thay thế bằng hộp chứa có nguồn cung cấp mới của chất in được nói đến. Các hộp chứa có các loại chất in khác nhau cũng có thể được chuyển đổi khi mong muốn. Như một ví dụ, hộp chứa có mực đa năng có thể được chuyển đổi cho hộp chứa có mực chất lượng ảnh trong thiết bị in phun mực khi mong muốn.

Các nhà sản xuất của các thiết bị in cũng thường sản xuất hoặc nếu không thì cung cấp chất in được sử dụng trong các thiết bị in. Từ quan điểm của người dùng cuối, việc sử dụng các hộp chứa chất in (print substance cartridge) được cung cấp bởi nhà sản xuất hoặc được chấp nhận bởi nhà sản xuất có thể tạo thuận lợi cho đầu ra mong muốn bởi các thiết bị in và/hoặc hạn chế hư hại cho các thiết bị in. Đối với OEM (original equipment manufacturer - nhà sản xuất thiết bị gốc) có thể khó bảo đảm đầu ra của thiết bị in hoặc chức năng của thiết bị in nếu thiết bị in sử dụng các hộp chứa của bên thứ ba.

Chất in của bên thứ ba vượt quá sự kiểm soát của OEM. Ví dụ, nó có thể cung cấp đầu ra in khác nhau hoặc đưa đến rủi ro cấp bằng sáng chế để rút ngắn tuổi thọ của thiết bị in. Trong một số tình huống, như các máy in 3D, thậm chí có thể có rủi ro về sự an toàn đối với người dùng khi chất in là chất in không được chấp nhận. Trong các tình huống nhất định, việc sử dụng chất in không được chấp nhận có thể làm ảnh hưởng đến sự bảo hành được kết hợp với thiết bị in.

Các nhà sản xuất theo đó có thể làm cho các hộp chứa có sự an toàn xác thực. Thiết bị in có thể hỏi hộp chứa để xác định liệu nó là xác thực. Nếu hộp chứa không xác thực (ví dụ, không được chấp nhận bởi OEM), thì thiết bị in có thể khởi đầu thủ tục nhất định, chẳng hạn như, thông báo cho người dùng cuối, như ngay lập tức hoặc sớm sau khi lắp đặt.

Các kỹ thuật được bộc lộ trong bản mô tả này cung cấp sơ đồ xác thực mới, cải tiến cho hộp chứa chất in cho thiết bị in, và tổng quát hơn là cho phần tử thay thế được cho thiết bị (chủ) trong đó phần tử có thể được lắp đặt (nghĩa là, tổng quát hơn, thiết bị mà phần tử có thể được kết nối với). Hộp chứa chất in lưu trữ số lượng trị số xác thực, hoặc mật khẩu. Hộp chứa bao gồm bộ phận lôgic (logic) (như hệ mạch như bộ xử lý và bộ nhớ lưu trữ mã mà bộ xử lý chạy) để cho phép chỉ lấy ra tập hợp con của các trị số xác thực này. Khi các trị số xác thực khác nhau được yêu cầu từ hộp chứa, hộp chứa có thể theo dõi số lượng các trị số khác nhau mà đã được trả về. Một khi hộp chứa đã cung cấp số lượng lớn nhất của các trị số xác thực duy nhất này, thì nó sẽ không cung cấp trị số xác thực bất kỳ trong số các trị số xác thực khác mà đã được lưu trữ trong hộp chứa lúc ban đầu. Tuy nhiên, hộp chứa tiếp tục cung cấp các trị số xác thực trước mà đã được yêu cầu và trả về.

Như một ví dụ, hộp chứa chất in có thể lưu trữ sáu mươi bốn mật khẩu khác nhau, hoặc trị số xác thực. Trong số sáu mươi bốn này, hộp chứa có thể đưa ra không nhiều hơn mười sáu trong số mật khẩu khác nhau. Một khi hộp chứa đã cung cấp mười sáu mật khẩu khác nhau, nó sẽ không mật khẩu bất kỳ trong số bốn mươi tám mật khẩu khác mà đã được lưu trữ trong hộp chứa. Tuy nhiên, hộp chứa có thể tiếp tục đáp lại các yêu cầu cho mười sáu mật khẩu khác nhau mà nó đã cung cấp.

Hộp chứa chất in cũng có thể lưu trữ các trị số băm của các trị số xác thực, hoặc mật khẩu. Các trị số băm cung cấp cách thức để xác định liệu trị số xác thực đã cho mà hộp chứa đã cung cấp là đúng. Hộp chứa có thể cung cấp các trị số băm của các trị số xác thực khi có yêu cầu, ngay cả cho các trị số mà hộp chứa sẽ không đưa ra. Theo ví dụ của đoạn trước, chẳng hạn, hộp chứa có thể cung cấp các trị số băm cho tất cả sáu mươi bốn mật khẩu, mặc dù hộp chứa sẽ cung cấp không nhiều hơn mười sáu trong số sáu mươi bốn mật khẩu.

Sơ đồ xác thực sử dụng hộp chứa chất in này có thể bao gồm thiết bị in chủ mà có thể yêu cầu bốn mật khẩu khác nhau, hoặc trị số xác thực, được lưu trữ trong hộp chứa. Các thiết bị in khác nhau có thể và có khả năng sẽ yêu cầu các mật khẩu khác nhau từ hộp chứa đã cho. Tương tự, thiết bị in đã cho có thể và có khả năng sẽ yêu cầu các mật khẩu khác nhau từ các hộp chứa khác nhau.

Việc có hộp chứa chất in trả về số lượng các trị số xác thực nhỏ hơn so với tổng số lượng các trị số xác thực được lưu trữ lúc ban đầu trong hộp chứa làm cho bên thứ ba khó khăn hơn nhiều để vô hiệu hóa sơ đồ xác thực này. Ngay cả nếu bên thứ ba vượt qua các biện pháp an toàn khác để thu được mười sáu trị số xác thực mà hộp chứa sẽ "từ bỏ", hoặc đưa ra hoặc cung cấp, thì khả năng mà hộp chứa của bên thứ ba chỉ lưu trữ mười sáu trị số này sẽ được xác thực bởi thiết bị in là thấp. Trong sơ đồ xác thực ví dụ mà đã được trình bày trên đây, thiết bị in có thể và sẽ có khả năng yêu cầu ít nhất một trị số xác thực mà không phải là một trong số mười sáu trị số mà hộp chứa của bên thứ ba dùng chung, làm cho không có khả năng là thiết bị in đã cho bất kỳ sẽ xác thực thành công hộp chứa này.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ của hộp chứa chất in ví dụ cho thiết bị in.

Fig.2 là biểu đồ tiến trình của phương pháp ví dụ mà hộp chứa chất in hoặc phần tử thay thế được khác cho thiết bị có thể thực hiện.

Fig.3 là biểu đồ tiến trình của phương pháp ví dụ mà hộp chứa chất in hoặc phần tử thay thế được khác cho thiết bị có thể thực hiện để tiến hành một phần của phương pháp trên Fig.2.

Fig.4 là biểu đồ tiến trình của một phương pháp ví dụ khác mà hộp chứa chất in hoặc phần tử thay thế được khác cho thiết bị có thể thực hiện để tiến hành một phần của phương pháp trên Fig.2.

Fig.5 là biểu đồ tiến trình của phương pháp ví dụ thứ ba mà hộp chứa chất in hoặc phần tử thay thế được khác cho thiết bị có thể thực hiện để tiến hành một phần của phương pháp trên Fig.2.

Fig.6 là biểu đồ tiến trình của phương pháp ví dụ thứ bốn mà hộp chứa chất in hoặc phần tử thay thế được khác cho thiết bị có thể thực hiện để tiến hành một phần của phương pháp trên Fig.2.

Mô tả chi tiết sáng chế

Fig.1 thể hiện hộp chứa chất in 100 ví dụ cho thiết bị in. Hộp chứa 100 bao gồm nguồn cung cấp chất in 102. Hộp chứa 100 có thể chứa thể tích chất in bất kỳ, như từ một vài mililít đến hàng chục lít. Các ví dụ khác nhau về chất in bao gồm mực cho thiết bị in phun mực, và mực toner dạng lỏng hoặc bột cho thiết bị in laze. Chính mực và mực toner này là các ví dụ của thuốc nhuộm màu 2D (two-dimensional - hai chiều), mà là thuốc nhuộm màu được sử dụng bởi thiết bị in thích hợp để tạo thành các ảnh trên phương tiện như giấy mà giảm thiểu nếu chút nào kéo dài theo chiều thứ ba vuông góc với hai chiều xác định mặt phẳng của bề mặt phương tiện mà trên đó các ảnh đã được tạo thành. Các ví dụ khác về chất in bao gồm tác nhân in 3D (three-dimensional - ba chiều) và vật liệu xây dựng in 3D, mà được sử dụng bởi thiết bị in 3D thích hợp để tạo thành vật thể 3D mà thường có thể tháo ra được khỏi nền bất kỳ mà vật thể được tạo trên đó. Các chất in nhất định, như mực, có thể được sử dụng cho cả in 2D và 3D.

Hộp chứa chất in 100 bao gồm bộ phận lôgic 104. Bộ phận lôgic 104 có thể được thực hiện như hệ mạch trong hộp chứa 100. Ví dụ, bộ phận lôgic 104 có thể bao gồm bộ xử lý, và vật ghi dữ liệu không khả biến đọc được bởi máy tính lưu trữ mã chạy được bởi máy tính mà bộ xử lý chạy. Như vậy, liên quan đến vấn đề này, theo một phương án thực hiện, bộ phận lôgic 104 có thể bao gồm bộ vi xử lý và phần mềm được cài được lưu trữ trên chính bộ vi xử lý, trong đó vật ghi dữ liệu không khả biến đọc được bởi máy tính được tích hợp bên trong bộ vi xử lý. Theo một phương án thực hiện khác, bộ phận

lôgic 104 có thể bao gồm bộ vi xử lý và phần mềm được cài bên trong phương tiện không khả biến tách rời khỏi bộ vi xử lý.

Như một ví dụ khác, bộ phận lôgic 104 có thể là hoặc bao gồm ASIC (application-specific integrated circuit - mạch tích hợp đặc trưng cho ứng dụng) hoặc FPGA (field-programmable gate array - mảng cổng lập trình được theo trường). Liên quan đến vấn đề này tổng quát hơn là, bộ phận lôgic 104 có thể được thực hiện bằng cách sử dụng các cổng lôgic. Như ví dụ thứ ba, bộ phận lôgic 104 có thể được thực hiện như kết hợp bất kỳ của bộ xử lý, phần mềm được lưu trữ trong bộ xử lý hoặc trên phương tiện tách rời đối với bộ xử lý, và các cổng lôgic.

Hộp chứa chất in 100 bao gồm bộ nhớ không khả biến 106. Bộ nhớ 106 có thể là bộ nhớ bán dẫn, và là không khả biến ở chỗ khi sự cấp nguồn được tháo khỏi hộp chứa 100, bộ nhớ 106 vẫn giữ lại các nội dung của nó. Bộ nhớ 106 lưu trữ các mật khẩu 108, mà cũng được gọi là các trị số xác thực trong bản mô tả này. Bộ nhớ 106 có thể lưu trữ các trị số băm 110 của, và mà theo cách riêng rẽ có thể tương ứng với, các mật khẩu 108. Bộ nhớ 106 có thể lưu trữ khóa mật mã 112 mà các mật khẩu 108 có thể được tạo ra từ đó.

Bộ nhớ 106 lưu trữ số lượng các mật khẩu 108, mà được gọi là tổng số lượng của các mật khẩu 108. Các mật khẩu 108, hoặc các trị số xác thực, được lưu trữ bởi hộp chứa 100 sao cho hộp chứa 100 có thể chứng minh với thiết bị in chủ rằng nó là xác thực. Phát biểu theo một cách khác, các mật khẩu 108 được sử dụng để xác thực hộp chứa 100 trong thiết bị in. Các mật khẩu 108 có thể được giữ an toàn theo cách mật mã được mã hóa, sao cho các mật khẩu 108 về cơ bản là không thể lấy ra được khỏi hộp chứa 100 ngoài các phương pháp tiếp cận được mô tả ở đây. Mỗi trong số các mật khẩu 108 có thể là dãy bit, như 256 bit.

Bộ nhớ 106 có thể lưu trữ một trị số băm 110 cho mỗi mật khẩu 108. Các trị số băm 110 được lưu trữ bởi hộp chứa 100 sao cho hộp chứa 100 có thể chứng minh với thiết bị in chủ rằng các mật khẩu 108 là đúng. Phát biểu theo một cách khác, các trị số băm 110 được sử dụng để xác minh các mật khẩu 108 được cung cấp bởi hộp chứa 100 trong thiết bị in. Các trị số băm 110 có thể không được giữ an toàn theo cách mật mã ở chỗ chúng có thể tự do lấy ra được khỏi hộp chứa 100, nhưng có thể được giữ an toàn

theo cách mật mã ở chỗ các trị số băm 110 không thể được sửa đổi. Các trị số băm 110 có thể là các trị số băm một chiều 110 của các mật khẩu 108, điều này có nghĩa là không thể xác định được mật khẩu 108 chỉ nhờ biết trị số băm 110 tương ứng của nó, ngay cả nếu biết được hàm băm một chiều được sử dụng để tạo ra trị số băm 110 từ mật khẩu 108.

Các trị số băm 110 có thể được cung cấp bởi hộp chứa 100 theo một phương án thực hiện theo cách sao cho thiết bị chủ có thể xác nhận tính hợp lệ cho các trị số băm 110 là đã được tạo ra bởi thực thể (nghĩa là, nhà sản xuất hoặc nhà cung cấp của hộp chứa 100) mà thiết bị chủ tin cậy. Như một ví dụ, các trị số băm 110 có thể được ký theo cách mật mã bằng khóa mật mã riêng trước khi lưu trữ trong hộp chứa 100. Thiết bị chủ có thể sử dụng khóa mật mã công khai tương ứng để xác nhận tính hợp lệ cho các trị số băm 110. Khóa riêng có thể không được lưu trữ trên hộp chứa 100, và không sẵn có theo cách công khai.

Bộ phận lôgic 104 cho phép lấy ra số lượng lớn nhất định trước của các mật khẩu 108, nhỏ hơn tổng số lượng của các mật khẩu 108 được lưu trữ trong bộ nhớ không khả biến 106. Bộ phận lôgic 104 có thể cho phép lấy ra số lượng nhỏ hơn này của các mật khẩu 108 (nghĩa là, số lượng lớn nhất định trước của các mật khẩu 108), tuy nhiên, với số lần không giới hạn từ bộ nhớ 106. Khi so sánh, bộ phận lôgic 104 cấm lấy ra mật khẩu 108 bất kỳ mà khác với số lượng lớn nhất định trước của các mật khẩu, dù là một lần, từ bộ nhớ 106.

Các mật khẩu nào trong số các mật khẩu 108 được lựa chọn làm số lượng lớn nhất định trước của các mật khẩu 108 mà bộ phận lôgic 104 của nó cho phép lấy ra có thể không xác định theo cách suy diễn. Ví dụ, khi thiết bị in chủ bất kỳ mà hộp chứa 100 được lắp đặt hiện thời trong đó hoặc nếu không thì hộp chứa 100 được kết nối vào đó yêu cầu các mật khẩu 108 cụ thể, bộ phận lôgic 104 có thể trả về các mật khẩu 108 được yêu cầu cho đến khi đã đạt đến số lượng lớn nhất định trước. Sau đó, bộ phận lôgic 104 sẽ chỉ trả về các mật khẩu 108 mà đã được yêu cầu, và không trả về mật khẩu bất kỳ trong số các mật khẩu 108 khác, một khi số lượng định trước của các mật khẩu 108 đã được lựa chọn. Phát biểu theo một cách khác, bộ phận lôgic 104 có thể lựa chọn số lượng

lớn nhất định trước cụ thể của các mật khẩu 108 khi thiết bị in chủ bất kỳ yêu cầu chúng, cho đến khi đã đạt đến số lượng lớn nhất.

Như một ví dụ, bộ nhớ không khả biến 106 có thể lưu trữ mười sáu mật khẩu 108, được đánh số từ một đến mười sáu, và bộ phận lôgic 104 có thể trả về chỉ bốn mật khẩu trong số các mật khẩu 108 này. Hộp chứa 100 có thể được lồng vào trong thiết bị in chủ thứ nhất, mà có thể yêu cầu và nhận các mật khẩu có các số một và mười ba. Do đó, bộ phận lôgic 104 đã lựa chọn theo cách hiệu quả hai trong số bốn mật khẩu 108 mà hộp chứa 100 sẽ tiết lộ, chúng được đánh số là một và mười ba. Sau đó hộp chứa có thể được tháo ra khỏi thiết bị in chủ này, và được lồng vào trong một thiết bị in chủ khác mà yêu cầu và nhận các mật khẩu có các số sáu và mười ba. Do đó, bộ phận lôgic 104 lúc ấy đã lựa chọn theo cách hiệu quả ba trong số bốn mật khẩu 108 mà hộp chứa 100 sẽ tiết lộ, chúng được đánh số là một, sáu, và mười ba.

Hộp chứa có thể được tháo ra khỏi thiết bị in chủ trong đó nó được lắp đặt hiện thời và được lồng vào trong thiết bị in chủ thứ ba, mà có thể yêu cầu và nhận các mật khẩu có các số bảy và mười ba. Do đó, bộ phận lôgic 104 lúc ấy đã lựa chọn theo cách hiệu quả tất cả bốn trong số bốn mật khẩu 108 mà hộp chứa 100 sẽ tiết lộ, chúng được đánh số là một, sáu, bảy, và mười ba. Bộ phận lôgic 104 có thể tiếp tục trả về bốn mật khẩu 108 này, nhưng sẽ không trả về mật khẩu 108 bất kỳ khác. Nghĩa là, bộ phận lôgic 104 sẽ không trả về mật khẩu 108 bất kỳ trừ khi nó có số là một, sáu, bảy, hoặc mười ba.

Bộ nhớ không khả biến 106 được sử dụng để lưu trữ các mật khẩu 108 có thể là bộ nhớ ghi một lần, đọc giới hạn (write-once, read-limited memory). Các mật khẩu 108 được ghi vào bộ nhớ 106 chỉ một lần, như trong quy trình sản xuất an toàn. Số lượng lớn nhất định trước của tổng số lượng của các mật khẩu 108 có thể được đọc với số lần không giới hạn. Các mật khẩu 108 khác với số lượng lớn nhất định trước này trở thành không thể đọc được một khi số lượng lớn nhất định trước của các mật khẩu 108 đã được lựa chọn cụ thể. Theo đó, mỗi mật khẩu 108 có thể lấy ra được với số lần không giới hạn hoặc không thể lấy ra được, nhưng bộ phận lôgic 104 không xác định trước thời hạn các mật khẩu 108 nào là thuộc loại nào.

Do đó, các mật khẩu 108 mà khác với số lượng lớn nhất định trước của các mật khẩu 108 được xóa ít nhất là theo chức năng một khi số lượng lớn nhất định trước của các mật khẩu 108 đã được lựa chọn cụ thể. Chúng có thể được xóa theo cách hoàn toàn và không thể tẩy xóa từ bộ nhớ 108 bởi bộ phận lôgic 104, chẳng hạn, theo cách sao cho "không xóa" hoặc sự khôi phục của các mật khẩu 108 được xóa được coi là không thể thực hiện được. Các mật khẩu 108 được nói đến có thể được xóa theo chức năng ở chỗ các mật khẩu 108 này vẫn được lưu trữ trong bộ nhớ 108, nhưng không thể lấy ra được. Ví dụ, các liên kết cầu chì đến các phần vật lý của bộ nhớ 108 tại đó các mật khẩu 108 được nói đến được lưu trữ có thể được làm đứt, làm cho các mật khẩu 108 không thể lấy ra được và theo đó được xóa theo chức năng mặc dù trên thực tế các mật khẩu 108 vẫn ở trong bộ nhớ.

Bộ nhớ 106 có thể lưu trữ khóa mật mã 112 thay cho các mật khẩu 108 khi sản xuất hộp chứa 100. Theo phương án thực hiện này, trước lần sử dụng đầu tiên của hộp chứa 100, không mật khẩu 108 nào có thể được lưu trữ trong hộp chứa 108. Đúng hơn là, khi mật khẩu 108 được yêu cầu, hộp chứa 100 tạo ra mật khẩu 108 "trong khi đang hoạt động", nếu số lượng lớn nhất định trước của các mật khẩu 108 duy nhất chưa được tạo ra và được cung cấp bởi hộp chứa 100. Một khi số lượng lớn nhất định trước của các mật khẩu 108 duy nhất đã được tạo ra, khóa mật mã 112 có thể được xóa ít nhất là theo chức năng, theo cách được mô tả trong đoạn trước.

Fig.2 thể hiện phương pháp ví dụ 200 mà phần tử thay thế được cho thiết bị, như hộp chứa chất in 100 cho thiết bị in, có thể thực hiện. Phương pháp 200 có thể được thực hiện như mã đọc được bởi máy tính được lưu trữ trên vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính và mà bộ xử lý chạy. Như vậy, bộ phận lôgic 104 của hộp chứa 100 có thể thực hiện, ví dụ, phương pháp 200. Phần tử thay thế được thực hiện phương pháp 200 một khi nó đã được lắp đặt trong thiết bị chủ.

Phần tử thay thế được nhận yêu cầu từ thiết bị chủ cho trị số xác thực cụ thể của số lượng các trị số xác thực mà phần tử có thể lưu trữ (202). Yêu cầu có thể được ký bằng khóa mật mã số, hoặc có thể được giữ an toàn theo một cách khác. Phần tử thay thế được xác định liệu nó đã gửi trước đó trị số xác thực được nói đến đến thiết bị chủ (203) bất kỳ, bao gồm thiết bị chủ trong đó phần tử được lắp đặt hiện thời, cũng như

thiết bị chủ bất kỳ khác. Nếu phần tử thay thế được đã gửi trước đó trị số xác thực (204) được yêu cầu, thì phần tử trả về trị số được yêu cầu cho thiết bị chủ (206).

Tuy nhiên, nếu phần tử thay thế được đã không gửi trước đó trị số xác thực (206) được yêu cầu, thì phần tử xác định liệu nó đã gửi số lượng lớn nhất của các trị số xác thực duy nhất (208). Ví dụ, trong số sáu mươi bốn trị số xác thực mà phần tử thay thế được có thể lưu trữ, phần tử có thể gửi không nhiều hơn mười sáu trong số các trị số này. Nếu phần tử thay thế đã gửi số lượng lớn nhất của các trị số xác thực duy nhất (210), thì phần tử không gửi trị số xác thực mà thiết bị chủ trong đó lắp đặt phần tử đã yêu cầu (212).

Tuy nhiên, nếu phần tử thay thế được chưa gửi số lượng lớn nhất của các trị số xác thực duy nhất, thì phần tử gửi trị số xác thực được yêu cầu đến thiết bị chủ (214). Phần tử thay thế được tiếp theo một lần nữa có thể xác định liệu số lượng lớn nhất của các trị số xác thực đã được gửi lúc ấy (216), bao gồm trị số xác thực mà phần tử vừa gửi trong phần 214. Ví dụ, nếu phần tử được cho phép gửi chỉ mười sáu trong số sáu mươi bốn trị số xác thực của nó, nếu mười lăm trị số được gửi trước sự thực hiện của phần 214, thì trị số xác thực thứ mười sáu khác được gửi trong phần 214, sao cho số lượng lớn nhất của mười sáu trị số xác thực khác nhau đã được gửi lúc ấy.

Nếu số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy (218), thì phần tử thay thế được có thể xóa ít nhất là theo chức năng các trị số xác thực mà nó lưu trữ và đã không được gửi (220). Như vậy, theo ví dụ đang tiến hành, một khi mười sáu trị số xác thực khác nhau đã được gửi, bốn mươi tám trị số xác thực khác được xóa. Lưu ý là mỗi lần thực hiện phương pháp 200 trên Fig.2, thì, phần tử thay thế được có thể gửi trị số xác thực bất kỳ mà nó đã gửi trước đó, và có thể gửi trị số xác thực bất kỳ mà nó đã không gửi trước đó miễn là số lượng lớn nhất của các trị số xác thực khác nhau mà phần tử sẽ gửi chưa được đạt đến.

Từ các phần 206, 212, và 220, và từ phần 218 khi số lượng lớn nhất của các trị số xác thực được gửi duy nhất chưa được đạt đến, hoặc như điểm vào đối với phương pháp 200, phần tử thay thế được có thể nhận từ thiết bị chủ yêu cầu cho một hoặc nhiều trị số băm tương ứng với một hoặc nhiều trị số xác thực (222). Ví dụ, phần tử thay thế được có thể nhận yêu cầu cho tất cả các trị số băm tương ứng với tất cả các trị số xác

thực, cho chỉ một trong số các trị số băm tương ứng với chỉ một trong số các trị số xác thực, và v.v.. Phần tử thay thế được có thể nhận yêu cầu cho một hoặc nhiều trị số băm ngay cả sau khi các trị số xác thực mà chưa bao giờ được gửi được xóa trong phần 220, sau khi số lượng lớn nhất của các trị số xác thực duy nhất mà phần tử sẽ gửi đã được đạt đến trong phần 218. Nghĩa là, phần tử thay thế được có thể không xóa các trị số băm cho các trị số xác thực mà nó xóa, chẳng hạn. Phần 222 có thể được coi như điểm vào đối với phương pháp 200 ở chỗ yêu cầu cho các trị số băm có thể được nhận trước khi nhận được yêu cầu cho trị số xác thực.

Fig.3 thể hiện phương pháp ví dụ 300 là một ví dụ về phương án thực hiện cụ thể của các phần từ 202 đến 220 của phương pháp 200. Các phần được đánh số giống nhau trên Fig.2 và Fig.3 được thực hiện trong phương pháp 300 ít nhất về cơ bản như được mô tả trên đây liên quan đến phương pháp 200. Các số trong các dấu ngoặc đơn biểu thị là phần đã cho của phương pháp 300 đang thực hiện phần tương ứng của phương pháp 200. Nghĩa là, Y(X) trên Fig.3 có nghĩa là phần Y của phương pháp 300 đang thực hiện phần X của phương pháp 200.

Trên Fig.3, các trị số xác thực có thể có các phần tử nhận dạng, như các phần tử nhận dạng duy nhất tương ứng, mà cũng có thể được gọi là các địa chỉ. Ví dụ, nếu phần tử thay thế được lưu trữ sáu mươi bốn trị số xác thực, các phần tử nhận dạng có thể là một, hai, ba, và v.v., cho đến sáu mươi bốn. Phần tử thay thế được nhận yêu cầu từ thiết bị chủ trong đó nó được lắp đặt cho trị số xác thực bởi phần tử nhận dạng (302). Ví dụ, thiết bị chủ có thể yêu cầu trị số xác thực có phần tử nhận dạng ABCD, có thể yêu cầu trị số xác thực thứ sáu, sao cho phần tử nhận dạng của trị số xác thực được yêu cầu là sáu, và v.v..

Trên Fig.3, phần tử thay thế được có thể có hai bảng. Bảng thứ nhất có số lượng các mục nhập bằng với số lượng lớn nhất của các trị số xác thực khác nhau mà phần tử thay thế được sẽ trả về cho thiết bị chủ bất kỳ. Khi phần tử thay thế được chưa được sử dụng trong thiết bị chủ bất kỳ, tất cả các mục nhập có thể trống. Nghĩa là, các mục nhập của bảng thứ nhất ban đầu là trống. Bảng thứ nhất lưu trữ ít nhất là các phần tử nhận dạng của các trị số xác thực mà phần tử thay thế được đã gửi đến thiết bị chủ bất kỳ.

Bảng thứ nhất cũng có thể lưu trữ chính các trị số xác thực. Phần tử thay thế được có thể lưu trữ bảng thứ nhất theo cách an toàn theo mật mã.

Bảng thứ hai có số lượng các mục nhập bằng với số lượng các trị số xác thực mà phần tử thay thế được lưu trữ, như trước khi phần tử thay thế được chưa phải được sử dụng trong thiết bị chủ bất kỳ. Mỗi mục nhập bao gồm ít nhất là trị số xác thực. Mỗi mục nhập còn có thể lưu trữ phần tử nhận dạng của trị số xác thực. Nếu các phần tử nhận dạng không được lưu trữ trong bảng thứ hai, thì chúng có thể xác định được nhờ tham chiếu. Ví dụ, nếu có sáu mươi bốn mục nhập, mục nhập thứ nhất có thể lưu trữ trị số xác thực với phần tử nhận dạng thấp nhất, mục nhập thứ hai có thể lưu trữ trị số xác thực với phần tử nhận dạng bằng với phần tử nhận dạng thấp nhất cộng trị số gia tăng, và mục nhập thứ ba có thể lưu trữ trị số xác thực với phần tử nhận dạng bằng với phần tử nhận dạng thấp nhất cộng hai lần trị số gia tăng, và v.v.. Theo đó, mục nhập thứ sáu mươi bốn có thể lưu trữ trị số xác thực có phần tử nhận dạng bằng với phần tử nhận dạng thấp nhất cộng sáu mươi ba lần trị số gia tăng. Nếu phần tử nhận dạng thấp nhất là BASE, và trị số gia tăng là INC, thì phần tử nhận dạng của trị số xác thực thứ n, trong đó n là trị số từ một (trị số xác thực đầu tiên) đến N (trị số xác thực cuối cùng) bằng BASE + INC x (n-1).

Theo đó, phần tử thay thế được tìm kiếm phần tử nhận dạng được yêu cầu trong bảng thứ nhất (303). Nghĩa là, nếu phần tử thay thế được đã nhận yêu cầu từ thiết bị chủ trong phần 302 cho trị số xác thực có phần tử nhận dạng đã cho, thì phần tử thay thế được tìm kiếm phần tử nhận dạng đã cho trong bảng thứ nhất. Nếu phần tử thay thế được đã nhận yêu cầu trong phần 302 cho trị số xác thực thứ năm, thì phần tử nhận dạng của trị số xác thực này có thể là năm, hoặc có thể được xác định như được mô tả trên đây, mà phần tử tiếp theo tìm kiếm trong bảng thứ nhất. Nếu phần tử nhận dạng được yêu cầu ở trong bảng thứ nhất, thì điều này có nghĩa là phần tử thay thế được đã gửi trước đó trị số xác thực có phần tử nhận dạng này. Nếu phần tử nhận dạng được yêu cầu không ở trong bảng thứ nhất, thì điều này có nghĩa là phần tử đã không gửi trước đó trị số xác thực có phần tử nhận dạng này.

Nếu phần tử nhận dạng ở trong bảng thứ nhất, thì phần tử thay thế được gửi trị số xác thực có phần tử nhận dạng này (206). Chẳng hạn, nếu bảng thứ nhất lưu trữ các

trị số xác thực cũng như các phần tử nhận dạng của chúng, thì phần tử thay thế được có thể lấy ra trị số xác thực được nói đến từ bảng thứ nhất. Nếu bảng thứ nhất chỉ lưu trữ các phần tử nhận dạng và không phải chính các trị số xác thực, thì phần tử thay thế được có thể lấy ra trị số xác thực có phần tử nhận dạng được nói đến từ bảng thứ hai để trả về cho thiết bị chủ.

Nếu phần tử nhận dạng không ở trong bảng thứ nhất, thì phần tử thay thế được xác định liệu có các mục nhập trống bất kỳ trong bảng thứ nhất (306). Nếu có các mục nhập trống trong bảng thứ nhất, thì điều này có nghĩa là phần tử thay thế được chưa gửi số lượng lớn nhất của các trị số xác thực khác nhau. Nếu không có các mục nhập trống trong bảng thứ nhất, thì điều này có nghĩa là phần tử thay thế được đã gửi số lượng lớn nhất của các trị số xác thực khác nhau. Do đó, nếu không có các mục nhập trống (308), thì phần tử thay thế được từ chối gửi trị số xác thực được yêu cầu (212).

Tuy nhiên, nếu có các mục nhập trống trong bảng thứ nhất (308), thì phần tử thay thế được lấy ra trị số xác thực có phần tử nhận dạng được yêu cầu từ bảng thứ hai (310). Phần tử định vị phần tử nhận dạng trống trong bảng thứ nhất (312), và lưu trữ ít nhất phần tử nhận dạng của trị số xác thực được lấy ra trong mục nhập trống (314) này. Chẳng hạn, phần tử có thể lưu trữ trị số xác thực trong mục nhập cũng như phần tử nhận dạng của trị số này. Sau đó, phần tử thay thế được gửi trị số xác thực trở lại cho thiết bị chủ mà đã yêu cầu trị số (214).

Tiếp theo, phần tử thay thế được xác định liệu bảng thứ nhất lúc ấy có các mục nhập trống bất kỳ (316). Nếu không có các mục nhập trống nào nữa sau khi mục nhập trống được định vị trong phần 312 được điền vào trong phần 314, thì điều này có nghĩa là đã đạt đến số lượng lớn nhất của các trị số xác thực khác nhau mà phần tử thay thế được có thể cung cấp. Nếu vẫn có ít nhất một mục nhập trống trong bảng thứ nhất sau khi mục nhập trống được định vị trong phần 312 được điền vào trong phần 314, thì điều này có nghĩa là chưa đạt đến số lượng lớn nhất của các trị số xác thực khác nhau mà phần tử thay thế được có thể cung cấp. Do đó, nếu có các mục nhập trống bất kỳ còn lại trong bảng thứ nhất (318), thì phương pháp 300 được hoàn thành (320).

Nếu không có các mục nhập trống bất kỳ còn lại trong bảng thứ nhất (318), thì phần tử thay thế được xóa các trị số xác thực khỏi bảng thứ hai (220). Phần tử thay thế

được có thể xóa khỏi bảng thứ hai chỉ các trị số xác thực mà nó đã không cung cấp, đó là các trị số xác thực mà có các phần tử nhận dạng không được lưu trữ trong bảng thứ nhất. Nếu bảng thứ nhất lưu trữ cả các phần tử nhận dạng và các trị số xác thực, trái ngược với chỉ các phần tử nhận dạng, thì phần tử thay thế được có thể xóa tất cả các trị số xác thực khỏi bảng thứ hai. Chẳng hạn, phần tử thay thế được có thể xóa hoàn toàn bảng thứ hai. Phần tử thay thế được có thể xóa bảng thứ hai bởi vì phần tử lưu trữ các trị số xác thực mà nó sẽ vẫn trả về đáp lại các yêu cầu thích hợp từ các thiết bị chủ trong bảng thứ nhất. Theo một phương án thực hiện khác, phần tử thay thế được đáp lại các yêu cầu cho các trị số xác thực từ bảng thứ nhất, và nếu trị số xác thực được yêu cầu không được lưu trữ trong bảng thứ nhất, có thể lấy ra trị số từ bảng thứ hai để lưu trữ trong bảng thứ nhất chỉ nếu có mục nhập trống sẵn có trong bảng thứ nhất mà để lưu trữ trị số được yêu cầu trong đó.

Fig.4 thể hiện phương pháp ví dụ 400 là một ví dụ khác về phương án thực hiện cụ thể của các phần từ 202 đến 220 của phương pháp 200. Các phần được đánh số giống nhau trên Fig.2 và Fig.4 được thực hiện trong phương pháp 400 ít nhất như đã được mô tả liên quan đến phương pháp 200. Các số trong các dấu ngoặc đơn biểu thị là phần đã cho của phương pháp 400 đang thực hiện phần tương ứng của phương pháp 200. Nghĩa là, Y(X) trên Fig.4 có nghĩa là phần Y của phương pháp 400 đang thực hiện phần X của phương pháp 200.

Phần tử thay thế được nhận yêu cầu cho trị số xác thực từ thiết bị chủ trong đó nó được lắp đặt (202). Phần tử thay thế được xác định liệu trị số xác thực đã được gửi trước đó (203). Nếu trị số xác thực đã được gửi trước đó (204), thì phần tử thay thế được gửi trị số xác thực mà đã được yêu cầu trở lại cho thiết bị chủ (206).

Phần tử thay thế được duy trì bộ đếm của số lượng các trị số xác thực duy nhất mà phần tử đã cung cấp cho thiết bị chủ bất kỳ theo phương án thực hiện trên Fig.4. Bộ đếm có thể là bộ đếm chỉ gia tăng, mà có thể được tăng và không được giảm. Bộ đếm được lưu trữ trong bộ nhớ không khả biến, như bộ nhớ không khả biến 106, và có thể được giữ an toàn theo cách mật mã.

Phần tử thay thế được xác định liệu bộ đếm có bằng với số lượng lớn nhất của các trị số xác thực duy nhất mà phần tử sẽ cung cấp cho thiết bị chủ bất kỳ nếu được yêu

cầu thích hợp (402). Nếu bộ đếm bằng với số lượng lớn nhất này của các trị số xác thực duy nhất, thì điều này có nghĩa là phần tử thay thế được đã cung cấp số lượng lớn nhất của các trị số xác thực khác nhau mà nó sẽ cung cấp cho thiết bị chủ bất kỳ. Do đó, nếu bộ đếm bằng với số lượng lớn nhất của các trị số xác thực duy nhất (404), thì phần tử thay thế được không gửi trị số xác thực được yêu cầu đến thiết bị chủ (212).

Nếu bộ đếm không bằng với số lượng lớn nhất của các trị số xác thực duy nhất (nghĩa là, bộ đếm nhỏ hơn số lượng này), thì điều này có nghĩa là phần tử thay thế được chưa cung cấp số lượng lớn nhất của các trị số xác thực khác nhau mà nó sẽ cung cấp cho thiết bị chủ bất kỳ. Do đó, phần tử thay thế được gửi trị số xác thực được yêu cầu trở lại cho thiết bị chủ (214). Phần tử thay thế được cũng gia tăng bộ đếm (406).

Phần tử thay thế được xác định liệu bộ đếm lúc ấy có bằng với số lượng lớn nhất của các trị số xác thực duy nhất mà nó sẽ cung cấp cho thiết bị chủ bất kỳ (408). Nếu bộ đếm chưa bằng với số lượng lớn nhất của các trị số xác thực duy nhất (410), thì phương pháp 400 được hoàn thành (412). Tuy nhiên, nếu bộ đếm lúc ấy bằng với số lượng (410) này, thì điều này có nghĩa là phần tử thay thế được lúc ấy đã gửi số lượng lớn nhất của các trị số xác thực khác nhau mà nó sẽ cung cấp, và như vậy, có thể xóa các trị số xác thực mà đã không được cung cấp hoặc được gửi đến thiết bị chủ (220) bất kỳ.

Fig.5 thể hiện phương pháp ví dụ 500 là ví dụ thứ ba về phương án thực hiện cụ thể của các phần từ 202 đến 220 của phương pháp 200. Các phần được đánh số giống nhau trên Fig.2 và 5 được thực hiện trong phương pháp 500 ít nhất như đã được mô tả liên quan đến phương pháp 200. Các số trong các dấu ngoặc đơn biểu thị là phần đã cho của phương pháp 500 đang thực hiện phần tương ứng của phương pháp 200. Nghĩa là, Y(X) trên Fig.5 có nghĩa là phần Y của phương pháp 500 đang thực hiện phần X của phương pháp 200.

Phần tử thay thế được nhận yêu cầu cho trị số xác thực từ thiết bị chủ trong đó nó được lắp đặt (202). Phần tử thay thế được xác định liệu trị số xác thực đã được gửi trước đó (203). Nếu trị số xác thực đã được gửi trước đó đến thiết bị chủ bất kỳ (204), thì phần tử thay thế được gửi trị số xác thực trở lại cho thiết bị chủ trong đó nó được lắp đặt (206).

Phần tử thay thế được duy trì cờ tương ứng với việc liệu phần tử đã cung cấp số lượng lớn nhất của các trị số xác thực duy nhất cho thiết bị chủ bất kỳ theo phương án thực hiện trên Fig.5. Cờ có thể là cờ chỉ có thể đặt được, mà có thể được đặt nhưng không thể xóa. Cờ được lưu trữ trong bộ nhớ không khả biến, như bộ nhớ không khả biến 106, và có thể được giữ an toàn theo cách mật mã.

Phần tử thay thế được xác định liệu cờ đã được đặt (502). Nếu cờ đã được đặt, điều này có nghĩa là phần tử thay thế được đã cung cấp số lượng lớn nhất của các trị số xác thực khác nhau mà nó sẽ cung cấp cho thiết bị chủ bất kỳ. Do đó, nếu cờ được đặt (504), thì phần tử thay thế được không gửi trị số xác thực được yêu cầu đến thiết bị chủ (212). Nếu cờ không được đặt, thì điều này có nghĩa là phần tử thay thế được chưa cung cấp số lượng lớn nhất của các trị số xác thực khác nhau mà nó sẽ cung cấp cho thiết bị chủ bất kỳ. Do đó, phần tử thay thế được gửi trị số xác thực được yêu cầu trở lại cho thiết bị chủ (214).

Phần tử thay thế được xác định liệu số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy (216). Nếu số lượng lớn nhất của các trị số xác thực khác nhau vẫn chưa được gửi (218), thì phương pháp 500 được hoàn thành. Tuy nhiên, nếu số lượng lớn nhất của các trị số xác thực khác nhau đã được gửi lúc ấy (218), thì phần tử thay thế được đặt cờ (508), và có thể xóa các trị số xác thực mà đã chưa được cung cấp hoặc được gửi đến thiết bị chủ bất kỳ (220).

Theo một phương án thực hiện khác, cờ được đặt trước khi gửi trị số xác thực. Nghĩa là, theo phương án thực hiện này, xác định được liệu số lượng lớn nhất của các xác thực sẽ được gửi lúc ấy với việc gửi trị số xác thực, và nếu như vậy, thì cờ được đặt, và sau khi cờ đã được đặt, trị số xác thực được gửi. Các trị số xác thực mà sẽ không được gửi cũng có thể được xóa theo phương án thực hiện này trước khi gửi trị số xác thực được nói đến. Tổng quát hơn, hành động bất kỳ mà được thực hiện do việc gửi trị số xác thực duy nhất cuối cùng mà sẽ được cung cấp nhờ phần tử thay thế được, như gia tăng bộ đếm, đặt cờ, lưu trữ trị số trong bảng, và v.v., có thể được thực hiện trước khi gửi trị số xác thực duy nhất cuối cùng này. Liên quan đến vấn đề này cần lưu ý là, còn tổng quát hơn là, hành động như vậy bất kỳ mà được thực hiện cùng với việc gửi trị số

xác thực (và không phải là trị số xác thực cuối cùng) có thể được thực hiện trước khi trị số xác thực thực sự được gửi.

Fig.6 thể hiện phương pháp ví dụ 600 là ví dụ thứ tư về phương án thực hiện cụ thể của các phần từ 202 đến 220 của phương pháp 200. Các phần được đánh số giống nhau trên Fig.2 và 6 được thực hiện trong phương pháp 600 ít nhất như đã được mô tả liên quan đến phương pháp 200. Các số trong các dấu ngoặc đơn biểu thị là phần đã cho của phương pháp 600 đang thực hiện phần tương ứng của phương pháp 200. Nghĩa là, Y(X) trên Fig.6 có nghĩa là phần Y của phương pháp 600 đang thực hiện phần X của phương pháp 200.

Phần tử thay thế được nhận yêu cầu cho trị số xác thực từ thiết bị chủ (202). Phần tử thay thế được xác định liệu trị số xác thực đã được gửi trước đó (203). Nếu trị số xác thực đã được gửi trước đó đến thiết bị chủ bất kỳ (204), thì phần tử thay thế được gửi trị số xác thực trở lại cho thiết bị chủ yêu cầu (206).

Nếu phần tử thay thế được đã không gửi trước đó trị số xác thực (206) được yêu cầu, thì phần tử xác định liệu nó đã gửi số lượng lớn nhất của các trị số xác thực duy nhất (208). Nếu phần tử thay thế đã gửi số lượng lớn nhất của các trị số xác thực duy nhất (210), thì phần tử không gửi trị số xác thực mà thiết bị chủ được nói đến đã yêu cầu (212). Phương pháp 600 theo đó được hoàn thành.

Tuy nhiên, nếu phần tử thay thế được chưa gửi số lượng lớn nhất của các trị số xác thực duy nhất (210), thì phần tử tạo ra trị số xác thực từ khóa mật mã (602), như khóa mật mã 112 của hộp chứa chất in 100 trên Fig.1. Theo phương án thực hiện trên Fig.6, thì, các mật khẩu 108 có thể không được tạo ra và được lưu trữ theo cách suy diễn trong hộp chứa 100 tại thời điểm sản xuất của hộp chứa 100. Hộp chứa in 100 chưa được sử dụng bao giờ có thể không có các mật khẩu 108 bất kỳ được lưu trữ trong đó, mà đúng hơn là chỉ lưu trữ khóa mật mã 112 mà các mật khẩu 108 có thể được tạo ra từ đó. Phần tử thay thế được theo đó gửi trị số xác thực mà đã được yêu cầu và mà phần tử vừa mới tạo ra đến thiết bị chủ (214). Liên quan đến vấn đề này, lưu ý là phương án thực hiện trên Fig.6 có thể được dùng cùng với ít nhất là một phần của phương án thực hiện trên Fig.3, trong đó các trị số được gửi được lưu trữ trong bảng thứ nhất. Như vậy, một khi trị số xác thực đã được tạo ra, nó có thể được lưu trữ trong bảng thứ nhất, sao cho

trị số không phải được tạo lại sau đó, và nếu hoặc khi khóa mật mã được xóa ít nhất là theo chức năng, thì trị số xác thực vẫn có thể được trả về.

Phần tử thay thế được có thể một lần nữa xác định liệu số lượng lớn nhất của các trị số xác thực đã được gửi lúc ấy (216), bao gồm trị số xác thực mà phần tử vừa gửi trong phần 214. Nếu số lượng lớn nhất của các trị số xác thực chưa được gửi (218), thì phương pháp 600 được hoàn thành. Tuy nhiên, nếu số lượng lớn nhất của các trị số xác thực đã được gửi lúc ấy (218), thì phần tử thay thế được có thể xóa ít nhất là theo chức năng khóa mật mã (606), sao cho các trị số xác thực bổ sung không thể được tạo ra. Khóa mật mã có thể được xóa ít nhất là theo chức năng một khi trị số xác thực đã được tạo ra trong phần 602, và trước khi thực sự gửi trị số xác thực trong phần 214 theo một phương án thực hiện.

Các phương án thực hiện khác nhau của các phần của phương pháp 200 mà đã được mô tả liên quan đến các phương pháp 300, 400, 500, và 600 có thể được kết hợp hoặc được biến đổi theo các cách khác nhau. Ví dụ, chỉ có bảng thứ nhất theo phương pháp 300 có thể được dùng. Một hoặc nhiều bảng theo phương pháp 300 có thể được dùng cùng với bộ đếm theo phương pháp 400 và/hoặc cờ theo phương pháp 500. Bộ đếm theo phương pháp 400 cũng có thể được sử dụng cùng với cờ theo phương pháp 500 mà không có mỗi bảng theo phương pháp 300. Bảng thứ nhất theo phương pháp 300, bộ đếm theo phương pháp 400, và/hoặc cờ theo phương pháp 500 có thể được sử dụng cùng với phương pháp tiếp cận theo phương pháp 600.

Các kỹ thuật được bộc lộ trong bản mô tả này có thể cải tiến, hoặc cung cấp một sơ đồ khác cho, sự an toàn mật mã của phần tử thay thế được cho thiết bị, như hộp chứa nguồn cung cấp in cho thiết bị in. Phần tử thay thế được cung cấp số lượng giới hạn của các trị số cấp phép, hoặc các mật khẩu, mà nó lưu trữ. Một khi số lượng lớn nhất của các trị số cấp phép khác nhau đã được cung cấp, các yêu cầu cho các trị số cấp phép khác sẽ không được trao cho, ngay cả nếu chúng vẫn được lưu trữ trong phần tử thay thế được. Phương pháp tiếp cận như vậy có thể giảm khả năng mà bên thứ ba sẽ thành công trong việc cố gắng lấy ra tất cả các trị số cấp phép từ phần tử thay thế được. Hơn nữa, khả năng mà việc chỉ sở hữu số lượng lớn nhất của các trị số cấp phép duy nhất sẽ dẫn đến sự xác thực thành công là rất thấp.

YÊU CẦU BẢO HỘ

1. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính lưu trữ mã chạy được bởi máy tính mà có thể chạy được bởi phần tử thay thế được để thực hiện phương pháp bao gồm các bước:

để đáp lại việc nhận yêu cầu định rõ phần tử nhận dạng của trị số xác thực cụ thể trong số nhiều trị số xác thực của phần tử thay thế được từ thiết bị chủ mà phần tử thay thế được đã được kết nối với, xác định liệu phần tử thay thế được đã gửi trước đó trị số xác thực cụ thể được định rõ bởi phần tử nhận dạng trong yêu cầu;

để đáp lại việc xác định là trị số xác thực cụ thể được định rõ bởi phần tử nhận dạng trong yêu cầu đã được gửi trước đó, gửi trị số xác thực cụ thể đến thiết bị chủ;

để đáp lại việc xác định là trị số xác thực cụ thể được định rõ bởi phần tử nhận dạng trong yêu cầu đã không được gửi trước đó:

xác định liệu phần tử thay thế được đã gửi trước đó số lượng lớn nhất của các trị số xác thực duy nhất của các trị số xác thực, số lượng lớn nhất của các trị số xác thực duy nhất nhỏ hơn tổng số lượng của các trị số xác thực;

để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã không được gửi, gửi trị số xác thực cụ thể được định rõ bởi phần tử nhận dạng trong yêu cầu đến thiết bị chủ; và

để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi, từ chối gửi trị số xác thực cụ thể được định rõ bởi phần tử nhận dạng trong yêu cầu đến thiết bị chủ.

2. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó mỗi trị số xác thực có phần tử nhận dạng khác nhau, trong đó yêu cầu bao gồm phần tử nhận dạng được yêu cầu của trị số xác thực,

trong đó bước xác định liệu phần tử thay thế được đã gửi trước đó trị số xác thực cụ thể bao gồm:

tìm kiếm phần tử nhận dạng được yêu cầu trong bảng của ít nhất các phần tử nhận dạng khác nhau của các trị số xác thực mà đã được gửi trước đó,

trong đó việc xác định là trị số xác thực cụ thể đã được gửi trước đó bao gồm:

xác định là phần tử nhận dạng được yêu cầu là một trong số các phần tử nhận dạng khác nhau trong bảng,

trong đó việc xác định là trị số xác thực cụ thể đã không được gửi trước đó bao gồm:

xác định là phần tử nhận dạng được yêu cầu không phải là một trong số các phần tử nhận dạng khác nhau trong bảng,

và trong đó phương pháp này còn bao gồm bước, để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã không được gửi:

lấy ra trị số xác thực cụ thể từ bảng khác nhau của tất cả trong số các trị số xác thực nhờ phần tử nhận dạng được yêu cầu; và

lưu trữ ít nhất phần tử nhận dạng khác nhau của trị số xác thực trong bảng của ít nhất các phần tử nhận dạng khác nhau của các trị số xác thực mà đã được gửi trước đó.

3. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 2, trong đó bảng của ít nhất các phần tử nhận dạng khác nhau của các trị số xác thực mà đã được gửi trước đó có số lượng các mục nhập được đặt trước mà ban đầu là trống, số lượng các mục nhập được đặt trước bằng với số lượng lớn nhất của các trị số xác thực duy nhất mà phần tử thay thế được cho phép gửi,

trong đó bước lưu trữ ít nhất phần tử nhận dạng khác nhau của trị số xác thực cụ thể trong bảng của ít nhất các phần tử nhận dạng khác nhau của các trị số xác thực mà đã được gửi trước đó bao gồm:

định vị mục nhập trống của bảng của ít nhất các phần tử nhận dạng khác nhau của các trị số xác thực mà đã được gửi trước đó; và

lưu trữ ít nhất phần tử nhận dạng khác nhau của trị số xác thực cụ thể trong mục nhập trống,

và trong đó bước xác định liệu phần tử thay thế được đã gửi trước đó số lượng lớn nhất của các trị số xác thực duy nhất bao gồm:

xác định liệu bảng của ít nhất các phần tử nhận dạng khác nhau của các trị số xác thực mà đã được gửi trước đó có các mục nhập trống bất kỳ.

4. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó bước xác định liệu phần tử thay thế được đã gửi trước đó số lượng lớn nhất của các trị số xác thực duy nhất bao gồm:

xác định liệu bộ đếm của số lượng duy nhất của các trị số xác thực mà phần tử thay thế được đã gửi trước đó có bằng với số lượng lớn nhất của các trị số xác thực duy nhất,

và trong đó phương pháp này còn bao gồm bước, để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã không được gửi:

gia tăng bộ đếm.

5. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó bước xác định liệu phần tử thay thế được đã gửi trước đó số lượng lớn nhất của các trị số xác thực duy nhất bao gồm:

xác định liệu đã đặt cờ tương ứng với số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi trước đó,

và trong đó phương pháp này còn bao gồm bước, để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã không được gửi:

xác định liệu số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy hoặc sẽ được gửi lúc ấy;

để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy hoặc sẽ được gửi lúc ấy,

đặt cờ.

6. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó phương pháp này còn bao gồm bước, để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã không được gửi:

một khi trị số xác thực cụ thể đã được gửi hoặc sẽ được gửi đến thiết bị chủ, xác định liệu số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy;

để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy hoặc sẽ được gửi,

xóa theo chức năng ít nhất các trị số xác thực khỏi phần tử thay thế được mà đã không được gửi.

7. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó phương pháp này còn bao gồm bước, để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực đã không được gửi:

tạo ra trị số xác thực cụ thể từ khóa mật mã được lưu trữ trong phần tử thay thế được.

8. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 7, trong đó phương pháp này còn bao gồm bước, để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực đã không được gửi:

một khi trị số xác thực cụ thể đã được gửi hoặc sẽ được gửi đến thiết bị chủ, xác định liệu số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy;

để đáp lại việc xác định là số lượng lớn nhất của các trị số xác thực duy nhất đã được gửi lúc ấy hoặc sẽ được gửi,

xóa theo chức năng khóa mật mã khỏi phần tử thay thế được sao cho không thể tạo ra các trị số xác thực mà đã không được gửi.

9. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó yêu cầu là yêu cầu thứ nhất, và phương pháp này còn bao gồm các bước:

nhận yêu cầu thứ hai, bởi phần tử thay thế từ thiết bị chủ, đối với trị số băm một chiều của trị số xác thực cụ thể; và

gửi trị số băm một chiều bởi phần tử thay thế đến thiết bị chủ,

trong đó yêu cầu thứ nhất được nhận trước hoặc sau khi yêu cầu thứ hai được nhận.

10. Vật ghi dữ liệu không chuyển tiếp đọc được bởi máy tính theo điểm 1, trong đó thiết bị chủ là thiết bị in, và phần tử thay thế được là hộp chứa chất in cho thiết bị in.

11. Hộp chứa chất in cho thiết bị in, bao gồm:

nguồn cung cấp của chất in cho thiết bị in;

bộ nhớ không khả biến lưu trữ nhiều mật khẩu và/hoặc khóa mật mã mà các mật khẩu có thể được tạo ra từ đó; và

bộ phận lôgic để:

cho phép lấy ra số lượng lớn nhất định trước của các mật khẩu, như được yêu cầu theo cách cụ thể bởi thiết bị in, nhỏ hơn tổng số lượng các mật khẩu, từ bộ nhớ không khả biến, để xác thực hộp chứa chất in trong thiết bị in;

cho phép lấy ra số lượng lớn nhất định trước của các mật khẩu với số lần không giới hạn từ bộ nhớ không khả biến; và

cấm lấy ra mật khẩu bất kỳ trong số các mật khẩu mà khác với số lượng lớn nhất định trước của các mật khẩu dù là một lần từ bộ nhớ không khả biến.

12. Hộp chứa chất in theo điểm 11, trong đó bộ phận lôgic còn để:

lựa chọn số lượng lớn nhất định trước của các mật khẩu khi thiết bị bất kỳ yêu cầu mật khẩu cụ thể trong số các mật khẩu từ bộ nhớ không khả biến, cho đến khi đã đạt đến số lượng lớn nhất định trước của các mật khẩu.

13. Hộp chứa chất in theo điểm 11, trong đó bộ nhớ không khả biến là bộ nhớ ghi một lần, đọc giới hạn trong đó số lượng lớn nhất định trước của các mật khẩu là có thể đọc được với số lần không giới hạn và các mật khẩu mà khác với số lượng lớn nhất định trước của các mật khẩu là không thể đọc được một khi số lượng lớn nhất định trước của các mật khẩu đã được lựa chọn.

14. Hộp chứa chất in theo điểm 11, trong đó bộ phận lôgic còn để:

xóa ít nhất là theo chức năng ít nhất các mật khẩu mà khác với số lượng lớn nhất định trước của các mật khẩu một khi số lượng lớn nhất định trước của các mật khẩu đã được lựa chọn.

15. Hộp chứa chất in theo điểm 11, trong đó bộ phận lôgic còn để, để đáp lại việc nhận yêu cầu đối với mật khẩu cụ thể trong số các mật khẩu:

nếu mật khẩu cụ thể đã được gửi trước đó, thì trả về mật khẩu cụ thể;

nếu mật khẩu cụ thể đã không được gửi trước đó và số lượng lớn nhất định trước của các mật khẩu đã không được gửi, thì tạo ra mật khẩu cụ thể từ khóa mật mã và trả về mật khẩu cụ thể; và

nếu mật khẩu cụ thể đã không được gửi trước đó và số lượng lớn nhất định trước của các mật khẩu đã được gửi, thì từ chối tạo ra và trả về mật khẩu cụ thể.

16. Hộp chứa chất in theo điểm 15, trong đó bộ phận lôgic còn để, sau khi tạo ra mật khẩu cụ thể từ khóa mật mã:

xóa ít nhất là theo chức năng khóa mật mã nếu số lượng lớn nhất định trước của các mật khẩu đã được gửi lúc ấy hoặc sẽ được gửi lúc ấy.

17. Hộp chứa chất in theo điểm 11, hộp chứa này còn bao gồm:

bộ nhớ không khả biến lưu trữ nhiều trị số băm của các mật khẩu,

trong đó bộ phận lôgic là để cho phép lấy ra trị số băm bất kỳ với số lần không giới hạn từ bộ nhớ không khả biến.

18. Hộp chứa chất in theo điểm 11, trong đó chất in là một hoặc nhiều trong số: mực, mực toner, thuốc nhuộm màu 2D (two-dimensional - hai chiều), tác nhân in 3D (three-dimensional - ba chiều), và vật liệu xây dựng in 3D.

FIG 1

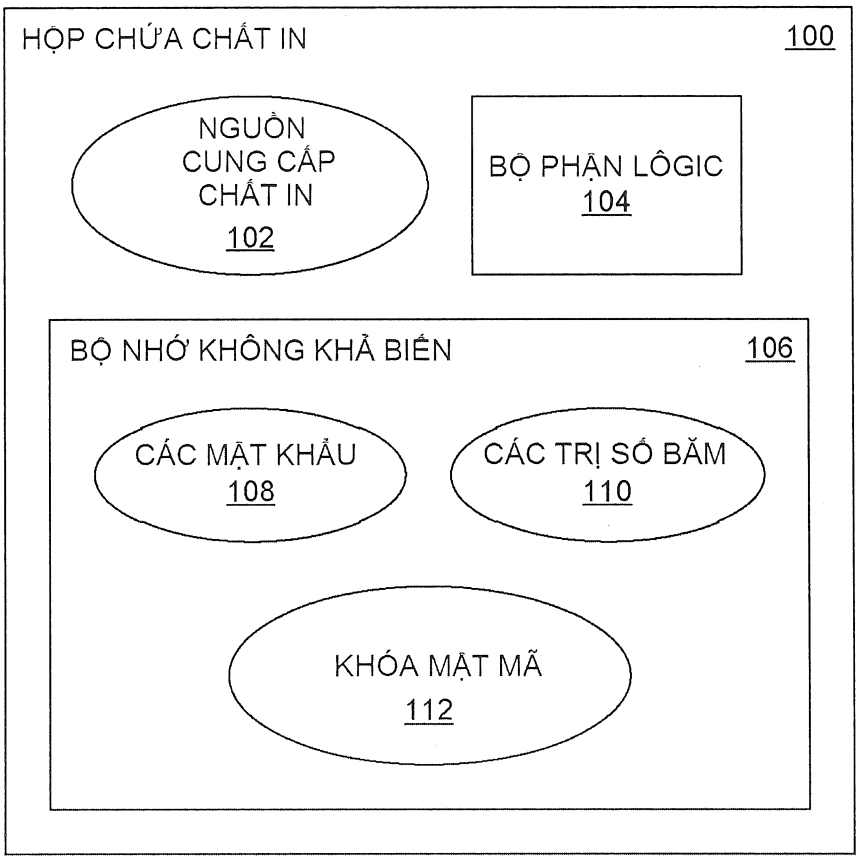
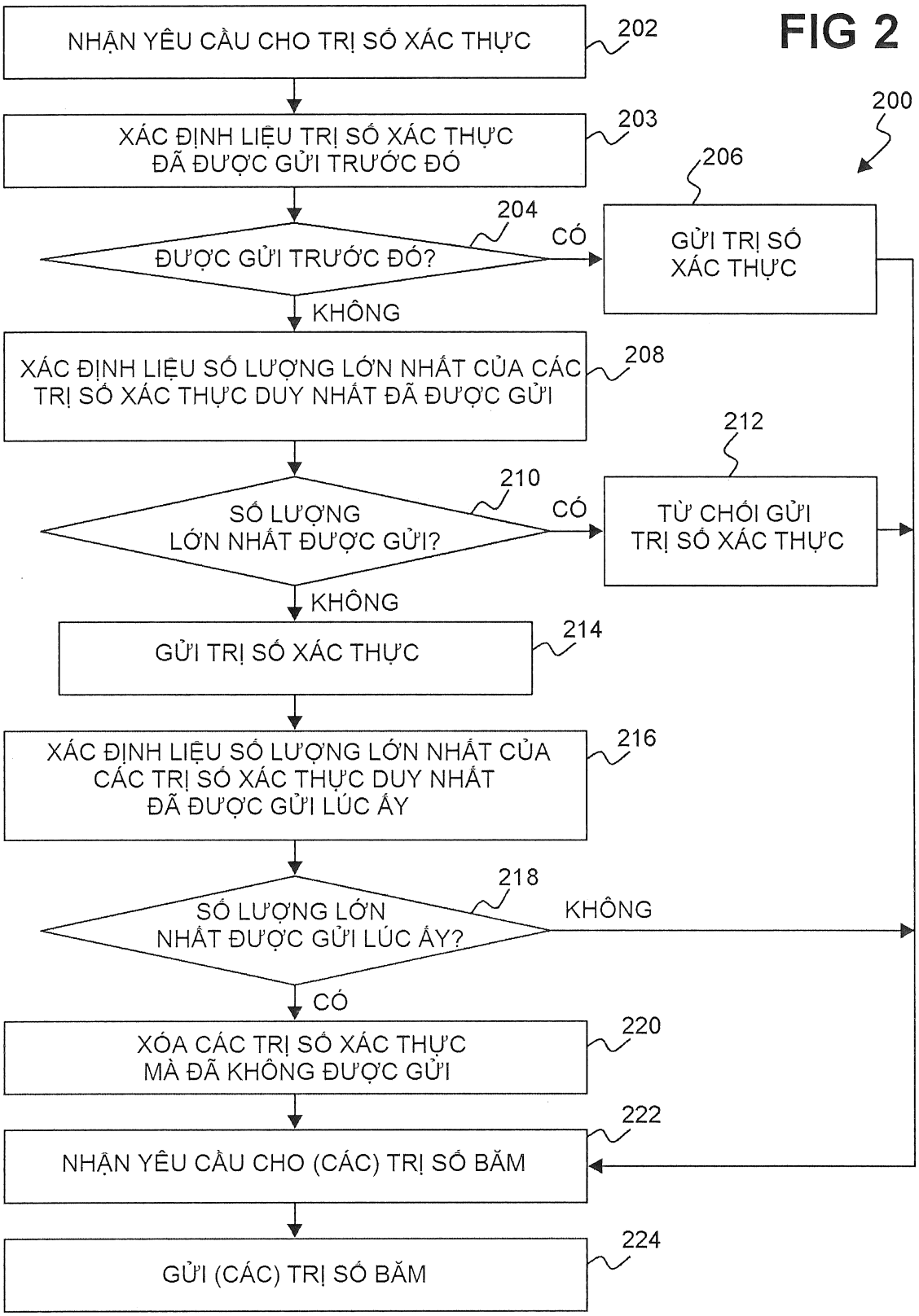

HỘP CHỨA CHẤT IN
100
NGUỒN CUNG CẤP CHẤT IN
102
BỘ PHẬN LÔGIC
104
BỘ NHỚ KHÔNG KHẢ BIẾN
106
CÁC MẬT KHẨU
108
CÁC TRỊ SỐ BĂM
110
KHÓA MẬT MÃ
112

FIG 2


NHẬN YÊU CẦU CHO TRỊ SỐ XÁC THỰC
202
XÁC ĐỊNH LIỆU TRỊ SỐ XÁC THỰC ĐÃ ĐƯỢC GỬI TRƯỚC ĐÓ
203
200
206
ĐƯỢC GỬI TRƯỚC ĐÓ?
204
CÓ
GỬI TRỊ SỐ XÁC THỰC
KHÔNG
XÁC ĐỊNH LIỆU SỐ LƯỢNG LỚN NHẤT CỦA CÁC TRỊ SỐ XÁC THỰC DUY NHẤT ĐÃ ĐƯỢC GỬI
208
212
SỐ LƯỢNG LỚN NHẤT ĐƯỢC GỬI?
210
CÓ
TỪ CHỐI GỬI TRỊ SỐ XÁC THỰC
KHÔNG
GỬI TRỊ SỐ XÁC THỰC
214
XÁC ĐỊNH LIỆU SỐ LƯỢNG LỚN NHẤT CỦA CÁC TRỊ SỐ XÁC THỰC DUY NHẤT ĐÃ ĐƯỢC GỬI LÚC ẤY
216
SỐ LƯỢNG LỚN NHẤT ĐƯỢC GỬI LÚC ẤY?
218
KHÔNG
CÓ
XÓA CÁC TRỊ SỐ XÁC THỰC MÀ ĐÃ KHÔNG ĐƯỢC GỬI
220
NHẬN YÊU CẦU CHO (CÁC) TRỊ SỐ BĂM
222
GỬI (CÁC) TRỊ SỐ BĂM
224

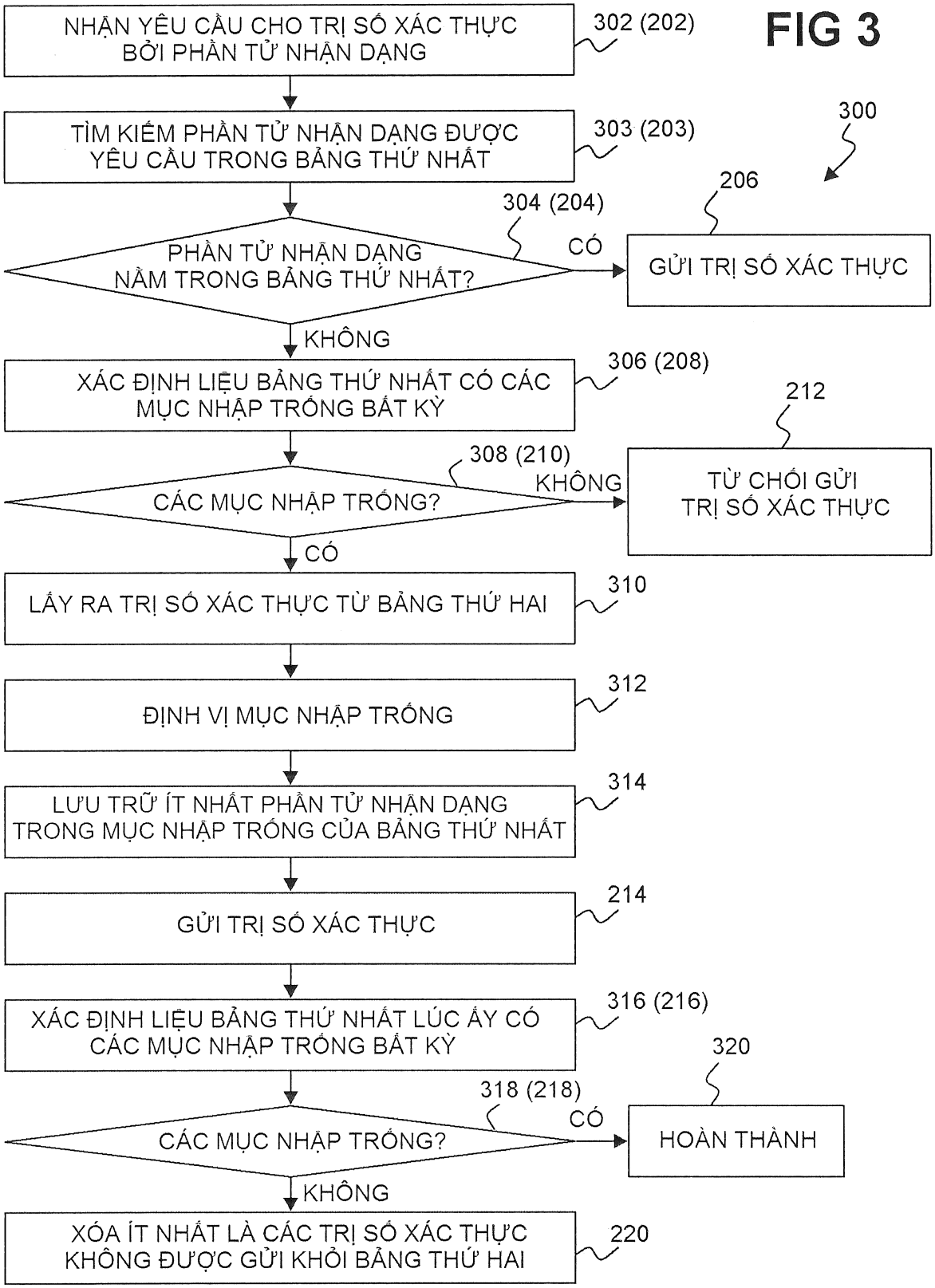

NHẬN YÊU CẦU CHO TRỊ SỐ XÁC THỰC BỞI PHẦN TỬ NHẬN DẠNG
302 (202)
TÌM KIẾM PHẦN TỬ NHẬN DẠNG ĐƯỢC YÊU CẦU TRONG BẢNG THỨ NHẤT
303 (203)
300
206
304 (204)
PHẦN TỬ NHẬN DẠNG NẰM TRONG BẢNG THỨ NHẤT?
CÓ
GỬI TRỊ SỐ XÁC THỰC
KHÔNG
XÁC ĐỊNH LIỆU BẢNG THỨ NHẤT CÓ CÁC MỤC NHẬP TRỐNG BẤT KỲ
306 (208)
212
308 (210)
CÁC MỤC NHẬP TRỐNG?
KHÔNG
TỪ CHỐI GỬI TRỊ SỐ XÁC THỰC
CÓ
LẤY RA TRỊ SỐ XÁC THỰC TỪ BẢNG THỨ HAI
310
ĐỊNH VỊ MỤC NHẬP TRỐNG
312
LƯU TRỮ ÍT NHẤT PHẦN TỬ NHẬN DẠNG TRONG MỤC NHẬP TRỐNG CỦA BẢNG THỨ NHẤT
314
GỬI TRỊ SỐ XÁC THỰC
214
XÁC ĐỊNH LIỆU BẢNG THỨ NHẤT LÚC ẤY CÓ CÁC MỤC NHẬP TRỐNG BẤT KỲ
316 (216)
320
318 (218)
CÁC MỤC NHẬP TRỐNG?
CÓ
HOÀN THÀNH
KHÔNG
XÓA ÍT NHẤT LÀ CÁC TRỊ SỐ XÁC THỰC KHÔNG ĐƯỢC GỬI KHỎI BẢNG THỨ HAI
220

FIG 3

FIG 4

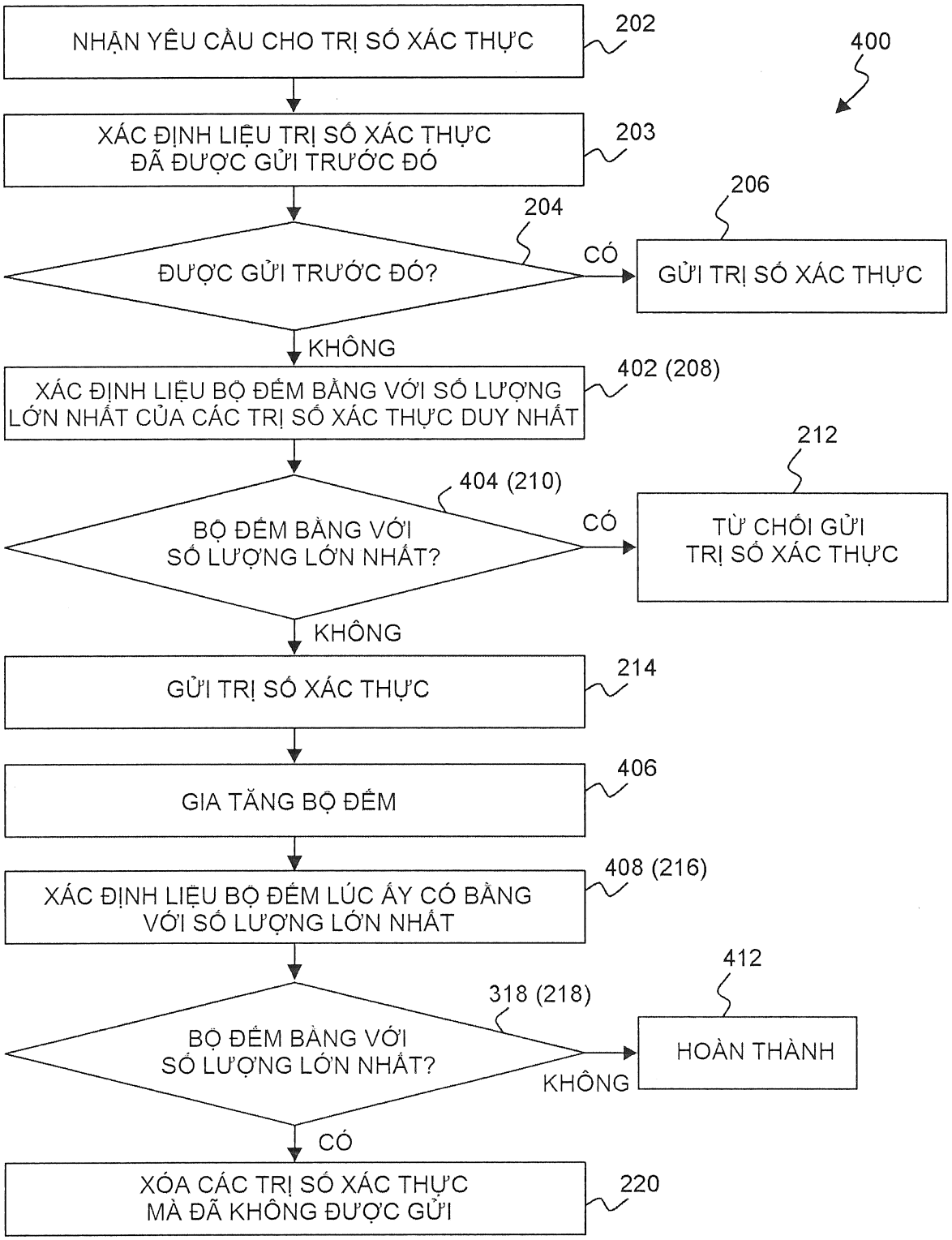

400
NHẬN YÊU CẦU CHO TRỊ SỐ XÁC THỰC
202
XÁC ĐỊNH LIỆU TRỊ SỐ XÁC THỰC ĐÃ ĐƯỢC GỬI TRƯỚC ĐÓ
203
ĐƯỢC GỬI TRƯỚC ĐÓ?
204
CÓ
206
GỬI TRỊ SỐ XÁC THỰC
KHÔNG
XÁC ĐỊNH LIỆU BỘ ĐẾM BẰNG VỚI SỐ LƯỢNG LỚN NHẤT CỦA CÁC TRỊ SỐ XÁC THỰC DUY NHẤT
402 (208)
BỘ ĐẾM BẰNG VỚI SỐ LƯỢNG LỚN NHẤT?
404 (210)
CÓ
212
TỪ CHỐI GỬI TRỊ SỐ XÁC THỰC
KHÔNG
GỬI TRỊ SỐ XÁC THỰC
214
GIA TĂNG BỘ ĐẾM
406
XÁC ĐỊNH LIỆU BỘ ĐẾM LÚC ẤY CÓ BẰNG VỚI SỐ LƯỢNG LỚN NHẤT
408 (216)
BỘ ĐẾM BẰNG VỚI SỐ LƯỢNG LỚN NHẤT?
318 (218)
KHÔNG
412
HOÀN THÀNH
CÓ
XÓA CÁC TRỊ SỐ XÁC THỰC MÀ ĐÃ KHÔNG ĐƯỢC GỬI
220

FIG 5

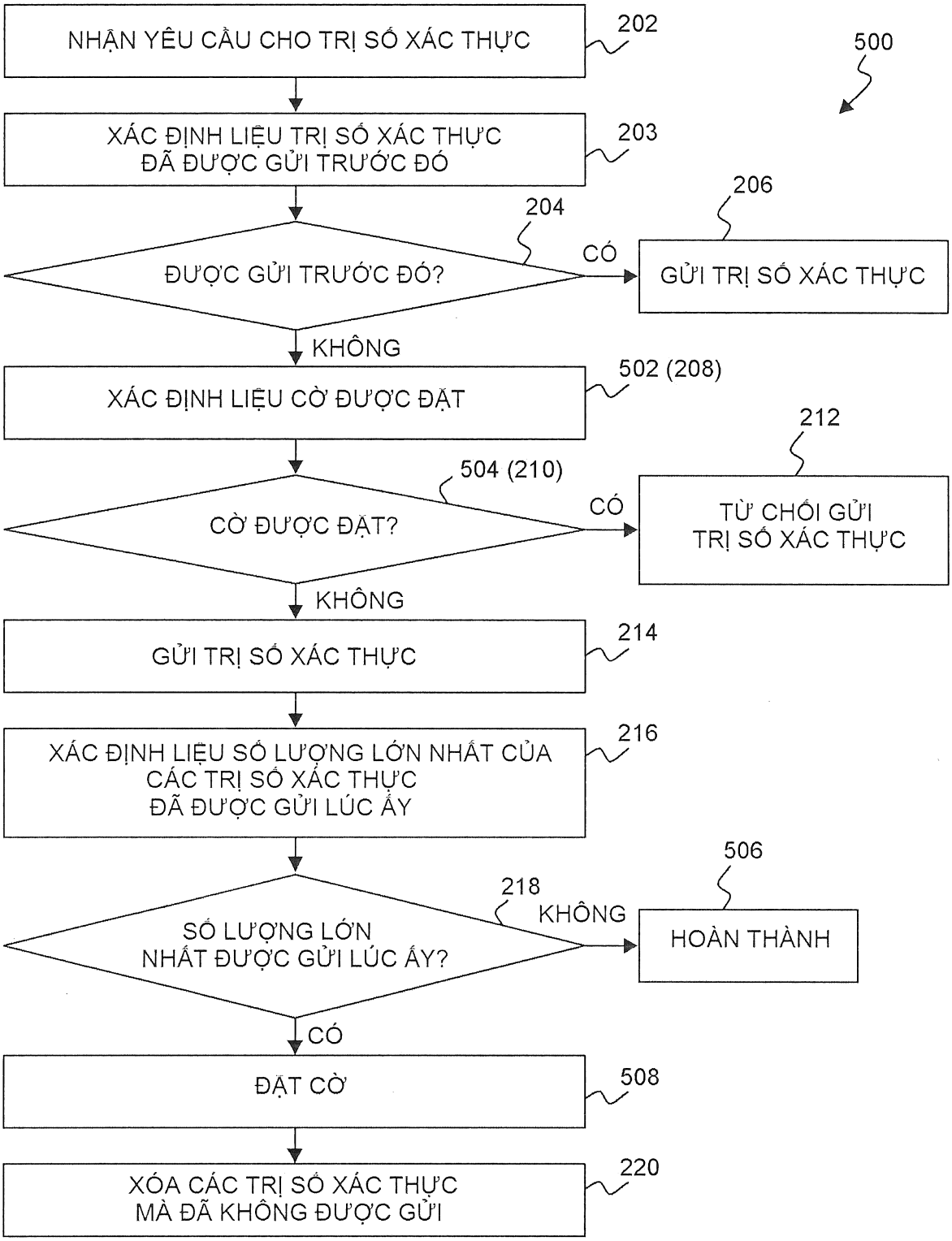
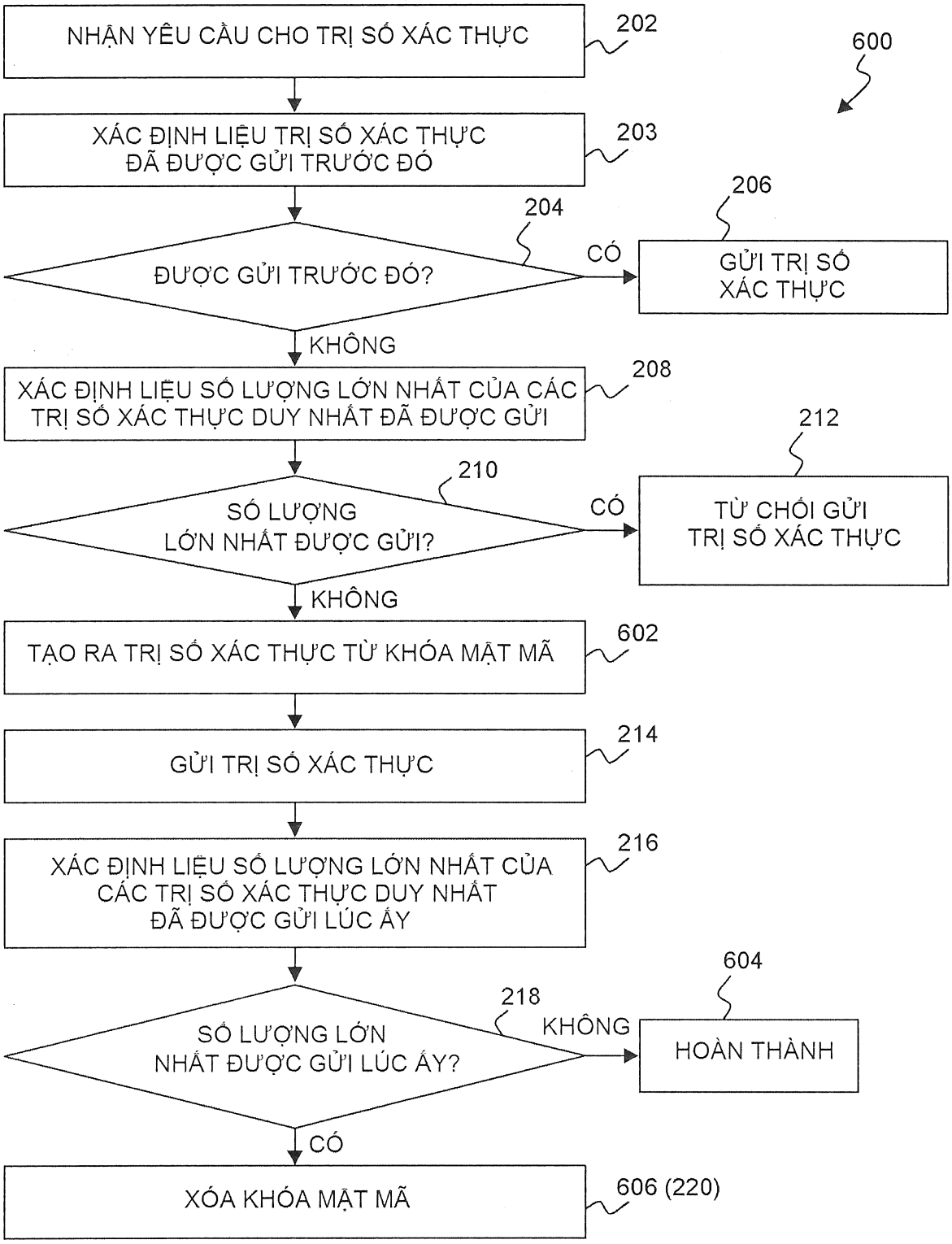

NHẬN YÊU CẦU CHO TRỊ SỐ XÁC THỰC
202
500
XÁC ĐỊNH LIỆU TRỊ SỐ XÁC THỰC ĐÃ ĐƯỢC GỬI TRƯỚC ĐÓ
203
206
204
ĐƯỢC GỬI TRƯỚC ĐÓ?
CÓ
GỬI TRỊ SỐ XÁC THỰC
KHÔNG
XÁC ĐỊNH LIỆU CỜ ĐƯỢC ĐẶT
502 (208)
212
504 (210)
CỜ ĐƯỢC ĐẶT?
CÓ
TỪ CHỐI GỬI TRỊ SỐ XÁC THỰC
KHÔNG
GỬI TRỊ SỐ XÁC THỰC
214
XÁC ĐỊNH LIỆU SỐ LƯỢNG LỚN NHẤT CỦA CÁC TRỊ SỐ XÁC THỰC ĐÃ ĐƯỢC GỬI LÚC ẤY
216
506
218
KHÔNG
SỐ LƯỢNG LỚN NHẤT ĐƯỢC GỬI LÚC ẤY?
HOÀN THÀNH
CÓ
ĐẶT CỜ
508
XÓA CÁC TRỊ SỐ XÁC THỰC MÀ ĐÃ KHÔNG ĐƯỢC GỬI
220

FIG 6


NHẬN YÊU CẦU CHO TRỊ SỐ XÁC THỰC
202
600
XÁC ĐỊNH LIỆU TRỊ SỐ XÁC THỰC ĐÃ ĐƯỢC GỬI TRƯỚC ĐÓ
203
206
204
ĐƯỢC GỬI TRƯỚC ĐÓ?
CÓ
GỬI TRỊ SỐ XÁC THỰC
KHÔNG
XÁC ĐỊNH LIỆU SỐ LƯỢNG LỚN NHẤT CỦA CÁC TRỊ SỐ XÁC THỰC DUY NHẤT ĐÃ ĐƯỢC GỬI
208
212
210
SỐ LƯỢNG LỚN NHẤT ĐƯỢC GỬI?
CÓ
TỪ CHỐI GỬI TRỊ SỐ XÁC THỰC
KHÔNG
TẠO RA TRỊ SỐ XÁC THỰC TỪ KHÓA MẬT MÃ
602
GỬI TRỊ SỐ XÁC THỰC
214
XÁC ĐỊNH LIỆU SỐ LƯỢNG LỚN NHẤT CỦA CÁC TRỊ SỐ XÁC THỰC DUY NHẤT ĐÃ ĐƯỢC GỬI LÚC ẤY
216
604
218
SỐ LƯỢNG LỚN NHẤT ĐƯỢC GỬI LÚC ẤY?
KHÔNG
HOÀN THÀNH
CÓ
XÓA KHÓA MẬT MÃ
606 (220)