(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) **1-0043431**

(51)[2020.01] **H04L 9/14**; H04L 9/32; H04L 9/28; G06F 21/60

(13) **B**

(21) 1-2020-04390
(22) 22/01/2019
(86) PCT/JP2019/001760 22/01/2019
(87) WO 2019/155861 A1 15/08/2019
(30) 2018-018907 06/02/2018 JP
(45) 25/02/2025 443
(43) 25/03/2021 396A
(73) SONY CORPORATION (JP)
1-7-1, Konan, Minato-ku, Tokyo 1080075, Japan
(72) NAKATSURU, Tsutomu (JP); SHIMOJI, Katsuya (JP); TAKEMURA, Toshiharu (JP); WANG, Yuhu (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

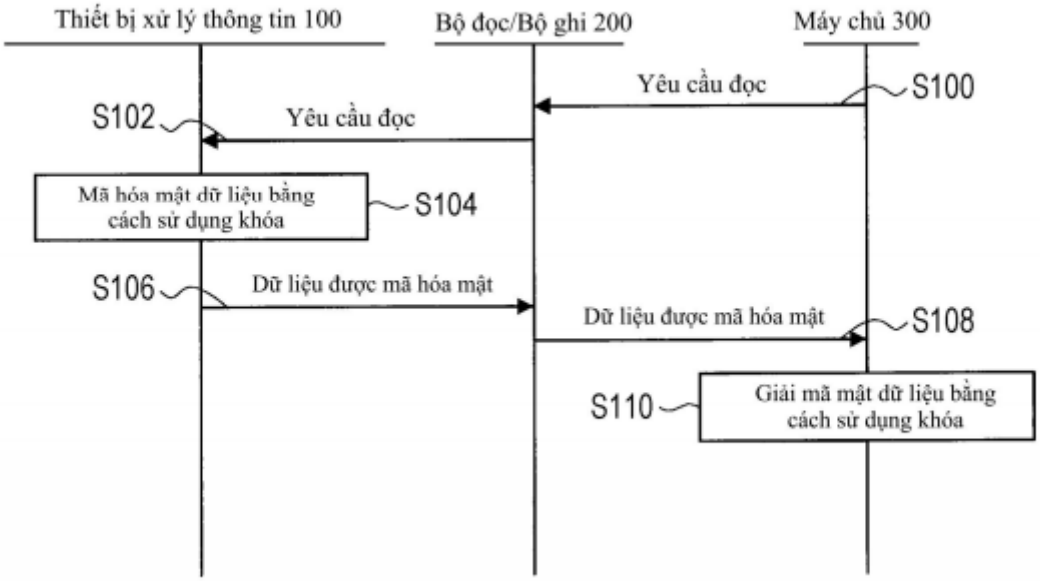
(54) THIẾT BỊ XỬ LÝ THÔNG TIN, PHƯƠNG PHÁP XỬ LÝ THÔNG TIN, PHƯƠNG TIỆN GHI VÀ HỆ THỐNG XỬ LÝ THÔNG TIN

(21) 1-2020-04390

(57) Sáng chế đề cập đến thiết bị xử lý thông tin, phương pháp xử lý thông tin, phương tiện ghi, và hệ thống xử lý thông tin mà có thể làm giảm thời gian xử lý để đọc trong khi đảm bảo sự bảo mật liên quan đến việc đọc dữ liệu.

Thiết bị xử lý thông tin được đề xuất bao gồm bộ xử lý mà, trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu, mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và truyền dữ liệu được mã hóa mật..

FIG. 11



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết bị xử lý thông tin, phương pháp xử lý thông tin, chương trình, và hệ thống xử lý thông tin.

Tình trạng kỹ thuật của sáng chế

Các kỹ thuật để điều khiển một cách hiệu quả các thiết bị được kết nối qua mạng đã được phát triển. Với kỹ thuật này, ví dụ, kỹ thuật được bộc lộ trong Tài liệu Sáng chế 1 được minh họa.

Tài liệu trích dẫn:

Tài liệu Sáng chế:

Tài liệu Sáng chế 1: Công bố đơn yêu cầu cấp bằng sáng chế Nhật Bản số 2004-186883

Vấn đề cần được giải quyết bởi sáng chế:

Ví dụ, khi một thiết bị khác đọc dữ liệu mà cần ủy quyền để đọc và được lưu trữ trong một thiết bị, việc xác thực được thực hiện giữa một thiết bị và thiết bị khác, và dữ liệu được đọc sau khi xác thực được hoàn thành.

Ở đây, ví dụ, trong trường hợp mà kỹ thuật được bộc lộ trong Tài liệu Sáng chế 1 được sử dụng, các lệnh được truyền một cách có chọn lọc trong một lần truyền thông. Do đó, trong trường hợp mà kỹ thuật được bộc lộ trong Tài liệu Sáng chế 1 được sử dụng, có thể giảm số lần truyền thông giữa các thiết bị được kết nối qua mạng. Tuy nhiên, ví dụ, kỹ thuật được bộc lộ trong Tài liệu Sáng chế 1 đơn giản là truyền một cách có chọn lọc các lệnh trong một lần truyền thông. Do đó, ví dụ, ngay cả nếu kỹ thuật được bộc lộ trong Tài liệu Sáng chế 1 được sử dụng, không thể bỏ qua việc "xác thực để đọc dữ liệu mà cần xác thực để đọc" theo quan điểm về bảo mật hoặc tương tự, và là khó khăn trong việc giảm thời gian xử lý để đọc.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là đề xuất thiết bị xử lý thông tin, phương pháp xử lý thông tin, chương trình, và hệ thống xử lý thông tin mà có thể giảm thời gian xử lý để đọc và là mới và được cải thiện trong khi đảm bảo sự bảo mật liên quan

đến việc đọc dữ liệu.

Cách thức giải quyết vấn đề:

Theo sáng chế, thiết bị xử lý thông tin được đề xuất bao gồm bộ xử lý mà, trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu, mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và truyền dữ liệu được mã hóa mật.

Hơn nữa, theo sáng chế, thiết bị xử lý thông tin được đề xuất bao gồm bộ xử lý mà giải mã mật dữ liệu được mã hóa mật mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước, chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất, và truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Hơn nữa, theo sáng chế, phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin được đề xuất, và phương pháp xử lý thông tin mà bao gồm bước mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu và bước truyền dữ liệu được mã hóa mật.

Hơn nữa, theo sáng chế, phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin được đề xuất, và phương pháp bao gồm bước giải mã mật dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước, bước chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất, và bước truyền thông tin nhận dạng thứ hai tới thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Hơn nữa, theo sáng chế, chương trình được đề xuất mà làm cho máy tính thực hiện bước mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu và

bước truyền dữ liệu được mã hóa mật.

Hơn nữa, theo sáng chế, chương trình được đề xuất mà làm cho máy tính thực hiện bước giải mã mật dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước, bước chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất, và bước truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Hơn nữa, theo sáng chế, hệ thống xử lý thông tin được đề xuất mà bao gồm thiết bị xử lý thông tin thứ nhất và thiết bị xử lý thông tin thứ hai, mà trong đó thiết bị xử lý thông tin thứ nhất bao gồm bộ xử lý mà mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu và truyền dữ liệu được mã hóa, và thiết bị xử lý thông tin thứ hai bao gồm bộ xử lý mà giải mã mật dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước, chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất, và truyền thông tin nhận dạng thứ hai tới thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Hiệu quả của sáng chế:

Theo sáng chế, thời gian xử lý để đọc có thể giảm đi trong khi đảm bảo sự bảo mật liên quan đến việc đọc dữ liệu.

Lưu ý rằng các hiệu quả trên không nhất thiết phải được giới hạn, và hiệu quả bất kỳ mà được mô tả trong bản mô tả này hoặc hiệu quả khác mà có thể được thấy từ bản mô tả này có thể được thu nhận cùng với hoặc thay cho các hiệu quả trên.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ giải thích minh họa cấu trúc minh họa của hệ thống xử lý thông tin theo phương án của sáng chế.

Fig.2 là sơ đồ khối chức năng minh họa cấu trúc minh họa của thiết bị xử lý thông tin (thiết bị xử lý thông tin thứ nhất) theo phương án của sáng chế.

Fig.3 là sơ đồ giải thích minh họa cấu trúc phần cứng minh họa của thiết bị xử lý thông tin (thiết bị xử lý thông tin thứ nhất) theo phương án của sáng chế.

Fig.4 là sơ đồ giải thích minh họa ví dụ các cấu trúc của chip IC và anten được minh họa trên Fig.3.

Fig.5 là sơ đồ khối chức năng minh họa cấu trúc minh họa của bộ đọc/bộ ghi (thiết bị chuyển tiếp) theo phương án của sáng chế.

Fig.6 là sơ đồ giải thích minh họa cấu trúc phần cứng minh họa của bộ đọc/bộ ghi (thiết bị chuyển tiếp) theo phương án của sáng chế.

Fig.7 là sơ đồ khối chức năng minh họa cấu trúc minh họa của máy chủ (thiết bị xử lý thông tin thứ hai) theo phương án của sáng chế.

Fig.8 là sơ đồ giải thích minh họa cấu trúc phần cứng minh họa của máy chủ (thiết bị xử lý thông tin thứ hai) theo phương án của sáng chế.

Fig.9 là sơ đồ giải thích minh họa ví dụ truyền thông liên quan đến việc đọc dữ liệu sử dụng sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết.

Fig.10 là sơ đồ giải thích minh họa phác thảo của thiết lập được xác định bởi thông tin thiết lập theo phương án của sáng chế.

Fig.11 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ nhất.

Fig.12 là sơ đồ giải thích minh họa ví dụ của việc xử lý bộ đọc/bộ ghi (thiết bị chuyển tiếp) được chứa trong hệ thống xử lý thông tin theo phương án thứ nhất.

Fig.13 là sơ đồ giải thích để giải thích ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ nhất.

Fig.14 là sơ đồ giải thích để giải thích ví dụ của yêu cầu đọc theo phương án của sáng chế.

Fig.15 là lưu đồ minh họa ví dụ của việc xử lý thiết bị xử lý thông tin theo phương án thứ nhất.

Fig.16 là sơ đồ giải thích minh họa ví dụ của trường hợp mà có thể xảy ra trong trường hợp mà không thể dùng cho máy chủ để chỉ rõ khi yêu cầu đọc tương ứng với dữ liệu được truyền.

Fig.17 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin theo phương án thứ hai.

Fig.18 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin theo phương án thứ hai.

Fig.19 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ hai.

Fig.20 là sơ đồ giải thích để giải thích ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ hai.

Fig.21 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó sự truyền thông từ bộ đọc/bộ ghi tới thiết bị xử lý thông tin bị sai lệch.

Fig.22 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin theo phương án thứ ba.

Fig.23 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ ba.

Fig.24 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó dữ liệu được mã hóa được truyền từ thiết bị xử lý thông tin tới bộ đọc/bộ ghi được quan sát bởi bên thứ ba.

Fig.25 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin theo phương án thứ tư.

Fig.26 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ tư.

Fig.27 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó dữ liệu được truyền từ thiết bị xử lý thông tin tới bộ đọc/bộ ghi được quan sát bởi bên thứ ba và được xác định là có lỗi xảy ra.

Fig.28 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin theo phương án thứ năm.

Fig.29 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó thông tin nhận dạng được lưu trữ trong thiết bị xử lý thông tin được sử dụng bởi các nhà điều hành kinh doanh.

Fig.30 là sơ đồ giải thích minh họa ví dụ của trường hợp sử dụng mà hệ thống xử lý thông tin theo phương án thứ sáu được áp dụng.

Fig.31 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin theo phương án thứ sáu.

Fig.32 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin theo phương án thứ sáu.

Mô tả chi tiết sáng chế

Sau đây, các phương án ưu tiên của sáng chế sẽ được mô tả chi tiết có viện dẫn đến các hình vẽ kèm theo. Lưu ý rằng, trong bản mô tả này và bộ hình vẽ, các thành phần về cơ bản có cùng cấu trúc chức năng được ký hiệu bằng các số tham chiếu giống nhau để bỏ qua việc mô tả dư thừa.

Hơn nữa, sau đây, phần mô tả được thực hiện theo thứ tự như sau.

1. Hệ thống xử lý thông tin theo phương án của sáng chế và Phương pháp xử lý thông tin theo phương án của sáng chế

[1] Cấu trúc của hệ thống xử lý thông tin theo phương án của sáng chế

[1-1] Thiết bị xử lý thông tin 100 (Thiết bị xử lý thông tin thứ nhất)

[1-2] Bộ đọc/bộ ghi 200 (Thiết bị chuyển tiếp)

[1-3] Máy chủ 300 (Thiết bị xử lý thông tin thứ hai)

[1-4] Ví dụ ứng dụng của mỗi thiết bị được chứa trong hệ thống xử lý thông tin theo phương án của sáng chế

[2] Xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế

[2-1] Phương pháp xử lý thông tin theo phương án thứ nhất

[2-2] Phương pháp xử lý thông tin theo phương án thứ hai

[2-3] Phương pháp xử lý thông tin theo phương án thứ ba

[2-4] Phương pháp xử lý thông tin theo phương án thứ tư

[2-5] Phương pháp xử lý thông tin theo phương án thứ năm

[2-6] Phương pháp xử lý thông tin theo phương án thứ sáu

[2-7] Phương pháp xử lý thông tin theo phương án khác

2. Chương trình theo phương án của sáng chế

Hệ thống xử lý thông tin theo phương án của sáng chế và Phương pháp xử lý thông tin theo phương án của sáng chế)

Sau đây, ví dụ của hệ thống xử lý thông tin theo phương án của sáng chế sẽ được mô tả đầu tiên. Sau đó, phương pháp xử lý thông tin theo phương án của sáng chế sẽ được mô tả bằng cách sử dụng trường hợp của ứng dụng cho hệ thống xử lý thông tin theo phương án của sáng chế làm chẳng hạn.

[1] Cấu trúc của hệ thống xử lý thông tin theo phương án của sáng chế

Fig.1 là sơ đồ giải thích minh họa cấu trúc minh họa của hệ thống xử lý thông tin 100 theo phương án của sáng chế. Hệ thống xử lý thông tin 1000 bao gồm, ví dụ, thiết bị xử lý thông tin 100 (thiết bị xử lý thông tin thứ nhất), bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp), và máy chủ 300 (thiết bị xử lý thông tin thứ hai).

Lưu ý rằng cấu trúc của hệ thống xử lý thông tin theo phương án của sáng chế không được giới hạn ở ví dụ được minh họa trên Fig.1. Ví dụ, hệ thống xử lý thông tin theo phương án của sáng chế có thể bao gồm các thiết bị xử lý thông tin 100. Hơn nữa, hệ thống xử lý thông tin theo phương án của sáng chế có thể bao gồm các bộ đọc/bộ ghi 200 và có thể bao gồm các máy chủ 300.

Thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 200 truyền thông với nhau bằng cách sử dụng truyền thông trường gần (NFC), ví dụ, của Loại A, Loại B, Loại F, hoặc loại tương tự.

Lưu ý rằng, trong hệ thống xử lý thông tin theo phương án của sáng chế, thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 200 có thể truyền thông với nhau, ví dụ, qua "truyền thông không dây sử dụng phương pháp truyền thông tùy ý, như là truyền thông không dây sử dụng IEEE802.15.1 như là Bluetooth năng lượng thấp (Bluetooth Low Energy, BLE), truyền thông không dây sử dụng IEEE802.11, truyền thông hồng ngoại, hoặc loại tương tự" hoặc "truyền thông có dây sử dụng truyền thông hoặc loại tương tự qua kênh truyền chuỗi toàn cầu (USB) và giao diện truyền thông dựa trên tiêu chuẩn ISO7816".

[0024]

Máy chủ 300 và bộ đọc/bộ ghi 200, ví dụ, được kết nối không dây hoặc có dây với nhau qua mạng và truyền thông với nhau qua việc truyền thông qua mạng (sau đây, được chỉ báo là "truyền thông mạng"). Đối với mạng theo phương án của sáng chế, ví dụ, mạng có dây như là Mạng vùng cục bộ (LAN) hoặc Mạng vùng cục bộ rộng (WAN), mạng không dây như là mạng vùng cục bộ không dây (WLAN), hoặc Internet sử dụng giao thức truyền thông như là

Giao thức điều khiển truyền/Giao thức Internet (TCP/IP), hoặc loại tương tự được minh họa.

Lưu ý rằng, trong hệ thống xử lý thông tin theo phương án của sáng chế, máy chủ 300 và bộ đọc/bộ ghi 200 có thể trực tiếp truyền thông với nhau mà không truyền thông qua mạng.

Máy chủ 300 và thiết bị xử lý thông tin 100 truyền thông với nhau qua bộ đọc/bộ ghi 200. Tức là, trong hệ thống xử lý thông tin 1000, bộ đọc/bộ ghi 200 đóng vai trò là thiết bị chuyển tiếp mà chuyển tiếp truyền thông giữa máy chủ 300 và thiết bị xử lý thông tin 100.

Lưu ý rằng, trong hệ thống xử lý thông tin theo phương án của sáng chế, máy chủ 300 và thiết bị xử lý thông tin 100 có thể trực tiếp truyền thông với nhau mà không sử dụng bộ đọc/bộ ghi 200. Trong trường hợp mà hệ thống xử lý thông tin theo phương án của sáng chế có "cấu trúc mà trong đó máy chủ 300 và thiết bị xử lý thông tin 100 trực tiếp truyền thông với nhau mà không sử dụng bộ đọc/bộ ghi 200", ví dụ, máy chủ 300 có thể có cấu trúc mà có chức năng của bộ đọc/bộ ghi 200. Tức là, không cần dùng cho hệ thống xử lý thông tin theo phương án của sáng chế để bao gồm thiết bị mà đóng vai trò là thiết bị chuyển tiếp như là bộ đọc/bộ ghi 200.

Sau đây, như được minh họa trên Fig.1, "trường hợp trong đó thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 200 truyền thông với nhau bởi NFC và máy chủ 300 và bộ đọc/bộ ghi 200 truyền thông với nhau qua truyền thông mạng" sẽ được mô tả làm chẳng hạn. Lưu ý rằng, như được mô tả ở trên, ví dụ của việc truyền thông của hệ thống xử lý thông tin theo phương án của sáng chế không được giới hạn ở ví dụ được minh họa trên Fig.1.

[1-1] Thiết bị xử lý thông tin 100 (Thiết bị xử lý thông tin thứ nhất)

Fig.2 là sơ đồ khối chức năng minh họa cấu trúc minh họa của thiết bị xử lý thông tin 100 (thiết bị xử lý thông tin thứ nhất) theo phương án của sáng chế.

Thiết bị xử lý thông tin 100 bao gồm, ví dụ, bộ truyền thông thứ nhất 102, bộ truyền thông thứ hai 104, và bộ điều khiển 106.

Hơn nữa, thiết bị xử lý thông tin 100 có thể bao gồm, ví dụ, bộ nhớ chỉ đọc (ROM, không được minh họa), bộ nhớ truy nhập ngẫu nhiên (RAM, không được minh họa), bộ thao tác (không được minh họa) mà có thể được thao tác bởi

người dùng của thiết bị xử lý thông tin 100, bộ hiển thị (không được minh họa) mà hiển thị các màn hình khác nhau trên màn hình hiển thị, hoặc loại tương tự. Thiết bị xử lý thông tin 100 kết nối giữa các thành phần, ví dụ, bởi kênh truyền làm đường dẫn truyền dữ liệu.

ROM (không được minh họa) lưu trữ dữ liệu điều khiển như là chương trình cần được sử dụng bởi bộ điều khiển 106 và tham số thao tác. RAM (không được minh họa) tạm thời lưu trữ chương trình được thực hiện bởi bộ điều khiển 106, hoặc loại tương tự.

Đối với bộ thao tác (không được minh họa), thiết bị nhập thao tác được chỉ báo trong cấu trúc phần cứng minh họa của thiết bị xử lý thông tin 100 được mô tả sau đây được minh họa. Hơn nữa, đối với bộ hiển thị (không được minh họa), thiết bị hiển thị được chỉ báo trong cấu trúc phần cứng minh họa của thiết bị xử lý thông tin 100 được mô tả sau đây được minh họa.

[Cấu trúc phần cứng minh họa của thiết bị xử lý thông tin 100]

Fig.3 là sơ đồ giải thích minh họa cấu trúc phần cứng minh họa của thiết bị xử lý thông tin 100 (thiết bị xử lý thông tin thứ nhất) theo phương án của sáng chế. Fig.3 minh họa cấu trúc phần cứng minh họa của thiết bị xử lý thông tin 100 trong trường hợp truyền thông với bộ đọc/bộ ghi 200 bởi NFC.

Thiết bị xử lý thông tin 100 bao gồm, ví dụ, MPU 150, ROM 152, RAM 154, phương tiện ghi 156, giao diện đầu vào/đầu ra 158, thiết bị nhập thao tác 160, thiết bị hiển thị 162, giao diện truyền thông 164, chip IC 166, và anten 168. Hơn nữa, thiết bị xử lý thông tin 100 kết nối giữa các thành phần, ví dụ, bởi kênh truyền 170 làm đường dẫn truyền dữ liệu. Hơn nữa, thiết bị xử lý thông tin 100 được điều khiển, ví dụ, bằng công suất được cung cấp từ phần cấp điện bên trong như pin được chứa trong thiết bị xử lý thông tin 100 hoặc công suất được cung cấp từ phần cấp điện bên ngoài đã kết nối.

MPU 150 bao gồm một hoặc hai hoặc nhiều bộ xử lý, các mạch xử lý khác nhau, hoặc loại tương tự bao gồm mạch thao tác, ví dụ, bộ xử lý micrô (MPU) hoặc loại tương tự và có chức năng như bộ điều khiển 106 mà điều khiển toàn bộ thiết bị xử lý thông tin 100. Hơn nữa, MPU 150 đóng vai trò như, ví dụ, bộ xử lý 110 được mô tả sau đây trong thiết bị xử lý thông tin 100.

ROM 152 lưu trữ, ví dụ, dữ liệu điều khiển như là chương trình cần được sử dụng bởi MPU 150 và tham số thao tác. RAM 154 tạm thời lưu trữ, ví dụ,

chương trình cần được thực hiện bởi MPU 150, hoặc loại tương tự.

Phương tiện ghi 156 là phương tiện ghi đơn lẻ mà có chức năng như bộ lưu trữ (không được minh họa). Phương tiện ghi 156 lưu trữ, ví dụ, dữ liệu khác nhau như là các ứng dụng khác nhau. Ở đây, đối với phương tiện ghi 156, ví dụ, phương tiện ghi từ tính như là đĩa cứng, bộ nhớ bất biến như là bộ nhớ chớp, hoặc loại tương tự được minh họa. Hơn nữa, phương tiện ghi 156 có thể tách được khỏi thiết bị xử lý thông tin 100.

Giao diện đầu vào/đầu ra 158 kết nối với, ví dụ, thiết bị nhập thao tác 160 và thiết bị hiển thị 162. Thiết bị nhập thao tác 160 có chức năng như bộ thao tác (không được minh họa). Hơn nữa, thiết bị hiển thị 162 có chức năng như bộ hiển thị (không được minh họa). Ở đây, đối với giao diện đầu vào/đầu ra 158, ví dụ, đầu cuối kênh truyền chuỗi toàn cầu (USB), đầu cuối giao diện trực quan kỹ thuật số (DVI), đầu cuối giao diện đa phương tiện độ phân giải cao (HDMI) (nhãn hiệu đã được đăng ký), các mạch xử lý khác nhau, hoặc loại tương tự được minh họa.

Hơn nữa, thiết bị nhập thao tác 160, ví dụ, được chứa trong thiết bị xử lý thông tin 100 và được kết nối với giao diện đầu vào/đầu ra 158 trong thiết bị xử lý thông tin 100. Đối với thiết bị nhập thao tác 160, ví dụ, nút, khóa định hướng, bộ lựa chọn xoay như là quay số chạy bộ, hoặc kết hợp của chúng, hoặc loại tương tự được minh họa.

Hơn nữa, thiết bị hiển thị 162, ví dụ, được chứa trong thiết bị xử lý thông tin 100 và được kết nối với giao diện đầu vào/đầu ra 158 trong thiết bị xử lý thông tin 100. Đối với thiết bị hiển thị 162, ví dụ, hiển thị tinh thể lỏng, hiển thị EL hữu cơ, hoặc loại tương tự được minh họa.

Lưu ý rằng hiển nhiên là giao diện đầu vào/đầu ra 158 có thể được kết nối với thiết bị phía ngoài như là thiết bị nhập thao tác bên ngoài (ví dụ, bàn phím, chuột, hoặc loại tương tự), thiết bị hiển thị bên ngoài, hoặc loại tương tự như thiết bị phía ngoài của thiết bị xử lý thông tin 100. Hơn nữa, thiết bị hiển thị 162 có thể là thiết bị mà có thể thực hiện việc hiển thị và thao tác người dùng, ví dụ, màn chạm hoặc loại tương tự.

Giao diện truyền thông 164 là bộ truyền thông mà được chứa trong thiết bị xử lý thông tin 100 và thực hiện truyền thông bằng cách sử dụng phương pháp truyền thông đơn lẻ, và có chức năng như bộ truyền thông thứ nhất 102. Ở đây,

đối với giao diện truyền thông 164, ví dụ, anten truyền thông và mạch tần số vô tuyến (RF) (truyền thông không dây), cổng IEEE802.15.1 và mạch truyền và thu (truyền thông không dây), cổng IEEE802.11 và mạch truyền và thu (truyền thông không dây), thiết bị đầu cuối LAN và mạch truyền và thu (truyền thông có dây), hoặc loại tương tự được minh họa.

Chip IC 166 và anten 168 là các bộ truyền thông, mà thực hiện truyền thông bằng cách sử dụng phương pháp truyền thông khác, được chứa trong thiết bị xử lý thông tin 100 và có chức năng như bộ truyền thông thứ hai 104. Chip IC 166 và anten 168 thực hiện truyền thông bởi NFC với thiết bị phía ngoài mà có chức năng của bộ đọc/bộ ghi như là bộ đọc/bộ ghi 200 bằng cách sử dụng sóng mang mà có tần số định trước, ví dụ, 13,56 [MHz] hoặc loại tương tự.

Anten 168 có vai trò để thu sóng mang và truyền tín hiệu phản hồi. Hơn nữa, chip IC 166 giải điều chế và xử lý tín hiệu sóng mang được truyền từ thiết bị phía ngoài như là bộ đọc/bộ ghi 200 trên cơ sở của sóng mang được thu và truyền tín hiệu phản hồi bởi sự điều chế tải.

Fig.4 là sơ đồ giải thích minh họa ví dụ các cấu trúc của chip IC 166 và anten 168 được minh họa trên Fig.3. Lưu ý rằng không cần thiết cho thiết bị xử lý thông tin 100 bao gồm cấu trúc của chip IC 166 được minh họa trên Fig.3 theo khuôn dạng của chip IC theo chẳng hạn.

Anten 168 bao gồm, ví dụ, bộ cộng hưởng bao gồm cuộn (cuộn cảm) L1 mà có điện cảm suất định trước và tụ điện C1 mà có điện dung định trước và tạo ra điện áp cảm ứng bởi cảm ứng điện từ để phản hồi việc thu sóng mang. Sau đó, anten 168 xuất ra điện áp thu thu được bằng cách cho cộng hưởng điện áp cảm ứng ở tần số cộng hưởng định trước. Ở đây, tần số cộng hưởng của anten 168 được thiết đặt theo tần số của sóng mang, ví dụ, 13,56 [MHz] hoặc loại tương tự. Với cấu trúc trên, anten 168 thu sóng mang và còn truyền tín hiệu phản hồi bởi sự điều chế tải được thực hiện bởi mạch điều chế tải 182 được chứa trong chip IC 166.

Chip IC 166 bao gồm, ví dụ, mạch phát hiện sóng mang 172, mạch phát hiện 174, bộ điều chỉnh 176, mạch giải điều chế 178, MPU 180, và mạch điều chế tải 182. Lưu ý rằng, mặc dù không được minh họa trên Fig.4, chip IC 166 có thể còn bao gồm, ví dụ, mạch bảo vệ (không được minh họa) mà ngăn việc sử dụng điện áp quá tải hoặc dòng điện quá tải cho MPU 180. Ở đây, đối với mạch

bảo vệ (không được minh họa), ví dụ, mạch kẹp bao gồm điôt hoặc loại tương tự được minh họa.

Hơn nữa, chip IC 166 bao gồm, ví dụ, ROM 184, RAM 186, và bộ nhớ bất biến 188. MPU 180, ROM 184, RAM 186, và bộ nhớ bất biến 188 được kết nối, ví dụ, bởi kênh truyền 190 làm đường dẫn truyền dữ liệu. Hơn nữa, kênh truyền 190 được kết nối với kênh truyền 170.

ROM 184 lưu trữ dữ liệu điều khiển như là chương trình cần được sử dụng bởi MPU 180 và tham số thao tác. RAM 186 tạm thời lưu trữ chương trình cần được thực hiện bởi MPU 180, kết quả thao tác, trạng thái thực hiện, hoặc loại tương tự.

Bộ nhớ bất biến 188 là một phương tiện ghi khác mà có chức năng như bộ lưu trữ (không được minh họa). Bộ nhớ bất biến 188 lưu trữ dữ liệu khác nhau, ví dụ, dữ liệu liên quan đến phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 như là "thông tin khóa chỉ báo khóa mã hóa mật được sử dụng cho việc xử lý liên quan đến sự mã hóa mật tùy ý và giải mã mật ở thời điểm xác thực trong truyền thông bằng cách sử dụng phương pháp truyền thông như là NFC", thông tin thiết đặt (được mô tả sau đây), hoặc loại tương tự, giá trị điện tử (dữ liệu có tiền hoặc giá trị tương đương với tiền), thông tin nhận dạng tùy ý như là ID của thiết bị xử lý thông tin 100, ID của dịch vụ, hoặc loại tương tự, dữ liệu tương ứng với các dịch vụ khác nhau, các ứng dụng khác nhau, hoặc loại tương tự. Đối với khóa mã hóa mật được chỉ báo bởi thông tin khóa, ví dụ, khóa mã hóa tương ứng với phương pháp mã hóa mật tùy ý như là phương pháp mã hóa mật dùng khóa chung hoặc phương pháp mã hóa mật dùng khóa công cộng được minh họa. Ở đây, đối với bộ nhớ bất biến 188, ví dụ, bộ nhớ chỉ đọc khả trình và xóa được bằng điện (EEPROM), bộ nhớ chớp, hoặc loại tương tự được minh họa. Bộ nhớ bất biến 188, ví dụ, chống trộm và tương ứng với ví dụ của phương tiện ghi bảo mật.

Mạch phát hiện sóng mang 172 tạo ra, ví dụ, tín hiệu phát hiện chữ nhật trên cơ sở của điện áp thu được truyền từ anten 168 và truyền tín hiệu phát hiện đến MPU 180. Hơn nữa, MPU 180 sử dụng tín hiệu phát hiện được truyền, ví dụ, làm đồng hồ xử lý để xử lý dữ liệu. Ở đây, vì tín hiệu phát hiện dựa trên điện áp thu được truyền từ anten 168, tín hiệu phát hiện được đồng bộ với tần số của sóng mang được truyền từ thiết bị phía ngoài như là bộ đọc/bộ ghi 200. Do đó,

chip IC 166 bao gồm mạch phát hiện sóng mang 172 để thực hiện việc xử lý với thiết bị phía ngoài như là bộ đọc/bộ ghi 200 khi đồng bộ với thiết bị phía ngoài.

Mạch phát hiện 174 chỉnh lưu điện áp thu xuất ra từ anten 168. Ở đây, mạch phát hiện 174 bao gồm, ví dụ, điốt D1 và tụ điện C2.

Bộ quản lý 176 làm mịn và ổn định điện áp thu và xuất ra điện áp dẫn động cho MPU 180. Ở đây, bộ quản lý 176 sử dụng thành phần DC của điện áp thu làm điện áp dẫn động.

Mạch giải điều chế 178 giải điều chế tín hiệu sóng mang trên cơ sở của điện áp thu và xuất ra dữ liệu tương ứng với tín hiệu sóng mang được chứa trong sóng mang (ví dụ, tín hiệu dữ liệu nhị phân của mức cao và mức thấp). Ở đây, mạch giải điều chế 178 xuất ra thành phần AC của điện áp thu làm dữ liệu.

MPU 180 được dẫn động bằng cách sử dụng điện áp dẫn động xuất ra từ bộ quản lý 176 làm nguồn điện và xử lý dữ liệu được giải điều chế bởi mạch giải điều chế 178. Ở đây, MPU 180 bao gồm một hoặc hai hoặc nhiều bộ xử lý, các mạch xử lý khác nhau, hoặc loại tương tự, ví dụ, đều bao gồm mạch thao tác như là MPU.

Hơn nữa, MPU 180 tạo ra tín hiệu điều khiển được sử dụng để điều khiển sự điều chế tải liên quan đến sự phản hồi thiết bị phía ngoài như là bộ đọc/bộ ghi 200 theo kết quả xử lý. Sau đó, MPU 180 xuất ra tín hiệu điều khiển cho mạch điều chế tải 182.

Mạch điều chế tải 182 bao gồm, ví dụ, tải Z và bộ chuyển mạch SW1 và thực hiện sự điều chế tải để kết nối có chọn lọc (xác nhận) tải Z theo tín hiệu điều khiển được truyền từ MPU 180. Ở đây, tải Z bao gồm, ví dụ, kháng trở có giá trị kháng trở định trước. Hơn nữa, bộ chuyển mạch SW1 bao gồm, ví dụ, tranzito hiệu ứng trường bán dẫn oxit kim loại kênh p (MOSFET) và MOSFET kênh n.

Với cấu trúc trên, chip IC 166 xử lý tín hiệu sóng mang được thu bởi anten 168 và làm cho anten 168 truyền tín hiệu phản hồi bởi sự điều chế tải.

Ví dụ, bằng các bao gồm cấu trúc được minh họa trên Fig.4, chip IC 166 và anten 168 thực hiện truyền thông bằng NFC với thiết bị phía ngoài như là bộ đọc/bộ ghi 200 bằng cách sử dụng sóng mang có tần số định trước. Lưu ý rằng hiển nhiên rằng các cấu trúc của chip IC 166 và anten 168 theo phương án của

sáng chế không được giới hạn ở trong ví dụ được minh họa trên Fig.4.

Ví dụ, với cấu trúc phần cứng được minh họa trên Fig.3, thiết bị xử lý thông tin 100 truyền thông với thiết bị phía ngoài như là bộ đọc/bộ ghi 200. Hơn nữa, ví dụ, với cấu trúc phần cứng được minh họa trên Fig.3, thiết bị xử lý thông tin 100 thực hiện xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 được mô tả sau đây. Lưu ý rằng cấu trúc phần cứng của thiết bị xử lý thông tin 100 theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.3.

Ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự như của giao diện truyền thông 164 hoặc trong trường hợp cấu trúc mà không thực hiện truyền thông bằng cách sử dụng phương pháp truyền thông đơn lẻ, không cần thiết là thiết bị xử lý thông tin 100 bao gồm giao diện truyền thông 164.

Hơn nữa, ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự như của chip IC 166 và anten 168, không cần thiết là thiết bị xử lý thông tin 100 bao gồm chip IC 166 và anten 168.

Hơn nữa, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện bằng cách sử dụng phương pháp truyền thông ngoài NFC như là truyền thông không dây sử dụng IEEE 802.15.1, không cần thiết là thiết bị xử lý thông tin 100 bao gồm chip IC 166 và anten 168. Trong trường hợp trên, thiết bị xử lý thông tin 100 truyền thông với thiết bị phía ngoài bằng cách bao gồm thiết bị truyền thông tương thích với phương pháp truyền thông khác ngoài NFC hoặc bằng cách sử dụng thiết bị truyền thông bên ngoài tương thích với phương pháp truyền thông khác ngoài NFC.

Hơn nữa, ví dụ, thiết bị xử lý thông tin 100 có thể có cấu trúc mà không bao gồm một phần hoặc tất cả trong số phương tiện ghi 156, thiết bị nhập thao tác 160, và thiết bị hiển thị 162.

Hơn nữa, thiết bị xử lý thông tin 100 có thể có cấu trúc phần cứng, ví dụ, theo ví dụ ứng dụng của thiết bị xử lý thông tin 100 được mô tả sau đây. Theo ví dụ, trong trường hợp mà thiết bị xử lý thông tin 100, ví dụ, là thẻ IC, thiết bị xử lý thông tin 100 có thể bao gồm chip IC 166 và anten 168. Trong trường hợp mà thiết bị xử lý thông tin 100 là thẻ IC, ví dụ, MPU 180 cấu hình chip IC 166 thực

hiện xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 được mô tả sau đây.

Hơn nữa, ví dụ, cấu trúc được minh họa trên Fig.3 (hoặc cấu trúc theo biến thể) có thể được nhận biết bởi một hoặc hai hoặc nhiều mạch tích hợp (IC).

Viện dẫn lại tới Fig.2, ví dụ về cấu trúc của thiết bị xử lý thông tin 100 sẽ được mô tả. Bộ truyền thông thứ nhất 102 truyền thông với thiết bị phía ngoài bởi truyền thông sử dụng phương pháp truyền thông đơn lẻ. Sự truyền thông của bộ truyền thông thứ nhất 102 được điều khiển bởi bộ điều khiển 106 theo chẳng hạn.

Ở đây, đối với bộ truyền thông thứ nhất 102, ví dụ, anten truyền thông và mạch RF(truyền thông không dây), cổng IEEE802.15.1 và mạch truyền và thu (truyền thông không dây), cổng IEEE802.11 và mạch truyền và thu (truyền thông không dây), thiết bị đầu cuối LAN và mạch truyền và thu (truyền thông có dây), hoặc loại tương tự được minh họa.

[0070]

Bộ truyền thông thứ hai 104 truyền thông với thiết bị phía ngoài bởi truyền thông sử dụng phương pháp truyền thông khác. Sự truyền thông của bộ truyền thông thứ hai 104 được điều khiển bởi bộ điều khiển 106 theo chẳng hạn.

Ở đây, đối với bộ truyền thông thứ hai 104, ví dụ, thiết bị truyền thông tương thích với NFC như là chip IC 166 và anten 168 được minh họa trên Fig.3 được minh họa. Lưu ý rằng, như được mô tả ở trên, bộ truyền thông thứ hai 104 có thể là thiết bị truyền thông mà tương thích với phương pháp truyền thông khác ngoài NFC, ví dụ, truyền thông không dây sử dụng IEEE 802.15.1 hoặc loại tương tự.

Bộ điều khiển 106 bao gồm, ví dụ, MPU hoặc loại tương tự và đóng vai trò điều khiển toàn bộ thiết bị xử lý thông tin 100. Hơn nữa, bộ điều khiển 106 bao gồm, ví dụ, bộ xử lý 110 và đóng vai trò dẫn dắt để thực hiện xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 được mô tả sau đây.

Bộ xử lý 110 đóng vai trò dẫn dắt để thực hiện xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100. Ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 sẽ được mô tả trong mỗi phương án được mô tả sau đây.

Lưu ý rằng cấu trúc của thiết bị xử lý thông tin (thiết bị xử lý thông tin thứ nhất) theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.2.

Ví dụ, thiết bị xử lý thông tin theo phương án của sáng chế một cách riêng biệt có thể bao gồm bộ xử lý 110 được minh họa trên Fig.2 từ bộ điều khiển 106 (ví dụ, để nhận biết bởi mạch xử lý khác).

Hơn nữa, cấu trúc của thiết bị xử lý thông tin theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.2, và thiết bị xử lý thông tin có thể có cấu trúc theo cách thức chia việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 được mô tả sau đây.

Hơn nữa, ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự như của bộ truyền thông thứ nhất 102 hoặc trong trường hợp của cấu trúc mà không thực hiện truyền thông bằng cách sử dụng phương pháp truyền thông đơn lẻ được mô tả nêu trên, không cần thiết là thiết bị xử lý thông tin theo phương án của sáng chế bao gồm bộ truyền thông thứ nhất 102.

Hơn nữa, ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự như của bộ truyền thông thứ hai 104, không cần thiết là thiết bị xử lý thông tin theo phương án của sáng chế bao gồm bộ truyền thông thứ hai 104.

[1-2] Bộ đọc/bộ ghi 200 (Thiết bị chuyển tiếp)

Fig.5 là sơ đồ khối chức năng minh họa ví dụ cấu trúc minh họa của bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp) theo phương án của sáng chế.

Bộ đọc/bộ ghi 200 bao gồm, ví dụ, bộ truyền thông thứ nhất 202, bộ truyền thông thứ hai 204, và bộ điều khiển 206.

Hơn nữa, bộ đọc/bộ ghi 200 có thể bao gồm, ví dụ, ROM (không được minh họa), RAM (không được minh họa), bộ lưu trữ (không được minh họa), bộ thao tác mà có thể được thao tác bởi người dùng (không được minh họa), bộ hiển thị (không được minh họa) mà hiển thị các màn hình khác nhau trên màn hình hiển thị, hoặc loại tương tự. Bộ đọc/bộ ghi 200 kết nối giữa các thành phần, ví dụ, bởi kênh truyền làm đường dẫn truyền dữ liệu.

ROM (không được minh họa) lưu trữ dữ liệu điều khiển như là chương

trình cần được sử dụng bởi bộ điều khiển 206 và tham số thao tác. RAM (không được minh họa) tạm thời lưu trữ chương trình được thực hiện bởi bộ điều khiển 206, hoặc loại tương tự.

Bộ lưu trữ (không được minh họa) là bộ lưu trữ được chứa trong bộ đọc/bộ ghi 200 và lưu trữ dữ liệu khác nhau, ví dụ, các ứng dụng khác nhau hoặc loại tương tự. Ở đây, đối với bộ lưu trữ (không được minh họa), ví dụ, phương tiện ghi từ tính như là đĩa cứng, bộ nhớ bất biến như là bộ nhớ chớp, hoặc loại tương tự được minh họa. Hơn nữa, bộ lưu trữ (không được minh họa) có thể tách được từ bộ đọc/bộ ghi 200.

Đối với bộ thao tác (không được minh họa), thiết bị nhập thao tác tương tự với thiết bị nhập thao tác 160 được minh họa trên Fig.3 được minh họa. Hơn nữa, đối với bộ hiển thị (không được minh họa), thiết bị hiển thị tương tự với thiết bị hiển thị 162 được minh họa trên Fig.3 được minh họa.

[Cấu trúc phần cứng ví dụ của bộ đọc/bộ ghi 200]

Fig.6 là sơ đồ giải thích minh họa cấu trúc phần cứng minh họa của bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp) theo phương án của sáng chế.

Bộ đọc/bộ ghi 200 bao gồm, ví dụ, MPU 250, ROM 252, RAM 254, phương tiện ghi 256, giao diện truyền thông 258, mạch truyền sóng mang 260, và anten 262. Hơn nữa, bộ đọc/bộ ghi 200 kết nối giữa các thành phần, ví dụ, bởi kênh truyền 264 làm đường dẫn truyền dữ liệu. Hơn nữa, bộ đọc/bộ ghi 200 được dẫn động, ví dụ, bằng công suất được lấy từ phần cấp điện bên trong như là pin được chứa trong bộ đọc/bộ ghi 200, công suất được lấy từ phần cấp điện bên ngoài đã kết nối, hoặc loại tương tự.

MPU 250 bao gồm một hoặc hai hoặc nhiều bộ xử lý, các mạch xử lý khác nhau, hoặc loại tương tự đều bao gồm mạch thao tác, ví dụ, MPU hoặc loại tương tự và có chức năng như bộ điều khiển 206 mà điều khiển toàn bộ bộ đọc/bộ ghi 200. Hơn nữa, MPU 250 đóng vai trò như, ví dụ, bộ xử lý 210 được mô tả sau đây trong bộ đọc/bộ ghi 200.

ROM 252 lưu trữ, ví dụ, dữ liệu điều khiển như là chương trình cần được sử dụng bởi MPU 250 và tham số thao tác. RAM 254 tạm thời lưu trữ, ví dụ, chương trình cần được thực hiện bởi MPU 250, hoặc loại tương tự.

Phương tiện ghi 256 có chức năng như bộ lưu trữ (không được minh họa)

và lưu trữ, ví dụ, dữ liệu khác nhau như là các ứng dụng khác nhau. Ở đây, đối với phương tiện ghi 256, ví dụ, phương tiện ghi từ tính như là đĩa cứng, bộ nhớ bất biến như là bộ nhớ chớp, hoặc loại tương tự được minh họa. Hơn nữa, phương tiện ghi 256 có thể tách được từ bộ đọc/bộ ghi 200.

Giao diện truyền thông 258 là bộ truyền thông mà được chứa trong bộ đọc/bộ ghi 200 và thực hiện truyền thông nhờ sử dụng phương pháp truyền thông đơn lẻ, và có chức năng như bộ truyền thông thứ nhất 202 mà truyền thông không dây hoặc có dây với thiết bị phía ngoài như là máy chủ 300 qua mạng (hoặc trực tiếp). Ở đây, đối với giao diện truyền thông 258, ví dụ, anten truyền thông và mạch RF (truyền thông không dây), cổng IEEE802.15.1 và mạch truyền và thu (truyền thông không dây), cổng IEEE802.11 và mạch truyền và thu (truyền thông không dây), thiết bị đầu cuối LAN và mạch truyền và thu (truyền thông có dây), hoặc loại tương tự được minh họa. Hơn nữa, giao diện truyền thông 258 có thể có cấu trúc bất kỳ tương thích với mạng theo phương án của sáng chế.

Mạch truyền sóng mang 260 và anten 262 là các bộ truyền thông mà được chứa trong bộ đọc/bộ ghi 200 và thực hiện truyền thông nhờ sử dụng phương pháp truyền thông khác và có chức năng như bộ truyền thông thứ hai 204 mà truyền thông không dây hoặc có dây với thiết bị phía ngoài như là thiết bị xử lý thông tin 100.

Anten 262 bao gồm, ví dụ, bộ cộng hưởng mà bao gồm cuộn cảm có điện cảm suất định trước như anten truyền/thu và tụ điện có điện dung định trước và mạch giải điều chế. Sau đó, bằng cách thu sóng mang có tần số định trước, ví dụ, 13,56 [MHz] hoặc loại tương tự, anten 262 giải điều chế, ví dụ, dữ liệu được truyền từ thiết bị phía ngoài như là thiết bị xử lý thông tin 100 bởi sự điều chế tải hoặc loại tương tự. Lưu ý rằng, ví dụ, trong trường hợp mà mạch truyền sóng mang 260 bao gồm mạch giải điều chế, anten 262 có thể bao gồm bộ cộng hưởng.

Mạch truyền sóng mang 260 bao gồm, ví dụ, mạch điều chế mà thực hiện sự điều chế như là Khóa thay đổi biên độ (ASK) và mạch khuếch đại mà khuếch đại đầu ra của mạch điều chế và truyền sóng mang mà tín hiệu sóng mang được sử dụng từ anten truyền/thu của anten 262. Hơn nữa, mạch truyền sóng mang 260 có thể bao gồm, ví dụ, mạch giải điều chế mà giải điều chế tín hiệu được thu

bởi anten 262. Mạch giải điều chế giải điều chế, ví dụ, tín hiệu được thu bởi anten 262 bằng cách thực hiện phát hiện đường bao trên thay đổi biên độ của điện áp giữa mạch điều chế (hoặc mạch khuếch đại) và bộ cộng hưởng của anten 262 và thực hiện nhị phân tín hiệu được phát hiện. Lưu ý rằng mạch giải điều chế có thể giải điều chế tín hiệu được thu bởi anten 262, ví dụ, bằng cách sử dụng thay đổi pha của điện áp giữa mạch điều chế (hoặc mạch khuếch đại) và bộ cộng hưởng của anten 262.

Bằng cách bao gồm mạch truyền sóng mang 260, bộ đọc/bộ ghi 200 có chức năng khởi tạo trong NFC và đóng vai trò như bộ đọc/bộ ghi. Ở đây, đối với tín hiệu sóng mang được truyền bởi mạch truyền sóng mang 260 từ anten 262, ví dụ, các tín hiệu khác nhau như là tín hiệu mời gửi, tín hiệu chỉ báo yêu cầu đọc được mô tả sau đây, hoặc loại tương tự được minh họa. Hơn nữa, trong mạch truyền sóng mang 260, ví dụ, MPU 250 điều khiển việc truyền của sóng mang.

Ví dụ, bằng cách bao gồm cấu trúc phần cứng được minh họa trên Fig.6, bộ đọc/bộ ghi 200 đóng vai trò như thiết bị chuyển tiếp. Lưu ý rằng cấu trúc phần cứng của bộ đọc/bộ ghi 200 theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.6.

Ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng tương tự như của giao diện truyền thông 258, không cần thiết là bộ đọc/bộ ghi 200 bao gồm giao diện truyền thông 258.

Hơn nữa, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng tương tự với mạch truyền sóng mang 260 và anten 262, không cần thiết là bộ đọc/bộ ghi 200 bao gồm mạch truyền sóng mang 260 và anten 262.

Hơn nữa, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện bằng cách sử dụng phương pháp truyền thông khác ngoài NFC như là truyền thông không dây sử dụng IEEE 802.15.1, không cần thiết là bộ đọc/bộ ghi 200 bao gồm mạch truyền sóng mang 260 và anten 262. Trong trường hợp trên, bộ đọc/bộ ghi 200 truyền thông với thiết bị phía ngoài bằng cách bao gồm thiết bị truyền thông tương thích với phương pháp truyền thông khác ngoài NFC hoặc bằng cách sử dụng thiết bị truyền thông bên ngoài tương thích với phương pháp truyền thông khác ngoài NFC.

Hơn nữa, bộ đọc/bộ ghi 200 có thể có, ví dụ cấu trúc mà không bao gồm phương tiện ghi 256.

Hơn nữa, bộ đọc/bộ ghi 200 có thể có cấu trúc phần cứng, ví dụ, theo ví dụ ứng dụng của bộ đọc/bộ ghi 200 được mô tả sau đây.

Hơn nữa, ví dụ, cấu trúc được minh họa trên Fig.6 (hoặc cấu trúc theo biến thể) có thể được nhận biết bởi một hoặc hai hoặc nhiều IC.

Viện dẫn lại tới Fig.5, ví dụ về cấu trúc của bộ đọc/bộ ghi 200 sẽ được mô tả.

Bộ truyền thông thứ nhất 202 truyền thông với thiết bị phía ngoài bởi truyền thông sử dụng phương pháp truyền thông đơn lẻ. Sự truyền thông của bộ truyền thông thứ nhất 202 sử dụng phương pháp truyền thông đơn lẻ được điều khiển bởi, ví dụ, bộ điều khiển 206.

Ở đây, đối với bộ truyền thông thứ nhất 202, ví dụ, anten truyền thông và mạch RF(truyền thông không dây), cổng IEEE802.15.1 và mạch truyền và thu (truyền thông không dây), cổng IEEE802.11 và mạch truyền và thu (truyền thông không dây), thiết bị đầu cuối LAN và mạch truyền và thu (truyền thông có dây), hoặc loại tương tự được minh họa.

Bộ truyền thông thứ hai 204 truyền thông với thiết bị phía ngoài bởi truyền thông sử dụng phương pháp truyền thông khác. Sự truyền thông của bộ truyền thông thứ hai 204 sử dụng phương pháp truyền thông khác được điều khiển bởi, ví dụ, bộ điều khiển 206.

Ở đây, đối với bộ truyền thông thứ hai 204, ví dụ, thiết bị truyền thông tương thích với NFC như là mạch truyền sóng mang 260 và anten 262 được minh họa trên Fig.6 được minh họa. Lưu ý rằng, như được mô tả ở trên, bộ truyền thông thứ hai 204 có thể là thiết bị truyền thông mà tương thích với phương pháp truyền thông khác ngoài NFC, ví dụ, truyền thông không dây sử dụng IEEE 802.15.1 hoặc loại tương tự.

Bộ điều khiển 206 bao gồm, ví dụ, MPU hoặc loại tương tự và đóng vai trò điều khiển toàn bộ bộ đọc/bộ ghi 200. Hơn nữa, bộ điều khiển 206 có thể bao gồm bộ xử lý 210 mà có thể thực hiện xử lý tùy ý, ví dụ, xử lý điều khiển truyền thông, xử lý quyết toán, hoặc loại tương tự.

Lưu ý rằng cấu trúc của bộ đọc/bộ ghi (thiết bị chuyển tiếp) theo phương án

của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.5.

Ví dụ, bộ đọc/bộ ghi theo phương án của sáng chế một cách riêng biệt có thể bao gồm bộ xử lý 210 được minh họa trên Fig.2 từ bộ điều khiển 206 (ví dụ, để nhận biết bởi mạch xử lý khác).

Hơn nữa, ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự với bộ truyền thông thứ nhất 202, không cần thiết là bộ đọc/bộ ghi theo phương án của sáng chế bao gồm bộ truyền thông thứ nhất 202.

Hơn nữa, ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự với bộ truyền thông thứ hai 204, không cần thiết là bộ đọc/bộ ghi theo phương án của sáng chế bao gồm bộ truyền thông thứ hai 204.

[1-3] Máy chủ 300 (Thiết bị xử lý thông tin thứ hai)

Fig.7 là sơ đồ khối chức năng minh họa cấu trúc minh họa của máy chủ 300 (thiết bị xử lý thông tin thứ hai) theo phương án của sáng chế. Máy chủ 300 bao gồm, ví dụ, bộ truyền thông 302 và bộ điều khiển 304. Hơn nữa, máy chủ 300 có thể, ví dụ, bao gồm ROM (không được minh họa), RAM (không được minh họa), bộ lưu trữ (không được minh họa), bộ thao tác mà có thể được thao tác bởi người dùng của máy chủ 300 (không được minh họa), bộ hiển thị (không được minh họa) mà hiển thị các màn hình khác nhau trên màn hình hiển thị, hoặc loại tương tự. Máy chủ 300 kết nối giữa các thành phần, ví dụ, bởi kênh truyền làm đường dẫn truyền dữ liệu.

ROM (không được minh họa) lưu trữ dữ liệu điều khiển như là chương trình cần được sử dụng bởi bộ điều khiển 304 và tham số thao tác. RAM (không được minh họa) tạm thời lưu trữ chương trình được thực hiện bởi bộ điều khiển 304, hoặc loại tương tự.

Bộ lưu trữ (không được minh họa) là bộ lưu trữ được chứa trong máy chủ 300 và lưu trữ dữ liệu khác nhau, ví dụ, dữ liệu liên quan đến phương pháp xử lý thông tin bởi máy chủ 300, các ứng dụng khác nhau, hoặc loại tương tự. Ở đây, đối với bộ lưu trữ (không được minh họa), ví dụ, phương tiện ghi từ tính như là đĩa cứng, bộ nhớ bất biến như là bộ nhớ chớp, hoặc loại tương tự được minh họa. Hơn nữa, bộ lưu trữ (không được minh họa) có thể tách được từ máy chủ 300.

Đối với bộ thao tác (không được minh họa), thiết bị nhập thao tác được chỉ báo trong cấu trúc phần cứng minh họa của máy chủ 300 được mô tả sau đây được minh họa. Hơn nữa, đối với bộ hiển thị (không được minh họa), thiết bị hiển thị được chỉ báo trong cấu trúc phần cứng minh họa của máy chủ 300 được mô tả sau đây được minh họa.

[Cấu trúc phần cứng ví dụ của máy chủ 300]

Fig.8 là sơ đồ giải thích minh họa cấu trúc phần cứng minh họa của máy chủ 300 (thiết bị xử lý thông tin thứ hai) theo phương án của sáng chế. Máy chủ 300 bao gồm, ví dụ, MPU 350, ROM 352, RAM 354, phương tiện ghi 356, giao diện đầu vào/đầu ra 358, thiết bị nhập thao tác 360, thiết bị hiển thị 362, và giao diện truyền thông 364. Hơn nữa, máy chủ 300 kết nối giữa các thành phần, ví dụ, bởi kênh truyền 366 làm đường dẫn truyền dữ liệu. Hơn nữa, máy chủ 300 được dẫn động, ví dụ, bằng công suất được lấy từ phần cấp điện bên trong như là pin được chứa trong máy chủ 300, công suất được lấy từ phần cấp điện bên ngoài đã kết nối, hoặc loại tương tự.

MPU 350 bao gồm một hoặc hai hoặc nhiều bộ xử lý, các mạch xử lý khác nhau, hoặc loại tương tự đều bao gồm mạch thao tác, ví dụ, MPU hoặc loại tương tự và có chức năng như bộ điều khiển 304 mà điều khiển toàn bộ máy chủ 300. Hơn nữa, MPU 350 đóng vai trò như, ví dụ, bộ xử lý 310 được mô tả sau đây trong máy chủ 300. Lưu ý rằng bộ xử lý 310 có thể bao gồm mạch dành riêng (hoặc mục đích chung) (ví dụ, bộ xử lý khác với MPU 350, hoặc loại tương tự).

ROM 352 lưu trữ, ví dụ, dữ liệu điều khiển như là chương trình cần được sử dụng bởi MPU 350 và tham số thao tác. RAM 354 tạm thời lưu trữ, ví dụ, chương trình cần được thực hiện bởi MPU 350, hoặc loại tương tự.

Phương tiện ghi 356 có chức năng như bộ lưu trữ (không được minh họa) và lưu trữ dữ liệu khác nhau, ví dụ, dữ liệu liên quan đến phương pháp xử lý thông tin bởi máy chủ 300, các ứng dụng khác nhau, hoặc loại tương tự. Ở đây, đối với phương tiện ghi 356, ví dụ, phương tiện ghi từ tính như là đĩa cứng, bộ nhớ bất biến như là bộ nhớ chớp, hoặc loại tương tự được minh họa. Hơn nữa, phương tiện ghi 356 có thể tách được từ máy chủ 300.

Giao diện đầu vào/đầu ra 358 kết nối với, ví dụ, thiết bị nhập thao tác 360 và thiết bị hiển thị 362. Thiết bị nhập thao tác 360 có chức năng như bộ thao tác

(không được minh họa). Hơn nữa, thiết bị hiển thị 362 có chức năng như bộ hiển thị (không được minh họa). Ở đây, đối với giao diện đầu vào/đầu ra 358, ví dụ, đầu cuối USB, đầu cuối DVI, đầu cuối HDMI (nhãn hiệu đã đăng ký), các mạch xử lý khác nhau, hoặc loại tương tự được minh họa.

Hơn nữa, thiết bị nhập thao tác 360, ví dụ, được chứa trong máy chủ 300 và được kết nối với giao diện đầu vào/đầu ra 358 trong máy chủ 300. Đối với thiết bị nhập thao tác 360, ví dụ, nút, khóa định hướng, bộ lựa chọn xoay như là quay số chạy bộ, hoặc kết hợp của chúng, hoặc loại tương tự được minh họa.

Hơn nữa, thiết bị hiển thị 362, ví dụ, được chứa trong máy chủ 300 và được kết nối với giao diện đầu vào/đầu ra 358 trong máy chủ 300. Đối với thiết bị hiển thị 362, ví dụ, hiển thị tinh thể lỏng, hiển thị EL hữu cơ, hoặc loại tương tự được minh họa.

Lưu ý rằng hiển nhiên là giao diện đầu vào/đầu ra 358 có thể được kết nối với thiết bị phía ngoài như là thiết bị nhập thao tác (ví dụ, bàn phím, chuột, và loại tương tự) bên ngoài máy chủ 300 hoặc thiết bị hiển thị bên ngoài. Hơn nữa, thiết bị hiển thị 362 có thể là thiết bị mà có thể thực hiện việc hiển thị và thao tác người dùng, ví dụ, màn chạm hoặc loại tương tự.

Giao diện truyền thông 364 là bộ truyền thông được chứa trong máy chủ 300 và có chức năng như bộ truyền thông 302 mà truyền thông không dây hoặc có dây với thiết bị phía ngoài như là bộ đọc/bộ ghi 200 qua mạng (hoặc trực tiếp). Ở đây, đối với giao diện truyền thông 364, ví dụ, anten truyền thông và mạch RF (truyền thông không dây), cổng IEEE802.15.1 và mạch truyền và thu (truyền thông không dây), cổng IEEE802.11 và mạch truyền và thu (truyền thông không dây), thiết bị đầu cuối LAN và mạch truyền và thu (truyền thông có dây), hoặc loại tương tự được minh họa. Hơn nữa, giao diện truyền thông 364 có thể có cấu trúc bất kỳ tương thích với mạng theo phương án của sáng chế.

Ví dụ, với cấu trúc phần cứng được minh họa trên Fig.8, máy chủ 300 thực hiện xử lý theo phương pháp xử lý thông tin bởi máy chủ 300 được mô tả sau đây. Lưu ý rằng cấu trúc phần cứng của máy chủ 300 theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.8.

Ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài hoặc loại tương tự được thực hiện qua thiết bị truyền thông bên ngoài đã được kết nối, không cần thiết là máy chủ 300 bao gồm giao diện truyền thông 364. Hơn nữa,

giao diện truyền thông 364 có thể có cấu trúc mà có thể truyền thông với, ví dụ, một hoặc hai hoặc nhiều thiết bị phía ngoài bằng cách sử dụng các phương pháp truyền thông.

Hơn nữa, ví dụ, máy chủ 300 có thể có cấu trúc mà không bao gồm một phần hoặc tất cả trong số phương tiện ghi 356, thiết bị nhập thao tác 360, và thiết bị hiển thị 362.

Hơn nữa, máy chủ 300 có thể có cấu trúc phần cứng, ví dụ, theo ví dụ ứng dụng của máy chủ 300 được mô tả sau đây.

Hơn nữa, ví dụ, một phần hoặc tất cả của cấu trúc phần cứng được minh họa trên Fig.8 (hoặc cấu trúc theo biến thể) có thể được nhân biết bởi một hoặc hai hoặc nhiều IC.

Viện dẫn lại tới Fig.7, ví dụ về cấu trúc của máy chủ 300 sẽ được mô tả. Bộ truyền thông 302 là bộ truyền thông được chứa trong máy chủ 300 và truyền thông không dây hoặc có dây với thiết bị phía ngoài như là bộ đọc/bộ ghi 200 qua mạng (hoặc trực tiếp). Hơn nữa, sự truyền thông của bộ truyền thông 302 được điều khiển bởi bộ điều khiển 304, chẳng hạn.

Ở đây, đối với bộ truyền thông 302, ví dụ, anten truyền thông, mạch RF, đầu cuối LAN, mạch truyền/thu, hoặc loại tương tự được minh họa. Tuy nhiên, cấu trúc của bộ truyền thông 302 không được giới hạn ở các loại được mô tả nêu trên. Ví dụ, bộ truyền thông 302 có thể có cấu trúc tương thích với tiêu chuẩn tùy ý mà có thể truyền thông với đầu cuối USB, đầu cuối truyền/thu, hoặc loại tương tự và cấu trúc tùy ý mà có thể truyền thông với thiết bị phía ngoài qua mạng. Hơn nữa, bộ truyền thông 302 có thể có cấu trúc mà có thể truyền thông với, ví dụ, một hoặc hai hoặc nhiều thiết bị phía ngoài bằng cách sử dụng các phương pháp truyền thông.

Bộ điều khiển 304 bao gồm, ví dụ, MPU hoặc loại tương tự và đóng vai trò điều khiển toàn bộ máy chủ 300. Hơn nữa, bộ điều khiển 304 bao gồm, ví dụ, bộ xử lý 310 và đóng vai trò dẫn dắt để thực hiện xử lý theo phương pháp xử lý thông tin bởi máy chủ 300 được mô tả sau đây.

Bộ xử lý 310 đóng vai trò dẫn dắt để thực hiện xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế bởi máy chủ 300. Ví dụ của việc xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế bởi máy chủ 300 sẽ được mô tả sau đây.

Lưu ý rằng cấu trúc của máy chủ (thiết bị xử lý thông tin thứ hai) theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.7.

Ví dụ, máy chủ theo phương án của sáng chế một cách riêng biệt có thể bao gồm bộ xử lý 310 được minh họa trên Fig.7 từ bộ điều khiển 304 (ví dụ, để nhận biết bởi mạch xử lý khác).

Hơn nữa, cấu trúc của máy chủ theo phương án của sáng chế không được giới hạn ở cấu trúc được minh họa trên Fig.7, và máy chủ có thể có cấu trúc theo cách thức chia việc xử lý theo phương pháp xử lý thông tin bởi máy chủ 300 được mô tả sau đây.

Hơn nữa, ví dụ, trong trường hợp mà truyền thông với thiết bị phía ngoài được thực hiện qua thiết bị truyền thông bên ngoài có chức năng và cấu trúc tương tự với bộ truyền thông 302, không cần thiết là máy chủ theo phương án của sáng chế bao gồm bộ truyền thông 302.

[1-4] Ví dụ ứng dụng của mỗi thiết bị được chứa trong hệ thống xử lý thông tin theo phương án của sáng chế

Thiết bị xử lý thông tin 100 (thiết bị xử lý thông tin thứ nhất) được mô tả nêu trên làm bộ phận của hệ thống xử lý thông tin theo phương án của sáng chế. Tuy nhiên, phương án của sáng chế không được giới hạn ở chế độ. Phương án của sáng chế có thể được áp dụng cho các thiết bị khác nhau mà có thể thực hiện xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 được mô tả sau đây, ví dụ, "thiết bị truyền thông như là điện thoại thông minh", "thẻ IC","thiết bị máy tính bảng", "máy chơi trò chơi", hoặc loại tương tự. Hơn nữa, phương án của sáng chế có thể được áp dụng cho, ví dụ, IC xử lý mà có thể kết hợp với thiết bị trên.

Hơn nữa, bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp) được mô tả là thành phần của hệ thống xử lý thông tin theo phương án của sáng chế. Tuy nhiên, phương án của sáng chế không được giới hạn ở chế độ. Phương án của sáng chế có thể được áp dụng cho thiết bị bất kỳ mà có chức năng chuyển tiếp sự truyền thông giữa các thiết bị, ví dụ, "bộ đọc/bộ ghi", "thiết bị mà có chức năng của bộ đọc/bộ ghi", "thiết bị truyền thông mà thực hiện truyền thông bởi truyền thông không dây sử dụng IEEE802.15.1 như là BLE hoặc loại tương tự", hoặc loại tương tự. Hơn nữa, phương án của sáng chế có thể được áp dụng cho, ví dụ, IC

xử lý mà có thể kết hợp với thiết bị trên.

[0141]

Hơn nữa, máy chủ 300 (thiết bị xử lý thông tin thứ hai) được mô tả là thành phần của hệ thống xử lý thông tin theo phương án của sáng chế. Tuy nhiên, phương án của sáng chế không được giới hạn ở chế độ. Phương án của sáng chế có thể được áp dụng cho các thiết bị khác nhau mà có thể thực hiện xử lý theo phương pháp xử lý thông tin bởi máy chủ 300 được mô tả sau đây, ví dụ, "máy tính như là máy tính cá nhân (PC) hoặc máy chủ", "thiết bị máy tính bảng", "thiết bị truyền thông như là điện thoại thông minh", "máy chơi trò chơi", hoặc loại tương tự. Hơn nữa, phương án của sáng chế có thể được áp dụng cho, ví dụ, IC xử lý mà có thể kết hợp với thiết bị trên.

Hơn nữa, máy chủ theo phương án của sáng chế có thể được áp dụng cho hệ thống xử lý trên cơ sở sự kết nối với mạng (hoặc truyền thông giữa các thiết bị), ví dụ, điện toán đám mây hoặc loại tương tự. Như ví dụ về hệ thống xử lý, ví dụ, "hệ thống mà trong đó một thiết bị được chứa trong hệ thống xử lý thực hiện một phần của xử lý theo phương pháp xử lý thông tin bởi máy chủ 300 được mô tả sau đây và một thiết bị khác được chứa trong hệ thống xử lý thực hiện xử lý khác ngoài một phần của xử lý ở trên theo phương pháp xử lý thông tin bởi máy chủ 300" hoặc loại tương tự được minh họa.

[2] Phương pháp xử lý thông tin theo phương án của sáng chế

Tiếp theo, việc xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế sẽ được mô tả bằng cách sử dụng hệ thống xử lý thông tin 1000 được minh họa trên Fig.1 làm chẳng hạn.

[2-1] Phương pháp xử lý thông tin theo phương án thứ nhất

[2-1-1] Phác thảo của hệ thống xử lý thông tin 1000 mà Phương pháp xử lý thông tin theo phương án thứ nhất được áp dụng

Như được mô tả ở trên, ví dụ, khi một thiết bị khác đọc dữ liệu mà cần ủy quyền để đọc và được lưu trữ trong một thiết bị, việc xác thực được thực hiện giữa một thiết bị và thiết bị khác, và dữ liệu được đọc sau khi xác thực được hoàn thành. Tức là, thiết bị khác đọc dữ liệu mà cần cấp quyền để đọc sau khi hoàn thành xác thực cho việc cấp quyền.

Ở đây, xác thực cho việc cấp quyền được thực hiện, ví dụ, bởi "phương

pháp truyền giá trị được coi là thử thách ngẫu nhiên (sau đây, được coi là "thử thách ngẫu nhiên") bởi một thiết bị, thực hiện thao tác bằng cách sử dụng khóa xác thực (khóa mã hóa mật được sử dụng cho sự xác thực) đối với giá trị bởi thiết bị khác, và truyền kết quả thao tác đến một thiết bị" (phương pháp thử thách và phản hồi).

Fig.9 là sơ đồ giải thích minh họa ví dụ truyền thông liên quan đến việc đọc dữ liệu sử dụng sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết. Fig.9 minh họa ví dụ về truyền thông bằng cách sử dụng sự truyền thông sử dụng NFC trong hệ thống xử lý thông tin mà có cấu trúc tương tự với hệ thống xử lý thông tin 1000 được minh họa trên Fig.1. Tức là, trong ví dụ được minh họa trên Fig.9, sự truyền thông bằng cách sử dụng NFC được thực hiện giữa thiết bị xử lý thông tin 10 và bộ đọc/bộ ghi 20, và truyền thông mạng được thực hiện giữa bộ đọc/bộ ghi 20 và máy chủ 30.

Thiết bị xử lý thông tin 10 truyền thử thách ngẫu nhiên đến bộ đọc/bộ ghi 20 (S10). Bộ đọc/bộ ghi 20 mà đã thu thử thách ngẫu nhiên được truyền từ thiết bị xử lý thông tin 10 trong bước S10 truyền thử thách ngẫu nhiên thu được đến máy chủ 30 (S12).

Máy chủ 30 mà đã thu thử thách ngẫu nhiên thực hiện thao tác định trước bằng cách sử dụng khóa xác thực (S14) và truyền kết quả thao tác đến bộ đọc/bộ ghi 20 (S16). Đối với thao tác định trước, xử lý để mã hóa mật thử thách ngẫu nhiên bằng cách sử dụng khóa xác thực được minh họa. Hơn nữa, kết quả thao tác được truyền từ máy chủ 30 trong bước S16 tương ứng với thử thách ngẫu nhiên được mã hóa mật.

Bộ đọc/bộ ghi 20 mà đã thu kết quả thao tác được truyền từ máy chủ 30 trong bước S16 truyền kết quả thao tác thu được đến thiết bị xử lý thông tin 10 (S18).

Thiết bị xử lý thông tin 10 mà đã thu kết quả thao tác được truyền từ bộ đọc/bộ ghi 20 trong bước S18 xác nhận kết quả thao tác thu được (S20). Sự xác nhận trong bước S20 bao gồm, ví dụ, "để giải mật mã kết quả thao tác thu được bằng cách sử dụng khóa mã hóa mật định trước và xác nhận xem có hay không việc giá trị được giải mã mật khớp với thử thách ngẫu nhiên" hoặc "để thực hiện thao tác giống như trong bước S14 bởi thiết bị xử lý thông tin 10 và xác nhận xem có hay không việc kết quả thao tác khớp với kết quả thao tác thu được".

Trong trường hợp mà được xác định trong bước S20 rằng kết quả xác nhận chỉ báo bình thường, thiết bị xử lý thông tin 10 xác thực rằng máy chủ 30 là thiết bị mà có quyền đọc. Tức là, việc xử lý trong các bước từ S10 đến S20 tương ứng với xử lý xác thực. sau đây, ví dụ về xử lý trong trường hợp mà sự xác thực được hoàn thành một cách bình thường trong bước S20 sẽ được mô tả.

Máy chủ 30 mà đã truyền kết quả thao tác trong bước S16 truyền yêu cầu đọc (S22). Yêu cầu đọc là, ví dụ, dữ liệu bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu được đọc.

Bộ đọc/bộ ghi 20 mà đã thu yêu cầu đọc được truyền từ máy chủ 30 trong bước S22 truyền yêu cầu đọc thu được đến thiết bị xử lý thông tin 10 (S24).

Thiết bị xử lý thông tin 10 mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 20 trong bước S26 đọc dữ liệu từ vùng của phương tiện ghi được chỉ báo bởi yêu cầu đọc và truyền dữ liệu được đọc (S26). Bộ đọc/bộ ghi 20 mà đã thu dữ liệu được truyền từ thiết bị xử lý thông tin 10 trong bước S26 truyền dữ liệu thu được đến máy chủ 30 (S28).

Dữ liệu được đọc bằng cách sử dụng sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết, ví dụ, như được minh họa trên Fig.9.

Trong trường hợp mà sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết được sử dụng, như được minh họa trên Fig.9, sự truyền thông liên quan đến việc đọc dữ liệu được thực hiện sau khi thực hiện truyền thông cho sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi. Do đó, trong trường hợp mà sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết được sử dụng, sự bảo mật liên quan đến việc đọc dữ liệu có thể được đảm bảo.

Tuy nhiên, trong trường hợp mà sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết được sử dụng, sự truyền thông liên quan đến việc đọc dữ liệu được thực hiện sau khi sự truyền thông liên quan đến sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi được thực hiện. Do đó, thời gian truyền thông bị kéo dài, và thời gian xử lý của toàn bộ hệ thống bị kéo dài.

Do đó, trong hệ thống xử lý thông tin 1000 (có thể được chỉ báo là "hệ thống xử lý thông tin 1000 theo phương án thứ nhất" sau đây) mà phương pháp xử lý thông tin theo phương án thứ nhất được áp dụng, sự xác thực bằng cách sử

dụng phương pháp thử thách và phản hồi đã biết không được thực hiện, và cả việc xác thực và việc đọc dữ liệu được thực hiện thông qua sự truyền thông liên quan đến việc đọc dữ liệu.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ nhất, bằng cách thực hiện việc xử lý trong thiết bị xử lý thông tin 100 được mô tả dưới đây (việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100), "để thực hiện cả việc xác thực và việc đọc dữ liệu qua sự truyền thông liên quan đến việc đọc dữ liệu" được nhận biết.

[2-1-2] Việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ nhất

Tiếp theo, ví dụ về việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ nhất sẽ được mô tả.

Trong trường hợp mà yêu cầu đọc được thu, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu tương ứng với vùng của phương tiện ghi được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Thiết bị xử lý thông tin 100 mã hóa mật dữ liệu bằng cách thực hiện thao tác bằng cách sử dụng phương pháp mã hóa mật tùy ý, ví dụ, tiêu chuẩn mã hóa mật dữ liệu (DES), tiêu chuẩn mã hóa mật nâng cao (AES), hoặc loại tương tự. Đối với phương tiện ghi mà thiết bị xử lý thông tin 100 đọc dữ liệu, ví dụ, phương tiện ghi có chống trộm như là bộ nhớ bất biến 188 được minh họa trên Fig.4 được minh họa. Sau đó, thiết bị xử lý thông tin 100 truyền dữ liệu được mã hóa mật.

Trong thiết bị xử lý thông tin 100, ví dụ, bộ xử lý 110 thực hiện việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 (việc xử lý tương tự áp dụng cho các phương án khác) như là việc xử lý để đọc dữ liệu tương ứng với yêu cầu đọc từ phương tiện ghi, việc xử lý để mã hóa mật dữ liệu đã được đọc, việc xử lý để làm cho thiết bị truyền thông truyền dữ liệu được mã hóa, hoặc loại tương tự.

Yêu cầu đọc theo phương án của sáng chế, ví dụ, là dữ liệu bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu được đọc.

Yêu cầu đọc có thể bao gồm các phần thông tin chỉ báo vùng, và thông tin chỉ báo vùng có thể chỉ báo các vùng. Tức là, một hoặc các phần dữ liệu có thể được đọc từ một hoặc các vùng để đáp lại yêu cầu đọc theo phương án của sáng

chế.

Lưu ý rằng yêu cầu đọc theo phương án của sáng chế không được giới hạn ở ví dụ được mô tả nêu trên. Ví dụ, yêu cầu đọc theo phương án của sáng chế có thể bao gồm thông tin khác như là thông tin liên quan đến mã hóa mật. Đối với thông tin liên quan đến việc mã hóa mật theo phương án của sáng chế, ví dụ, một hoặc cả dữ liệu chỉ báo xem có hay không việc mã hóa mật dữ liệu được đọc từ vùng được chỉ báo bởi thông tin chỉ báo vùng và dữ liệu chỉ rõ khóa mã hóa mật được minh họa. Hơn nữa, như được chỉ báo bởi phương pháp xử lý thông tin theo phương án thứ tư được mô tả sau đây, thông tin liên quan đến mã hóa mật theo phương án của sáng chế có thể còn bao gồm dữ liệu chỉ báo xem có hay không việc tạo ra "khóa mã hóa mật tương ứng với yêu cầu đọc".

Cụ thể hơn, thiết bị xử lý thông tin 100 đọc dữ liệu từ vùng được chỉ báo bởi thông tin chỉ báo vùng được chứa trong yêu cầu đọc. Sau đó, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu đã được đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Hơn nữa, trong trường hợp mà yêu cầu đọc chỉ báo các vùng, thiết bị xử lý thông tin 100 đọc dữ liệu từ mỗi trong các vùng đó. Sau đó, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu được đọc từ mỗi trong các vùng đó được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Thiết bị xử lý thông tin 100 chỉ rõ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc, ví dụ, trên cơ sở của việc thiết đặt thông tin được kết hợp với vùng của phương tiện ghi theo chẳng hạn. Sau đó, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu đã được đọc (dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc) bằng cách sử dụng khóa mã hóa mật được mã hóa mật.

Thông tin thiết đặt theo phương án của sáng chế là dữ liệu chỉ báo sự thiết đặt liên quan đến mã hóa mật của vùng của phương tiện ghi.

Đối với thông tin thiết đặt, ví dụ, "Bảng (hoặc Cơ sở dữ liệu) ghi địa chỉ chỉ báo vùng của phương tiện ghi và khóa mã hóa liên kết cho mỗi vùng" được minh họa. Hơn nữa, thông tin thiết đặt có thể còn được kết hợp với thông tin để xác định xem có hay không việc mã hóa mật được thực hiện (sau đây, được coi là "thông tin về sự cần thiết mã hóa mật") cho mỗi vùng. Đối với thông tin về sự cần thiết mã hóa mật, ví dụ, dữ liệu chỉ báo việc bất kỳ trong số các việc "mã

hóa mật liên tục", "văn bản gốc liên tục" (không thực hiện liên tục mã hóa mật), hoặc "tuân theo yêu cầu đọc" được minh họa. Lưu ý rằng thông tin thiết đặt theo phương án của sáng chế không được giới hạn ở Bảng (hoặc Cơ sở dữ liệu) như được mô tả ở trên và có thể là dữ liệu theo khuôn dạng bất kỳ, ví dụ, dữ liệu cho mỗi vùng, hoặc loại tương tự.

Trong trường hợp mà thông tin thiết đặt được chứa trong thông tin về sự cần thiết mã hóa mật, thiết bị xử lý thông tin 100 xác định xem có hay không việc mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin thiết đặt. Sau đó, thiết bị xử lý thông tin 100 mã hóa mật một cách chọn lọc dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc theo kết quả xác định. Đối với ví dụ cụ thể, trong trường hợp mà được xác định rằng dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc được mã hóa mật, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Hơn nữa, trong trường hợp mà không được xác định rằng dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc được mã hóa mật, thiết bị xử lý thông tin 100 không mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Lưu ý rằng thông tin thiết đặt theo phương án của sáng chế không được giới hạn ở ví dụ được mô tả nêu trên.

Ví dụ, như được chỉ báo trong phương pháp xử lý thông tin theo phương án thứ tư được mô tả sau đây, thông tin thiết đặt có thể còn được kết hợp với thông tin để xác định xem có hay không việc tạo ra "khóa mã hóa tương ứng với yêu cầu đọc" (sau đây, được coi là "thông tin sự cần thiết của việc tạo khóa mã hóa mật") cho mỗi vùng. Đối với thông tin sự cần thiết của việc tạo khóa mã hóa mật, ví dụ, dữ liệu chỉ báo việc bất kỳ trong số các việc "để tạo ra liên tục "khóa mã hóa mật tương ứng với yêu cầu đọc"", "không tạo ra liên tục" khóa mã hóa mật tương ứng với yêu cầu đọc"", hoặc "để tuân theo yêu cầu đọc" được minh họa.

Fig.10 là sơ đồ giải thích minh họa sự phác thảo của việc thiết đặt được xác định bởi thông tin thiết đặt theo phương án của sáng chế và minh họa ví dụ về thiết đặt trong vùng A. Trên Fig.10, khóa mã hóa mật được chỉ báo là "khóa" (tương tự áp dụng cho các hình vẽ khác).

Như được minh họa trên Fig.10, thiết bị xử lý thông tin 100 xác định vùng,

khóa mã hóa, và sự cần thiết của mã hóa mật (xem có hay không việc thực hiện mã hóa mật) theo thông tin thiết đặt. Thiết bị xử lý thông tin 100 chỉ rõ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc có viện dẫn tới thông tin thiết đặt tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Hơn nữa, thiết bị xử lý thông tin 100 chỉ rõ xem có hay không việc thực hiện mã hóa mật trên dữ liệu được đọc từ vùng có viện dẫn tới thông tin thiết đặt tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Lưu ý rằng, như được mô tả ở trên, trong thông tin thiết đặt, không cần thiết liên kết vùng với sự cần thiết mã hóa mật. Hơn nữa, trong thông tin thiết đặt, không cần thiết liên kết khóa mã hóa mật với vùng được kết hợp với thông tin về sự cần thiết mã hóa mật chỉ báo rằng mã hóa mật không được thực hiện.

Trong trường hợp mà khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc không được chỉ rõ hoặc trong trường hợp mà thông tin về sự cần thiết mã hóa mật được chứa trong thông tin thiết đặt chỉ báo rằng việc mã hóa mật không được thực hiện, thiết bị xử lý thông tin 100 truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc mà không mã hóa mật dữ liệu.

Fig.11 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ nhất. Trên Fig.11, dữ liệu mà được mã hóa mật được chỉ báo là “dữ liệu được mã hóa” (tương tự áp dụng cho các hình vẽ khác).

[0179]

Máy chủ 300 truyền yêu cầu đọc (S100).

Bộ đọc/bộ ghi 200 mà đã thu yêu cầu đọc được truyền từ máy chủ 300 trong bước S100 truyền yêu cầu đọc thu được đến thiết bị xử lý thông tin 100 (S102).

Ở đây, trong trường hợp mà bộ đọc/bộ ghi 200 lưu trữ thông tin thiết đặt trong phương tiện ghi, bộ đọc/bộ ghi 200 có thể mã hóa mật một phần của yêu cầu đọc được thu bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và truyền yêu cầu đọc được mã hóa mật đến thiết bị xử lý thông tin 100.

Fig.12 là sơ đồ giải thích minh họa ví dụ của việc xử lý bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp) được chứa trong hệ thống xử lý thông tin 1000 theo

phương án thứ nhất. A của Fig.12 minh họa ví dụ về yêu cầu đọc được truyền từ máy chủ 300, và B của Fig.12 minh họa phác thảo của việc thiết đặt được xác định bởi thông tin thiết đặt như trên Fig.10. C của Fig.12 minh họa ví dụ về yêu cầu đọc được mã hóa mật bởi bộ đọc/bộ ghi 200.

Ví dụ, như được minh họa trên Fig.12, trong trường hợp mà bộ đọc/bộ ghi 200 mã hóa mật yêu cầu đọc được thu bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc, thiết bị xử lý thông tin 100 mà thu yêu cầu đọc được mã hóa mật giải mã mật yêu cầu đọc, mà được mã hóa mật theo phần, bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và thực hiện xử lý.

Viện dẫn lại tới Fig.11, ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ nhất sẽ được mô tả. Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 200 trong bước S102 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc (S104). Sau đó, thiết bị xử lý thông tin 100 truyền dữ liệu được mã hóa (S106).

Fig.13 là sơ đồ giải thích để giải thích ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ nhất. A của Fig.13 minh họa một cách giản lược ví dụ của yêu cầu đọc được truyền từ máy chủ 300, và B của Fig.13 minh họa ví dụ của dữ liệu được mã hóa được truyền bởi thiết bị xử lý thông tin 100.

Như được minh họa trong A của Fig.13, có trường hợp trong đó yêu cầu đọc xác định việc đọc dữ liệu từ các vùng. Như được mô tả ở trên, trong trường hợp mà yêu cầu đọc chỉ báo các vùng, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu được đọc cho mỗi vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc như được minh họa trong B của Fig.13.

Viện dẫn lại tới Fig.11, ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ nhất sẽ được mô tả. Bộ đọc/bộ ghi 200 mà đã thu dữ liệu được mã hóa được truyền từ thiết bị xử lý thông tin 100 trong bước S106 truyền dữ liệu thu được được mã hóa đến máy chủ 300 (S108).

Máy chủ 300 mà đã thu dữ liệu được mã hóa được truyền từ bộ đọc/bộ ghi 200 trong bước S108 giải mã mật dữ liệu thu được được mã hóa bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc được

truyền trong bước S100 (S110). Máy chủ 300 có thể sử dụng dữ liệu được giải mã mật, ví dụ, để xử lý tùy ý phụ thuộc vào dịch vụ được cung cấp bởi máy chủ 300.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ nhất, ví dụ, bằng cách thực hiện việc xử lý được minh họa trên Fig.11, việc đọc dữ liệu từ thiết bị xử lý thông tin 100 bởi máy chủ 300 được nhận biết.

Ở đây, ngay cả khi thiết bị khác ngoài thiết bị có khóa mã hóa mật hợp lệ như là máy chủ 300 (sau đây, được coi là "thiết bị bên thứ ba") thu được dữ liệu được mã hóa được truyền từ thiết bị xử lý thông tin 100, thiết bị bên thứ ba không thể giải mật mã dữ liệu được mã hóa mật. Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ nhất, sự bảo mật để đọc dữ liệu mà cần sự ủy quyền để đọc được đảm bảo.

Hơn nữa, khi sự truyền thông của hệ thống xử lý thông tin 1000 theo phương án thứ nhất được minh họa trên Fig.11 được so sánh với sự truyền thông liên quan đến việc đọc dữ liệu bằng cách sử dụng sự xác thực bởi phương pháp thử thách và phản hồi đã biết được minh họa trên Fig.9, số lần truyền thông của sự truyền thông được minh họa trên Fig.11 là nhỏ hơn.

Tức là, hệ thống xử lý thông tin 1000 theo phương án thứ nhất rút ngắn thời gian truyền thông và rút ngắn thời gian xử lý của toàn bộ hệ thống sao với trường hợp trong đó sự xác thực bằng cách sử dụng phương pháp thử thách và phản hồi đã biết được sử dụng.

Do đó, trong hệ thống xử lý thông tin 1000 bao gồm thiết bị xử lý thông tin 100 theo phương án thứ nhất, việc giảm thời gian xử lý liên quan đến việc đọc được nhận biết trong khi đảm bảo sự bảo mật liên quan đến việc đọc dữ liệu.

Lưu ý rằng việc xử lý của thiết bị xử lý thông tin 100 Theo phương án thứ nhất không được giới hạn ở ví dụ được mô tả nêu trên.

Như được mô tả ở trên, yêu cầu đọc có thể bao gồm thông tin liên quan đến việc mã hóa mật. Fig.14 là sơ đồ giải thích để giải thích ví dụ của yêu cầu đọc theo phương án của sáng chế và minh họa ví dụ của yêu cầu đọc bao gồm thông tin liên quan đến việc mã hóa mật. "Yêu cầu mã hóa mật" được minh họa trên Fig.14 tương ứng với thông tin liên quan đến việc mã hóa mật.

Trong trường hợp mà không được xác định rằng dữ liệu tương ứng với

vùng được chỉ báo bởi yêu cầu đọc được mã hóa mật trên cơ sở của thông tin thiết đặt khi yêu cầu đọc bao gồm thông tin liên quan đến việc mã hóa mật như được minh họa trên Fig.14, thiết bị xử lý thông tin 100 có thể mã hóa mật một cách chọn lọc dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin liên quan đến việc mã hóa mật được chứa trong yêu cầu đọc. Ở đây, mã hóa mật chọn lọc dựa trên thông tin liên quan đến việc mã hóa mật bao gồm "xem có hay không việc thực hiện mã hóa mật" hoặc "xem có hay không việc thực hiện mã hóa mật và khóa mã hóa mật được sử dụng trong trường hợp mà việc mã hóa mật được thực hiện".

Đối với ví dụ cụ thể, trong trường hợp mà thông tin liên quan đến việc mã hóa mật được chứa trong yêu cầu đọc chỉ báo rằng việc mã hóa mật được thực hiện, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Ở thời điểm này, thiết bị xử lý thông tin 100 có thể thực hiện việc mã hóa mật bằng cách sử dụng khóa mã hóa được chỉ rõ bởi thông tin liên quan đến việc mã hóa mật. Hơn nữa, trong trường hợp mà thông tin liên quan đến việc mã hóa mật được chứa trong yêu cầu đọc không chỉ báo rằng việc mã hóa mật được thực hiện, thiết bị xử lý thông tin 100 không mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Tức là, trong trường hợp mà việc xử lý được thực hiện trên cơ sở của thông tin liên quan đến việc mã hóa mật được chứa trong yêu cầu đọc, thiết bị xử lý thông tin 100 truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc hoặc dữ liệu được mã hóa mật.

Fig.15 là lưu đồ minh họa ví dụ của việc xử lý thiết bị xử lý thông tin 100 theo phương án thứ nhất. Fig.15 minh họa ví dụ của việc xử lý của thiết bị xử lý thông tin 100 sau khi thu yêu cầu đọc bao gồm thông tin liên quan đến việc mã hóa mật. Trên Fig.15, vùng được chỉ báo bởi yêu cầu đọc được chỉ báo như "vùng mục tiêu đọc".

Thiết bị xử lý thông tin 100 xác định xem có hay không việc thiết đặt của vùng được chỉ báo bởi yêu cầu đọc là "mã hóa mật liên tục" (S200). Thiết bị xử lý thông tin 100 làm cho việc xác định trong bước S200 bằng cách viện dẫn tới thông tin về sự cần thiết mã hóa mật được chứa trong thông tin thiết đặt.

Trong trường hợp mà được xác định trong bước S200 mà việc thiết đặt là "mã hóa mật liên tục", thiết bị xử lý thông tin 100 thực hiện xử lý trong bước

S208 được mô tả sau đây.

Hơn nữa, trong trường hợp mà không được xác định trong bước S200 mà việc thiết đặt là "mã hóa mật liên tục", thiết bị xử lý thông tin 100 xác định xem có hay không việc thiết đặt của vùng được chỉ báo bởi yêu cầu đọc là "văn bản gốc liên tục" (S202). Thiết bị xử lý thông tin 100 làm cho việc xác định trong bước S202 bằng cách viện dẫn tới thông tin về sự cần thiết mã hóa mật được chứa trong thông tin thiết đặt.

Trong trường hợp mà được xác định trong bước S202 mà việc thiết đặt là "văn bản gốc liên tục", thiết bị xử lý thông tin 100 thực hiện xử lý trong bước S206 được mô tả sau đây.

Hơn nữa, trong trường hợp mà không được xác định trong bước S200 mà việc thiết đặt là "văn bản gốc liên tục", thiết bị xử lý thông tin 100 xác định xem có hay không việc thông tin liên quan đến việc mã hóa mật được chứa trong yêu cầu đọc yêu cầu mã hóa mật (S204).

Trong trường hợp mà không được xác định trong bước S204 mà việc mã hóa mật được yêu cầu hoặc trong trường hợp mà được xác định trong bước S202 mà việc thiết đặt là "văn bản gốc liên tục", thiết bị xử lý thông tin 100 không mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc (S206). Trong trường hợp này, thiết bị xử lý thông tin 100 truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Hơn nữa, trong trường hợp mà được xác định trong bước S204 mà việc mã hóa mật được yêu cầu hoặc trong trường hợp mà được xác định trong bước S200 mà việc thiết đặt là "mã hóa mật liên tục", thiết bị xử lý thông tin 100 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc (S208). Trong trường hợp này, thiết bị xử lý thông tin 100 truyền dữ liệu được mã hóa mật.

Trong trường hợp mà yêu cầu đọc bao gồm thông tin liên quan đến việc mã hóa mật được thu, thiết bị xử lý thông tin 100 thực hiện, ví dụ, việc xử lý được minh họa trên Fig.15. Lưu ý rằng hiển nhiên rằng việc xử lý của thiết bị xử lý thông tin 100 trong trường hợp mà yêu cầu đọc bao gồm thông tin liên quan đến việc mã hóa mật được thu không được giới hạn ở ví dụ được minh họa trên Fig.15.

[2-1-3] Thao tác và Hiệu quả của hệ thống xử lý thông tin 1000 theo phương án thứ nhất

Trong hệ thống xử lý thông tin thứ nhất 1000, ví dụ, các thao tác dưới đây được nhận biết. Hơn nữa, bằng cách sử dụng hệ thống xử lý thông tin thứ nhất 1000, ví dụ, thu được các hiệu ứng dưới đây. Lưu ý rằng hiển nhiên rằng các thao tác của hệ thống xử lý thông tin 1000 theo phương án thứ nhất và các hiệu quả thu được bằng cách sử dụng hệ thống xử lý thông tin theo phương án thứ nhất không được giới hạn ở các ví dụ dưới đây.

· Việc đọc có thể được thực hiện mà không xác thực việc ủy quyền. Để đáp lại yêu cầu đọc (lệnh), thiết bị xử lý thông tin 100 phản hồi dữ liệu được mã hóa thu được bằng cách mã hóa mật dữ liệu bằng cách sử dụng khóa được kết hợp với vùng. Dữ liệu được mã hóa được giải mã mật bởi thiết bị bao gồm khóa (máy chủ 300, bộ đọc/bộ ghi 200, hoặc loại tương tự).

· Trong trường hợp mà yêu cầu đọc được thu, thiết bị xử lý thông tin 100 xác định xem có hay không việc thiết bị xử lý thông tin 100 mã hóa mật và phản hồi dữ liệu và loại khóa được sử dụng để mã hóa mật khi các khóa được kết hợp với vùng bằng cách viện dẫn tới thông tin thiết đặt mà được thiết đặt cho vùng trước.

· Đối với vùng mà được thiết đặt là "có thể hoặc không được mã hóa mật", xem có hay không việc thực hiện việc mã hóa mật có thể được chỉ rõ theo tham số của yêu cầu đọc (ví dụ của thông tin liên quan đến mã hóa mật). Hơn nữa, loại khóa được sử dụng cho vùng mà được thiết đặt là "có thể hoặc không được mã hóa mật" có thể được chỉ rõ theo tham số của yêu cầu đọc (ví dụ của thông tin liên quan đến mã hóa mật).

· Trong trường hợp mà yêu cầu đọc đơn lẻ bao gồm việc đọc của các vùng, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu được đọc từ mỗi vùng bằng cách sử dụng khóa được kết hợp với mỗi vùng.

· Để ngăn sự nghe trộm, bộ đọc/bộ ghi 200 có thể mã hóa mật tham số của yêu cầu đọc với khóa được kết hợp với vùng như được minh họa trên Fig.12.

[2-2] Phương pháp xử lý thông tin theo phương án thứ hai

[2-2-1] Phác thảo của hệ thống xử lý thông tin 1000 mà Phương pháp xử lý thông tin theo phương án thứ hai được áp dụng

Ví dụ, bằng cách sử dụng hệ thống xử lý thông tin thứ nhất 1000, việc giảm thời gian xử lý liên quan đến việc đọc được nhận biết trong khi đảm bảo sự bảo

mật liên quan đến việc đọc dữ liệu.

Tuy nhiên, trong hệ thống xử lý thông tin thứ nhất 1000, không thể dùng cho máy chủ 300 để chỉ rõ khi yêu cầu đọc tương ứng với dữ liệu thu được được truyền từ dữ liệu thu được.

Như được mô tả ở trên, trong trường hợp mà không thể dùng cho máy chủ 300 để chỉ rõ khi yêu cầu đọc tương ứng với dữ liệu thu được được truyền, có khả năng là các sự kiện không mong muốn xảy ra như kết quả của việc thực hiện một số xử lý trên dữ liệu thu nhận được bằng cách giải mã mật dữ liệu thu được.

Fig.16 là sơ đồ giải thích minh họa ví dụ của trường hợp mà có thể xảy ra trong trường hợp mà không thể dùng cho máy chủ 300 để chỉ rõ khi yêu cầu đọc tương ứng với dữ liệu thu được được truyền. Fig.16 minh họa ví dụ của việc xử lý của hệ thống xử lý thông tin bao gồm thiết bị xử lý thông tin 100, máy chủ 300, và bộ đọc/bộ ghi 20. Trong ví dụ được minh họa trên Fig.16, truyền thông bằng cách sử dụng NFC được thực hiện giữa thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 20, và truyền thông mạng được thực hiện giữa bộ đọc/bộ ghi 20 và máy chủ 300.

Bộ đọc/bộ ghi 20 truyền yêu cầu đọc như trong bước S102 trên Fig.11 (S30). Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 20 trong bước S30 truyền dữ liệu được mã hóa như trong bước S106 trên Fig.11 (S32).

Bộ đọc/bộ ghi 20 mà đã thu dữ liệu được mã hóa được truyền từ thiết bị xử lý thông tin 100 trong bước S32 ghi dữ liệu thu được được mã hóa trong phương tiện ghi tùy ý (S34).

Máy chủ 300 truyền yêu cầu đọc đến bộ đọc/bộ ghi 20 (S36).

Bộ đọc/bộ ghi 20 mà đã thu yêu cầu đọc được truyền từ máy chủ 300 trong bước S36 đọc dữ liệu được mã hóa được ghi trong phương tiện ghi trong bước S34 (S38) và truyền dữ liệu đã được đọc đến máy chủ 300 (S40).

Ví dụ, trong trường hợp mà việc xử lý được minh họa trên Fig.16 được thực hiện, máy chủ 300 xử lý dữ liệu được mã hóa được truyền từ bộ đọc/bộ ghi 20 trong bước S40 là dữ liệu tương ứng với yêu cầu đọc được truyền trong bước S36. Do đó, trong ví dụ được minh họa trên Fig.16, có khả năng là các sự kiện không mong muốn xảy ra như kết quả của việc thực hiện xử lý trên dữ liệu thu

được (hoặc dữ liệu được thu nhận bởi giải mã mật dữ liệu thu được được mã hóa) bởi máy chủ 300.

Lưu ý rằng trường hợp mà có thể xảy ra trong trường hợp mà không thể dùng cho máy chủ 300 để chỉ rõ khi yêu cầu đọc tương ứng với dữ liệu được truyền không được giới hạn ở ví dụ được minh họa trên Fig.16. Ví dụ, trong trường hợp mà hệ thống xử lý thông tin theo phương án thứ nhất có cấu trúc mà trong đó thiết bị xử lý thông tin 100 và máy chủ 300 trực tiếp truyền thông với nhau (bao gồm cấu trúc mà trong đó máy chủ 300 có chức năng như bộ đọc/bộ ghi 200), có khả năng là các sự kiện không mong muốn một cách tương tự xảy ra trong trường hợp mà cuộc tấn công giữa chừng được thực hiện trên sự truyền thông giữa thiết bị xử lý thông tin 100 và máy chủ 300.

Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ hai, máy chủ 300 truyền yêu cầu đọc và thông tin chỉ báo giá trị. "Để truyền yêu cầu đọc và thông tin chỉ báo giá trị" theo phương án của sáng chế nghĩa là "để truyền yêu cầu đọc bao gồm thông tin chỉ báo giá trị" hoặc "để truyền thông tin chỉ báo giá trị là dữ liệu khác với yêu cầu đọc". Hơn nữa, việc tương tự áp dụng cho trường hợp trong đó dữ liệu được truyền cùng với yêu cầu đọc là dữ liệu khác ngoài thông tin chỉ báo giá trị.

Giá trị được chỉ báo bởi thông tin chỉ báo giá trị theo phương án của sáng chế bao gồm giá trị số, chuỗi ký tự, hoặc kết hợp của chúng. Giá trị được chỉ báo bởi thông tin chỉ báo giá trị, ví dụ, được tạo bằng cách tạo số ngẫu nhiên bởi máy chủ 300 hoặc được chỉ rõ bằng cách đọc giá trị của mạch đếm hoặc đồng hồ được chứa trong máy chủ 300 bởi máy chủ 300. Giá trị được chỉ báo bởi thông tin chỉ báo giá trị đóng vai trò như, ví dụ, tham số của yêu cầu đọc. Sau đây, trường hợp trong đó giá trị được chỉ báo bởi thông tin chỉ báo giá trị theo phương án của sáng chế là số ngẫu nhiên sẽ được mô tả là chẳng hạn.

Lưu ý rằng, trong hệ thống xử lý thông tin 1000 theo phương án thứ hai, bộ đọc/bộ ghi 200 mà đã thu yêu cầu đọc được truyền từ máy chủ 300 có thể truyền yêu cầu đọc thu được và thông tin chỉ báo giá trị đến thiết bị xử lý thông tin 100. Trong trường hợp này, giá trị được chỉ báo bởi thông tin chỉ báo giá trị được tạo ra, ví dụ, bằng cách tạo ra số ngẫu nhiên bởi bộ đọc/bộ ghi 200. Hơn nữa, bộ đọc/bộ ghi 200 truyền thông tin chỉ báo giá trị đến máy chủ 300.

Trong trường hợp mà thông tin chỉ báo giá trị được thu cùng với yêu cầu

đọc, thiết bị xử lý thông tin 100 thực hiện xử lý dưới đây. Lưu ý rằng thiết bị xử lý thông tin 100 có thể thực hiện xử lý dưới đây ngoài việc xử lý theo phương pháp xử lý thông tin theo phương án thứ nhất.

Thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử từ dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc. sau đó, thiết bị xử lý thông tin 100 truyền chữ ký điện tử được tạo cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Ở đây, dữ liệu được truyền bởi thiết bị xử lý thông tin 100 có thể được mã hóa mật hoặc có thể không được mã hóa mật.

Fig.17 là sơ đồ giải thích để giải thích ví dụ của việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 theo phương án thứ hai và minh họa ví dụ của việc tạo chữ ký điện tử. Trên Fig.17, chữ ký điện tử được chỉ báo là "chữ ký" (việc tương tự áp dụng cho các hình vẽ khác).

Như được minh họa trên Fig.17, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử bằng cách tính toán thuật toán tùy ý như là "Sha-256 với mã hóa mật RSA" bằng cách sử dụng dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, số ngẫu nhiên (ví dụ của giá trị được chỉ báo bởi thông tin chỉ báo giá trị), và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Lưu ý rằng, trong trường hợp mà phương pháp xử lý thông tin theo phương án thứ hai được kết hợp với phương pháp xử lý thông tin theo phương án khác được mô tả sau đây, thiết bị xử lý thông tin 100 có thể tạo ra chữ ký điện tử bằng cách sử dụng thông tin khác nữa. Tức là, thiết bị xử lý thông tin 100 theo phương án thứ hai tạo ra chữ ký điện tử từ, ít nhất, dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Lưu ý rằng việc xử lý của thiết bị xử lý thông tin 100 không được giới hạn ở ví dụ được mô tả nêu trên.

Ví dụ, trong trường hợp mà yêu cầu đọc chỉ báo các vùng, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử cho mỗi vùng được chỉ báo bởi yêu cầu đọc như trong ví dụ được minh họa trên Fig.17. Sau đó, thiết bị xử lý thông tin 100 còn truyền chữ ký điện tử được tạo cho mỗi vùng cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Hơn nữa, trong trường hợp mà yêu cầu đọc chỉ báo các vùng, thiết bị xử lý thông tin 100 tạo ra khóa mã hóa cho chữ ký trên cơ sở của khóa mã hóa mật tương ứng với các vùng được chỉ báo bởi yêu cầu đọc. Khóa mã hóa mật cho chữ ký được tạo ra, ví dụ, bằng cách không tạo các khóa mã hóa mật (kết hợp các khóa mã hóa mật).

Khi khóa mã hóa mật cho chữ ký được tạo ra, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử từ dữ liệu tương ứng với các vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật cho chữ ký như trong ví dụ được minh họa trên Fig.17. Sau đó, thiết bị xử lý thông tin 100 truyền chữ ký điện tử được tạo cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Fig.18 là sơ đồ giải thích để giải thích ví dụ của việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 theo phương án thứ hai và minh họa ví dụ khác của việc tạo chữ ký điện tử. A của Fig.18 minh họa ví dụ mà trong đó chữ ký điện tử được tạo ra cho mỗi vùng được chỉ báo bởi yêu cầu đọc như trong ví dụ được minh họa trên Fig.17. B của Fig.18 minh họa ví dụ mà trong đó chữ ký điện tử được tạo ra từ dữ liệu tương ứng với các vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật cho chữ ký như trong ví dụ được minh họa trên Fig.17.

Hơn nữa, trong trường hợp mà thông tin chỉ báo giá trị được thu cùng với yêu cầu đọc khi phương pháp mã hóa mật dùng khóa chung được sử dụng, thiết bị xử lý thông tin 100 có thể tạo ra Mã xác thực bản tin (MAC) trên cơ sở của thông tin chỉ báo giá trị và có thể truyền MAC được tạo ra cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Ở đây, dữ liệu được truyền bởi thiết bị xử lý thông tin 100 có thể được mã hóa mật hoặc có thể không được mã hóa mật. Sau đây, trong các phương án khác, chữ ký điện tử có thể được thay thế bằng MAC.

Máy chủ 300 mà có dữ liệu thu được và chữ ký điện tử (hoặc MAC, việc tương tự áp dụng dưới đây) được truyền từ thiết bị xử lý thông tin 100 xác minh chữ ký điện tử thu được. Lưu ý rằng bộ đọc/bộ ghi 200 có thể xác minh chữ ký điện tử. Sau đó, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử là thông thường, máy chủ 300 sử dụng dữ liệu thu được (hoặc dữ liệu thu nhận được bằng cách giải mã mật dữ liệu thu được) cho việc xử lý tùy ý. Hơn

nữa, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử không phải là thông thường, máy chủ 300 không sử dụng dữ liệu thu được (hoặc dữ liệu thu nhận được bằng cách giải mã mật dữ liệu thu được) cho việc xử lý tùy ý. Máy chủ 300 so sánh, ví dụ, giá trị thu nhận được bằng cách giải mã mật chữ ký điện tử thu được với giá trị được chỉ báo bởi thông tin chỉ báo giá trị được truyền cùng với yêu cầu đọc, và trong trường hợp mà các giá trị này trùng hợp với nhau, máy chủ 300 xác định rằng việc xác minh được thực hiện một cách thông thường.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ hai, như được mô tả ở trên, máy chủ 300 có thể xác minh dữ liệu bằng cách sử dụng chữ ký điện tử. Do đó, máy chủ 300 có thể chỉ rõ, từ dữ liệu thu được, xem có hay không việc dữ liệu thu được là dữ liệu được truyền tương ứng với yêu cầu đọc.

[2-2-2] Việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ hai

Tiếp theo, ví dụ về việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ hai sẽ được mô tả.

Fig.19 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ hai.

Máy chủ 300 truyền số ngẫu nhiên (ví dụ của thông tin chỉ báo giá trị, việc tương tự áp dụng dưới đây) cùng với yêu cầu đọc (S300).

Bộ đọc/bộ ghi 200 mà đã thu yêu cầu đọc và số ngẫu nhiên được truyền từ máy chủ 300 trong bước S300 truyền yêu cầu đọc thu được và số ngẫu nhiên đến thiết bị xử lý thông tin 100 (S302). Lưu ý rằng, như trong bước S102 trên Fig.11, bộ đọc/bộ ghi 200 có thể mã hóa mật yêu cầu đọc hoặc yêu cầu đọc và số ngẫu nhiên.

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc và số ngẫu nhiên được truyền từ bộ đọc/bộ ghi 200 trong bước S302 tạo ra chữ ký điện tử (S304). Sau đó, thiết bị xử lý thông tin 100 truyền chữ ký điện tử cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc (S306). Lưu ý rằng, như trong bước S104 trên Fig.11, thiết bị xử lý thông tin 100 có thể mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Fig.20 là sơ đồ giải thích để giải thích ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ hai và minh họa ví dụ của dữ liệu được truyền bởi thiết bị xử lý thông tin 100 trong bước S306 trên Fig.19.

Ví dụ, như được minh họa trên Fig.20, thiết bị xử lý thông tin 100 truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và chữ ký điện tử là phần đơn lẻ của dữ liệu. Lưu ý rằng thiết bị xử lý thông tin 100 có thể truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và chữ ký điện tử là các phần khác nhau của dữ liệu.

Viện dẫn lại tới Fig.19, ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ hai sẽ được mô tả. Bộ đọc/bộ ghi 200 mà đã thu dữ liệu được truyền từ thiết bị xử lý thông tin 100 trong bước S306 (ví dụ, dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và dữ liệu bao gồm chữ ký điện tử như được minh họa trên Fig.20) truyền dữ liệu thu được đến máy chủ 300 (S308).

Máy chủ 300 mà đã thu dữ liệu được truyền từ bộ đọc/bộ ghi 200 trong bước S308 (ví dụ, dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và dữ liệu bao gồm chữ ký điện tử như được minh họa trên Fig.20) xác minh chữ ký điện tử (S310).

Sau đó, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử là thông thường, máy chủ 300 sử dụng dữ liệu thu được (hoặc dữ liệu thu nhận được bằng cách giải mã mật dữ liệu thu được) cho việc xử lý tùy ý. Hơn nữa, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử không phải là thông thường, máy chủ 300 không sử dụng dữ liệu thu được (hoặc dữ liệu thu nhận được bằng cách giải mã mật dữ liệu thu được) cho việc xử lý tùy ý.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ hai, ví dụ, bằng cách thực hiện việc xử lý được minh họa trên Fig.19, máy chủ 300 có thể chỉ rõ, từ dữ liệu thu được, xem có hay không việc dữ liệu thu được là dữ liệu tương ứng với yêu cầu đọc được truyền.

Hơn nữa, hệ thống xử lý thông tin 1000 theo phương án thứ hai có thể còn thực hiện xử lý tương tự với của hệ thống xử lý thông tin 1000 theo phương án thứ nhất. Do đó, hệ thống xử lý thông tin 1000 theo phương án thứ hai có thể thu nhận các hiệu quả thu nhận được bằng cách hệ thống xử lý thông tin 1000 theo phương án thứ nhất.

[2-2-3] Thao tác và Hiệu quả của hệ thống xử lý thông tin 1000 theo phương án thứ hai

Trong hệ thống xử lý thông tin thứ hai 1000, ví dụ, các thao tác dưới đây được nhận biết. Hơn nữa, bằng cách sử dụng hệ thống xử lý thông tin thứ hai 1000, ví dụ, thu được các hiệu ứng dưới đây. Lưu ý rằng hiển nhiên rằng các thao tác của hệ thống xử lý thông tin 1000 theo phương án thứ hai và các hiệu quả thu được bằng cách sử dụng hệ thống xử lý thông tin theo phương án thứ hai không được giới hạn ở các ví dụ dưới đây.

Giá trị được tạo ra bởi máy chủ 300 (ví dụ, số ngẫu nhiên) được chuyển đến thiết bị xử lý thông tin 100 làm tham số của yêu cầu đọc. Hơn nữa, đối với tham số của yêu cầu đọc, giá trị được tạo ra bởi bộ đọc/bộ ghi 200 (ví dụ, số ngẫu nhiên) có thể được chuyển đến thiết bị xử lý thông tin 100.

Thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử (MAC trong trường hợp mà phương pháp mã hóa mật khóa chung được sử dụng) đối với dữ liệu được đọc (dữ liệu trước khi được mã hóa mật hoặc dữ liệu được mã hóa) và số ngẫu nhiên và truyền chữ ký điện tử cùng với dữ liệu đến bộ đọc/bộ ghi 200.

Thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử bằng cách sử dụng khóa được kết hợp với vùng theo chẳng hạn.

Máy chủ 300 (hoặc bộ đọc/bộ ghi 200) có thể xác định xem có hay không việc dữ liệu là dữ liệu mà được đọc ở thời điểm này bằng cách xác minh chữ ký điện tử và có thể phát hiện sai lệch của dữ liệu đã được đọc.

[2-3] Phương pháp xử lý thông tin theo phương án thứ ba

[2-3-1] Phác thảo của hệ thống xử lý thông tin 1000 mà Phương pháp xử lý thông tin theo phương án thứ ba được áp dụng

Ví dụ, trong hệ thống xử lý thông tin 1000 có cấu trúc được minh họa trên Fig.1, có khả năng là sự truyền thông từ bộ đọc/bộ ghi 200 đến thiết bị xử lý thông tin 100 bị sai lệch bằng cách sử dụng phương pháp như là sự tấn công giữa chừng. Ví dụ của sự sai lệch bao gồm vùng mục tiêu đọc được chỉ báo bởi thông tin chỉ báo vùng được chứa trong yêu cầu đọc được ghi lại.

Fig.21 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó sự truyền thông từ bộ đọc/bộ ghi 200 tới thiết bị xử lý thông tin 100 bị sai lệch. Trên Fig.21, thiết bị làm sai lệch sự truyền thông từ bộ đọc/bộ ghi 200 đến thiết bị xử

lý thông tin 100 bởi sự tấn công giữa chừng hoặc loại tương tự được minh họa như "kẻ tấn công X".

Bộ đọc/bộ ghi 200 truyền yêu cầu đọc đến thiết bị xử lý thông tin 100 như trong bước S102 được minh họa trên Fig.11 (S50).

Kẻ tấn công X mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 200 trong bước S50 làm sai lệch vùng mục tiêu đọc được chỉ báo bởi thông tin chỉ báo vùng được chứa trong yêu cầu đọc (S52). Sau đó, kẻ tấn công X truyền yêu cầu đọc bị sai lệch đến thiết bị xử lý thông tin 100 (S54).

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc được truyền từ kẻ tấn công X trong bước S54 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và truyền dữ liệu được mã hóa theo cách tương ứng như trong các bước từ S104 và S106 được minh họa trên Fig.11 (S56).

Ví dụ, trong ví dụ được minh họa trên Fig.21, thiết bị xử lý thông tin 100 truyền dữ liệu được đọc từ vùng khác với vùng được chỉ báo bởi yêu cầu đọc được truyền từ bộ đọc/bộ ghi 200 trong bước S50 (dữ liệu được đọc từ vùng sai).

Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ ba, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử từ dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, thông tin được chứa trong yêu cầu đọc, và khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Đối với thông tin được chứa trong yêu cầu đọc theo phương án của sáng chế, ví dụ, tham số của yêu cầu đọc như là thông tin chỉ báo vùng được minh họa. sau đó, thiết bị xử lý thông tin 100 truyền chữ ký điện tử được tạo cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Ở đây, dữ liệu được truyền bởi thiết bị xử lý thông tin 100 có thể được mã hóa mật hoặc có thể không được mã hóa mật.

Fig.22 là sơ đồ giải thích để giải thích ví dụ của việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 theo phương án thứ ba và minh họa ví dụ của việc tạo chữ ký điện tử. Ví dụ của việc tạo ra chữ ký điện tử được minh họa trên Fig.22 là ví dụ về việc tạo ra chữ ký điện tử trong trường hợp mà phương pháp xử lý thông tin theo phương án thứ hai và phương pháp xử lý thông tin theo phương án thứ ba được kết hợp.

Như được minh họa trên Fig.22, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử bằng cách tính toán thuật toán tùy ý bằng cách sử dụng, ví dụ, dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, số ngẫu nhiên (ví dụ của giá

trị được chỉ báo bởi thông tin chỉ báo giá trị), tham số của yêu cầu đọc (thông tin được chứa trong yêu cầu đọc), và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Lưu ý rằng, trong trường hợp mà chữ ký điện tử được tạo ra chỉ bằng phương pháp xử lý thông tin theo phương án thứ ba, không cần thiết là thiết bị xử lý thông tin 100 để tạo ra chữ ký điện tử bằng cách sử dụng số ngẫu nhiên được minh họa trên Fig.22. Tức là, thiết bị xử lý thông tin 100 theo phương án thứ ba tạo ra chữ ký điện tử từ, ít nhất, dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, thông tin được chứa trong yêu cầu đọc, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Lưu ý rằng việc xử lý của thiết bị xử lý thông tin 100 không được giới hạn ở ví dụ được mô tả nêu trên.

Ví dụ, trong trường hợp mà thông tin chỉ báo giá trị được thu cùng với yêu cầu đọc khi phương pháp mã hóa mật dùng khóa chung được sử dụng, thiết bị xử lý thông tin 100 có thể tạo ra MAC trên cơ sở của tham số của yêu cầu đọc (thông tin được chứa trong yêu cầu đọc) và có thể truyền MAC được tạo ra cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc. Ở đây, dữ liệu được truyền bởi thiết bị xử lý thông tin 100 có thể được mã hóa mật hoặc có thể không được mã hóa mật.

Máy chủ 300 mà có dữ liệu thu được và chữ ký điện tử (hoặc MAC) được truyền từ thiết bị xử lý thông tin 100 xác minh chữ ký điện tử thu được. Lưu ý rằng bộ đọc/bộ ghi 200 có thể xác minh chữ ký điện tử. Bằng cách xác minh chữ ký điện tử, hệ thống xử lý thông tin 1000 theo phương án thứ ba có thể xác minh xem có hay không việc yêu cầu đọc bị sai lệch.

Hơn nữa, trong hệ thống xử lý thông tin 1000 theo phương án thứ ba, việc xử lý tương tự với của một hoặc cả hệ thống xử lý thông tin 1000 theo phương án thứ nhất và hệ thống xử lý thông tin 1000 theo phương án thứ hai có thể còn được thực hiện. Do đó, hệ thống xử lý thông tin 1000 theo phương án thứ ba có thể thu nhận các hiệu quả thu nhận được bằng cách một hoặc cả hệ thống xử lý thông tin 1000 theo phương án thứ nhất và hệ thống xử lý thông tin 1000 theo phương án thứ hai.

[2-3-2] Việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ ba

Tiếp theo, ví dụ về việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ ba sẽ được mô tả.

Fig.23 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ ba. Fig.23 minh họa ví dụ của việc xử lý trong trường hợp mà phương pháp xử lý thông tin theo phương án thứ nhất đến phương pháp xử lý thông tin theo phương án thứ ba được kết hợp.

Máy chủ 300 truyền số ngẫu nhiên cùng với yêu cầu đọc như trong bước S300 trên Fig.19 (S400). Lưu ý rằng, trong trường hợp mà việc xử lý theo phương pháp xử lý thông tin theo phương án thứ hai không được thực hiện, không cần thiết là máy chủ 300 truyền số ngẫu nhiên.

Bộ đọc/bộ ghi 200 mà đã thu yêu cầu đọc và số ngẫu nhiên được truyền từ máy chủ 300 trong bước S400 truyền yêu cầu đọc thu được và số ngẫu nhiên đến thiết bị xử lý thông tin 100 như trong bước S300 trên Fig.19 (S402).

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc và số ngẫu nhiên được truyền từ bộ đọc/bộ ghi 200 trong bước S402 tạo ra chữ ký điện tử như trên Fig.22 (S404). Sau đó, thiết bị xử lý thông tin 100 truyền chữ ký điện tử cùng với dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc (S406).

Bộ đọc/bộ ghi 200 mà đã thu dữ liệu được truyền từ thiết bị xử lý thông tin 100 trong bước S406 truyền dữ liệu thu được đến máy chủ 300 (S408).

Máy chủ 300 mà đã thu dữ liệu được truyền từ bộ đọc/bộ ghi 200 trong bước S408 xác minh chữ ký điện tử (S410).

Sau đó, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử là bình thường, máy chủ 300 xác định rằng yêu cầu đọc không bị sai lệch. Sau đó, máy chủ 300 giải mã mật dữ liệu được mã hóa mà được yêu cầu và sử dụng dữ liệu được giải mã mật để xử lý tùy ý.

Hơn nữa, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử không phải bình thường, máy chủ 300 xác định rằng yêu cầu đọc bị sai lệch, và không xử lý dữ liệu được mã hóa mà được yêu cầu.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ ba, ví dụ, bằng cách thực hiện việc xử lý được minh họa trên Fig.23, máy chủ 300 có thể xác nhận xem có hay không việc yêu cầu đọc bị sai lệch.

[2-3-3] Thao tác và Hiệu quả của hệ thống xử lý thông tin 1000 theo

phương án thứ ba

Trong hệ thống xử lý thông tin thứ ba 1000, ví dụ, các thao tác dưới đây được nhận biết. Hơn nữa, bằng cách sử dụng hệ thống xử lý thông tin thứ ba 1000, ví dụ, thu được các hiệu ứng dưới đây. Lưu ý rằng hiển nhiên rằng các thao tác của hệ thống xử lý thông tin 1000 theo phương án thứ ba và các hiệu quả thu được bằng cách sử dụng hệ thống xử lý thông tin theo phương án thứ ba không được giới hạn ở các ví dụ dưới đây.

Việc đáp lại yêu cầu đọc, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử (MAC trong trường hợp mà phương pháp mã hóa mật khóa chung được sử dụng) đối với dữ liệu được đọc (dữ liệu trước khi được mã hóa mật hoặc dữ liệu được mã hóa) và tham số của yêu cầu đọc (ví dụ, thông số kỹ thuật của đích đọc) và truyền chữ ký điện tử đến bộ đọc/bộ ghi 200 cùng với dữ liệu.

Thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử bằng cách sử dụng khóa được kết hợp với vùng theo chẳng hạn.

Bằng cách xác minh chữ ký điện tử, máy chủ 300 (hoặc bộ đọc/bộ ghi 200) có thể xác nhận rằng tham số của yêu cầu đọc không bị sai lệch.

[2-4] Phương pháp xử lý thông tin theo phương án thứ tư

[2-4-1] Phác thảo của hệ thống xử lý thông tin 1000 mà Phương pháp xử lý thông tin theo phương án thứ tư được áp dụng

Ví dụ, với hệ thống xử lý thông tin 1000 có cấu trúc được minh họa trên Fig.1, có khả năng là, bằng cách quan sát dữ liệu được mã hóa được truyền từ thiết bị xử lý thông tin 100 đến bộ đọc/bộ ghi 200 bởi bên thứ ba, bên thứ ba có thể xác định xem có hay không việc dữ liệu được mã hóa là giống nhau, mặc dù nội dung của dữ liệu chưa được biết.

Fig.24 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó dữ liệu được mã hóa được truyền từ thiết bị xử lý thông tin 100 tới bộ đọc/bộ ghi 200 được quan sát bởi bên thứ ba. Fig.24 minh họa các bộ đọc/bộ ghi 200A và 200B có các chức năng tương tự với bộ đọc/bộ ghi 200 được minh họa trên Fig.1.

Bộ đọc/bộ ghi 200A truyền yêu cầu đọc đến thiết bị xử lý thông tin 100 như trong bước S102 được minh họa trên Fig.11 (S60).

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 200A trong bước S60 mã hóa mật dữ liệu tương ứng với vùng được

chỉ báo bởi yêu cầu đọc và truyền dữ liệu được mã hóa theo cách tương ứng như trong các bước từ S104 và S106 được minh họa trên Fig.11 (S62).

Bộ đọc/bộ ghi 200B truyền yêu cầu đọc đến thiết bị xử lý thông tin 100 như trong bước S102 được minh họa trên Fig.11 (S64).

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 200B trong bước S64 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và truyền dữ liệu được mã hóa theo cách tương ứng như trong các bước từ S104 và S106 được minh họa trên Fig.11 (S66).

Ví dụ, trong ví dụ được minh họa trên Fig.24, bộ quan sát có thể xác định xem có hay không việc các phần dữ liệu trước khi được mã hóa mật (văn bản gốc) là giống nhau bằng cách so sánh dữ liệu được mã hóa được truyền trong bước S62 với dữ liệu được mã hóa được truyền trong bước S66.

Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ tư, thiết bị xử lý thông tin 100 tạo ra khóa mã hóa tương ứng với yêu cầu đọc, ví dụ, cho mỗi yêu cầu đọc thu được. Thiết bị xử lý thông tin 100 tạo ra khóa mã hóa mật tương ứng với yêu cầu đọc trên cơ sở của khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc thu được và giá trị tương ứng với yêu cầu đọc khác nhau cho mỗi yêu cầu đọc thu được. Khóa mã hóa mật tương ứng với yêu cầu đọc được tạo ra bằng cách tính toán thuật toán tạo khóa mã hóa mật tùy ý bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và giá trị tương ứng với yêu cầu đọc.

Ví dụ, giá trị tương ứng với yêu cầu đọc theo phương án của sáng chế được tạo ra bằng cách tạo ra số ngẫu nhiên bởi thiết bị xử lý thông tin 100 hoặc được chỉ rõ bằng cách đọc giá trị của mạch đếm được chứa trong thiết bị xử lý thông tin 100 bởi thiết bị xử lý thông tin 100.

Sau đây, để phân biệt khóa mã hóa mật tương ứng với yêu cầu đọc từ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc, có trường hợp trong đó khóa mã hóa mật tương ứng với yêu cầu đọc được chỉ báo là "khóa mã hóa mật".

Khóa mã hóa mật trở thành khóa mã hóa khác dùng cho mỗi yêu cầu đọc bằng cách tạo ra khóa mã hóa mật (khóa mã hóa mật tương ứng với yêu cầu đọc) bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và giá trị tương ứng với yêu cầu đọc khác dùng cho mỗi yêu cầu đọc.

Do đó, ngay cả khi các phần của dữ liệu trước khi được mã hóa mật là giống nhau, dữ liệu được mã hóa mật trên cơ sở của yêu cầu đọc là khác dùng cho mỗi yêu cầu đọc thu được bởi thiết bị xử lý thông tin 100.

Hơn nữa, thiết bị xử lý thông tin 100 có thể sử dụng khóa mã hóa mật được tạo ra là khóa mã hóa cho chữ ký được sử dụng để tạo ra chữ ký điện tử bằng cách sử dụng phương pháp xử lý thông tin theo phương án của sáng chế.

Fig.25 là sơ đồ giải thích để giải thích ví dụ của việc xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 theo phương án thứ tư và minh họa ví dụ của khóa mã hóa mật (khóa mã hóa mật tương ứng với yêu cầu đọc).

Hơn nữa, Fig.25 minh họa ví dụ mà trong đó khóa mã hóa mật cũng được sử dụng làm khóa mã hóa cho chữ ký. Như trên Fig.22, ví dụ của việc tạo ra chữ ký điện tử được minh họa trên Fig.25 là ví dụ về việc tạo ra chữ ký điện tử trong trường hợp mà phương pháp xử lý thông tin theo phương án thứ hai và phương pháp xử lý thông tin theo phương án thứ ba được kết hợp.

Như được minh họa trên Fig.25, thiết bị xử lý thông tin 100 tạo ra khóa mã hóa mật, ví dụ, từ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và số ngẫu nhiên C (ví dụ của giá trị tương ứng với yêu cầu đọc). Sau đó, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu văn bản gốc (dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc) bằng cách sử dụng khóa mã hóa mật được tạo ra. Hơn nữa, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử như trên Fig.22 bằng cách sử dụng khóa mã hóa mật được tạo ra thay vì khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Thiết bị xử lý thông tin 100 truyền giá trị tương ứng với yêu cầu đọc được sử dụng để tạo ra khóa mã hóa mật cùng với dữ liệu được mã hóa mật bằng cách sử dụng khóa mã hóa mật được tạo ra. Hơn nữa, trong trường hợp mà chữ ký điện tử được tạo ra như được minh họa trên Fig.25, thiết bị xử lý thông tin 100 có thể còn truyền chữ ký điện tử được tạo.

"Thiết bị xử lý thông tin 100 truyền giá trị tương ứng với yêu cầu đọc được sử dụng để tạo ra khóa mã hóa mật cùng với dữ liệu được mã hóa mật bằng cách sử dụng khóa mã hóa mật" sao cho thiết bị như là máy chủ 300 mà có khóa mã hóa mật hợp lệ có thể giải mật mã dữ liệu được mã hóa mật.

Lưu ý rằng việc xử lý của thiết bị xử lý thông tin 100 không được giới hạn

ở ví dụ được mô tả nêu trên.

Ví dụ, thiết bị xử lý thông tin 100 chỉ rõ xem có hay không việc tạo ra khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và khóa mã hóa mật (khóa mã hóa mật tương ứng với yêu cầu đọc) trên cơ sở của thông tin thiết đặt được kết hợp với vùng của phương tiện ghi.

Có hay không việc tạo ra khóa mã hóa mật được chỉ rõ, ví dụ, bằng cách viện dẫn tới thông tin sự cần thiết của việc tạo khóa mã hóa mật được chứa trong thông tin thiết đặt.

Ví dụ, trong trường hợp mà thông tin sự cần thiết của việc tạo khóa mã hóa mật chỉ báo "để tạo ra liên tục "khóa mã hóa mật tương ứng với yêu cầu đọc", thiết bị xử lý thông tin 100 tạo ra khóa mã hóa mật và mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc như được minh họa trên Fig.25. Hơn nữa, ví dụ, trong trường hợp mà thông tin sự cần thiết của việc tạo khóa mã hóa mật chỉ báo "không để tạo ra liên tục "khóa mã hóa mật tương ứng với yêu cầu đọc", thiết bị xử lý thông tin 100 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

Hơn nữa, ví dụ, trong trường hợp mà thông tin sự cần thiết của việc tạo khóa mã hóa mật chỉ báo "để tuân theo yêu cầu đọc", thiết bị xử lý thông tin 100 một cách chọn lọc tạo ra khóa mã hóa mật theo dữ liệu (ví dụ của thông tin liên quan đến mã hóa mật) chỉ báo xem có hay không việc tạo ra "khóa mã hóa mật tương ứng với yêu cầu đọc" được chứa trong yêu cầu đọc. Trong trường hợp này, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc hoặc khóa mã hóa mật được tạo ra.

Như được mô tả ở trên, trong hệ thống xử lý thông tin 1000 theo phương án thứ tư, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu bằng cách sử dụng khóa mã hóa mật sao cho dữ liệu được mã hóa mật trên cơ sở của yêu cầu đọc là khác dùng cho mỗi yêu cầu đọc thu được bởi thiết bị xử lý thông tin 100 ngay cả khi các phần của dữ liệu trước khi được mã hóa mật là giống nhau.

Do đó, hệ thống xử lý thông tin 1000 theo phương án thứ tư ngăn việc "bên thứ ba có thể xác định xem có hay không việc dữ liệu được mã hóa là dữ liệu tương tự".

Hơn nữa, trong hệ thống xử lý thông tin 1000 theo phương án thứ tư, việc xử lý tương tự với của một hoặc nhiều hệ thống xử lý thông tin 1000 theo phương án thứ nhất đến hệ thống xử lý thông tin 1000 theo phương án thứ ba có thể còn được thực hiện. Do đó, hệ thống xử lý thông tin 1000 theo phương án thứ tư có thể thu nhận các hiệu quả thu nhận được bằng cách một hoặc nhiều hệ thống xử lý thông tin 1000 theo phương án thứ nhất đến hệ thống xử lý thông tin 1000 theo phương án thứ ba.

[2-4-2] Việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ tư

Tiếp theo, ví dụ về việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ tư sẽ được mô tả.

Fig.26 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ tư. Fig.26 minh họa ví dụ của việc xử lý trong trường hợp mà phương pháp xử lý thông tin theo phương án thứ nhất đến phương pháp xử lý thông tin theo phương án thứ ba được kết hợp.

Máy chủ 300 truyền số ngẫu nhiên R cùng với yêu cầu đọc như trong bước S300 trên Fig.19 (S500). Lưu ý rằng, trong trường hợp mà việc xử lý theo phương pháp xử lý thông tin theo phương án thứ hai không được thực hiện, không cần thiết là máy chủ 300 truyền số ngẫu nhiên.

Bộ đọc/bộ ghi 200 mà đã thu yêu cầu đọc và số ngẫu nhiên được truyền từ máy chủ 300 trong bước S500 truyền yêu cầu đọc thu được và số ngẫu nhiên R đến thiết bị xử lý thông tin 100 như trong bước S300 trên Fig.19 (S502).

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc và số ngẫu nhiên R được truyền từ bộ đọc/bộ ghi 200 trong bước S502 mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc và tạo ra chữ ký điện tử như trên Fig.25 (S504). Sau đó, thiết bị xử lý thông tin 100 truyền số ngẫu nhiên C (ví dụ của giá trị tương ứng với yêu cầu đọc) và chữ ký điện tử cùng với dữ liệu được mã hóa (S506).

Bộ đọc/bộ ghi 200 mà đã thu dữ liệu được truyền từ thiết bị xử lý thông tin 100 trong bước S506 truyền dữ liệu thu được đến máy chủ 300 (S508).

Máy chủ 300 mà đã thu dữ liệu được truyền từ bộ đọc/bộ ghi 200 trong bước S508 giải mã mật dữ liệu được mã hóa và xác minh chữ ký điện tử (S510).

Sau đó, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử là bình thường, máy chủ 300 sử dụng dữ liệu được giải mã mật cho việc xử lý tùy ý. Hơn nữa, trong trường hợp mà kết quả xác nhận chỉ báo rằng chữ ký điện tử không là bình thường, máy chủ 300 không sử dụng dữ liệu được giải mã mật cho việc xử lý tùy ý.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ tư, ví dụ, "bên thứ ba có thể xác định xem có hay không việc dữ liệu được mã hóa là cùng một dữ liệu" được ngăn bằng cách thực hiện việc xử lý được minh họa trên Fig.26.

[2-4-3] Thao tác và Hiệu quả của hệ thống xử lý thông tin 1000 theo phương án thứ tư

Trong hệ thống xử lý thông tin thứ tư 1000, ví dụ, các thao tác dưới đây được nhận biết. Hơn nữa, bằng cách sử dụng hệ thống xử lý thông tin thứ tư 1000, ví dụ, thu được các hiệu ứng dưới đây. Lưu ý rằng hiển nhiên rằng các thao tác của hệ thống xử lý thông tin 1000 theo phương án thứ tư và các hiệu quả thu được bằng cách sử dụng hệ thống xử lý thông tin theo phương án thứ tư không được giới hạn ở các ví dụ dưới đây.

Thiết bị xử lý thông tin 100 tạo ra giá trị (số ngẫu nhiên, giá trị bộ đếm được giữ trong thiết bị xử lý thông tin 100, hoặc loại tương tự) khác dùng cho mỗi yêu cầu đọc.

Khi mã hóa mật dữ liệu được đọc, thiết bị xử lý thông tin 100 mã hóa mật dữ liệu bằng cách sử dụng khóa mã hóa mật được tạo ra từ giá trị khác dùng cho mỗi yêu cầu đọc.

Thiết bị xử lý thông tin 100 truyền giá trị khác dùng cho mỗi yêu cầu đọc đến bộ đọc/bộ ghi 200 cùng với dữ liệu được mã hóa mật.

Trên cơ sở của thông tin thiết đặt mà được thiết đặt cho vùng trước, thiết bị xử lý thông tin 100 xác định xem có hay không việc tạo ra khóa mã hóa mật từ giá trị khác dùng cho mỗi yêu cầu đọc và loại khóa được sử dụng để tạo ra khóa mã hóa mật khi các khóa được kết hợp với vùng.

Đối với vùng mà được thiết đặt là "không cần tạo ra khóa mã hóa mật", xem có hay không việc tạo ra khóa mã hóa mật có thể được chỉ rõ theo tham số của yêu cầu đọc (ví dụ của thông tin liên quan đến mã hóa mật). Hơn nữa, khóa nào được sử dụng cho vùng mà được thiết đặt là "không cần tạo ra khóa mã hóa

mật" có thể được chỉ rõ theo tham số của yêu cầu đọc (ví dụ của thông tin liên quan đến mã hóa mật).

[2-5] Phương pháp xử lý thông tin theo phương án thứ năm

[2-5-1] Phác thảo của hệ thống xử lý thông tin 1000 mà Phương pháp xử lý thông tin theo phương án thứ năm được áp dụng

Ví dụ, với hệ thống xử lý thông tin 1000 có cấu trúc được minh họa trên Fig.1, trong trường hợp mà thiết bị xử lý thông tin 100 truyền thông tin lỗi chỉ báo lỗi khi thiết bị xử lý thông tin 100 thất bại trong việc đọc dữ liệu để đáp lại yêu cầu đọc, có khả năng là bên thứ ba có thể xác định rằng lỗi xảy ra bằng cách quan sát dữ liệu được truyền từ thiết bị xử lý thông tin 100 đến bộ đọc/bộ ghi 200 bởi bên thứ ba. Ví dụ, trong trường hợp mà độ dài dữ liệu của thông tin lỗi được xác định phụ thuộc vào tiêu chuẩn hoặc loại tương tự, có khả năng là bên thứ ba có thể xác định rằng lỗi xảy ra kể cả việc xem có hay không việc dữ liệu được mã hóa mật theo độ dài dữ liệu của dữ liệu được truyền từ thiết bị xử lý thông tin 100 đến bộ đọc/bộ ghi 200.

Fig.27 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó bên thứ ba quan sát dữ liệu được truyền từ thiết bị xử lý thông tin 100 đến bộ đọc/bộ ghi 200 và được xác định là lỗi xảy ra.

Bộ đọc/bộ ghi 200 truyền yêu cầu đọc đến thiết bị xử lý thông tin 100 như trong bước S102 được minh họa trên Fig.11 (S70).

Thiết bị xử lý thông tin 100 mà đã thu yêu cầu đọc được truyền từ bộ đọc/bộ ghi 200 trong bước S70 truyền thông tin lỗi trong trường hợp mà vùng được chỉ báo bởi yêu cầu đọc không tồn tại (S72).

Ví dụ, trong ví dụ được minh họa trên Fig.27, có khả năng là bộ quan sát có thể xác định rằng lỗi xảy ra kể cả việc xem có hay không việc dữ liệu được mã hóa mật theo độ dài dữ liệu của dữ liệu được truyền trong bước S72. Hơn nữa, trong ví dụ được minh họa Fig.27, có khả năng là bộ quan sát chỉ rõ nguyên nhân của lỗi, ví dụ, vì vùng được chỉ báo bởi yêu cầu đọc không tồn tại.

Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ năm, ví dụ, trong trường hợp mà không thể đọc dữ liệu từ vùng được chỉ báo bởi yêu cầu đọc, thiết bị xử lý thông tin 100 mã hóa mật thông tin lỗi và dữ liệu giả bằng cách sử dụng khóa mã hóa mật định trước.

Đối với dữ liệu giả theo phương án của sáng chế, ví dụ, dữ liệu số ngẫu nhiên, dữ liệu của tất cả các số không, hoặc loại tương tự được minh họa. Ví dụ, trong trường hợp mà độ dài dữ liệu khi dữ liệu được đọc một cách bình thường để đáp lại yêu cầu đọc được xác định phụ thuộc vào tiêu chuẩn hoặc loại tương tự, độ dài dữ liệu của dữ liệu giả có thể là "độ dài dữ liệu thu nhận được bằng cách loại bỏ độ dài dữ liệu của thông tin lỗi khỏi độ dài dữ liệu đã được xác định".

Đối với khóa mã hóa mật định trước theo phương án thứ năm, ví dụ, khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc hoặc khóa mã hóa mật được chỉ báo trong phương án thứ tư (khóa mã hóa mật tương ứng với yêu cầu đọc) được minh họa.

Fig.28 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100 theo phương án thứ năm. Fig.28 minh họa ví dụ mà trong đó thông tin lỗi và dữ liệu giả được mã hóa mật bằng cách sử dụng khóa mã hóa mật (khóa mã hóa mật tương ứng với yêu cầu đọc). Hơn nữa, Fig.28 minh họa ví dụ mà trong đó khóa mã hóa mật cũng được sử dụng làm khóa mã hóa cho chữ ký như trên Fig.25.

Như được minh họa trên Fig.28, thiết bị xử lý thông tin 100 tạo ra khóa mã hóa mật từ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và số ngẫu nhiên C (ví dụ của giá trị tương ứng với yêu cầu đọc) như trên Fig.25. Sau đó, thiết bị xử lý thông tin 100 mã hóa mật thông tin lỗi và dữ liệu giả bằng cách sử dụng khóa mã hóa mật được tạo ra. Hơn nữa, thiết bị xử lý thông tin 100 tạo ra chữ ký điện tử như trên Fig.25.

Khi thông tin lỗi và dữ liệu giả được mã hóa mật, thiết bị xử lý thông tin 100 truyền dữ liệu được mã hóa mật. Tức là, dữ liệu được mã hóa được truyền bởi thiết bị xử lý thông tin 100 là khác với dữ liệu thu nhận được bằng cách mã hóa mật đơn giản thông tin lỗi.

Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ năm, ngay cả khi trường hợp trong đó bên thứ ba quan sát dữ liệu được truyền từ thiết bị xử lý thông tin 100 đến bộ đọc/bộ ghi 200, khó dùng cho bên thứ ba xác định rằng lỗi xảy ra.

[2-5-2] Việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ năm

Tiếp theo, ví dụ về việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ năm sẽ được mô tả.

Hệ thống xử lý thông tin 1000 theo phương án thứ năm có thể về cơ bản thực hiện xử lý tương tự với việc xử lý được minh họa trên Fig.11 (xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ nhất), việc xử lý được minh họa trên Fig.19 (xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ hai), việc xử lý được minh họa trên Fig.23 (xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ ba), và việc xử lý được minh họa trên Fig.26 (xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ tư). Sự khác biệt từ các xử lý này là việc thiết bị xử lý thông tin 100 theo phương án thứ năm "mã hóa mật thông tin lỗi và dữ liệu giả bằng cách sử dụng khóa mã hóa mật định trước và truyền dữ liệu được mã hóa trong trường hợp mà không thể đọc dữ liệu từ vùng được chỉ báo bởi yêu cầu đọc".

[2-5-3] Thao tác và Hiệu quả của hệ thống xử lý thông tin 1000 theo phương án thứ năm

Trong hệ thống xử lý thông tin thứ năm 1000, ví dụ, các thao tác dưới đây được nhận biết. Hơn nữa, bằng cách sử dụng hệ thống xử lý thông tin thứ năm 1000, ví dụ, thu được các hiệu ứng dưới đây. Lưu ý rằng hiển nhiên rằng các thao tác của hệ thống xử lý thông tin 1000 theo phương án thứ năm và các hiệu quả thu được bằng cách sử dụng hệ thống xử lý thông tin theo phương án thứ năm không được giới hạn ở các ví dụ dưới đây.

Trong trường hợp mà lỗi xảy ra, thiết bị xử lý thông tin 100 truyền thông tin lỗi và dữ liệu giả (ví dụ, dữ liệu số ngẫu nhiên và dữ liệu của tất cả các số không) đến bộ đọc/bộ ghi 200. Thiết bị xử lý thông tin 100 mã hóa mật dữ liệu giả và thông tin lỗi.

[2-6] Phương pháp xử lý thông tin theo phương án thứ sáu

[2-6-1] Phác thảo của hệ thống xử lý thông tin 1000 mà Phương pháp xử lý thông tin theo phương án thứ sáu được áp dụng

Ví dụ, trong trường hợp mà thông tin nhận dạng như là ID được lưu trữ trong thiết bị xử lý thông tin 100, thiết bị phía ngoài của thiết bị xử lý thông tin 100 như là máy chủ 300 và bộ đọc/bộ ghi 200 có thể thực hiện xử lý khác nhau

bằng cách sử dụng thông tin nhận dạng được lưu trong thiết bị xử lý thông tin 100.

Ở đây, khi trường hợp sử dụng được giả thiết mà trong đó thông tin nhận dạng được lưu trong thiết bị xử lý thông tin 100 được sử dụng bởi các nhà điều hành kinh doanh, có sự liên hệ sau đây.

Trong trường hợp mà nhà điều hành kinh doanh cụ thể liên kết thông tin nhận dạng với thông tin quan trọng, có khả năng là một nhà điều hành kinh doanh khác có thể có thông tin quan trọng từ thông tin nhận dạng đã được đọc. Ví dụ, xét đến việc "mã quốc gia (ví dụ của thông tin nhận dạng) được đọc từ bộ đọc/bộ ghi của cửa hàng chung được truyền đến người mà có quyền truy nhập vào cơ sở dữ liệu mã quốc gia sao cho thông tin thanh toán thuế (ví dụ của thông tin quan trọng) được kết hợp với mã quốc gia được viện dẫn tới".

Trong trường hợp mà thông tin nhận dạng có thể được đọc mà không cần xác thực, có khả năng là bên thứ ba có thể thấy được thông tin quan trọng từ thông tin nhận dạng.

Trong trường hợp mà thông tin nhận dạng có thể được đọc chỉ sau khi sự xác thực, khóa mã hóa cho việc xác thực được sử dụng để đọc thông tin nhận dạng được sử dụng bởi các nhà điều hành kinh doanh. Việc này làm tăng rủi ro rò rỉ khóa mã hóa mật cho việc xác thực.

Fig.29 là sơ đồ giải thích minh họa ví dụ của trường hợp trong đó thông tin nhận dạng được lưu trữ trong thiết bị xử lý thông tin được sử dụng bởi các nhà điều hành kinh doanh. Fig.29 minh họa ID là thông tin nhận dạng.

Như được minh họa trên Fig.29, có thể là trường hợp trong đó ID được lưu trong thiết bị xử lý thông tin được quản lý bởi cơ sở dữ liệu được quản lý bởi các nhà điều hành kinh doanh. Như được minh họa trên Fig.29, trong trường hợp mà nhà điều hành A làm cho nhà điều hành B sử dụng ID được lưu trong thiết bị xử lý thông tin, có rủi ro liên quan được mô tả nêu trên.

Do đó, trong hệ thống xử lý thông tin 1000 theo phương án thứ sáu, thiết bị xử lý thông tin 100 truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách thực hiện việc xử lý theo phương pháp xử lý thông tin theo phương án thứ nhất đến việc xử lý theo phương pháp xử lý thông tin theo phương án thứ năm.

Hơn nữa, trong hệ thống xử lý thông tin 1000 theo phương án thứ sáu, trong trường hợp mà dữ liệu được thu từ thiết bị xử lý thông tin 100 bao gồm thông tin nhận dạng thứ nhất, máy chủ 300 chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai mà khác với thông tin nhận dạng thứ nhất.

Đối với thông tin nhận dạng thứ nhất, ví dụ, ID tùy ý như là ID của thiết bị xử lý thông tin 100 hoặc ID của dịch vụ được minh họa. Hơn nữa, đối với thông tin nhận dạng thứ hai, ID tùy ý khác với thông tin nhận dạng thứ nhất như là ID của dịch vụ khác với dịch vụ tương ứng với thông tin nhận dạng thứ nhất được minh họa.

Máy chủ 300 chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai, ví dụ, bằng cách viện dẫn tới "Bảng (hoặc Cơ sở dữ liệu) mà trong đó thông tin nhận dạng thứ nhất, thông tin nhận dạng thứ hai, và thông tin kỹ thuật điểm đích chuyển đổi được liên kết với nhau". Với Bảng, dữ liệu (ví dụ, dữ liệu chỉ báo địa chỉ Giao thức Internet (IP), địa chỉ thư, hoặc loại tương tự) chỉ báo điểm đích truyền mà thông tin nhận dạng thứ hai được truyền có thể còn được liên kết. Sau đây, Bảng được gọi là "Bảng chuyển đổi".

Ở đây, thông tin kỹ thuật điểm đích chuyển đổi là dữ liệu được sử dụng để chỉ rõ duy nhất thông tin nhận dạng thứ hai được kết hợp với thông tin nhận dạng thứ nhất. Đối với thông tin kỹ thuật điểm đích chuyển đổi, ví dụ, dữ liệu tùy ý mà đích mà thông tin nhận dạng thứ hai được cung cấp (nhà điều hành kinh doanh hoặc loại tương tự) có thể được chỉ rõ như là ID của bộ đọc/bộ ghi (ví dụ của thiết bị chuyển tiếp) mà chuyển tiếp dữ liệu được truyền từ thiết bị xử lý thông tin 100, ID của thiết bị mà yêu cầu máy chủ 300 để truyền yêu cầu đọc, hoặc loại tương tự được minh họa.

Lưu ý rằng máy chủ 300 có thể chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai bằng cách thực hiện xử lý thuật toán tùy ý mà có thể chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai.

Khi thông tin nhận dạng thứ nhất được chuyển đổi thành thông tin nhận dạng thứ hai, máy chủ 300 truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Trong hệ thống xử lý thông tin 1000 theo phương án thứ sáu, máy chủ 300

chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai và truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Do đó, hệ thống xử lý thông tin 1000 theo phương án thứ sáu nhận biết rằng "mỗi nhà điều hành kinh doanh cung cấp dịch vụ dựa trên thông tin nhận dạng mà không cần chia sẻ thông tin nhận dạng được lưu trong thiết bị xử lý thông tin 100 bởi các nhà điều hành kinh doanh". Tức là, hệ thống xử lý thông tin 1000 theo phương án thứ sáu không gây ra sự trở ngại được mô tả nêu trên.

[2-6-2] Việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ sáu

Tiếp theo, ví dụ về việc xử lý theo phương pháp xử lý thông tin bởi hệ thống xử lý thông tin 1000 theo phương án thứ sáu sẽ được mô tả.

Fig.30 là sơ đồ giải thích minh họa ví dụ của trường hợp sử dụng mà hệ thống xử lý thông tin 1000 theo phương án thứ sáu được áp dụng. Trên Fig.30, thiết bị xử lý thông tin 100 tương ứng với nhà điều hành kinh doanh A được gọi là "thiết bị xử lý thông tin 100A". Hơn nữa, trên Fig.30, bộ đọc/bộ ghi 200 tương ứng với nhà điều hành kinh doanh B được gọi là "bộ đọc/bộ ghi 200B". Hơn nữa, trên Fig.30, máy chủ 300 tương ứng với nhà điều hành kinh doanh A được gọi là "máy chủ 300A", và máy chủ 300 tương ứng với nhà điều hành kinh doanh B được gọi là "máy chủ 300B".

Trong trường hợp mà dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc là ID_A (ví dụ của thông tin nhận dạng thứ nhất), thiết bị xử lý thông tin 100A mã hóa mật ID_A. Sau đây, ID được mã hóa mật được gọi là "ID ẩn danh". Đối với ID ẩn danh, ví dụ, giá trị được tạo ra bởi thao tác đảo ngược từ giá trị khóa mật được minh họa.

Fig.31 là sơ đồ giải thích để giải thích ví dụ của xử lý theo phương pháp xử lý thông tin bởi thiết bị xử lý thông tin 100A theo phương án thứ sáu. Fig.31 minh họa "ví dụ mà trong đó thiết bị xử lý thông tin 100A mã hóa mật ID_A và tạo ra chữ ký điện tử như trên Fig.25".

Thiết bị xử lý thông tin 100A truyền dữ liệu bao gồm ID ẩn danh đến bộ đọc/bộ ghi 200.

Bộ đọc/bộ ghi 200B mà đã thu dữ liệu bao gồm ID ẩn danh truyền dữ liệu

thu được bao gồm ID ẩn danh đến máy chủ 300A. Điểm đích truyền mà bộ đọc/bộ ghi 200B truyền dữ liệu có thể được thiết đặt trước hoặc có thể được xác định theo dữ liệu được chứa trong yêu cầu đọc hoặc loại tương tự.

Máy chủ 300A mà đã thu dữ liệu bao gồm ID ẩn danh giải mã mật ID ẩn danh và thu được ID_A. Khi ID_A được thu, máy chủ 300A chuyển đổi ID_A thành ID_B (thông tin nhận dạng thứ hai).

Sau đó, máy chủ 300A truyền ID_B đến máy chủ 300B. Máy chủ 300A chỉ rõ điểm đích truyền mà ID_B được truyền, ví dụ, bằng cách viện dẫn tới dữ liệu chỉ báo điểm đích truyền được ghi trong bảng chuyển đổi.

Máy chủ 300B mà đã thu ID_B chỉ rõ điểm được kết hợp với ID_B thu được (ví dụ của dữ liệu được kết hợp với thông tin nhận dạng thứ hai) và sử dụng điểm được chỉ rõ dùng cho việc xử lý tùy ý.

Fig.32 là sơ đồ giải thích minh họa ví dụ của việc xử lý hệ thống xử lý thông tin 1000 theo phương án thứ sáu và minh họa ví dụ của việc xử lý tương ứng với trường hợp sử dụng được minh họa trên Fig.30. Fig.32 minh họa ví dụ của việc xử lý trong trường hợp mà phương pháp xử lý thông tin theo phương án thứ nhất đến phương pháp xử lý thông tin theo phương án thứ ba được kết hợp như trên Fig.26. Hơn nữa, trên Fig.32, giả thiết rằng yêu cầu đọc là yêu cầu đọc để đọc ID_A.

Máy chủ 300A truyền số ngẫu nhiên R cùng với yêu cầu đọc như trong bước S300 trên Fig.19 (S600).

Bộ đọc/bộ ghi 200B mà đã thu yêu cầu đọc và số ngẫu nhiên R được truyền từ máy chủ 300A trong bước S600 truyền yêu cầu đọc thu được và số ngẫu nhiên R đến thiết bị xử lý thông tin 100A như trong bước S300 trên Fig.19 (S602). Lưu ý rằng yêu cầu đọc và số ngẫu nhiên R được thu bởi bộ đọc/bộ ghi 200B không được truyền từ máy chủ 300A.

Thiết bị xử lý thông tin 100A mà đã thu yêu cầu đọc và số ngẫu nhiên R được truyền từ bộ đọc/bộ ghi 200B trong bước S602 tạo ra ID ẩn danh và tạo ra chữ ký điện tử như trên Fig.31 (S604). Sau đó, thiết bị xử lý thông tin 100A truyền số ngẫu nhiên C (ví dụ của giá trị tương ứng với yêu cầu đọc) và chữ ký điện tử cùng với ID ẩn danh (S606).

Bộ đọc/bộ ghi 200B mà đã thu dữ liệu được truyền từ thiết bị xử lý thông

tin 100A trong bước S606 truyền dữ liệu thu được đến máy chủ 300A (S608).

Máy chủ 300A mà đã thu dữ liệu được truyền từ bộ đọc/bộ ghi 200B trong bước S608 xác minh chữ ký điện tử, giải mã mật ID ẩn danh, và chuyển đổi ID_A được giải mã mật (S610).

Máy chủ 300A truyền ID_B thu nhận được bằng cách chuyển đổi ID_A trong bước S610 đến máy chủ 300B (S612). Lưu ý rằng đích truyền của ID_B không được giới hạn ở máy chủ 300B và có thể là thiết bị khác như là bộ đọc/bộ ghi 200B.

Ví dụ, bằng cách xử lý được minh họa trên Fig.31, trường hợp sử dụng được mô tả có viện dẫn tới Fig.30 được nhận biết. Lưu ý rằng hiển nhiên rằng việc xử lý để nhận biết trường hợp sử dụng được mô tả có viện dẫn tới Fig.30 không được giới hạn ở ví dụ được minh họa trên Fig.31.

[2-6-3] Thao tác và Hiệu quả của hệ thống xử lý thông tin 1000 theo phương án thứ sáu

Trong hệ thống xử lý thông tin thứ sáu 1000, ví dụ, các thao tác dưới đây được nhận biết. Hơn nữa, bằng cách sử dụng hệ thống xử lý thông tin thứ sáu 1000, ví dụ, thu được các hiệu ứng dưới đây. Lưu ý rằng hiển nhiên rằng các thao tác của hệ thống xử lý thông tin 1000 theo phương án thứ sáu và các hiệu quả thu được bằng cách sử dụng hệ thống xử lý thông tin theo phương án thứ sáu không được giới hạn ở các ví dụ dưới đây.

· Khi ID được đọc từ thiết bị xử lý thông tin 100, thiết bị xử lý thông tin 100 truyền ID, số ngẫu nhiên được tạo ra bởi thiết bị xử lý thông tin 100, và ID ẩn danh (ví dụ, giá trị được tạo ra bởi thao tác đảo ngược từ giá trị khóa mật), thay vì ID của nó, đến bộ đọc/bộ ghi 200.

· Bộ đọc/bộ ghi 200 truyền ID ẩn danh đến máy chủ 300.

· Máy chủ 300 thu nhận ID ban đầu từ ID ẩn danh bằng cách thực hiện thao tác đảo ngược. Hơn nữa, máy chủ 300 chuyển đổi ID thu nhận được thành một ID khác mà được sử dụng bởi một thiết bị khác.

· ID được lưu trong thiết bị xử lý thông tin 100 không được bộc lộ cho các thiết bị khác ngoài máy chủ 300.

[2-7] Phương pháp xử lý thông tin theo phương án khác

Việc xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế không được giới hạn ở việc xử lý theo phương pháp xử lý thông tin theo phương án thứ nhất đến việc xử lý theo phương pháp xử lý thông tin theo phương án thứ sáu.

Ví dụ, việc xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế có thể được xử lý kết hợp hai hoặc nhiều xử lý theo phương pháp xử lý thông tin theo phương án thứ nhất đến việc xử lý theo phương pháp xử lý thông tin theo phương án thứ sáu.

(Chương trình theo phương án của sáng chế)

[I] Chương trình có chức năng như thiết bị xử lý thông tin (Thiết bị xử lý thông tin thứ nhất) theo phương án của sáng chế

Bằng cách thực hiện chương trình mà làm cho hệ thống máy tính có chức năng như thiết bị xử lý thông tin theo phương án của sáng chế (ví dụ, chương trình mà có thể nhận biết chức năng của bộ xử lý 110 được minh họa trên Fig.2) bởi bộ xử lý hoặc loại tương tự trong hệ thống máy tính, "hệ thống xử lý thông tin mà có thể giảm thời gian xử lý để đọc trong khi đảm bảo sự bảo mật liên quan đến việc đọc dữ liệu" được nhận biết. Ở đây, đối với hệ thống máy tính theo phương án của sáng chế, máy tính đơn lẻ hoặc các máy tính được minh họa. Chuỗi xử lý được thực hiện bởi hệ thống máy tính theo phương án của sáng chế.

Hơn nữa, bằng cách thực hiện chương trình mà làm cho hệ thống máy tính có chức năng như thiết bị xử lý thông tin theo phương án của sáng chế bởi bộ xử lý hoặc loại tương tự trong hệ thống máy tính, các hiệu quả thu nhận được bằng cách việc xử lý theo phương pháp xử lý thông tin theo mỗi phương án có thể được thu nhận.

[II] Chương trình có chức năng như Máy chủ (Thiết bị xử lý thông tin thứ hai) theo phương án của sáng chế

Bằng cách thực hiện chương trình mà làm cho hệ thống máy tính có chức năng như máy chủ theo phương án của sáng chế (ví dụ, chương trình mà có thể nhận biết chức năng của bộ xử lý 310 được minh họa trên Fig.7) bởi bộ xử lý hoặc loại tương tự trong hệ thống máy tính, "hệ thống xử lý thông tin mà có thể giảm thời gian xử lý để đọc trong khi đảm bảo sự bảo mật liên quan đến việc đọc dữ liệu" được nhận biết.

Hơn nữa, bằng cách thực hiện chương trình mà làm cho hệ thống máy tính có chức năng như máy chủ theo phương án của sáng chế bởi bộ xử lý hoặc loại tương tự trong hệ thống máy tính, các hiệu quả thu nhận được bằng cách việc xử lý theo phương pháp xử lý thông tin theo mỗi phương án có thể được thu nhận.

Các phương án ưu tiên của sáng chế được mô tả cụ thể ở trên có viện dẫn tới bộ hình vẽ. Tuy nhiên, phạm vi kỹ thuật của sáng chế không bị giới hạn ở các ví dụ này. Hiển nhiên là người có hiểu biết trung bình trong lĩnh vực kỹ thuật được đề cập của sáng chế có thể thu được các biến thể và sửa đổi khác nhau trong phạm vi của các ý tưởng kỹ thuật được mô tả trong bộ yêu cầu bảo hộ. Cần hiểu rằng các biến thể và sửa đổi bản chất thuộc về phạm vi kỹ thuật của sáng chế.

Ví dụ, trong phần trên, được mô tả rằng chương trình mà làm cho hệ thống máy tính có chức năng như thiết bị xử lý thông tin theo phương án của sáng chế (chương trình máy tính) và chương trình mà làm cho hệ thống máy tính có chức năng như máy chủ theo phương án của sáng chế (chương trình máy tính) được cung cấp riêng biệt. Tuy nhiên, phương án của sáng chế có thể cung cấp các phương tiện ghi mà theo cách tương ứng lưu trữ các chương trình hoặc phương tiện ghi mà lưu trữ cả hai chương trình.

Cấu trúc được mô tả nêu trên chỉ báo ví dụ của phương án của sáng chế và về bản chất thuộc phạm vi kỹ thuật của sáng chế.

Hơn nữa, các hiệu quả được mô tả trong bản mô tả này chỉ mang tính minh họa và làm mẫu và không bị giới hạn. Tức là, kỹ thuật theo sáng chế có thể mang tới các hiệu quả khác là rõ ràng với những người có hiểu biết trung bình trong lĩnh vực kỹ thuật từ phần mô tả trong bản mô tả này cùng với hoặc thay cho các hiệu quả được mô tả ở trên.

Lưu ý rằng cấu trúc sau thuộc về phạm vi kỹ thuật của sáng chế.

(1)

Thiết bị xử lý thông tin bao gồm:

bộ xử lý có cấu trúc để, trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu, mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu

đọc và truyền dữ liệu được mã hóa mật.

(2)

Thiết bị xử lý thông tin Theo (1), mà trong đó bộ xử lý chỉ rõ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin thiết đặt được kết hợp với vùng của phương tiện ghi và mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật được mã hóa mật.

(3)

Thiết bị xử lý thông tin theo (2), mà trong đó trong trường hợp mà khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc không được chỉ rõ, bộ xử lý truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc mà không mã hóa mật dữ liệu.

(4)

Thiết bị xử lý thông tin theo (2) hoặc (3), mà trong đó

bộ xử lý

xác định xem có hay không việc mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin thiết đặt, và

mã hóa mật một cách chọn lọc dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc theo kết quả xác định.

(5)

Thiết bị xử lý thông tin theo (4), mà trong đó

trong trường hợp mà không được xác định rằng dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc được mã hóa mật,

bộ xử lý

mã hóa mật một cách chọn lọc dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin liên quan đến mã hóa mật được chứa trong yêu cầu đọc, và

truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc hoặc dữ liệu được mã hóa mật.

(6)

Thiết bị xử lý thông tin theo phần bất kỳ trong số các phần từ (1) đến (5), mà trong đó trong trường hợp mà yêu cầu đọc chỉ báo các vùng, bộ xử lý thực hiện mã hóa mật cho mỗi trong các vùng đó được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

(7)

Thiết bị xử lý thông tin theo phần bất kỳ trong số các phần từ (1) đến (6), mà trong đó

trong trường hợp mà thông tin chỉ báo giá trị được thu cùng với yêu cầu đọc,

bộ xử lý

tạo ra chữ ký điện tử từ ít nhất dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và

còn truyền chữ ký điện tử được tạo.

(8)

Thiết bị xử lý thông tin theo (7), mà trong đó

trong trường hợp mà yêu cầu đọc chỉ báo các vùng,

bộ xử lý

tạo ra chữ ký điện tử cho mỗi trong số các vùng đó được chỉ báo bởi yêu cầu đọc hoặc

tạo ra chữ ký điện tử từ dữ liệu tương ứng với các vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa cho chữ ký được tạo ra trên cơ sở của khóa mã hóa mật tương ứng với các vùng được chỉ báo bởi yêu cầu đọc.

(9)

Thiết bị xử lý thông tin theo phần bất kỳ trong số các phần từ (1) đến (7), mà trong đó

bộ xử lý

tạo ra chữ ký điện tử từ ít nhất dữ liệu tương ứng với vùng được chỉ báo bởi

yêu cầu đọc, thông tin được chứa trong yêu cầu đọc, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và

còn truyền chữ ký điện tử được tạo.

(10)

Thiết bị xử lý thông tin theo phần bất kỳ trong số các phần từ (1) đến (9), mà trong đó

bộ xử lý

tạo ra khóa mã hóa tương ứng với yêu cầu đọc trên cơ sở của khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và giá trị tương ứng với yêu cầu đọc, và

trong trường hợp mà khóa mã hóa mật tương ứng với yêu cầu đọc được tạo ra, mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật được tạo ra tương ứng với yêu cầu đọc và truyền dữ liệu được mã hóa và giá trị tương ứng với yêu cầu đọc.

(11)

Thiết bị xử lý thông tin theo (10), mà trong đó

bộ xử lý

chỉ rõ xem có hay không việc tạo ra khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và khóa mã hóa mật tương ứng với yêu cầu đọc trên cơ sở của thông tin thiết đặt được kết hợp với vùng của phương tiện ghi và

mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc hoặc khóa mã hóa mật được tạo ra tương ứng với yêu cầu đọc trên cơ sở của kết quả kỹ thuật.

(12)

Thiết bị xử lý thông tin theo phần bất kỳ trong số các phần từ (1) đến (11), mà trong đó

trong trường hợp mà không thể đọc dữ liệu từ vùng được chỉ báo bởi yêu cầu đọc,

bộ xử lý mã hóa mật thông tin lỗi chỉ báo lỗi và dữ liệu giả bằng cách sử

dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

(13)

Thiết bị xử lý thông tin bao gồm:

bộ xử lý có cấu trúc để giải mật mã dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước, chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất, và truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

(14)

Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp bao gồm:

bước mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu; và

bước truyền dữ liệu được mã hóa mật.

(15)

Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp bao gồm:

bước giải mã mật dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước;

bước chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất; và

bước truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

(16)

Chương trình làm cho máy tính thực hiện:

bước mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu

đọc trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu; và

bước truyền dữ liệu được mã hóa mật.

(17)

Chương trình làm cho máy tính thực hiện:

bước giải mã mật dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước;

bước chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất; và

bước truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

(18)

Hệ thống xử lý thông tin bao gồm:

thiết bị xử lý thông tin thứ nhất; và

thiết bị xử lý thông tin thứ hai, mà trong đó

thiết bị xử lý thông tin thứ nhất bao gồm

bộ xử lý mà mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa tương ứng với vùng được chỉ báo bởi yêu cầu đọc trong trường hợp mà yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà dữ liệu đã đọc được yêu cầu và truyền dữ liệu được mã hóa, và

thiết bị xử lý thông tin thứ hai bao gồm

bộ xử lý mà giải mã mật dữ liệu được mã hóa mà được yêu cầu bằng cách sử dụng khóa mã hóa mật định trước, chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất, và truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài tương ứng với thông tin nhận dạng thứ hai.

Danh mục số chỉ dẫn

10, 100, 100A Thiết bị xử lý thông tin

20, 200, 200A, 200B Bộ đọc/bộ ghi

30, 300, 300A, 300B Máy chủ

102, 202 Bộ truyền thông thứ nhất

104, 204 Bộ truyền thông thứ hai

106, 206, 304 Bộ điều khiển

110, 210, 310 Bộ xử lý

1000 Hệ thống xử lý thông tin

YÊU CẦU BẢO HỘ

1. Thiết bị xử lý thông tin (100) bao gồm:

bộ xử lý (110) có cấu trúc để, khi phản hồi việc nhận yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà từ đó dữ liệu được đọc, mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và truyền dữ liệu được mã hóa mật.

2. Thiết bị xử lý thông tin theo điểm 1, trong đó bộ xử lý chỉ rõ khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin thiết đặt được kết hợp với vùng của phương tiện ghi và mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật được chỉ rõ.

3. Thiết bị xử lý thông tin theo điểm 2, trong đó trong trường hợp mà khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc không được chỉ rõ, bộ xử lý truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc mà không mã hóa mật dữ liệu.

4. Thiết bị xử lý thông tin theo điểm 2, trong đó:

bộ xử lý

xác định xem có mã hóa mật hay không dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin thiết đặt, và

mã hóa mật một cách chọn lọc dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc theo kết quả xác định.

5. Thiết bị xử lý thông tin theo điểm 4, trong đó:

trong trường hợp mà không được xác định rằng dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc được mã hóa mật,

bộ xử lý

mã hóa mật một cách chọn lọc dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc trên cơ sở của thông tin liên quan đến mã hóa mật được chứa trong yêu cầu đọc, và

truyền dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc hoặc dữ

liệu được mã hóa mật.

6. Thiết bị xử lý thông tin theo điểm 1, trong đó trong trường hợp mà yêu cầu đọc chỉ báo các vùng, bộ xử lý thực hiện mã hóa mật cho mỗi trong các vùng đó được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc.

7. Thiết bị xử lý thông tin theo điểm 1, trong đó:

trong trường hợp mà thông tin chỉ báo giá trị được thu cùng với yêu cầu đọc,

bộ xử lý

tạo ra chữ ký điện tử từ ít nhất dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và

còn truyền chữ ký điện tử được tạo.

8. Thiết bị xử lý thông tin theo điểm 7, trong đó:

trong trường hợp mà yêu cầu đọc chỉ báo các vùng,

bộ xử lý

tạo ra chữ ký điện tử cho mỗi trong số các vùng đó được chỉ báo bởi yêu cầu đọc hoặc

tạo ra chữ ký điện tử từ dữ liệu tương ứng với các vùng được chỉ báo bởi yêu cầu đọc, giá trị được chỉ báo bởi thông tin chỉ báo giá trị, và khóa mã hóa mật cho chữ ký được tạo ra trên cơ sở của khóa mã hóa mật tương ứng với các vùng được chỉ báo bởi yêu cầu đọc.

9. Thiết bị xử lý thông tin theo điểm 1, trong đó:

bộ xử lý

tạo ra chữ ký điện tử từ ít nhất dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc, thông tin được chứa trong yêu cầu đọc, và khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc và

còn truyền chữ ký điện tử được tạo.

10. Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin (100), phương pháp này bao gồm:

bước mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc để phản hồi việc nhận yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà từ đó dữ liệu được đọc; và

bước truyền dữ liệu được mã hóa mật.

11. Phương tiện ghi chứa chương trình làm cho máy tính thực hiện:

bước mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc để phản hồi việc nhận yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà từ đó dữ liệu được đọc; và

bước truyền dữ liệu được mã hóa mật.

12. Hệ thống xử lý thông tin bao gồm:

thiết bị xử lý thông tin thứ nhất (100); và

thiết bị xử lý thông tin thứ hai (300), trong đó:

thiết bị xử lý thông tin thứ hai có cấu trúc để truyền yêu cầu đọc đến thiết bị xử lý thông tin thứ nhất

thiết bị xử lý thông tin thứ nhất có cấu trúc:

để nhận yêu cầu đọc từ thiết bị xử lý thông tin thứ hai,

để mã hóa mật dữ liệu tương ứng với vùng được chỉ báo bởi yêu cầu đọc bằng cách sử dụng khóa mã hóa mật tương ứng với vùng được chỉ báo bởi yêu cầu đọc để phản hồi yêu cầu đọc bao gồm lệnh đọc dữ liệu và thông tin chỉ báo vùng của phương tiện ghi mà từ đó dữ liệu được đọc, và

để truyền dữ liệu được mã hóa mật đến thiết bị xử lý thông tin thứ hai, và thiết bị xử lý thông tin thứ hai có cấu trúc:

để nhận dữ liệu được mã hóa mật từ thiết bị xử lý thông tin thứ nhất,

để giải mật mã dữ liệu được mã hóa mật bằng cách sử dụng khóa mã hóa mật định trước,

để chuyển đổi thông tin nhận dạng thứ nhất thành thông tin nhận dạng thứ hai khác nhau trong trường hợp mà dữ liệu được giải mã mật là thông tin nhận dạng thứ nhất bằng cách viện dẫn tới bảng chuyển đổi có thể truy nhập

được đến thiết bị xử lý thông tin thứ nhất, và xác định sự kết hợp giữa thông tin nhận dạng thứ nhất và thông tin thứ hai, và

truyền thông tin nhận dạng thứ hai đến thiết bị phía ngoài được xác định bởi thiết bị xử lý thông tin thứ hai tương ứng với thông tin nhận dạng thứ hai bằng cách viện dẫn tới bảng chuyển đổi.

FIG. 1

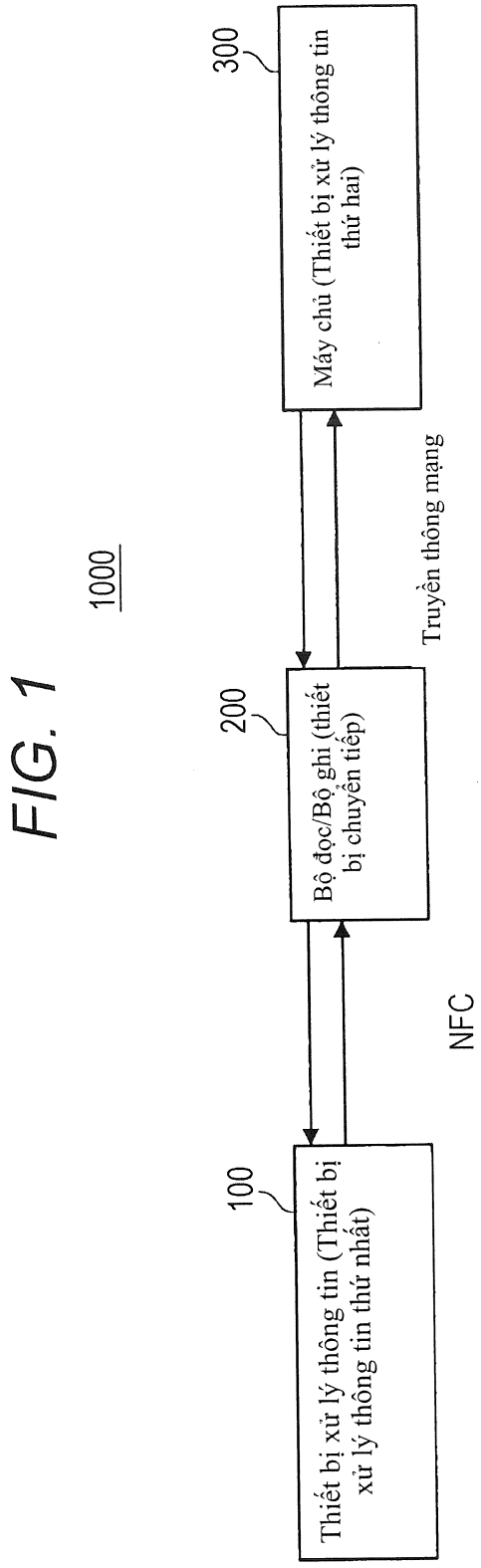

1000
300
Máy chủ (Thiết bị xử lý thông tin thứ hai)
Truyền thông mạng
200
Bộ đọc/Bộ ghi (thiết bị chuyển tiếp)
NFC
100
Thiết bị xử lý thông tin (Thiết bị xử lý thông tin thứ nhất)

FIG. 2

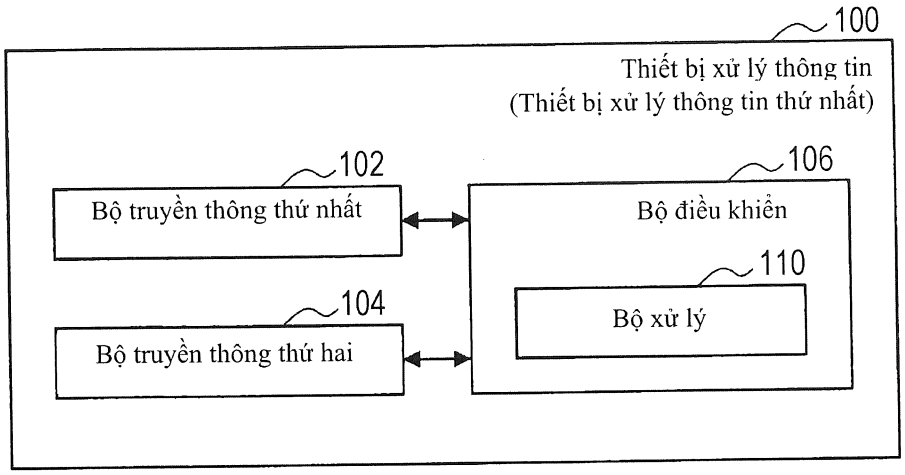

100
Thiết bị xử lý thông tin
(Thiết bị xử lý thông tin thứ nhất)
102
Bộ truyền thông thứ nhất
106
Bộ điều khiển
110
Bộ xử lý
104
Bộ truyền thông thứ hai

FIG. 3

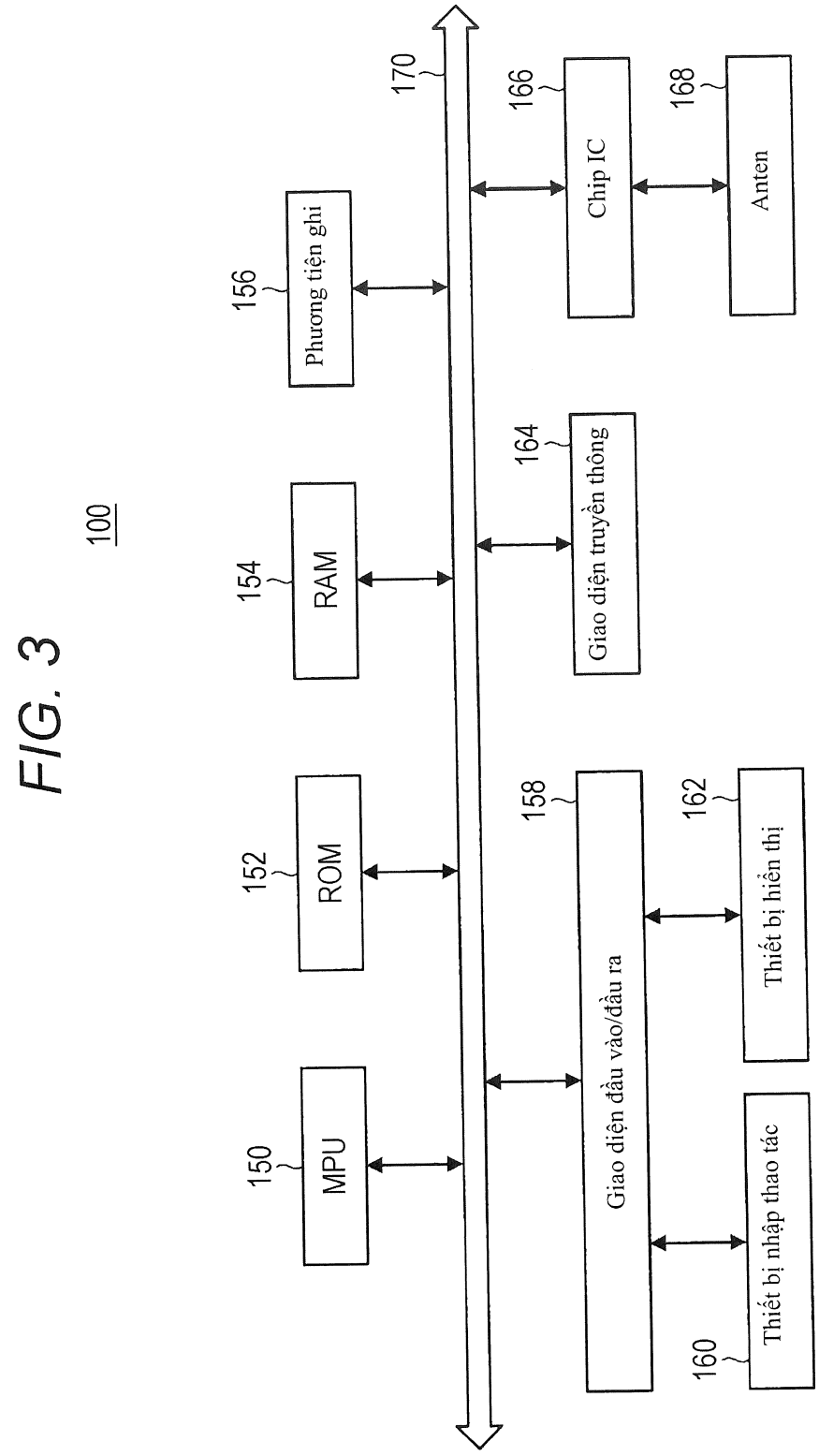

100
150
MPU
152
ROM
154
RAM
156
Phương tiện ghi
158
Giao diện đầu vào/đầu ra
160
Thiết bị nhập thao tác
162
Thiết bị hiển thị
164
Giao diện truyền thông
166
Chip IC
168
Anten
170

FIG. 4

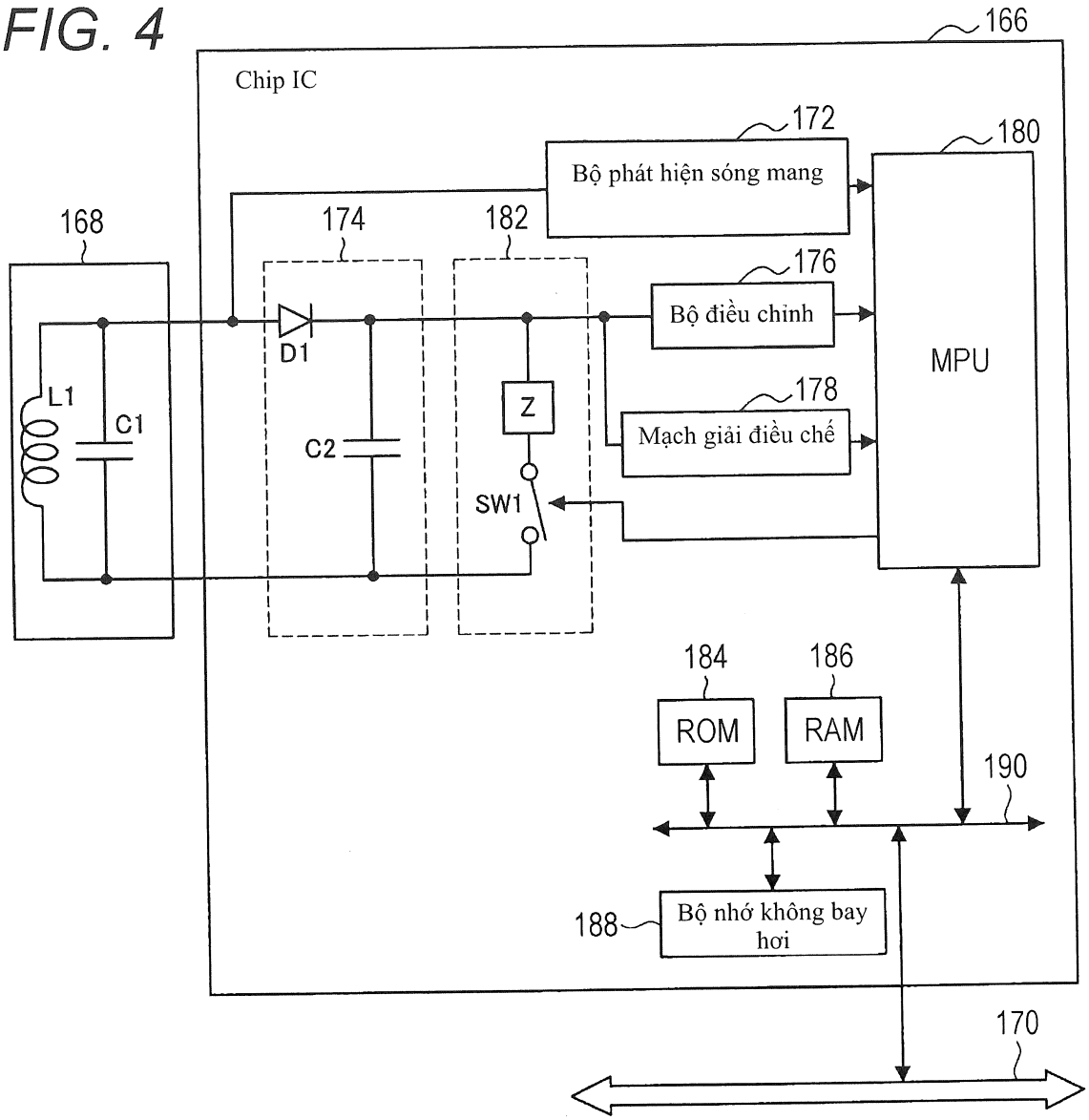

166
Chip IC
172
Bộ phát hiện sóng mang
180
168
174
182
176
Bộ điều chỉnh
MPU
D1
L1
C1
C2
Z
178
Mạch giải điều chế
SW1
184
186
ROM
RAM
190
188
Bộ nhớ không bay hơi
170

FIG. 5

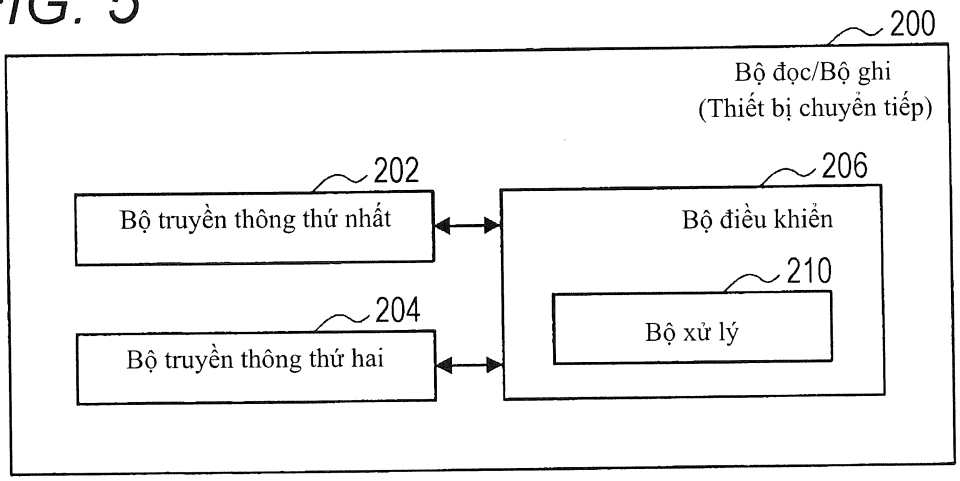

200
Bộ đọc/Bộ ghi
(Thiết bị chuyển tiếp)
202
Bộ truyền thông thứ nhất
206
Bộ điều khiển
210
Bộ xử lý
204
Bộ truyền thông thứ hai

FIG. 6

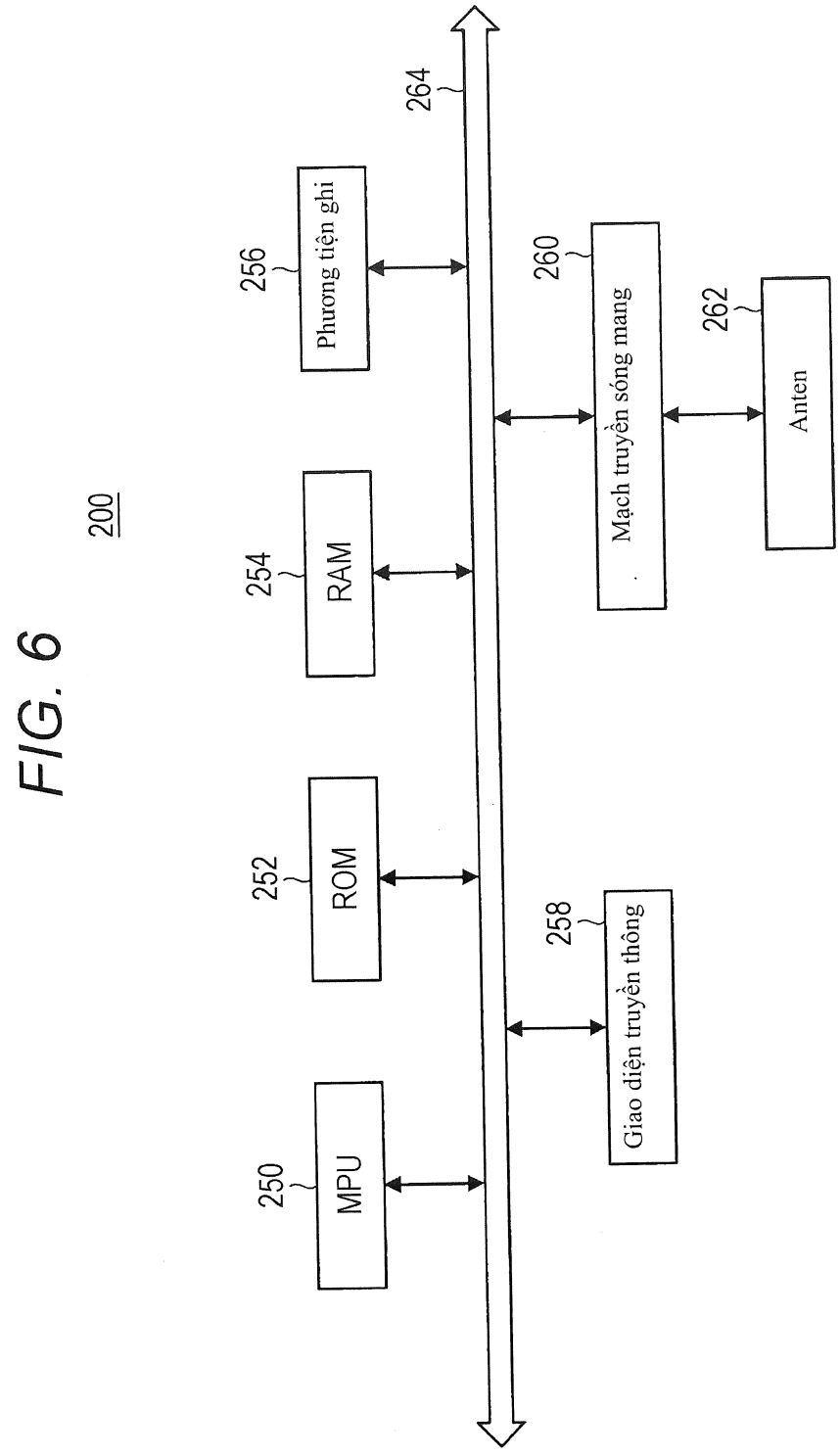

200
250
MPU
252
ROM
254
RAM
256
Phương tiện ghi
258
Giao diện truyền thông
260
Mạch truyền sóng mang
262
Anten
264

FIG. 7

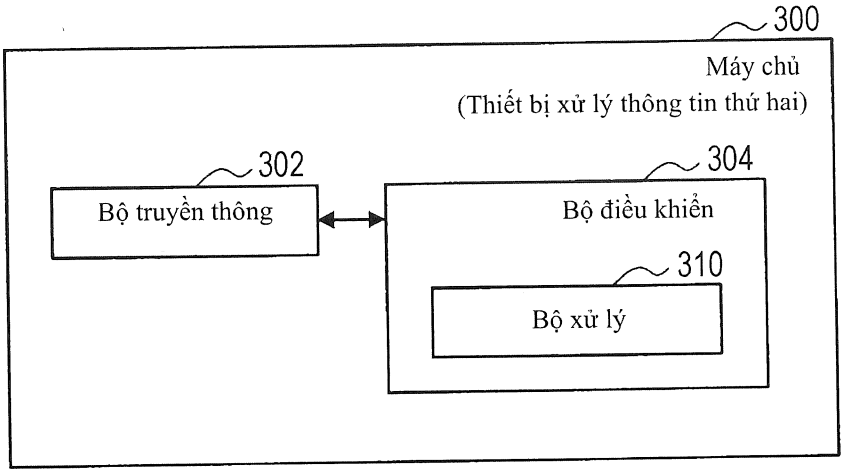

300
Máy chủ
(Thiết bị xử lý thông tin thứ hai)
302
Bộ truyền thông
304
Bộ điều khiển
310
Bộ xử lý

FIG. 8

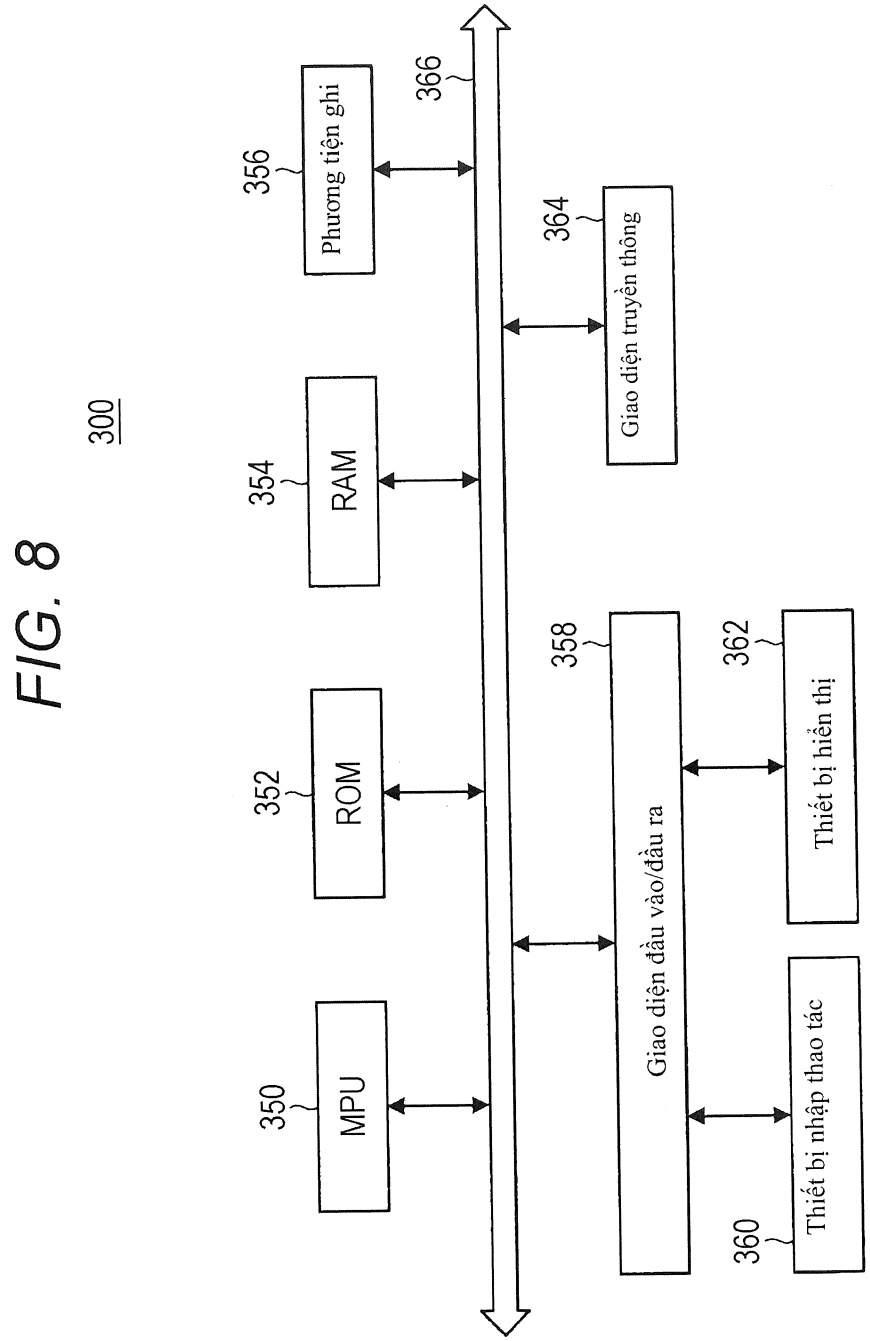

300
350
MPU
352
ROM
354
RAM
356
Phương tiện ghi
358
Giao diện đầu vào/đầu ra
360
Thiết bị nhập thao tác
362
Thiết bị hiển thị
364
Giao diện truyền thông
366

FIG. 9

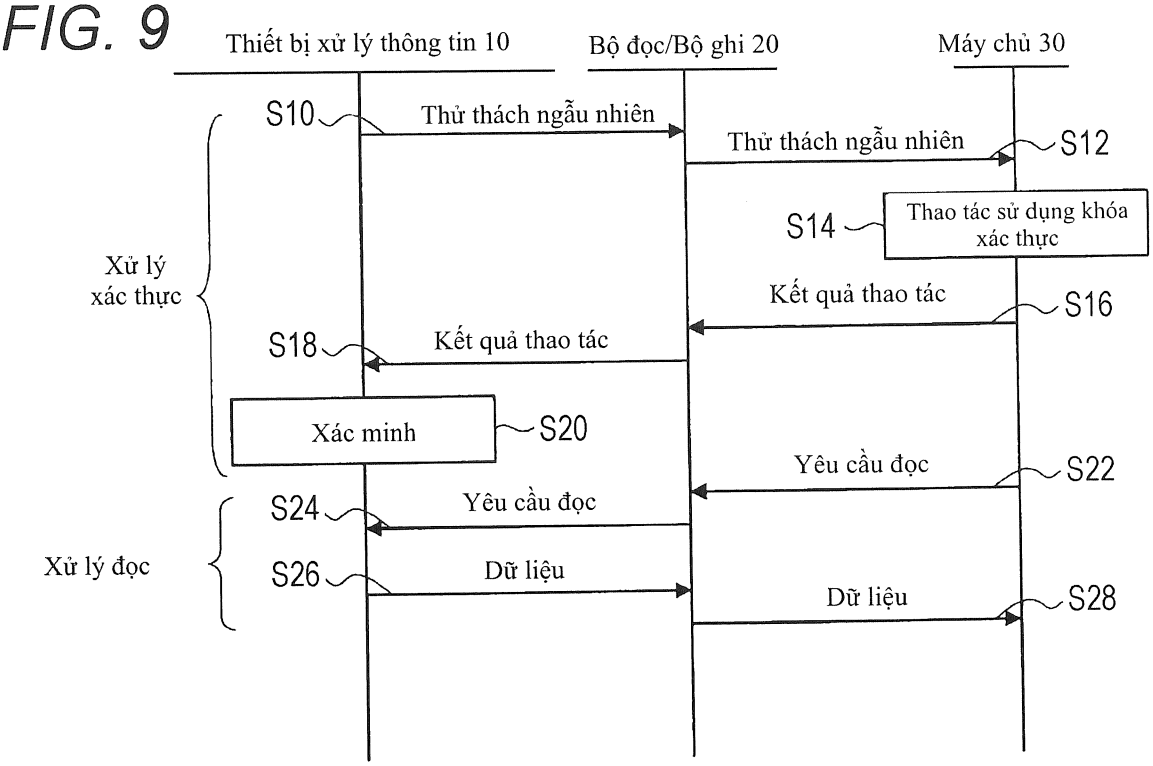


FIG. 10

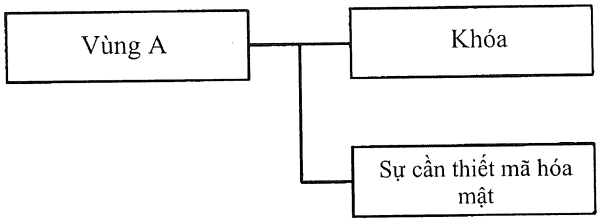


FIG. 11

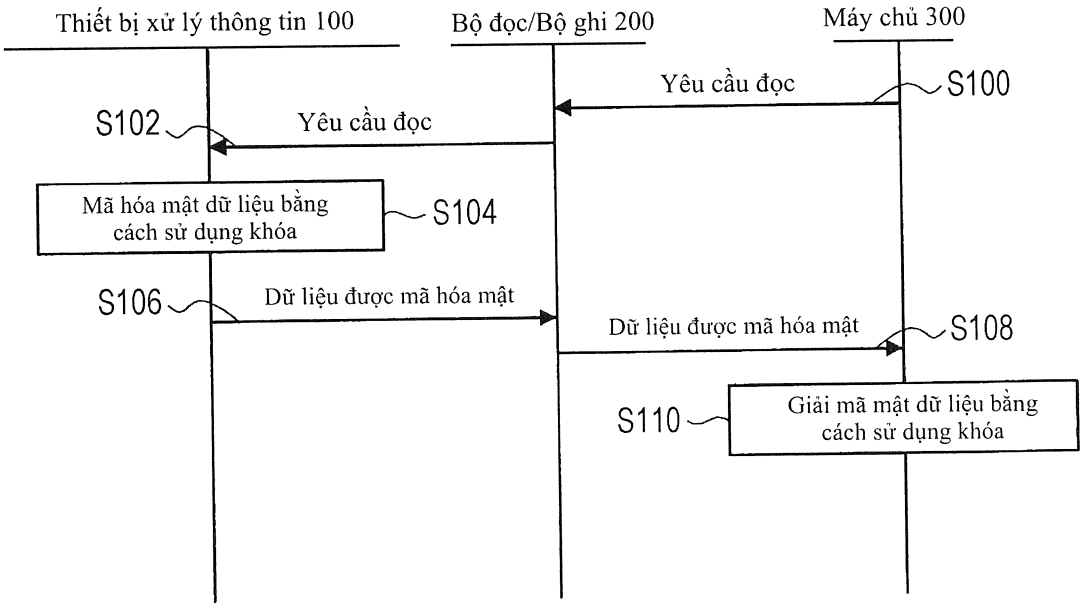


FIG. 12

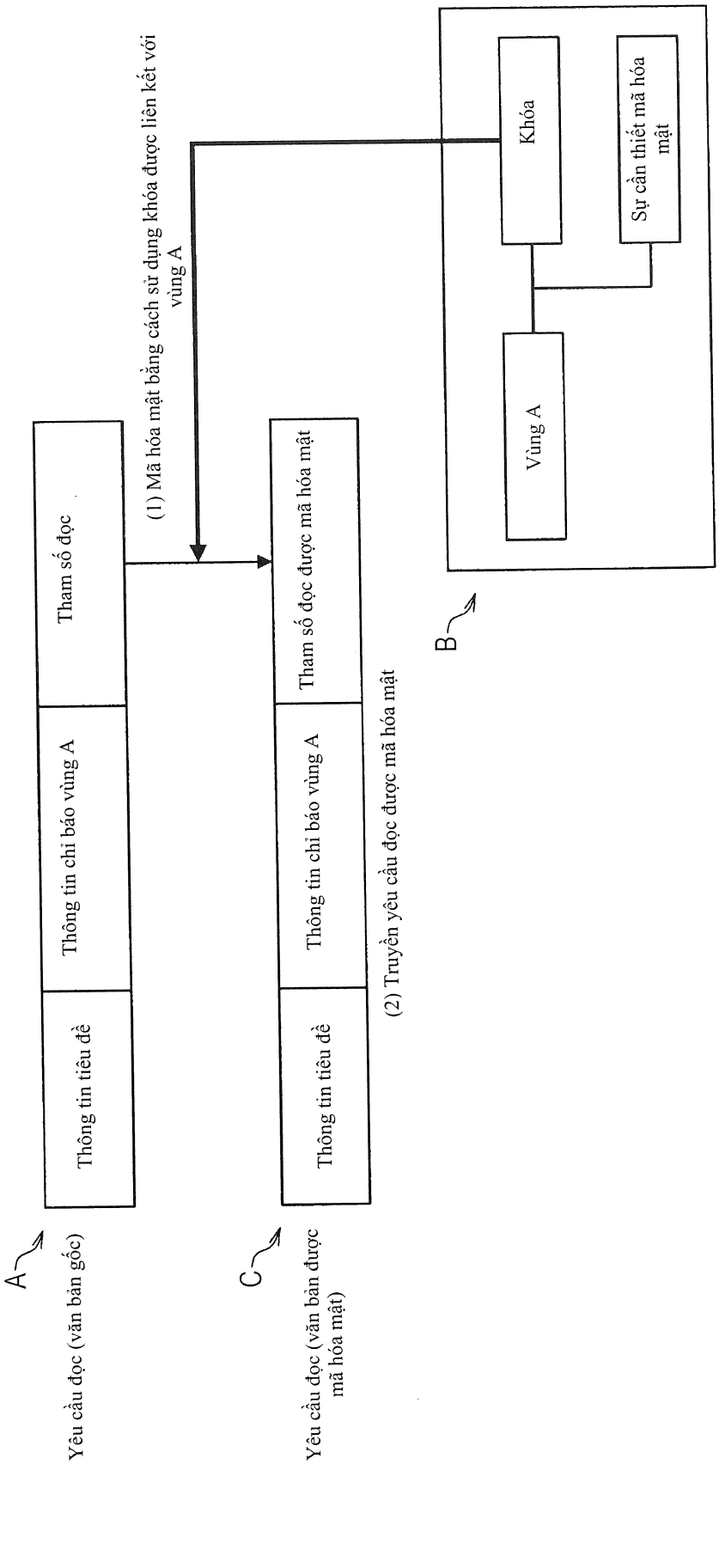

A
Yêu cầu đọc (văn bản gốc)
Thông tin tiêu đề
Thông tin chỉ báo vùng A
Tham số đọc
(1) Mã hóa mật bằng cách sử dụng khóa được liên kết với vùng A
(2) Truyền yêu cầu đọc được mã hóa mật
C
Yêu cầu đọc (văn bản được mã hóa mật)
Thông tin tiêu đề
Thông tin chỉ báo vùng A
Tham số đọc được mã hóa mật
B
Vùng A
Khóa
Sự cần thiết mã hóa mật

FIG. 13

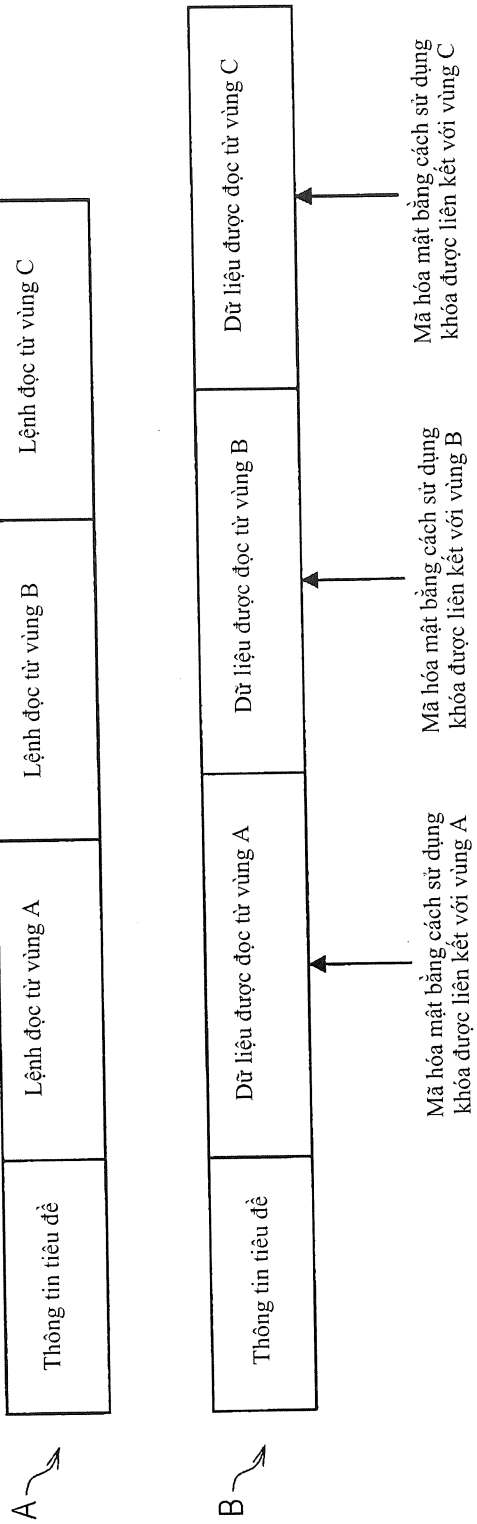

A
Thông tin tiêu đề
Lệnh đọc từ vùng A
Lệnh đọc từ vùng B
Lệnh đọc từ vùng C
B
Thông tin tiêu đề
Dữ liệu được đọc từ vùng A
Dữ liệu được đọc từ vùng B
Dữ liệu được đọc từ vùng C
Mã hóa mật bằng cách sử dụng khóa được liên kết với vùng A
Mã hóa mật bằng cách sử dụng khóa được liên kết với vùng B
Mã hóa mật bằng cách sử dụng khóa được liên kết với vùng C

FIG. 14

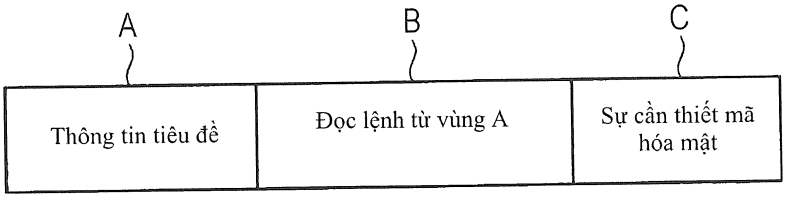

A
B
C
Thông tin tiêu đề
Đọc lệnh từ vùng A
Sự cần thiết mã hóa mật

FIG. 15

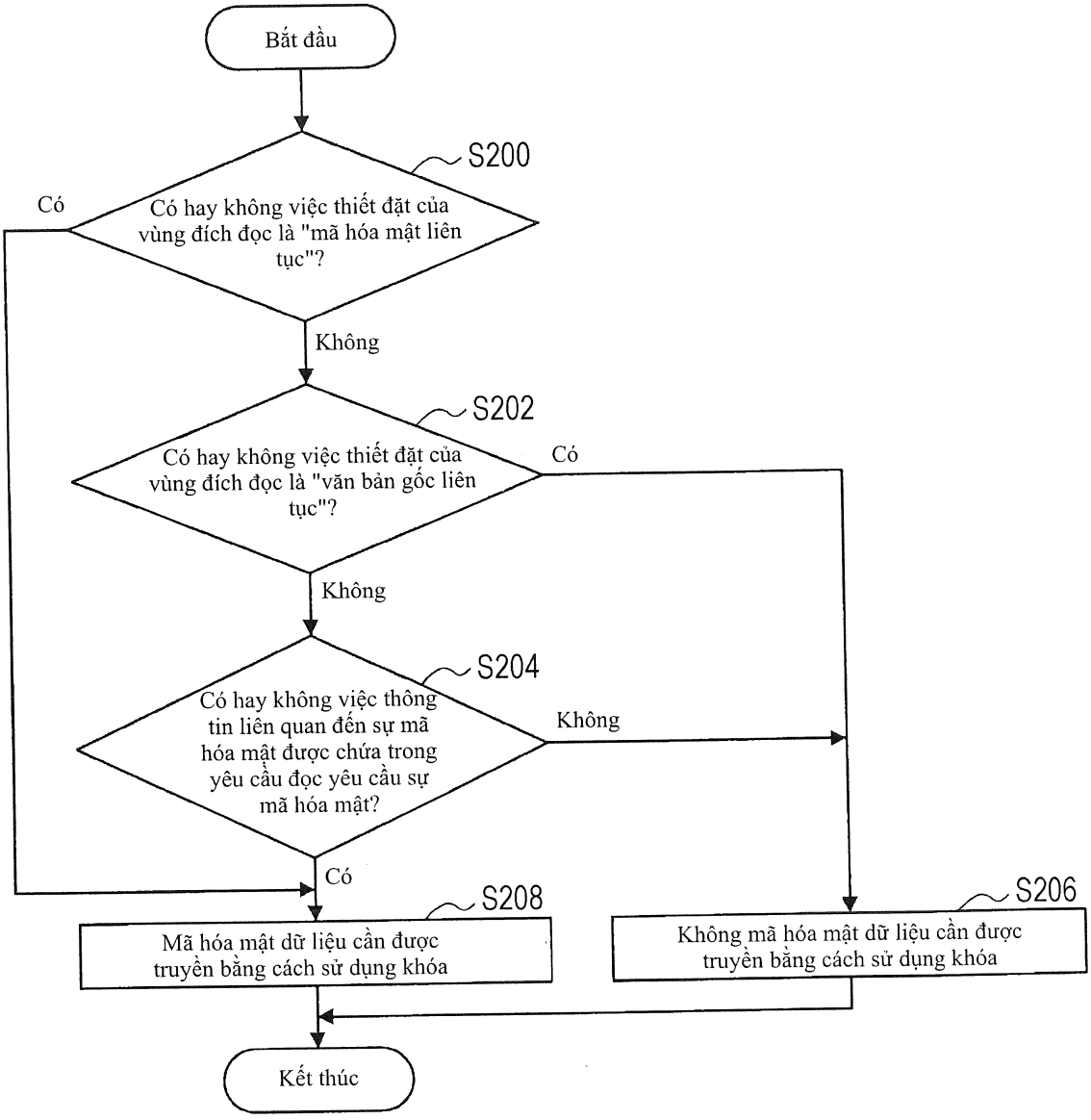

Bắt đầu
S200
Có hay không việc thiết đặt của vùng đích đọc là "mã hóa mật liên tục"?
Có
Không
S202
Có hay không việc thiết đặt của vùng đích đọc là "văn bản gốc liên tục"?
Có
Không
S204
Có hay không việc thông tin liên quan đến sự mã hóa mật được chứa trong yêu cầu đọc yêu cầu sự mã hóa mật?
Không
Có
S208
Mã hóa mật dữ liệu cần được truyền bằng cách sử dụng khóa
S206
Không mã hóa mật dữ liệu cần được truyền bằng cách sử dụng khóa
Kết thúc

FIG. 16

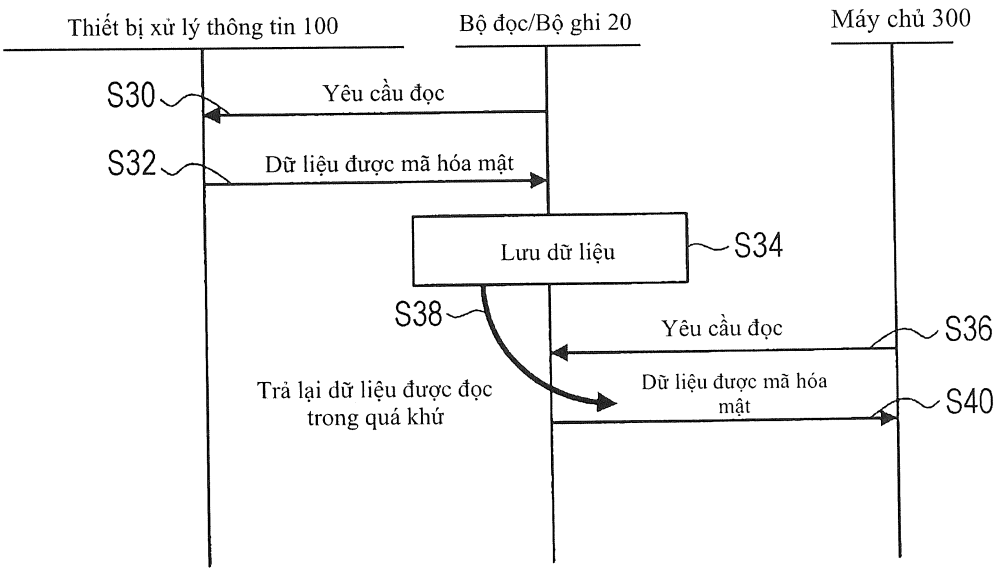

Thiết bị xử lý thông tin 100
Bộ đọc/Bộ ghi 20
Máy chủ 300
S30
Yêu cầu đọc
S32
Dữ liệu được mã hóa mật
Lưu dữ liệu
S34
S38
Yêu cầu đọc
S36
Trả lại dữ liệu được đọc trong quá khứ
Dữ liệu được mã hóa mật
S40

FIG. 17

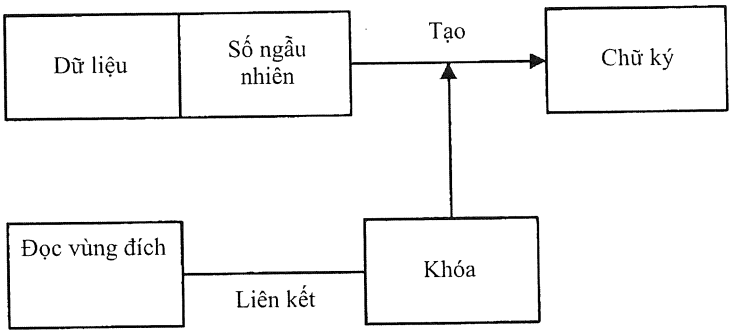
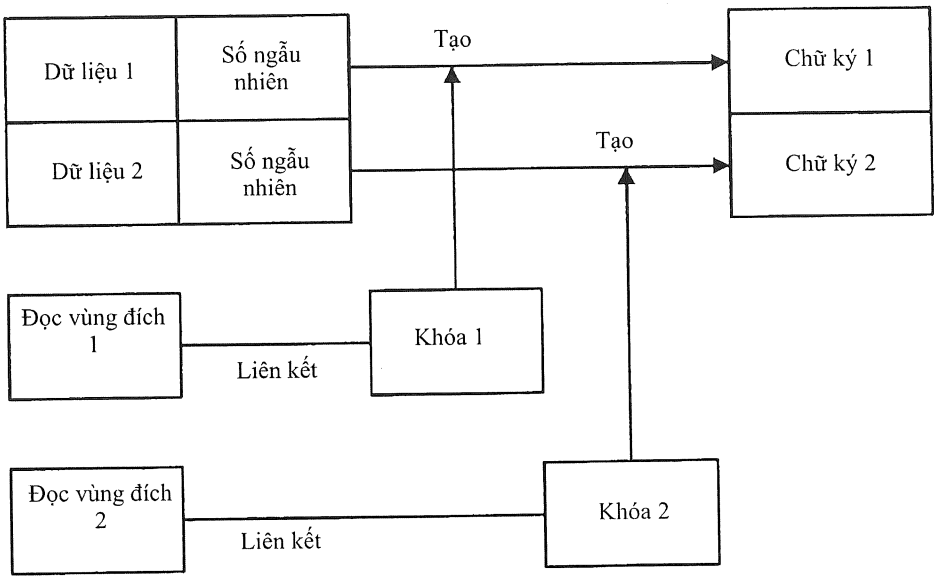

Dữ liệu
Số ngẫu nhiên
Tạo
Chữ ký
Đọc vùng đích
Liên kết
Khóa

FIG. 18

A


Dữ liệu 1
Số ngẫu nhiên
Dữ liệu 2
Số ngẫu nhiên
Tạo
Tạo
Chữ ký 1
Chữ ký 2
Đọc vùng đích 1
Liên kết
Khóa 1
Đọc vùng đích 2
Liên kết
Khóa 2

B

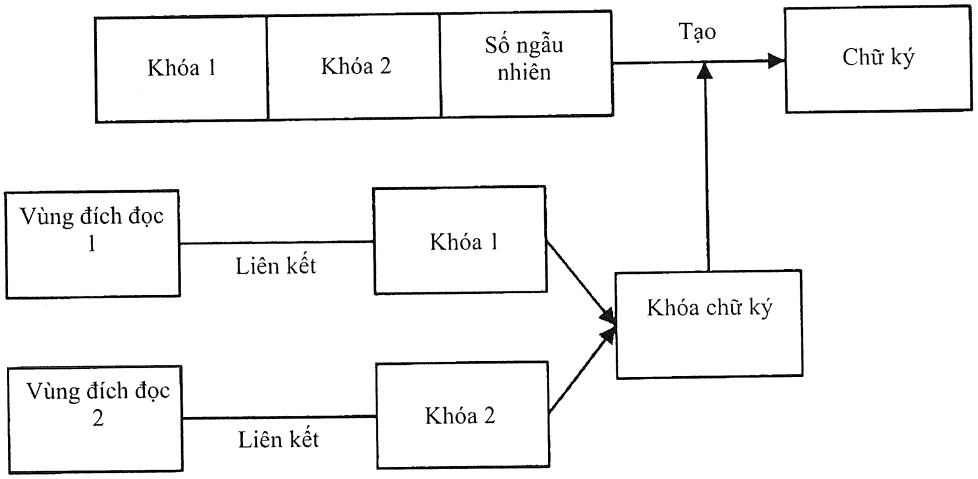

Khóa 1
Khóa 2
Số ngẫu nhiên
Tạo
Chữ ký
Vùng đích đọc 1
Liên kết
Khóa 1
Khóa chữ ký
Vùng đích đọc 2
Liên kết
Khóa 2

FIG. 19

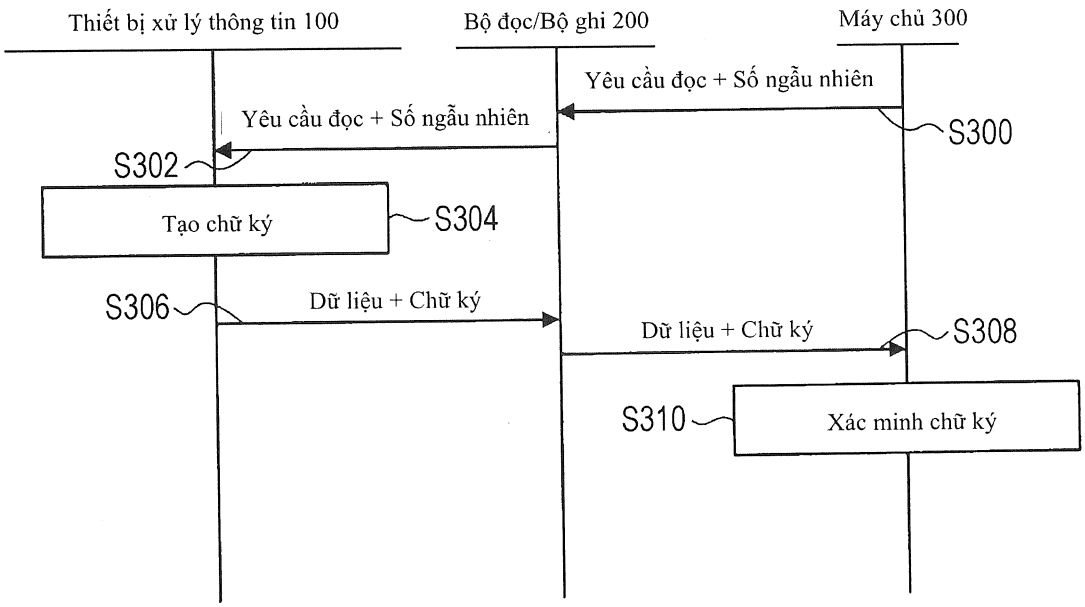


FIG. 20

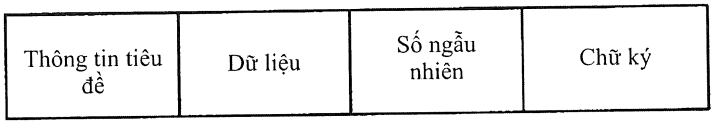


FIG. 21

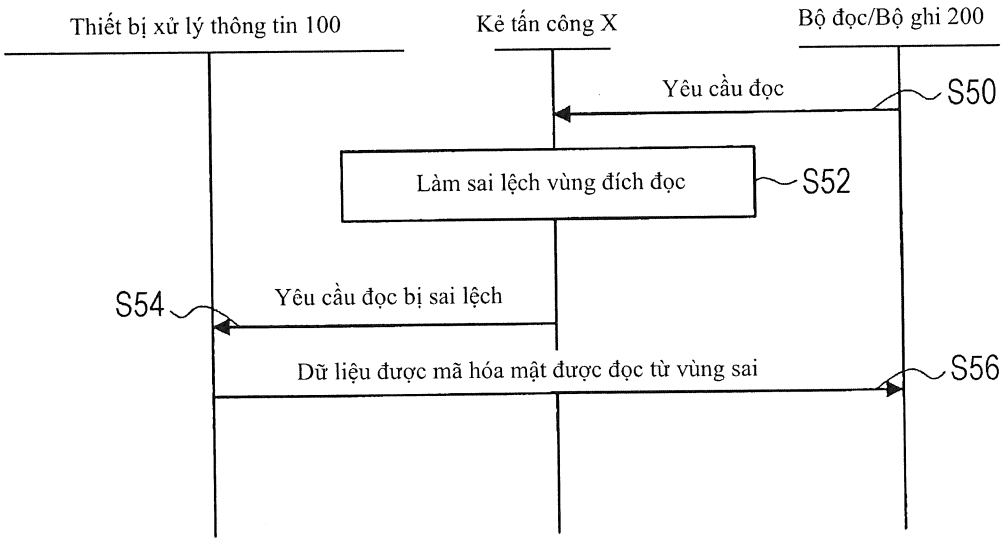


FIG. 22

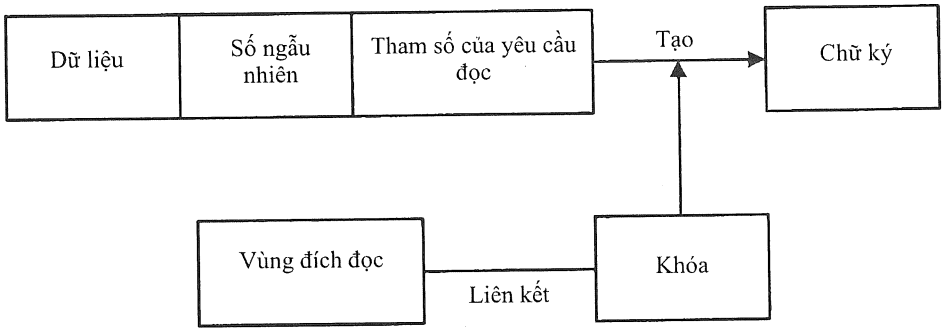


FIG. 23

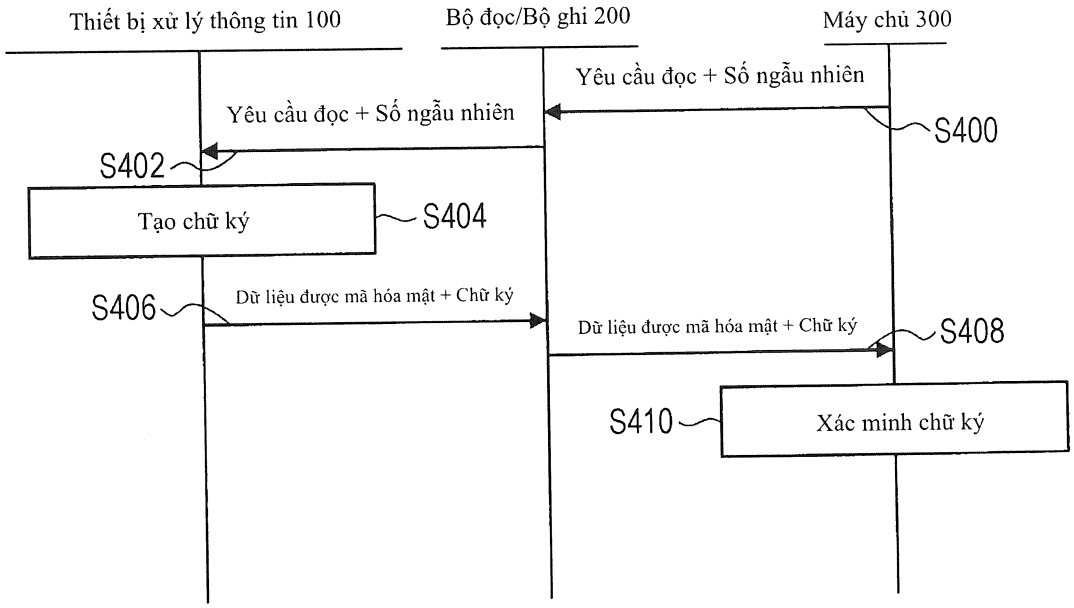


FIG. 24

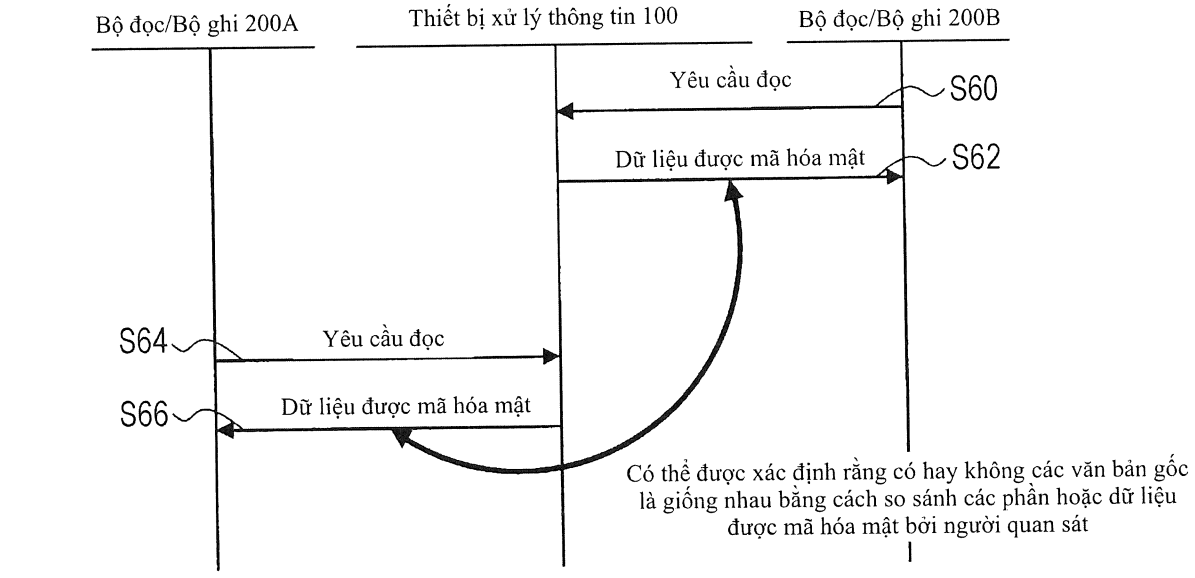


FIG. 25

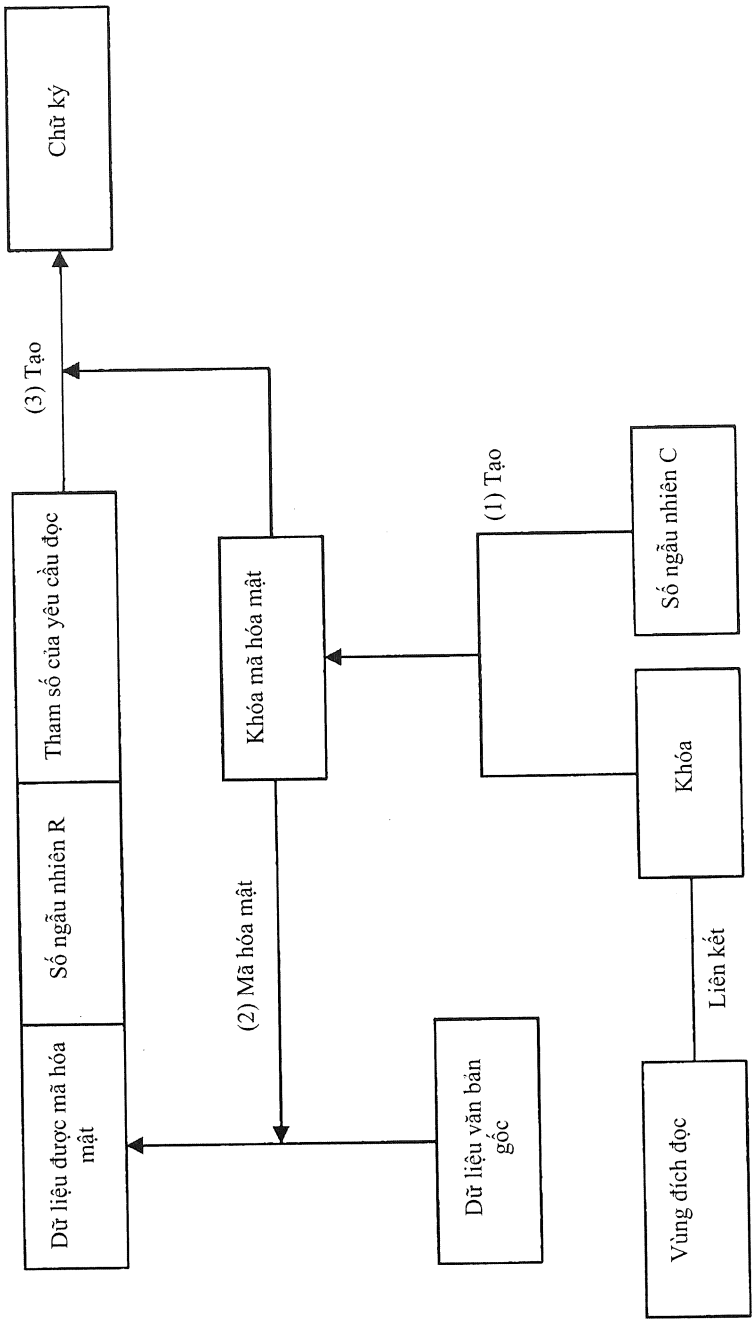

Chữ ký
(3) Tạo
Tham số của yêu cầu đọc
Số ngẫu nhiên R
Dữ liệu được mã hóa mật
Khóa mã hóa mật
(1) Tạo
Số ngẫu nhiên C
Khóa
(2) Mã hóa mật
Dữ liệu văn bản gốc
Liên kết
Vùng đích đọc

FIG. 26

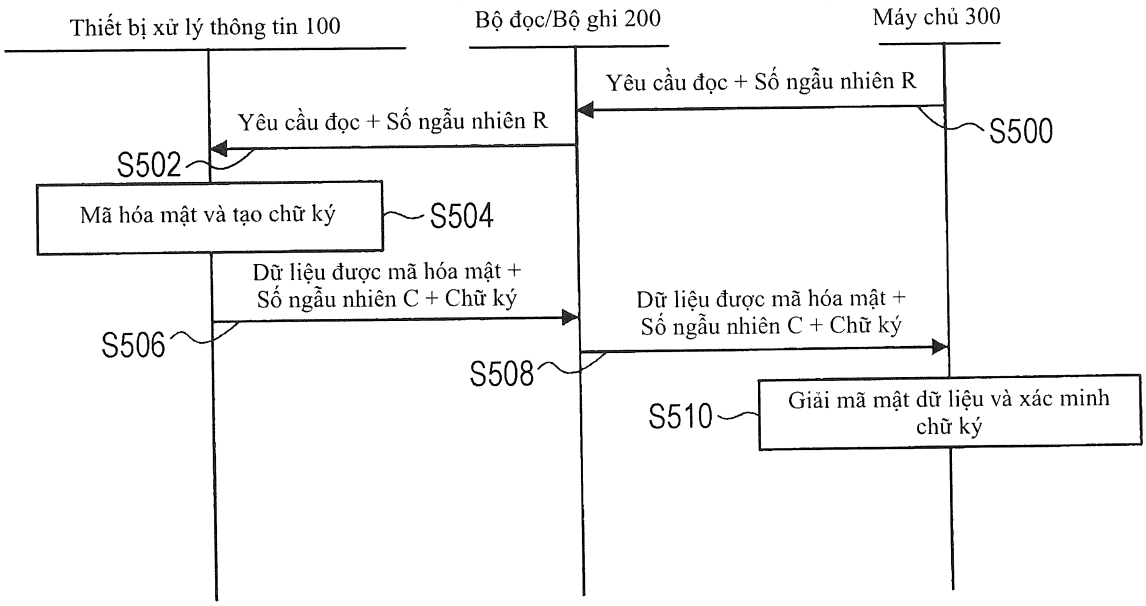

Thiết bị xử lý thông tin 100
Bộ đọc/Bộ ghi 200
Máy chủ 300
Yêu cầu đọc + Số ngẫu nhiên R
S500
Yêu cầu đọc + Số ngẫu nhiên R
S502
Mã hóa mật và tạo chữ ký
S504
Dữ liệu được mã hóa mật + Số ngẫu nhiên C + Chữ ký
S506
Dữ liệu được mã hóa mật + Số ngẫu nhiên C + Chữ ký
S508
S510
Giải mã mật dữ liệu và xác minh chữ ký

FIG. 27

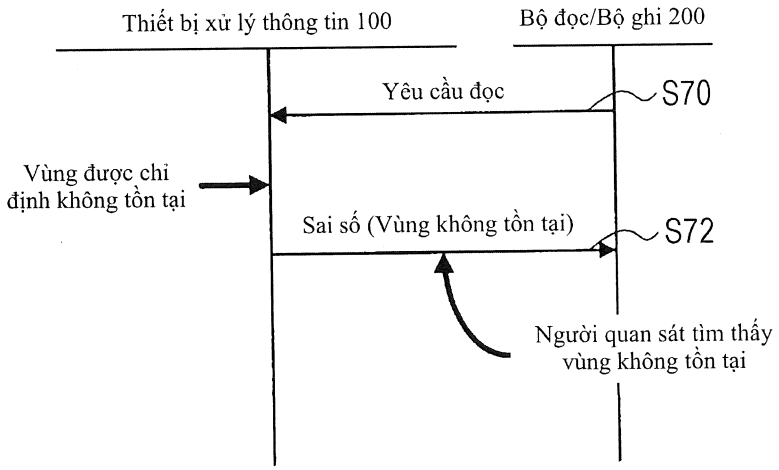

Thiết bị xử lý thông tin 100
Bộ đọc/Bộ ghi 200
Yêu cầu đọc
S70
Vùng được chỉ định không tồn tại
Sai số (Vùng không tồn tại)
S72
Người quan sát tìm thấy vùng không tồn tại

FIG. 28

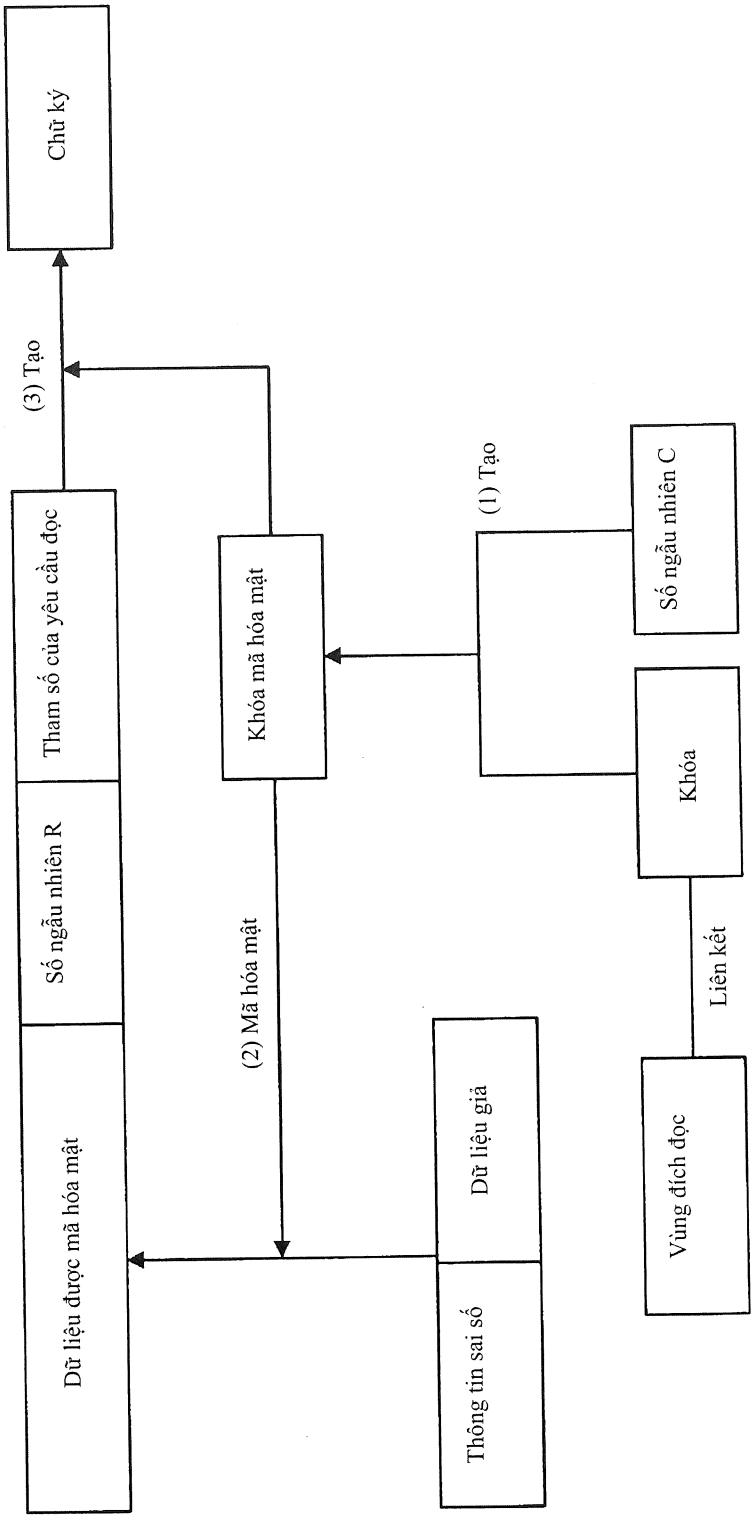

Chữ ký
(3) Tạo
Tham số của yêu cầu đọc
Số ngẫu nhiên R
Dữ liệu được mã hóa mật
Khóa mã hóa mật
(2) Mã hóa mật
(1) Tạo
Số ngẫu nhiên C
Khóa
Liên kết
Vùng đích đọc
Dữ liệu giả
Thông tin sai số

FIG. 29

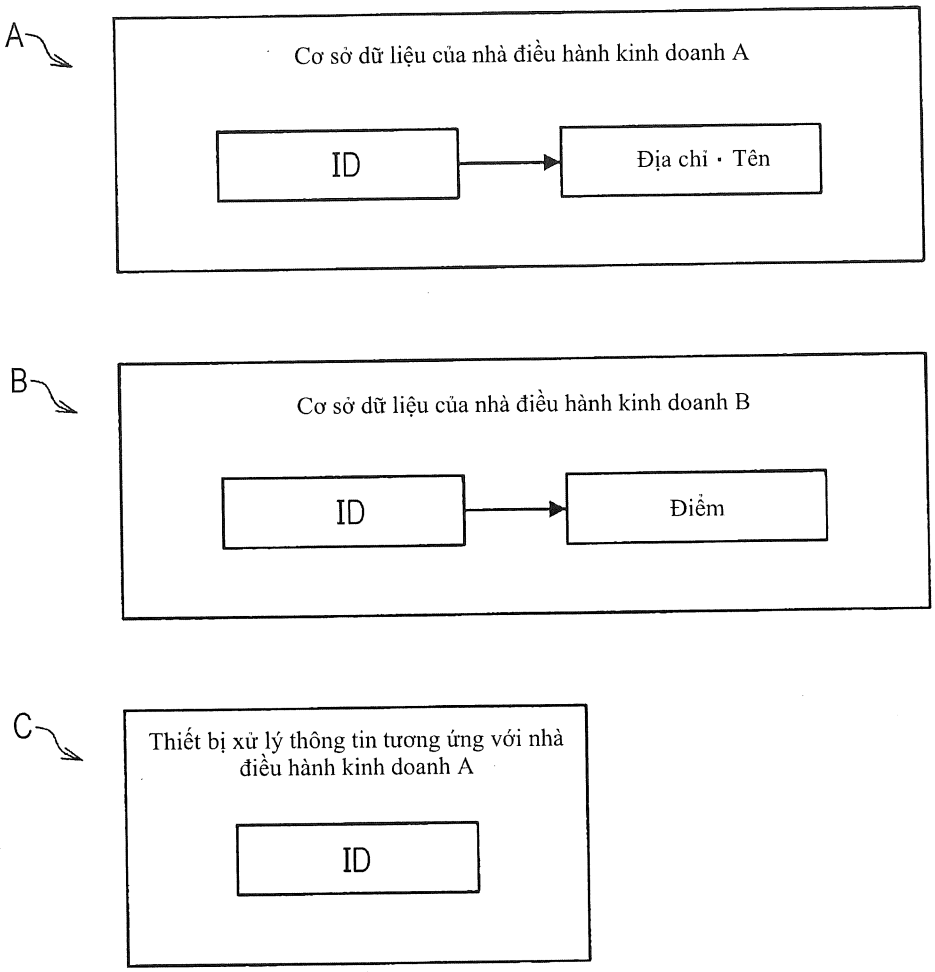

A
Cơ sở dữ liệu của nhà điều hành kinh doanh A
ID
Địa chỉ · Tên
B
Cơ sở dữ liệu của nhà điều hành kinh doanh B
ID
Điểm
C
Thiết bị xử lý thông tin tương ứng với nhà điều hành kinh doanh A
ID

FIG. 30

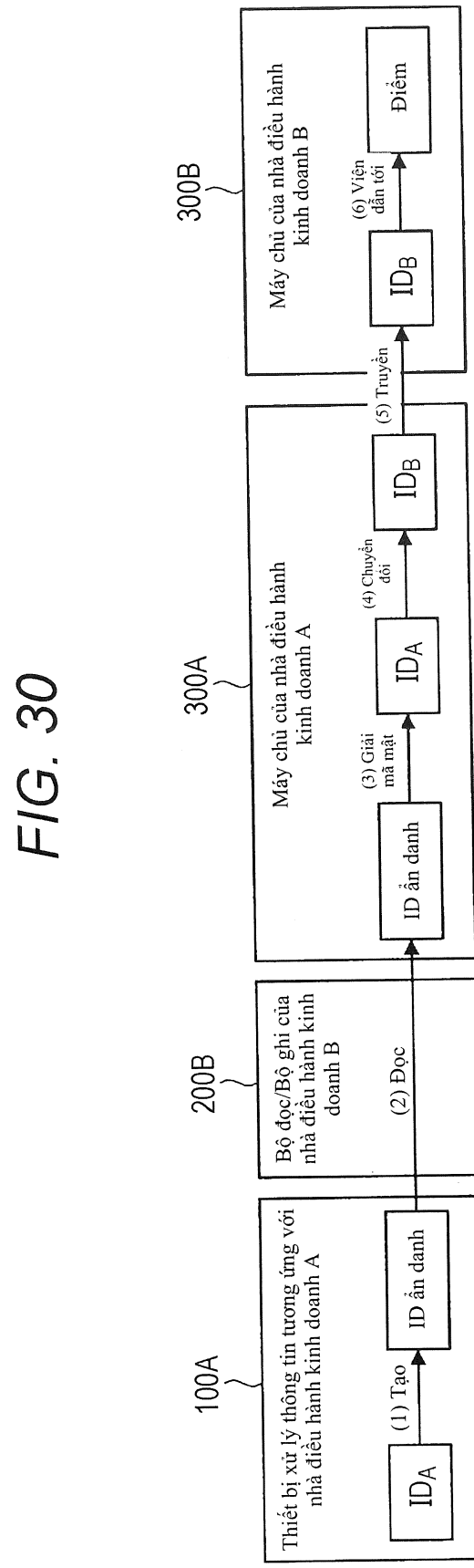

100A
Thiết bị xử lý thông tin tương ứng với nhà điều hành kinh doanh A
ID_A
(1) Tạo
ID ẩn danh
200B
Bộ đọc/Bộ ghi của nhà điều hành kinh doanh B
(2) Đọc
300A
Máy chủ của nhà điều hành kinh doanh A
ID ẩn danh
(3) Giải mã mật
ID_A
(4) Chuyển đổi
ID_B
(5) Truyền
300B
Máy chủ của nhà điều hành kinh doanh B
ID_B
(6) Viện dẫn tới
Điểm

FIG. 31

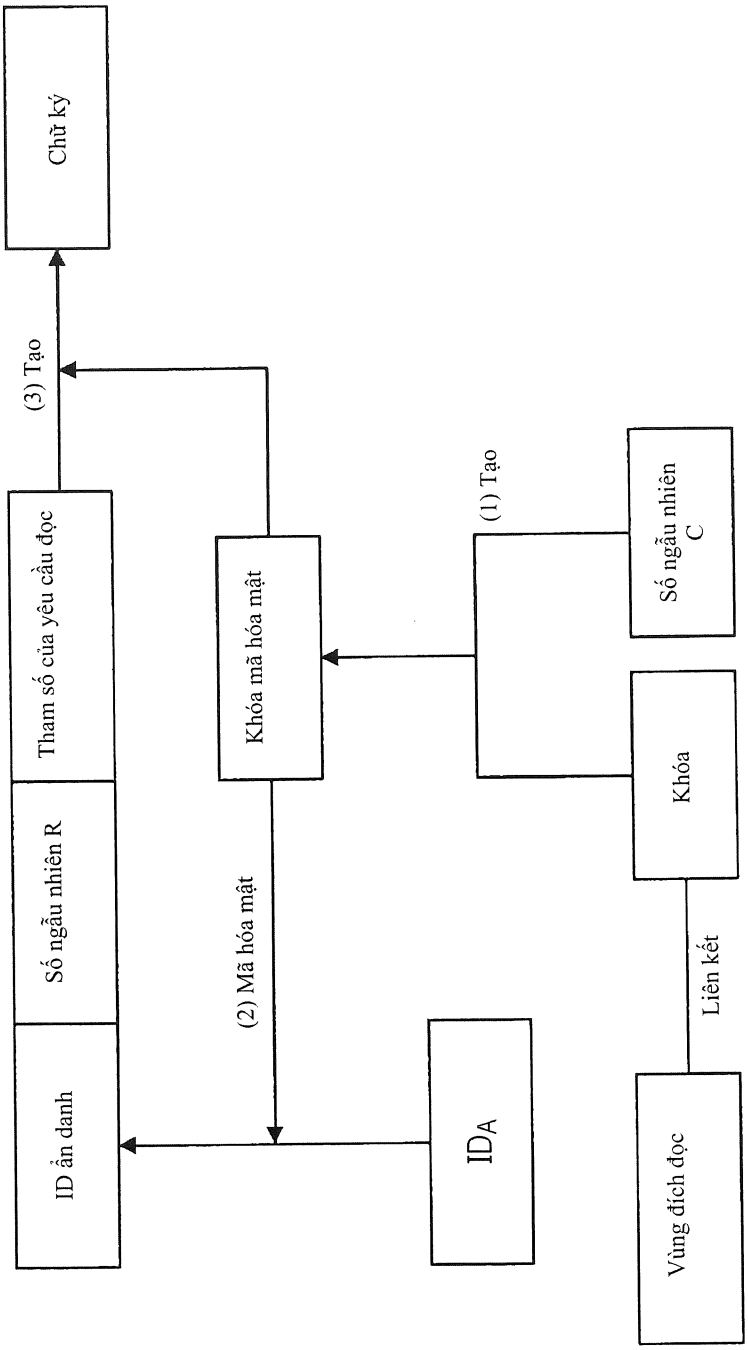
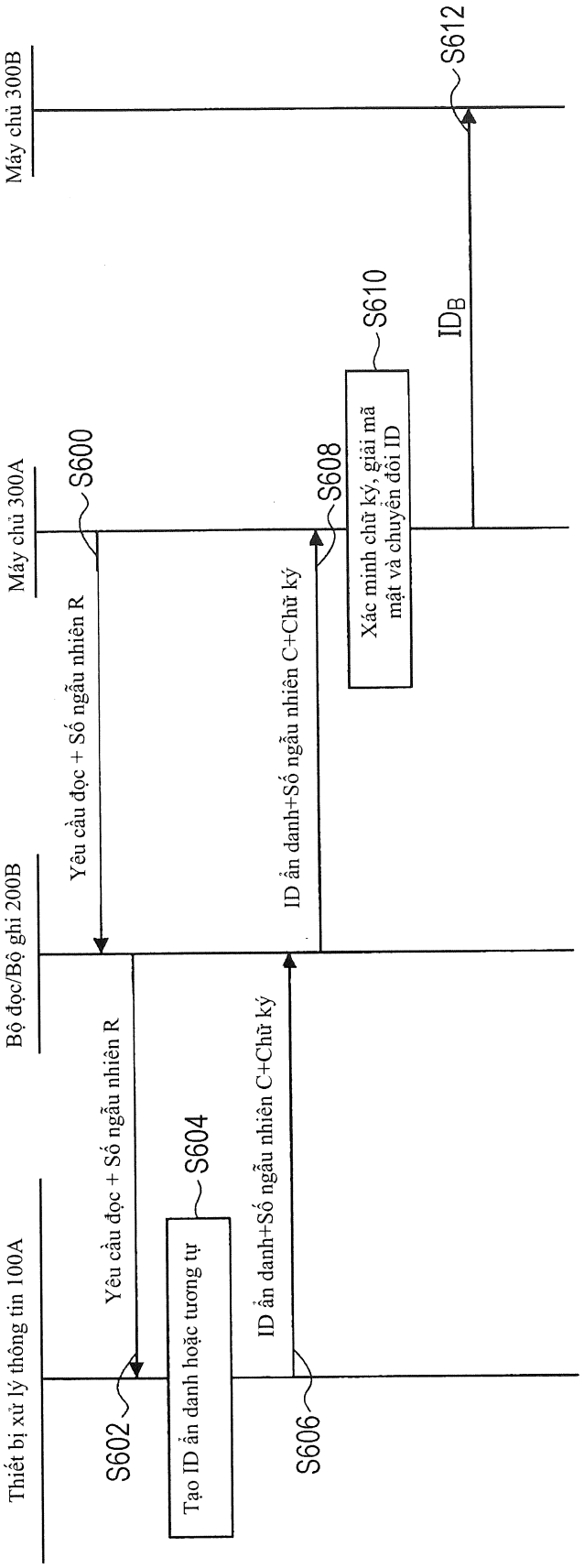

Chữ ký
(3) Tạo
Tham số của yêu cầu đọc
Số ngẫu nhiên R
ID ẩn danh
Khóa mã hóa mật
(2) Mã hóa mật
(1) Tạo
Số ngẫu nhiên C
Khóa
Liên kết
Vùng đích đọc
IDA

FIG. 32


Thiết bị xử lý thông tin 100A
Bộ đọc/Bộ ghi 200B
Máy chủ 300A
Máy chủ 300B
Yêu cầu đọc + Số ngẫu nhiên R
Yêu cầu đọc + Số ngẫu nhiên R
ID ẩn danh+Số ngẫu nhiên C+Chữ ký
ID ẩn danh+Số ngẫu nhiên C+Chữ ký
Tạo ID ẩn danh hoặc tương tự
Xác minh chữ ký, giải mã mật và chuyển đổi ID
ID_B
S600
S602
S604
S606
S608
S610
S612