



(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)



1-0043395

(51)^{2020.01} H04L 9/08; H04L 9/32; H04L 9/14

(13) B

(21) 1-2020-04391

(22) 11/01/2019

(86) PCT/JP2019/000750 11/01/2019

(87) WO2019/155821 A1 15/08/2019

(30) 2018-018895 06/02/2018 JP

(45) 25/02/2025 443

(43) 25/05/2021 398A

(73) SONY CORPORATION (JP)

1-7-1, Konan, Minato-ku, Tokyo 1080075, Japan

(72) NAKATSURU, Tsutomu (JP); SHIMOJI, Katsuya (JP).

(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 VÀ
PHƯƠNG TIỆN ĐỌC ĐƯỢC BỞI MÁY TÍNH KHÔNG TẠM THỜI

(21) 1-2020-04391

(57) Sáng chế đề cập đến thiết bị xử lý thông tin bao gồm: bộ xử lý được tạo cấu hình để thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực. Bộ xử lý tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử dụng trong việc tính toán.

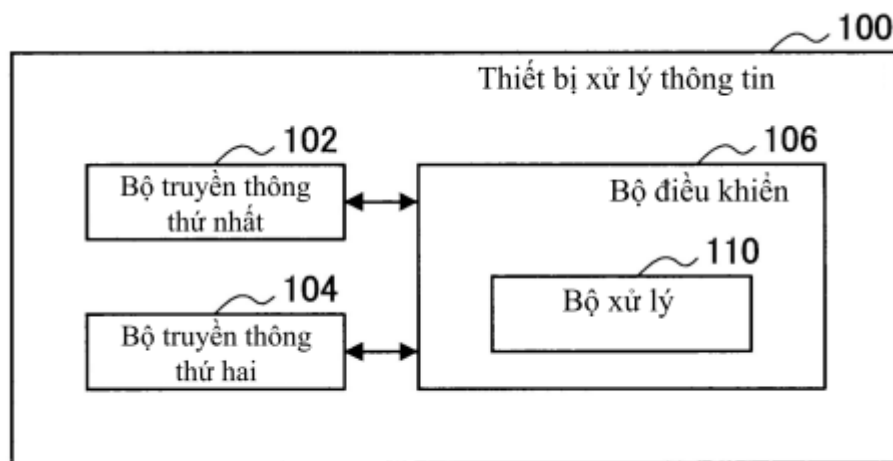


FIG.2

Lĩnh vực kỹ thuật được đề cập

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

Tình trạng kỹ thuật của sáng chế

Kỹ thuật để quản lý các tài nguyên của các thiết bị lưu trữ dữ liệu như các thẻ IC chẳng hạn đã được phát triển. Đối với kỹ thuật nêu trên, ví dụ, có kỹ thuật được mô tả trong tài liệu sáng chế 1 dưới đây.

Danh mục tài liệu trích dẫn

Tài liệu sáng chế

Tài liệu sáng chế 1: JP 2000-36021A

Vấn đề cần được giải quyết bởi sáng chế

Ví dụ, có các thiết bị mà được yêu cầu thực hiện việc xác thực nhờ sử dụng khóa xác thực để truy nhập vùng, dữ liệu, hoặc loại tương tự của phương tiện ghi.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất thiết bị xử lý thông tin, phương pháp xử lý thông tin, và chương trình mà là mới và được cải tiến và có thể cải thiện sự thuận tiện của việc xác thực nhờ sử dụng khóa xác thực.

Cách thức giải quyết vấn đề

Theo phương án của sáng chế, có đề xuất thiết bị xử lý thông tin bao gồm: bộ xử lý được tạo cấu hình để thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực. Bộ xử lý

tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử dụng trong việc tính toán.

Ngoài ra, theo phương án của sáng chế, có đề xuất thiết bị xử lý thông tin bao gồm: bộ xử lý được tạo cấu hình để tạo ra khóa xác thực được sử dụng trong xử lý xác thực và thực hiện xử lý xác thực nhờ sử dụng khóa xác thực đã được tạo ra. Bộ xử lý tạo ra các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi, tạo ra khóa suy biến thứ hai thu được bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra, và thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thứ hai làm khóa xác thực.

Ngoài ra, theo phương án của sáng chế, có đề xuất thiết bị xử lý thông tin bao gồm: bộ xử lý được tạo cấu hình để thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi làm khóa xác thực và điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực. Trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, bộ xử lý làm cho xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể thực hiện được.

Ngoài ra, theo phương án của sáng chế, có đề xuất phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước: thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực. Trong bước tạo ra khóa xác thực, khóa xác thực được tạo ra bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương

pháp chuyển đổi được kết hợp với các khóa được sử dụng trong việc tính toán.

Ngoài ra, theo phương án của sáng chế, có đề xuất phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước: tạo ra khóa xác thực được sử dụng trong xử lý xác thực; và thực hiện xử lý xác thực nhờ sử dụng khóa xác thực đã được tạo ra. Trong bước tạo ra khóa xác thực, các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi được tạo ra, và khóa suy biến thứ hai thu được bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra, và trong bước thực hiện xử lý xác thực, xử lý xác thực được thực hiện nhờ sử dụng khóa suy biến thứ hai làm khóa xác thực.

Ngoài ra, theo phương án của sáng chế, có đề xuất phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước: thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi làm khóa xác thực; và điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực. Trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, trong bước điều khiển việc thực hiện, xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực được làm cho có thể được thực hiện.

Ngoài ra, theo phương án của sáng chế, có đề xuất chương trình mà khiến máy tính thực hiện: chức năng để thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực. Chức năng để tạo khóa xác thực bao gồm tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử

dụng trong việc tính toán.

Ngoài ra, theo phương án của sáng chế, có đề xuất chương trình mà khiến máy tính thực hiện: chức năng để tạo ra khóa xác thực được sử dụng trong xử lý xác thực; và chức năng để thực hiện xử lý xác thực nhờ sử dụng khóa xác thực đã được tạo ra. Chức năng tạo ra bao gồm tạo ra các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi, và tạo ra khóa suy biến thứ hai thu được bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra, và chức năng để thực hiện xử lý xác thực bao gồm thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thứ hai làm khóa xác thực.

Ngoài ra, theo phương án của sáng chế, có đề xuất chương trình mà khiến máy tính thực hiện: chức năng để thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi làm khóa xác thực; và chức năng để điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực. Trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, chức năng để điều khiển việc thực hiện bao gồm làm cho xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể được thực hiện.

Hiệu quả của sáng chế

Theo phương án của sáng chế, có thể cải thiện sự tiện lợi của việc xác thực nhờ sử dụng khóa xác thực.

Lưu ý rằng các hiệu quả được mô tả ở trên không nhất thiết phải bị giới hạn. Ngoài các hiệu quả nêu trên, có thể đạt được bất kỳ các hiệu quả được mô tả trong bản mô tả này hoặc các hiệu quả khác mà có thể thu được từ bản mô tả này.

Mô tả vắn tắt các hình vẽ

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

Fig.2 là sơ đồ khối chức năng minh họa ví dụ về cấu hình của thiết bị xử lý thông tin theo phương án của sáng chế.

Fig.3 là sơ đồ giải thích minh họa ví dụ về cấu hình phần cứng của thiết bị xử lý thông tin theo phương án của sáng chế.

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

Fig.5 là sơ đồ giải thích minh họa ví dụ về cấu hình phần cứng của bộ đọc/bộ ghi (thiết bị chuyển tiếp) theo phương án của sáng chế.

Fig.6 là sơ đồ giải thích minh họa ví dụ về cấu hình phần cứng của máy chủ theo phương án của sáng chế.

Fig.7 là sơ đồ giải thích được sử dụng để mô tả phương pháp xử lý thông tin theo phương án của sáng chế.

Fig.8 là sơ đồ giải thích minh họa ví dụ tạo ra thứ nhất về khóa xác thực liên quan đến phương pháp xử lý thông tin theo phương án thứ nhất.

Fig.9 là sơ đồ giải thích minh họa ví dụ tạo ra thứ hai về khóa xác thực liên quan đến phương pháp xử lý thông tin theo phương án thứ nhất.

Fig.10 là sơ đồ giải thích minh họa ví dụ tạo ra thứ ba của khóa xác thực liên quan đến phương pháp xử lý thông tin theo phương án thứ nhất.

Fig.11 là sơ đồ giải thích minh họa ví dụ tạo ra khóa xác thực liên quan đến phương pháp xử lý thông tin theo phương án thứ hai.

Fig.12 là sơ đồ giải thích để mô tả xử lý theo phương pháp xử lý thông tin theo phương án thứ ba.

Mô tả chi tiết sáng chế

Sau đây, (các) phương án ưu tiên của sáng chế sẽ được mô tả chi tiết có dựa vào các hình vẽ kèm theo. Lưu ý rằng, trong bản mô tả này và hình vẽ kèm theo, các bộ phận cấu tạo mà về cơ bản có cùng chức năng và cấu hình được ký hiệu với cùng số tham chiếu, và phần giải thích lặp lại của các bộ phận cấu tạo này được bỏ qua.

Hơn nữa, phần mô tả chi tiết dưới đây sẽ được tiến hành theo thứ tự.

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 hình của hệ thống xử lý thông tin theo phương án của sáng chế

(1-1) Thiết bị xử lý thông tin 100

(1-2) Bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp)

(1-3) Máy chủ 300

(1-4) Ví dụ ứng dụng của mỗi thiết bị mà cấu thành 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 các 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 về hệ thống xử lý thông tin theo phương án của sáng chế sẽ được mô tả trước, và sau đó phương pháp xử lý thông tin theo phương án của sáng chế sẽ được mô tả nhờ sử dụng trường hợp được áp dụng cho hệ thống xử lý thông tin theo phương án của sáng chế làm ví dụ.

(1) Cấu hình của hệ thống xử lý thông tin theo phương án của sáng chế

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

Ngoài ra, cấu hình của hệ thống xử lý thông tin theo phương án của sáng chế không bị 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. Ngoài ra, hệ thống xử lý thông tin theo phương án của sáng chế có thể bao gồm các bộ đọc/bộ ghi 200 hoặc các máy chủ 300.

Thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 200 thực hiện việc truyền thông thông qua, ví dụ, truyền thông trường gần (NFC-near field communication) của loại-A, loại-B, loại-F, hoặc loại tương tự.

Ngoài ra, trong hệ thống xử lý thông tin theo phương án của sáng chế, ví dụ, thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 200 có thể thực hiện việc truyền thông theo “việc truyền thông không dây của phương pháp truyền thông tùy ý như việc truyền thông không dây sử dụng IEEE 802.15.1 như Bluetooth năng lượng thấp (BLE-Bluetooth low energy), việc truyền thông không dây sử dụng IEEE 802.11, hoặc việc truyền thông hồng ngoại” hoặc “việc truyền thông có dây sử dụng truyền thông thông qua giao diện truyền thông hoặc loại tương tự dựa trên kênh truyền nối tiếp đa năng (USB-Universal Serial Bus) hoặc tiêu

chuẩn ISO 7816”.

Máy chủ 300 và bộ đọc/bộ ghi 200 được kết nối, ví dụ, thông qua mạng theo cách thức có dây hoặc không dây, và thực hiện việc truyền thông bằng cách truyền thông thông qua mạng (sau đây được gọi là “truyền thông mạng”). Các ví dụ về mạng theo phương án của sáng chế bao gồm mạng có dây như mạng vùng cục bộ (LAN-local area network) hoặc mạng diện rộng (WAN-wide area network), mạng không dây như mạng vùng cục bộ không dây (WLAN-wireless local area network), và Internet sử dụng giao thức truyền thông như Giao thức điều khiển truyền/Giao thức Internet (TCP/IP-Transmission Control Protocol/Internet Protocol).

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

Máy chủ 300 và thiết bị xử lý thông tin 100 thực hiện việc truyền thông thông qua bộ đọc/bộ ghi 200. Nói cách khác, trong hệ thống xử lý thông tin 1000, bộ đọc/bộ ghi 200 đóng vai trò là thiết bị chuyển tiếp mà chuyển tiếp việc truyền thông giữa máy chủ 300 và thiết bị xử lý thông tin 100.

Ngoài ra, trong hệ thống xử lý thông tin theo phương án của sáng chế, máy chủ 300 và thiết bị xử lý thông tin 100 cũng có thể truyền thông với nhau mà không đi qua bộ đọc/bộ ghi 200. Trong trường hợp trong đó hệ thống xử lý thông tin theo phương án của sáng chế có “cấu hình trong đó máy chủ 300 và thiết bị xử lý thông tin 100 truyền thông trực tiếp mà không đi qua bộ đọc/bộ ghi 200,” ví dụ, máy chủ 300 có thể có chức năng của bộ đọc/bộ ghi 200. Nói cách khác, hệ thống xử lý thông tin theo phương án của sáng chế có thể không có thiết bị đóng vai trò là thiết bị chuyển tiếp như bộ đọc/bộ ghi 200.

Sau đây, trường hợp trong đó “thiết bị xử lý thông tin 100 và bộ đọc/bộ ghi 200 thực hiện việc truyền thông theo NFC, và máy chủ 300 và bộ đọc/bộ ghi 200 thực hiện việc truyền thông theo việc truyền thông mạng” như được minh họa trên Fig.1 sẽ được mô tả dưới dạng ví dụ. Ngoài ra, như được mô tả ở trên, các ví dụ về việc truyền thông trong hệ thống xử lý thông tin theo phương án của sáng chế không bị giới hạn ở ví dụ được minh họa trên Fig.1.

(1-1) Thiết bị xử lý thông tin 100

Fig.2 là sơ đồ khối chức năng minh họa ví dụ về cấu hình của thiết bị xử lý thông tin 100 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.

Ngoài ra, thiết bị xử lý thông tin 100 có thể bao gồm, ví dụ, bộ nhớ chỉ đọc (ROM-read only memory) (không được minh họa), bộ nhớ truy nhập ngẫu nhiên (RAM-random access memory) (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 cảnh khác nhau trên màn hiển thị, và loại tương tự. Ví dụ, các bộ phận tương ứng của thiết bị xử lý thông tin 100 được kết nối với nhau thông qua kênh truyền mà đóng vai trò là đường truyền dữ liệu.

ROM (không được minh họa) lưu trữ chương trình và dữ liệu điều khiển như các tham số tính toán mà được sử dụng bởi bộ điều khiển 106. RAM (không được minh họa) lưu trữ tạm thời chương trình được thực hiện bởi bộ điều khiển 106 và loại tương tự.

Thiết bị nhập thao tác được minh họa trong ví dụ cấu hình phần cứng của thiết bị xử lý thông tin 100 được mô tả sau đây có thể được sử dụng làm bộ thao

tác (không được minh họa). Ngoài ra, thiết bị hiển thị được minh họa trong ví dụ cấu hình phần cứng của thiết bị xử lý thông tin 100 được mô tả sau đây có thể được sử dụng làm bộ hiển thị (không được minh họa).

(Ví dụ về cấu hình phần cứng của thiết bị xử lý thông tin 100)

Fig.3 là sơ đồ giải thích minh họa ví dụ về cấu hình phần cứng của thiết bị xử lý thông tin 100 theo phương án của sáng chế. Fig.3 minh họa ví dụ về cấu hình phần cứng của thiết bị xử lý thông tin 100 trong trường hợp trong đó việc truyền thông với bộ đọc/bộ ghi 200 được thực hiện theo 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. Ngoài ra, ví dụ, các bộ phận tương ứng của thiết bị xử lý thông tin 100 được kết nối với nhau thông qua kênh truyền 170 mà đóng vai trò là đường truyền dữ liệu. Ngoài ra, thiết bị xử lý thông tin 100 được điều khiển bởi, ví dụ, điện năng được cấp từ nguồn điện bên trong như pin được chứa trong thiết bị xử lý thông tin 100, điện năng được cấp từ nguồn điện phía ngoài được kết nối, hoặc loại tương tự.

MPU 150 được cấu thành bởi một hoặc nhiều bộ xử lý được cấu thành bởi bộ xử lý micro (MPU-micro processing unit) hoặc loại tương tự, các loại mạch xử lý khác nhau, hoặc loại tương tự, và có chức năng như bộ điều khiển 106 mà điều khiển thiết bị xử lý thông tin 100 nói chung. Ngoài ra, trong thiết bị xử lý thông tin 100, MPU 150 cũng thực hiện chức năng là, ví dụ, bộ xử lý 110 được mô tả sau đây.

ROM 152 lưu trữ chương trình, dữ liệu điều khiển như các tham số tính toán, và loại tương tự mà được sử dụng bởi MPU 150. RAM 154 lưu trữ tạm

thời, ví dụ, chương trình hoặc loại tương tự được thực hiện bởi MPU 150.

Phương tiện ghi 156 là phương tiện ghi đơn có chức năng như bộ lưu trữ (không được minh họa). Phương tiện ghi 156 lưu trữ, ví dụ, các loại dữ liệu khác nhau như các loại ứng dụng khác nhau. Ở đây, các ví dụ về phương tiện ghi 156 bao gồm phương tiện ghi từ như đĩa cứng chẳng hạn và bộ nhớ bất biến như bộ nhớ chớp chẳng hạn. Ngoài ra, phương tiện ghi 156 có thể tháo rời được khỏi thiết bị xử lý thông tin 100.

Giao diện đầu vào/đầu ra 158 kết nối, ví dụ, thiết bị nhập thao tác 160 hoặc thiết bị hiển thị 162. Thiết bị nhập thao tác 160 thực hiện chức năng là bộ thao tác (không được minh họa), và thiết bị hiển thị 162 thực hiện chức năng là bộ hiển thị (không được minh họa). Ở đây, các ví dụ về giao diện đầu vào/đầu ra 158 bao gồm đầu cuối kênh truyền nối tiếp đa năng (USB-Universal Serial Bus), đầu cuối giao diện trực quan số (DVI-digital visual interface), đầu cuối giao diện đa phương tiện độ phân giải cao (HDMI-high-definition multimedia interface) (nhãn hiệu được đăng ký), và các loại mạch xử lý khác nhau.

Ngoài ra, ví dụ, thiết bị nhập thao tác 160 được cài đặt trên 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. Ví dụ, nút bấm, phím hướng, bộ lựa chọn kiểu quay như con cuộn, hoặc kết hợp của chúng có thể được sử dụng làm thiết bị nhập thao tác 160.

Ngoài ra, ví dụ, thiết bị hiển thị 162 được cài đặt trên 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. Ví dụ, màn hình tinh thể lỏng, màn hình EL hữu cơ, hoặc loại tương tự có thể được sử dụng làm thiết bị hiển thị 162.

Ngoài ra, sẽ được hiểu rằng giao diện đầu vào/đầu ra 158 có thể được kết

nổi tới thiết bị phía ngoài như thiết bị nhập thao tác phía ngoài (ví dụ, bàn phím hoặc chuột) hoặc thiết bị hiển thị phía ngoài đóng vai trò là thiết bị phía ngoài của thiết bị xử lý thông tin 100. Ngoài ra, ví dụ, thiết bị hiển thị 162 có thể là thiết bị mà trên đó việc hiển thị và thao tác người dùng có thể được thực hiện như màn chạm.

Giao diện truyền thông 164 là thiết bị truyền thông để thực hiện việc truyền thông của một phương pháp truyền thông được hỗ trợ bởi thiết bị xử lý thông tin 100 và thực hiện chức năng là bộ truyền thông thứ nhất 102. Ở đây, ví dụ, anten truyền thông và mạch tần số vô tuyến (RF-radio frequency) (truyền thông không dây), cổng IEEE 802.15.1 và mạch thu phát (truyền thông không dây), cổng IEEE 802.11 và mạch thu phát (truyền thông không dây), thiết bị đầu cuối LAN và mạch thu phát (truyền thông có dây), hoặc loại tương tự có thể được sử dụng làm giao diện truyền thông 164.

Chip IC 166 và anten 168 là các thiết bị truyền thông mà thực hiện việc truyền thông của các phương pháp truyền thông khác được hỗ trợ bởi thiết bị xử lý thông tin 100 và thực hiện chức năng là bộ truyền thông thứ hai 104. Ví dụ, chip IC 166 và anten 168 thực hiện việc truyền thông NFC với thiết bị phía ngoài mà có bộ đọc/bộ ghi thực hiện chức năng như bộ đọc/bộ ghi 200 thông qua các sóng mang có tần số định trước như 13,56 MHz.

Anten 168 đóng vai trò thu các sóng mang và truyền tín hiệu phản hồi. Ngoài ra, chip IC 166 giải điều biến và xử lý tín hiệu sóng mang được truyền từ thiết bị phía ngoài như bộ đọc/bộ ghi 200 trên cơ sở của các sóng mang thu được, và làm cho tín hiệu phản hồi được truyền thông qua việc điều biến tải.

Fig.4 là sơ đồ giải thích minh họa ví dụ về cấu hình của chip IC 166 và anten 168 được minh họa trên Fig.3. Ngoài ra, ví dụ, thiết bị xử lý thông tin 100 có thể không có cấu hình của chip IC 166 được minh họa trên Fig.3 dưới dạng

của chip IC.

Anten 168 được cấu thành bởi mạch cộng hưởng bao gồm, ví dụ, cuộn dây (cuộn cảm) L1 mà có độ tự cảm định trước và tụ điện C1 mà có điện dung định trước, và tạo ra điện áp cảm ứng thông qua cảm ứng điện từ để phản hồi lại việc thu của sóng mang. Ngoài ra, anten 168 xuất ra điện áp thu thu được bằng cách cộng hưởng điện áp cảm ứng tại tần số cộng hưởng định trước. Ở đây, tần số cộng hưởng của anten 168 được thiết lập theo tần số của sóng mang như, ví dụ, 13,56 MHz. Anten 168 thu sóng mang thông qua cấu hình nêu trên và truyền tín hiệu phản hồi thông qua việc điều biến tải được thực hiện trong mạch điều biến tải 182 của chip IC 166.

Chip IC 166 bao gồm, ví dụ, mạch dò tìm sóng mang 172, mạch dò tìm 174, bộ điều chỉnh 176, mạch giải điều biến 178, MPU 180, và mạch điều biến tải 182. Ngoài ra, 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) để ngăn việc quá tải điện áp hoặc quá tải dòng điện khỏi được đặt vào MPU 180. Ở đây, ví dụ, mạch ghim hoặc loại tương tự được cấu thành bởi điôt hoặc loại tương tự có thể được sử dụng làm mạch bảo vệ (không được minh họa).

Ngoài ra, chip IC 166 bao gồm, ví dụ, ROM 184, RAM 186, và bộ nhớ bất biến 188. Ví dụ, MPU 180, ROM 184, RAM 186, và bộ nhớ bất biến 188 được kết nối thông qua kênh truyền 190 như là đường truyền dữ liệu. Ngoài ra, kênh truyền 190 được kết nối tới kênh truyền 170.

ROM 184 lưu trữ chương trình và dữ liệu điều khiển như các tham số tính toán mà được sử dụng bởi MPU 180 chẳng hạn. RAM 186 lưu trữ tạm thời chương trình được thực hiện bởi MPU 180, kết quả tính toán, trạng thái thực hiện, hoặc loại tương tự.

Bộ nhớ bất biến 188 là phương tiện ghi khác có chức năng như bộ lưu trữ (không được minh họa). Bộ nhớ bất biến 188 lưu trữ các loại dữ liệu khác nhau như, ví dụ, “dữ liệu liên quan đến phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 như thông tin khóa (được mô tả sau đây) hoặc thông tin thiết lập (được mô tả sau đây),” giá trị điện tử (tiền tệ hoặc dữ liệu mà có giá trị tương ứng với tiền tệ), dữ liệu tương ứng với các loại dịch vụ khác nhau, và các loại ứng dụng khác nhau. Thông tin khóa theo phương án của sáng chế là dữ liệu mà được sử dụng trong việc xác thực trong việc truyền thông theo phương pháp truyền thông tùy ý như NFC (bao gồm xác thực để truy nhập vùng của phương tiện ghi), các xử lý liên quan đến mã hóa/giải mã mật tùy ý, hoặc loại tương tự. Sau đây, khóa được sử dụng cho việc xác thực trong số thông tin khóa được gọi là “khóa xác thực”. Ngoài ra, khóa xác thực theo phương án của sáng chế và khóa được sử dụng cho việc mã hóa hoặc giải mã mật có thể là khóa giống nhau hoặc có thể là các khóa khác nhau. Nói cách khác, khóa được chỉ báo bởi thông tin khóa theo phương án của sáng chế có thể đảm nhận một trong số hoặc cả khóa xác thực và khóa được sử dụng cho việc mã hóa hoặc giải mã mật.

Ở đây, các ví dụ về bộ nhớ bất biến 188 bao gồm bộ nhớ chỉ đọc khả trình và có thể xóa bằng điện (EEPROM-electrically erasable and programmable read only memory), bộ nhớ chớp, và loại tương tự. Bộ nhớ bất biến 188, ví dụ, có khả năng chống đánh cắp và tương ứng với ví dụ về phương tiện ghi bảo mật.

Mạch dò tìm sóng mang 172 tạo ra, ví dụ, tín hiệu dò tìm chữ nhật trên cơ sở của điện áp thu được truyền từ anten 168, và truyền tín hiệu dò tìm tới MPU 180. Ngoài ra, ví dụ, MPU 180 sử dụng tín hiệu dò tìm được truyền làm xung nhịp xử lý để xử lý dữ liệu. Ở đây, do tín hiệu dò tìm là tín hiệu dựa trên điện áp thu được truyền từ anten 168, tín hiệu dò tìm được đồng bộ với tần số của sóng mang được truyền từ thiết bị phía ngoài như bộ đọc/bộ ghi 200. Do đó, do mạch

dò tìm sóng mang 172 được cài đặt, chip IC 166 có thể thực hiện xử lý với thiết bị phía ngoài như bộ đọc/bộ ghi 200 một cách đồng bộ với thiết bị phía ngoài.

Mạch dò tìm 174 chỉnh lưu điện áp thu được xuất ra từ anten 168. Ở đây, mạch dò tìm 174 bao gồm, ví dụ, điôt D1 và tụ điện C2.

Bộ điều chỉnh 176 san bằng điện áp thu thành điện áp không đổi, và xuất ra điện áp điều khiển tới MPU 180. Ở đây, bộ điều chỉnh 176 sử dụng thành phần DC của điện áp thu là điện áp điều khiển.

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

MPU 180 được điều khiển nhờ sử dụng điện áp điều khiển được xuất ra từ bộ điều chỉnh 176 làm điện năng và xử lý dữ liệu được giải điều biến trong mạch giải điều biến 178. Ở đây, MPU 180 bao gồm một hoặc nhiều bộ xử lý được cấu thành bởi mạch tính toán như, ví dụ, MPU, các loại mạch xử lý khác nhau, hoặc loại tương tự.

Ngoài ra, MPU 180 tạo ra tín hiệu điều khiển để điều khiển việc điều biến tải liên quan đến việc phản hồi lại thiết bị phía ngoài như bộ đọc/bộ ghi 200 theo kết quả xử lý. Sau đó, MPU 180 xuất ra tín hiệu điều khiển tới mạch điều biến tải 182.

Mạch điều biến tải 182 bao gồm, ví dụ, tải Z và công tắc SW1, và kết nối một cách chọn lọc (kích hoạt) tải Z theo tín hiệu điều khiển được truyền từ MPU 180 và thực hiện việc điều biến tải. Ở đây, tải Z bao gồm, ví dụ, điện trở mà có giá trị điện trở định trước. Ngoài ra, công tắc SW1 được cấu thành bởi, ví dụ,

tranzito hiệu ứng trường bán dẫn oxit kim loại (MOSFET-metal oxide semiconductor field effect transistor) kênh p hoặc MOSFET kênh n.

Với cấu hình nêu trên, chip IC 166 xử lý tín hiệu sóng mang thu được bởi anten 168 và làm cho anten 168 truyền tín hiệu phản hồi thông qua việc điều biến tải.

Chip IC 166 và anten 168 có, ví dụ, cấu hình được minh họa trên Fig.4, và thực hiện việc truyền thông NFC với thiết bị phía ngoài như bộ đọc/bộ ghi 200 hoặc loại tương tự nhờ sử dụng các sóng mang có tần số định trước. Ngoài ra, sẽ được hiểu rằng cấu hình của chip IC 166 và anten 168 theo phương án của sáng chế không bị giới hạn ở ví dụ được minh họa trên Fig.4.

Thiết bị xử lý thông tin 100 truyền thông với thiết bị phía ngoài như bộ đọc/bộ ghi 200, ví dụ, với cấu hình phần cứng được minh họa trên Fig.3. Ngoài ra, thiết bị xử lý thông tin 100 thực hiện xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 được mô tả sau đây, ví dụ, với cấu hình phần cứng được minh họa trên Fig.3. Ngoài ra, cấu hình phần cứng của thiết bị xử lý thông tin 100 theo phương án của sáng chế không bị giới hạn ở cấu hình được minh họa trên Fig.3.

Ví dụ, trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện thông qua thiết bị truyền thông phía ngoài mà có chức năng và cấu hình tương tự chức năng và cấu hình của giao diện truyền thông 164, hoặc trong trường hợp trong đó việc truyền thông theo một phương pháp truyền thông được mô tả ở trên không được thực hiện, thiết bị xử lý thông tin 100 có thể không bao gồm giao diện truyền thông 164.

Ngoài ra, ví dụ, trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện thông qua thiết bị truyền thông phía ngoài mà có chức

năng và cấu hình tương tự chức năng và cấu hình của chip IC 166 và anten 168, thiết bị xử lý thông tin 100 có thể không bao gồm chip IC 166 và anten 168.

Ngoài ra, trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện trong theo phương pháp truyền thông khác NFC như việc truyền thông không dây sử dụng IEEE 802.15.1, thiết bị xử lý thông tin 100 có thể không bao gồm chip IC 166 và anten 168. Trong trường hợp của ví dụ nêu trên, thiết bị xử lý thông tin 100 thực hiện việc truyền thông với thiết bị phía ngoài thông qua thiết bị truyền thông mà hỗ trợ phương pháp truyền thông khác NFC hoặc thiết bị truyền thông phía ngoài mà hỗ trợ phương pháp truyền thông khác NFC.

Ngoài ra, thiết bị xử lý thông tin 100 có thể được tạo cấu hình trong đó, ví dụ, một vài hoặc tất cả trong số phương tiện ghi 156, thiết bị nhập thao tác 160, và thiết bị hiển thị 162 không được bao gồm.

Ngoài ra, ví dụ, thiết bị xử lý thông tin 100 có thể được tạo cấu hình phần cứng theo ví dụ ứng dụng của thiết bị xử lý thông tin 100 được mô tả sau đây. Theo ví dụ của sáng chế, ví dụ, trong trường hợp trong đó thiết bị xử lý thông tin 100 là thẻ IC, thiết bị xử lý thông tin 100 có thể được cấu thành bởi chip IC 166 và anten 168. Trong trường hợp trong đó thiết bị xử lý thông tin 100 là thẻ IC, ví dụ, MPU 180 mà cấu thành chip IC 166 thực hiện xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 được mô tả sau đây.

Ngoài ra, ví dụ, cấu hình được minh họa trên Fig.3 (hoặc cấu hình theo ví dụ cải biến) có thể được thực hiện bởi một hoặc hai mạch tích hợp (IC-integrated circuit) hoặc nhiều hơn.

Ví dụ về cấu hình của thiết bị xử lý thông tin 100 sẽ được mô tả dựa vào Fig.2. Bộ truyền thông thứ nhất 102 truyền thông với thiết bị phía ngoài theo

việc truyền thông của một phương pháp truyền thông. Ví dụ, việc truyền thông trong bộ truyền thông thứ nhất 102 được điều khiển bởi bộ điều khiển 106.

Ở đây, ví dụ, anten truyền thông và mạch RF (truyền thông không dây), cổng IEEE 802.15.1 và mạch thu phát (truyền thông không dây), cổng IEEE 802.11 và mạch thu phát (truyền thông không dây), thiết bị đầu cuối LAN và mạch thu phát (truyền thông có dây), hoặc loại tương tự có thể được sử dụng làm bộ truyền thông thứ nhất 102.

Bộ truyền thông thứ hai 104 truyền thông với thiết bị phía ngoài theo việc truyền thông của phương pháp truyền thông khác. Ví dụ, việc truyền thông trong bộ truyền thông thứ hai 104 được điều khiển bởi bộ điều khiển 106.

Ở đây, ví dụ, thiết bị truyền thông mà hỗ trợ NFC như chip IC 166 và anten 168 được minh họa trên Fig.3 có thể được sử dụng làm bộ truyền thông thứ hai 104. Ngoài ra, như được mô tả ở trên, bộ truyền thông thứ hai 104 có thể là thiết bị truyền thông mà hỗ trợ phương pháp truyền thông khác NFC như, ví dụ, truyền thông không dây nhờ sử dụng IEEE 802.15.1.

Bộ điều khiển 106 được cấu thành bởi, ví dụ, MPU hoặc loại tương tự và đóng vai trò để điều khiển thiết bị xử lý thông tin 100 nói chung. Ngoài ra, bộ điều khiển 106 bao gồm, ví dụ, bộ xử lý 110 và đóng vai trò chính trong việc thực hiện xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 được mô tả sau đây.

bộ xử lý 110 đóng vai trò chính trong việc xử lý quy trình theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100. Ví dụ về xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 sẽ được mô tả trong mỗi phương án được mô tả sau đây.

Ngoài ra, cấu hình của thiết bị xử lý thông tin theo phương án của sáng chế

không bị giới hạn ở cấu hình được minh họa trên Fig.2.

Ví dụ, thiết bị xử lý thông tin theo phương án của sáng chế có thể bao gồm bộ xử lý 110 được minh họa trên Fig.2 tách biệt với bộ điều khiển 106 (mà được thực hiện bởi, ví dụ, mạch xử lý khác).

Ngoài ra, cấu hình của thiết bị xử lý thông tin theo phương án của sáng chế không bị giới hạn ở cấu hình được minh họa trên Fig.2, và có thể sử dụng cấu hình tương ứng với cách thức tách biệt xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 được mô tả sau đây.

Ngoài ra, ví dụ, trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện thông qua thiết bị truyền thông phía ngoài mà có chức năng và cấu hình tương tự chức năng và cấu hình của bộ truyền thông thứ nhất 102 hoặc trong trường hợp trong đó đây là cấu hình trong đó việc truyền thông của một phương pháp truyền thông được mô tả ở trên không được thực hiện, thiết bị xử lý thông tin theo phương án của sáng chế có thể không bao gồm bộ truyền thông thứ nhất 102.

Ngoài ra, ví dụ, trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện thông qua thiết bị truyền thông phía ngoài mà có chức năng và cấu hình tương tự chức năng và cấu hình của bộ truyền thông thứ hai 104, thiết bị xử lý thông tin theo phương án của sáng chế có thể không bao gồm bộ truyền thông thứ hai 104.

(1-2) Bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp)

Bộ đọc/bộ ghi 200 (thiết bị chuyển tiếp) là thiết bị mà đóng vai trò là thiết bị chuyển tiếp mà chuyển tiếp việc truyền thông giữa máy chủ 300 và thiết bị xử lý thông tin 100.

(Ví dụ cấu hình phân cứng của bộ đọc/bộ ghi 200)

Fig.5 là sơ đồ giải thích minh họa ví dụ về cấu hình phần cứng của bộ đọc/bộ ghi 200 (thiết bị chuyên 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. Ngoài ra, ví dụ, các bộ phận tương ứng của bộ đọc/bộ ghi 200 được kết nối với nhau thông qua kênh truyền 264 mà đóng vai trò là đường truyền dữ liệu. Ngoài ra, bộ đọc/bộ ghi 200 được điều khiển bởi, ví dụ, điện năng được cấp từ nguồn điện bên trong như pin được chứa trong bộ đọc/bộ ghi 200, điện năng được cấp từ nguồn điện phía ngoài được kết nối, hoặc loại tương tự.

MPU 250 được cấu thành bởi một hoặc nhiều bộ xử lý được cấu thành bởi mạch tính toán như, ví dụ, MPU, các loại mạch xử lý khác nhau, hoặc loại tương tự, và thực hiện chức năng là bộ điều khiển (không được minh họa) mà điều khiển bộ đọc/bộ ghi 200 nói chung.

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

Phương tiện ghi 256 thực hiện chức năng là bộ lưu trữ (không được minh họa) và lưu trữ các loại dữ liệu khác nhau như, ví dụ, các loại ứng dụng khác nhau. Ở đây, các ví dụ về phương tiện ghi 256 bao gồm phương tiện ghi từ như đĩa cứng và bộ nhớ bất biến như bộ nhớ chớp. Ngoài ra, phương tiện ghi 256 có thể được tách rời khỏi bộ đọc/bộ ghi 200.

Giao diện truyền thông 258 là thiết bị truyền thông mà thực hiện việc truyền thông theo một phương pháp truyền thông được hỗ trợ bởi bộ đọc/bộ ghi 200 và thực hiện chức năng là bộ truyền thông thứ nhất (không được minh họa)

mà thực hiện việc truyền thông với thiết bị phía ngoài như máy chủ 300 theo cách thức có dây hoặc không dây thông qua mạng (hoặc một cách trực tiếp). Ở đây, ví dụ, anten truyền thông và mạch RF (truyền thông không dây), cổng IEEE 802.15.1 và mạch thu phát (truyền thông không dây), cổng IEEE 802.11 và mạch thu phát (truyền thông không dây), thiết bị đầu cuối LAN và mạch thu phát (truyền thông có dây), hoặc loại tương tự có thể được sử dụng làm giao diện truyền thông 258. Ngoài ra, giao diện truyền thông 258 có thể là cấu hình bất kỳ tương ứng với mạng theo phương án của sáng chế.

Mạch truyền sóng mang 260 và anten 262 là thiết bị truyền thông mà thực hiện việc truyền thông theo các phương pháp truyền thông khác được hỗ trợ trong bộ đọc/bộ ghi 200, và thực hiện chức năng là bộ truyền thông thứ hai (không được minh họa) mà thực hiện việc truyền thông với thiết bị phía ngoài như thiết bị xử lý thông tin 100 theo cách thức có dây hoặc không dây.

Anten 262 được cấu thành bởi, ví dụ, mạch cộng hưởng bao gồm cuộn dây mà có độ tự cảm định trước mà đóng vai trò là anten thu phát và tụ điện mà có điện dung định trước và mạch giải điều biến. Ngoài ra, anten 262 thu các sóng mang có tần số định trước như, ví dụ, 13,56 MHz, và giải điều biến dữ liệu hoặc loại tương tự được truyền thông qua việc điều biến tải hoặc loại tương tự từ thiết bị phía ngoài như thiết bị xử lý thông tin 100. Ngoài ra, ví dụ, trong trường hợp trong đó mạch truyền sóng mang 260 bao gồm mạch giải điều biến, anten 262 có thể được cấu thành bởi mạch cộng hưởng.

Mạch truyền sóng mang 260 bao gồm, ví dụ, mạch điều biến mà thực hiện việc điều biến như khóa dịch biên độ (ASK-amplitude shift keying) và mạch khuếch đại mà khuếch đại đầu ra của mạch điều biến, và làm cho các sóng mang mà tín hiệu sóng mang từ anten thu phát của anten 262 được truyền. Ngoài ra, mạch truyền sóng mang 260 có thể bao gồm mạch giải điều biến mà giải điều

biến tín hiệu thu được bởi anten 262, chẳng hạn. Ví dụ, mạch giải điều biến thực hiện việc dò tìm đường bao của thay đổi biên độ trong điện áp giữa mạch điều biến (hoặc mạch khuếch đại) và mạch cộng hưởng của anten 262, nhị phân hóa tín hiệu được phát hiện, và giải điều biến tín hiệu thu được bởi anten 262. Ngoài ra, mạch giải điều biến có thể giải điều biến tín hiệu thu được bởi anten 262, ví dụ, bằng cách sử dụng sự thay đổi pha trong điện áp giữa mạch điều biến (hoặc mạch khuếch đại) và mạch cộng hưởng của anten 262.

Khi mạch truyền sóng mang 260 được cài đặt, bộ đọc/bộ ghi 200 có chức năng bộ khởi tạo trong NFC và đảm nhận là bộ đọc/bộ ghi. Ở đây, các tín hiệu khác nhau như, ví dụ, tín hiệu hỏi vòng (polling) và tín hiệu mà chỉ báo các loại yêu cầu khác nhau như yêu cầu đọc có thể được sử dụng làm tín hiệu sóng mang được truyền từ anten 262 bởi mạch truyền sóng mang 260. Ngoài ra, ví dụ, mạch truyền sóng mang 260 điều khiển việc truyền của sóng mang bởi MPU 250.

Bộ đọc/bộ ghi 200 có, ví dụ, cấu hình phần cứng được minh họa trên Fig.5 và do đó đảm nhận là thiết bị chuyển tiếp. Ngoài ra, cấu hình phần cứng của bộ đọc/bộ ghi 200 theo phương án của sáng chế không bị giới hạn ở cấu hình được minh họa trên Fig.5.

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

Ngoài ra, bộ đọc/bộ ghi 200 có thể không bao gồm mạch truyền sóng mang 260 và anten 262 trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện thông qua thiết bị truyền thông phía ngoài mà có các chức năng tương tự như của mạch truyền sóng mang 260 và anten 262.

Ngoài ra, bộ đọc/bộ ghi 200 có thể không bao gồm mạch truyền sóng mang 260 và anten 262 trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài được thực hiện theo phương pháp truyền thông khác NFC như việc truyền thông không dây sử dụng IEEE 802.15.1. Trong trường hợp của ví dụ nêu trên, bộ đọc/bộ ghi 200 thực hiện việc truyền thông với thiết bị phía ngoài thông qua thiết bị truyền thông mà hỗ trợ phương pháp truyền thông khác NFC hoặc thiết bị truyền thông phía ngoài mà hỗ trợ phương pháp truyền thông khác NFC.

Ngoài ra, bộ đọc/bộ ghi 200 có thể được tạo cấu hình trong đó, ví dụ, phương tiện ghi 256 không được bao gồm.

Ngoài ra, ví dụ, bộ đọc/bộ ghi 200 có thể được tạo cấu hình phần cứng theo ví dụ ứng dụng của bộ đọc/bộ ghi 200 được mô tả sau đây.

Ngoài ra, ví dụ, cấu hình được minh họa trên Fig.5 (hoặc cấu hình theo ví dụ cải biến) có thể được thực hiện bởi một hoặc hai mạch tích hợp (IC-integrated circuit) hoặc nhiều hơn.

(1-3) Máy chủ 300

Máy chủ 300 là thiết bị mà truyền thông với thiết bị xử lý thông tin 100 thông qua bộ đọc/bộ ghi 200 (hoặc một cách trực tiếp). Máy chủ 300 có thể thực hiện các xử lý khác nhau như xử lý thanh toán nhờ sử dụng, ví dụ, giá trị điện tử bằng cách truyền thông với thiết bị xử lý thông tin 100.

(Ví dụ cấu hình phần cứng của máy chủ 300)

Fig.6 là sơ đồ giải thích minh họa ví dụ về cấu hình phần cứng của máy chủ 300 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. Ngoài ra, ví dụ, các bộ phận tương ứng của máy chủ 300 được kết nối với nhau thông

qua kênh truyền 366 mà đóng vai trò là đường truyền dữ liệu. Ngoài ra, máy chủ 300 được điều khiển bởi, ví dụ, điện năng được cấp từ nguồn điện bên trong như pin được chứa trong máy chủ 300, điện năng được cấp từ nguồn điện phía ngoài được kết nối, hoặc loại tương tự.

MPU 350 được cấu thành bởi một hoặc nhiều bộ xử lý được cấu thành bởi mạch tính toán như, ví dụ, MPU, các loại mạch xử lý khác nhau, hoặc loại tương tự, và thực hiện chức năng là bộ điều khiển (không được minh họa) mà điều khiển máy chủ 300 nói chung.

ROM 352 lưu trữ chương trình, dữ liệu điều khiển như các tham số tính toán, và loại tương tự mà được sử dụng bởi MPU 350. RAM 354 lưu trữ tạm thời, ví dụ, chương trình được thực hiện bởi MPU 350.

Phương tiện ghi 356 thực hiện chức năng là bộ lưu trữ (không được minh họa), và lưu trữ các loại dữ liệu khác nhau như, ví dụ, dữ liệu liên quan đến phương pháp xử lý thông tin trong máy chủ 300 hoặc các loại ứng dụng khác nhau. Ở đây, các ví dụ về phương tiện ghi 356 bao gồm phương tiện ghi từ như đĩa cứng và bộ nhớ bất biến như bộ nhớ chớp. Ngoài ra, phương tiện ghi 356 có thể tháo rời được khỏi máy chủ 300.

Giao diện đầu vào/đầu ra 358 kết nối, ví dụ, thiết bị nhập thao tác 360 hoặc thiết bị hiển thị 362. Thiết bị nhập thao tác 360 thực hiện chức năng là bộ thao tác (không được minh họa), và thiết bị hiển thị 362 thực hiện chức năng là bộ hiển thị (không được minh họa). Ở đây, các ví dụ về giao diện đầu vào/đầu ra 358 bao gồm đầu cuối USB, đầu cuối DVI, đầu cuối HDMI (nhãn hiệu được đăng ký), và các loại mạch xử lý khác nhau.

Ngoài ra, ví dụ, thiết bị nhập thao tác 360 được cài đặt trên máy chủ 300 và được kết nối với giao diện đầu vào/đầu ra 358 trong máy chủ 300. Ví dụ, nút

bấm, phím hướng, bộ lựa chọn kiểu quay như con cuộn, kết hợp của chúng, hoặc loại tương tự có thể được sử dụng làm thiết bị nhập thao tác 360.

Ngoài ra, ví dụ, thiết bị hiển thị 362 được cài đặt trên máy chủ 300 và được kết nối với giao diện đầu vào/đầu ra 358 trong máy chủ 300. Ví dụ, màn hình tinh thể lỏng hoặc màn hình EL hữu cơ có thể được sử dụng làm thiết bị hiển thị 362.

Ngoài ra, sẽ được hiểu rằng giao diện đầu vào/đầu ra 358 có thể được kết nối tới thiết bị phía ngoài như thiết bị nhập thao tác (ví dụ, bàn phím, chuột, hoặc loại tương tự) phía ngoài máy chủ 300 hoặc thiết bị hiển thị phía ngoài. Ngoài ra, thiết bị hiển thị 362 có thể là thiết bị mà trên đó việc hiển thị và thao tác người dùng có thể được thực hiện như màn chạm.

Giao diện truyền thông 364 là thiết bị truyền thông để thực hiện việc truyền thông của một phương pháp truyền thông được hỗ trợ bởi máy chủ 300, và thực hiện chức năng là bộ truyền thông (không được minh họa) để thực hiện việc truyền thông có dây hoặc không dây với thiết bị phía ngoài như bộ đọc/bộ ghi 200 thông qua mạng (hoặc một cách trực tiếp). Ở đây, ví dụ, anten truyền thông và mạch RF (truyền thông không dây), cổng IEEE 802.15.1 và mạch thu phát (truyền thông không dây), cổng IEEE 802.11 và mạch thu phát (truyền thông không dây), thiết bị đầu cuối LAN và mạch thu phát (truyền thông có dây), hoặc loại tương tự có thể được sử dụng làm giao diện truyền thông 364. Ngoài ra, giao diện truyền thông 364 có thể là cấu hình bất kỳ tương ứng với mạng theo phương án của sáng chế.

Máy chủ 300 thực hiện các xử lý khác nhau như xử lý thanh toán, ví dụ, bởi cấu hình phần cứng được minh họa trên Fig.6. Ngoài ra, cấu hình phần cứng của máy chủ 300 theo phương án của sáng chế không bị giới hạn ở cấu hình được minh họa trên Fig.6.

Ví dụ, trong trường hợp trong đó việc truyền thông với thiết bị phía ngoài hoặc loại tương tự được thực hiện thông qua thiết bị truyền thông phía ngoài được kết nối, máy chủ 300 có thể không bao gồm giao diện truyền thông 364. Ngoài ra, giao diện truyền thông 364 có thể được tạo cấu hình mà có thể thực hiện việc truyền thông với một hoặc nhiều thiết bị phía ngoài hoặc loại tương tự theo nhiều phương pháp truyền thông.

Ngoài ra, máy chủ 300 có thể được tạo cấu hình trong đó, ví dụ, một vài hoặc tất cả trong số phương tiện ghi 356, thiết bị nhập thao tác 360, và thiết bị hiển thị 362 không được bao gồm.

Ngoài ra, ví dụ, máy chủ 300 có thể được tạo cấu hình phần cứng theo ví dụ ứng dụng của máy chủ 300 được mô tả sau đây.

Ngoài ra, ví dụ, một phần hoặc tất cả cấu hình phần cứng được minh họa trên Fig.6 (hoặc cấu hình theo ví dụ cải biến) có thể được thực hiện bởi một hoặc hai IC hoặc nhiều hơn.

(1-4) Ví dụ ứng dụng của mỗi thiết bị mà cấu thành hệ thống xử lý thông tin theo phương án của sáng chế

Mặc dù thiết bị xử lý thông tin 100 đã được mô tả ở trên như là bộ phận của hệ thống xử lý thông tin theo phương án của sáng chế, phương án này không bị giới hạn ở dạng này. 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 trong thiết bị xử lý thông tin 100 (được mô tả sau đây) như, ví dụ, “thiết bị truyền thông như điện thoại thông minh”, “thẻ IC”, “thiết bị loại bảng”, hoặc “máy chơi trò chơi”. Ngoài ra, phương án của sáng chế cũng có thể được áp dụng cho IC xử lý mà có thể được kết hợp vào, ví dụ, các thiết bị được đề cập nêu trên.

Ngoài ra, mặc dù bộ đọc/bộ ghi 200 (thiết bị chuyên tiếp) đã được mô tả là

bộ phận của hệ thống xử lý thông tin theo phương án của sáng chế, phương án này không bị giới hạn ở dạng này. Ví dụ, phương án của sáng chế có thể được áp dụng cho thiết bị tùy ý mà có chức năng chuyển tiếp truyền thông giữa các thiết bị như “bộ đọc/bộ ghi”, “thiết bị có chức năng bộ đọc/bộ ghi”, và “thiết bị truyền thông mà thực hiện việc truyền thông theo việc truyền thông không dây sử dụng IEEE 802.15.1 như BLE” hoặc loại tương tự. Ngoài ra, phương án của sáng chế cũng có thể được áp dụng cho IC xử lý mà có thể được kết hợp vào, ví dụ, các thiết bị được đề cập nêu trên.

Ngoài ra, mặc dù máy chủ 300 đã được mô tả là bộ phận của hệ thống xử lý thông tin theo phương án của sáng chế, phương án này không bị giới hạn ở dạng này. Phương án của sáng chế có thể được áp dụng cho các thiết bị khác nhau như “máy tính như máy tính cá nhân (PC) hoặc máy chủ chẳng hạn”, “thiết bị kiểu bảng”, “thiết bị truyền thông như điện thoại thông minh”, “máy chơi trò chơi” và loại tương tự. Ngoài ra, phương án của sáng chế cũng có thể được áp dụng cho IC xử lý mà có thể được kết hợp vào, ví dụ, các thiết bị được đề cập nêu trên.

(2) Phương pháp xử lý thông tin theo phương án của sáng chế

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

(2-1) Phương pháp xử lý thông tin theo phương án thứ nhất

(2-1-1) Tổng quát của hệ thống xử lý thông tin 1000 mà phương pháp xử lý thông tin theo phương án thứ nhất được áp dụng

Ví dụ, các phần sau đây được thể hiện trong tài liệu sáng chế 1:

- khóa xác thực được tạo ra nhờ sử dụng các khóa phân cấp hoặc các khóa

vùng lưu trữ: và

- khóa xác thực được chuyển đổi trên cơ sở của thông tin dành riêng cho thiết bị, và việc xác thực được thực hiện nhờ sử dụng kết quả chuyển đổi.

Fig.7 là sơ đồ giải thích được sử dụng để mô tả phương pháp xử lý thông tin theo phương án của sáng chế và minh họa một cách giản lược khóa xác thực được mô tả trong tài liệu sáng chế 1.

Ví dụ, như được minh họa trong các bước S10, S12, S14, ... được minh họa trên Fig.7, trong kỹ thuật được bộc lộ trong tài liệu sáng chế 1, khóa suy biến mà có thể đảm nhận khóa xác thực được tạo ra, ví dụ, bằng cách thực hiện việc tính toán nhờ sử dụng các khóa phân cấp hoặc các khóa vùng lưu trữ trên trị số đóng vai trò là cơ sở như số ngẫu nhiên. Khóa suy biến được tạo ra, ví dụ, bằng cách thực hiện tuần tự việc mã hóa nhờ sử dụng mỗi khóa trên giá trị đóng vai trò là cơ sở.

Ngoài ra, như được minh họa trong bước S16 trên Fig.7, trong kỹ thuật được bộc lộ trong tài liệu sáng chế 1, khóa suy biến được chuyển đổi trên cơ sở của thông tin dành riêng cho thiết bị mà là dữ liệu dành riêng cho thiết bị như ID sản xuất chẳng hạn, và kết quả chuyển đổi được sử dụng làm khóa xác thực. Trong kỹ thuật được bộc lộ trong tài liệu sáng chế 1, khóa suy biến được chuyển đổi, ví dụ, bằng cách thực hiện XOR giữa khóa suy biến và thông tin dành riêng cho thiết bị hoặc bằng cách thực hiện việc mã hóa nhờ sử dụng thông tin dành riêng cho thiết bị làm khóa trên khóa suy biến.

Ví dụ, như được minh họa trên Fig.7, đối với khóa suy biến được chuyển đổi nhờ sử dụng thông tin dành riêng cho thiết bị, khóa xác thực khác nhau đối với mỗi thiết bị, và do đó tính bảo mật có thể được cải thiện.

Ở đây, khi khóa xác thực được chuyển đổi nhờ sử dụng thông tin dành riêng

cho thiết bị như trong kỹ thuật được bộc lộ trong tài liệu sáng chế 1, phương pháp chuyển đổi thường được giữ bí mật. Một trong số các lý do tại sao phương pháp chuyển đổi được giữ bí mật là, ví dụ, do việc chuyển đổi ngược có thể được thực hiện nếu phương pháp chuyển đổi đã được biết trong trường hợp trong đó việc chuyển đổi được thực hiện theo phương pháp mã hóa khóa chung.

Trong trường hợp trong đó phương tiện ghi được lắp đặt trong một thiết bị bao gồm các vùng của các nhà điều hành kinh doanh hoặc trong trường hợp trong đó bí mật của phương pháp chuyển đổi lộ ra khỏi một nhà điều hành kinh doanh, điều này ảnh hưởng tới tất cả các nhà điều hành kinh doanh khác. Do đó, về mặt kỹ thuật có thể chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh, nhưng sẽ khó khăn về mặt thực tiễn.

Liên quan đến việc này, thiết bị xử lý thông tin 100 mà phương pháp xử lý thông tin theo phương án thứ nhất được áp dụng, thực hiện “việc tạo ra khóa xác thực trên cơ sở của thông tin dành riêng cho thiết bị mà không chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh”.

Do khóa xác thực được tạo ra trên cơ sở của thông tin dành riêng cho thiết bị và khóa xác thực này khác nhau đối với mỗi thiết bị, tính bảo mật có thể được cải thiện. Ngoài ra, đối với khóa xác thực được tạo ra trên cơ sở của thông tin dành riêng cho thiết bị mà không chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh, có thể làm giảm ảnh hưởng khi bí mật của phương pháp chuyển đổi lộ ra ngoài, và do đó có thể cải thiện “sự thuận tiện của việc xác thực nhờ sử dụng khóa xác thực trong “mỗi nhà điều hành kinh doanh và mỗi người dùng của thiết bị xử lý thông tin 100” so với trường hợp trong đó kỹ thuật hiện nay được sử dụng.

Do đó, thiết bị xử lý thông tin 100 mà phương pháp xử lý thông tin theo phương án thứ nhất được áp dụng, có thể cải thiện sự thuận tiện của việc xác

thực nhờ sử dụng khóa xác thực.

(2-1-2) Xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 theo phương án thứ nhất

Tiếp theo, ví dụ về xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 theo phương án thứ nhất sẽ được mô tả.

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa được gán cho mỗi vùng trong số nhiều vùng của phương tiện ghi và tạo ra khóa xác thực. Các ví dụ về vùng của phương tiện ghi theo phương án của sáng chế bao gồm vùng của phương tiện ghi được lắp đặt trong thiết bị xử lý thông tin 100 như bộ nhớ bất biến 188 được minh họa trên Fig.4 và vùng của phương tiện ghi phía ngoài mà có thể truy nhập được bởi thiết bị xử lý thông tin 100 (điều tương tự áp dụng sau đây).

Đối với khóa liên quan đến phương án của sáng chế, ví dụ, hoặc một trong số hoặc cả khóa vùng để cho phép truy nhập tới vùng cụ thể của phương tiện ghi và khóa dịch vụ để cho phép truy nhập tới dữ liệu cụ thể được lưu trữ trong vùng của phương tiện ghi có thể được sử dụng. Ngoài ra, khóa theo phương án của sáng chế không bị giới hạn ở ví dụ được mô tả ở trên mà có thể là, ví dụ, khóa phân cấp được mô tả trong tài liệu sáng chế 1.

Trong bản mô tả này, có các trường hợp trong đó “vùng” chỉ báo, ví dụ, “vùng” trong hệ thống tệp của hệ điều hành (OS) FeliCa (nhãn hiệu được đăng ký). Trong trường hợp này, “vùng” tương ứng với thư mục (hoặc danh mục).

Ngoài ra, trong bản mô tả này, có các trường hợp trong đó “dịch vụ” chỉ báo, ví dụ, “dịch vụ” trong hệ thống tệp của hệ điều hành (OS) FeliCa (nhãn hiệu được đăng ký). Trong trường hợp này, “dịch vụ” tương ứng với dữ liệu (hoặc tệp) để cung cấp dịch vụ định trước.

Đối với việc tính toán nhờ sử dụng khóa theo phương án của sáng chế, ví dụ, việc mã hóa theo phương pháp mã hóa tùy ý có thể được sử dụng.

Ngoài ra, khi khóa xác thực được tạo ra, thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng “trị số chuyển đổi tương ứng với khóa được sử dụng trong việc tính toán”.

Việc mã hóa theo phương pháp mã hóa tùy ý có thể được sử dụng làm việc tính toán nhờ sử dụng trị số chuyển đổi theo phương án của sáng chế.

Trị số chuyển đổi tương ứng với khóa theo phương án của sáng chế là giá trị thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với mỗi khóa được sử dụng trong việc tính toán. Đối với thông tin dành riêng cho thiết bị trong phương án này, ví dụ, dữ liệu dành riêng cho thiết bị xử lý thông tin 100 như ID sản xuất được lưu trữ trong phương tiện ghi tùy ý được lắp đặt trong thiết bị xử lý thông tin 100 có thể được sử dụng.

Thiết bị xử lý thông tin 100 chỉ rõ phương pháp chuyển đổi được kết hợp với mỗi khóa, ví dụ, trên cơ sở của thông tin thiết lập được kết hợp với vùng của phương tiện ghi.

Thông tin thiết lập theo phương án của sáng chế là dữ liệu mà chỉ báo thiết lập liên quan đến vùng của phương tiện ghi.

Đối với thông tin thiết lập, ví dụ, “Bảng (hoặc cơ sở dữ liệu) trong đó địa chỉ mà chỉ báo vùng của phương tiện ghi, khóa, và dữ liệu mà chỉ báo phương pháp chuyển đổi được ghi kết hợp với mỗi vùng” có thể được sử dụng. Đối với dữ liệu mà chỉ báo phương pháp chuyển đổi, ví dụ, dữ liệu mà chỉ báo thuật toán chuyển đổi mà sử dụng ít nhất thông tin dành riêng cho thiết bị làm đầu vào có thể được sử dụng. Các phương pháp chuyển đổi được kết hợp với mỗi khóa có

thể đều giống nhau, hoặc nhiều phương pháp chuyển đổi có thể được bao gồm.

Ví dụ, đối với phương pháp chuyển đổi được lưu trữ trong thông tin thiết lập, ví dụ, thuật toán tùy ý có khả năng chuyển đổi giá trị được chỉ báo bởi thông tin dành riêng cho thiết bị thành giá trị khác có thể được sử dụng.

Ngoài ra, phương pháp chuyển đổi theo phương án của sáng chế không bị giới hạn ở ví dụ được mô tả ở trên. Ví dụ, phương pháp chuyển đổi theo phương án của sáng chế có thể bao gồm không chuyển đổi thông tin dành riêng cho thiết bị thành giá trị khác.

Ví dụ, trong trường hợp trong đó phương pháp chuyển đổi được kết hợp với một khóa chỉ báo rằng thông tin dành riêng cho thiết bị không được chuyển đổi, thiết bị xử lý thông tin 100 không thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với một khóa.

Sau đây, ví dụ tạo ra khóa xác thực theo phương pháp xử lý thông tin theo phương án thứ nhất sẽ được mô tả.

(A) Ví dụ tạo ra thứ nhất về khóa xác thực theo phương án thứ nhất

Fig.8 là sơ đồ giải thích minh họa ví dụ tạo ra thứ nhất về khóa xác thực theo phương pháp xử lý thông tin theo phương án thứ nhất.

“Khóa vùng/dịch vụ A” được minh họa trên Fig.8 chỉ báo khóa vùng hoặc khóa dịch vụ mà được gán cho vùng A trong phương tiện ghi như bộ nhớ bất biến 188. Ngoài ra, “khóa vùng/dịch vụ B” được minh họa trên Fig.8 chỉ báo khóa vùng hoặc khóa dịch vụ mà được gán cho vùng B trong phương tiện ghi như bộ nhớ bất biến 188, và “khóa vùng/dịch vụ C” được minh họa trên Fig.8 chỉ báo khóa vùng hoặc khóa dịch vụ mà được gán cho vùng C trong phương tiện ghi như bộ nhớ bất biến 188. Nói cách khác, “khóa vùng/dịch vụ” được minh họa trên Fig.8 là ví dụ về khóa được gán cho mỗi vùng. Sau đây, điều

tương tự áp dụng tới các hình vẽ khác.

Ngoài ra, “số ngẫu nhiên” được minh họa trên Fig.8 là ví dụ về giá trị mà đóng vai trò là cơ sở của khóa xác thực. Ngoài ra, sẽ được hiểu rằng giá trị mà đóng vai trò là cơ sở của khóa xác thực theo phương án của sáng chế, bao gồm các ví dụ được minh họa trên các hình vẽ từ Fig.9 đến Fig.12 được mô tả sau đây, không bị giới hạn ở số ngẫu nhiên. Phần mô tả sau đây sẽ mô tả trường hợp trong đó giá trị mà đóng vai trò là cơ sở của khóa xác thực là số ngẫu nhiên.

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng số ngẫu nhiên và khóa được gán cho vùng A (S100). Sau đây, kết quả tính toán của việc tính toán được thực hiện trong xử lý tạo khóa xác thực như kết quả tính toán của bước S100 được gọi là “khóa trung gian”.

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi A được kết hợp với khóa được gán cho vùng A được sử dụng trong bước S100 và thu nhận trị số chuyển đổi A (S102).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S100 và trị số chuyển đổi A (S104).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S104 và khóa được gán cho vùng B (S106).

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi B được kết hợp với khóa được gán cho vùng B được sử dụng trong bước S106 và thu nhận trị số chuyển đổi B (S108).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S106 và trị số chuyển đổi B (S110).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa

trung gian thu được trong xử lý của bước S110 và khóa được gán cho vùng C (S112).

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi C được kết hợp với khóa được gán cho vùng C được sử dụng trong bước S112 và thu nhận trị số chuyển đổi C (S114).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S114 và trị số chuyển đổi C (S116). Trong ví dụ được minh họa trên Fig.8, kết quả của xử lý trong bước S116 tương ứng với khóa xác thực.

Ví dụ, như được minh họa trên Fig.8, thiết bị xử lý thông tin 100 tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với khóa được sử dụng trong việc tính toán được thực hiện mỗi lần việc tính toán sử dụng khóa này được thực hiện. Trị số chuyển đổi được sử dụng trong ví dụ tạo ra thứ nhất về khóa xác thực là giá trị thu được bằng cách thực hiện việc chuyển đổi nhờ sử dụng phương pháp chuyển đổi được kết hợp với mỗi khóa được sử dụng trong mỗi tính toán sử dụng khóa này. Do đó, trong ví dụ tạo ra thứ nhất về khóa xác thực được minh họa trên Fig.8, không cần thiết phải chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh để tạo ra khóa xác thực. Do đó, trong ví dụ tạo ra thứ nhất về khóa xác thực được minh họa trên Fig.8, việc “tạo ra khóa xác thực dựa trên thông tin dành riêng cho thiết bị mà không chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh” được thực hiện.

Ngoài ra, ví dụ tạo ra thứ nhất về khóa xác thực theo phương án thứ nhất không bị giới hạn ở ví dụ được minh họa trên Fig.8.

Ví dụ, trong ví dụ được minh họa trên Fig.8, ví dụ trong đó việc tính toán

nhờ sử dụng khóa được thực hiện tuần tự ba lần được minh họa, nhưng số lượng tính toán được thực hiện nhờ sử dụng khóa có thể là số lượng tùy ý mà là hai hoặc lớn hơn.

Ngoài ra, như được mô tả ở trên, phương pháp chuyển đổi theo phương án của sáng chế có thể bao gồm không chuyển đổi thông tin dành riêng cho thiết bị thành giá trị khác. Ngoài ra, trong trường hợp trong đó phương pháp chuyển đổi được kết hợp với một khóa chỉ báo rằng thông tin dành riêng cho thiết bị không được chuyển đổi, thiết bị xử lý thông tin 100 có thể không thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với một khóa.

(B) Ví dụ tạo ra thứ hai về khóa xác thực theo phương án thứ nhất

Fig.9 là sơ đồ giải thích minh họa ví dụ tạo ra thứ hai về khóa xác thực theo phương pháp xử lý thông tin theo phương án thứ nhất.

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng số ngẫu nhiên và khóa được gán cho vùng A (S200).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S200 và khóa được gán cho vùng B (S202).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S202 và khóa được gán cho vùng C (S204). Kết quả của việc thực hiện tuần tự các việc tính toán nhờ sử dụng các khóa được minh họa trong các bước S200 đến S204 tương ứng với, ví dụ, khóa suy biến trong đó các khóa được tổng hợp.

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi A được kết hợp với khóa được gán cho vùng A được sử dụng trong bước S200 và thu nhận trị số chuyển đổi A (S206).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S204 và trị số chuyển đổi A (S208).

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi B được kết hợp với khóa được gán cho vùng B được sử dụng trong bước S202 và thu nhận trị số chuyển đổi B (S210).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S208 và trị số chuyển đổi B (S212).

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi C được kết hợp với khóa được gán cho vùng C được sử dụng trong bước S204 và thu nhận trị số chuyển đổi C (S214).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S212 và trị số chuyển đổi C (S216). Trong ví dụ được minh họa trên Fig.9, kết quả xử lý của bước S216 tương ứng với khóa xác thực.

Ví dụ, như được minh họa trên Fig.9, thiết bị xử lý thông tin 100 tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng khóa và sau đó thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với mỗi khóa. Trị số chuyển đổi được sử dụng trong ví dụ tạo ra thứ hai của khóa xác thực là giá trị thu được bằng cách thực hiện việc chuyển đổi nhờ sử dụng phương pháp chuyển đổi được kết hợp với mỗi khóa được sử dụng trong mỗi tính toán nhờ sử dụng khóa, tương tự ví dụ tạo ra thứ nhất về khóa xác thực được minh họa trên Fig.8. Do đó, trong ví dụ tạo ra thứ hai về khóa xác thực được minh họa trên Fig.9, không cần thiết phải chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh để tạo ra khóa xác thực. Do đó, trong ví dụ tạo ra thứ hai về khóa xác thực được minh họa trên Fig.9, việc “tạo ra khóa xác thực dựa

trên thông tin dành riêng cho thiết bị mà không chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh” được thực hiện.

Ngoài ra, ví dụ tạo ra thứ hai về khóa xác thực theo phương án thứ nhất không bị giới hạn ở ví dụ được minh họa trên Fig.9.

Trong ví dụ tạo ra thứ hai của khóa xác thực, ví dụ, tương tự ví dụ tạo ra thứ nhất về khóa xác thực, việc tính toán nhờ sử dụng khóa có thể được thực hiện với số lần tùy ý mà là hai lần hoặc nhiều hơn. Ngoài ra, trong ví dụ tạo ra thứ hai của khóa xác thực, tương tự ví dụ tạo ra thứ nhất về khóa xác thực, ví dụ, trong trường hợp trong đó phương pháp chuyển đổi được kết hợp với một khóa chỉ báo rằng thông tin dành riêng cho thiết bị không được chuyển đổi, việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với một khóa có thể không được thực hiện.

(C) Ví dụ tạo ra thứ ba của khóa xác thực theo phương án thứ nhất

Fig.10 là sơ đồ giải thích minh họa ví dụ tạo ra thứ ba của khóa xác thực theo phương pháp xử lý thông tin theo phương án thứ nhất.

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng số ngẫu nhiên và khóa được gán cho vùng A (S300).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S300 và khóa được gán cho vùng B (S302).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S302 và khóa được gán cho vùng C (S304). Kết quả của việc thực hiện tuần tự các việc tính toán nhờ sử dụng các khóa được minh họa trong các bước S300 đến S304 tương ứng với, ví dụ, khóa suy biến trong đó các khóa được tổng hợp.

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi A được kết hợp với khóa được gán cho vùng A được sử dụng trong bước S300 và thu nhận trị số chuyển đổi A (S306).

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi B được kết hợp với khóa được gán cho vùng B được sử dụng trong bước S302 và thu nhận trị số chuyển đổi B (S308).

Thiết bị xử lý thông tin 100 chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi C được kết hợp với khóa được gán cho vùng C được sử dụng trong bước S304 và thu nhận trị số chuyển đổi C (S310).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán tùy ý mà có khả năng tạo ra một giá trị từ trị số chuyển đổi A, trị số chuyển đổi B, và trị số chuyển đổi C, và tính toán một giá trị trên cơ sở của trị số chuyển đổi A, trị số chuyển đổi B, và trị số chuyển đổi C (S312). Ở đây, một giá trị được tạo ra trong xử lý trong bước S312 tương ứng với trị số tổng hợp thu được bằng cách tổng hợp trị số chuyển đổi A, trị số chuyển đổi B, và trị số chuyển đổi C.

Thiết bị xử lý thông tin 100 thực hiện việc tính toán nhờ sử dụng khóa trung gian thu được trong xử lý của bước S304 và trị số tổng hợp thu được trong xử lý của bước S312 (S314). Ở đây, do trị số tổng hợp là giá trị dựa trên trị số chuyển đổi A, trị số chuyển đổi B, và trị số chuyển đổi C, xử lý của bước S314 tương ứng với ví dụ về việc tính toán nhờ sử dụng các trị số chuyển đổi lần lượt tương ứng với các khóa. Ngoài ra, trong ví dụ được minh họa trên Fig.10, kết quả xử lý của bước S314 tương ứng với khóa xác thực.

Ví dụ, như được minh họa trên Fig.10, thiết bị xử lý thông tin 100 tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng khóa và sau đó thực hiện việc tính toán nhờ sử dụng trị số tổng hợp thu được bằng cách tổng

hợp các trị số chuyển đổi tương ứng với các khóa tương ứng. Trị số tổng hợp được sử dụng trong ví dụ tạo ra thứ ba của khóa xác thực là giá trị thu được bằng cách tổng hợp các trị số chuyển đổi thu được bằng cách thực hiện việc chuyển đổi nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử dụng trong các việc tính toán tương ứng. Do đó, trong ví dụ tạo ra thứ ba của khóa xác thực được minh họa trên Fig.10, không cần thiết phải chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh để tạo ra khóa xác thực. Do đó, trong ví dụ tạo ra thứ ba của khóa xác thực được minh họa trên Fig.10, việc “tạo ra khóa xác thực dựa trên thông tin dành riêng cho thiết bị mà không chia sẻ bí mật của phương pháp chuyển đổi giữa các nhà điều hành kinh doanh” được thực hiện.

Ngoài ra, ví dụ tạo ra thứ ba của khóa xác thực theo phương án thứ nhất không bị giới hạn ở ví dụ được minh họa trên Fig.10.

Trong ví dụ tạo ra thứ ba của khóa xác thực, ví dụ, tương tự ví dụ tạo ra thứ nhất về khóa xác thực, việc tính toán nhờ sử dụng khóa có thể được thực hiện với số lần tùy ý mà là hai lần hoặc nhiều hơn. Ngoài ra, trong ví dụ tạo ra thứ ba của khóa xác thực, tương tự ví dụ tạo ra thứ nhất về khóa xác thực, ví dụ, trong trường hợp trong đó phương pháp chuyển đổi được kết hợp với một khóa chỉ báo rằng thông tin dành riêng cho thiết bị không được chuyển đổi, việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với một khóa có thể không được thực hiện.

(2-2) Phương pháp xử lý thông tin theo phương án thứ hai

(2-2-1) Tổng quát của hệ thống xử lý thông tin 1000 mà phương pháp xử lý thông tin theo phương án thứ hai được áp dụng cho

Ví dụ, các phần sau đây được thể hiện trong tài liệu sáng chế 1:

- khóa suy biến được tạo ra nhờ sử dụng các khóa vùng hoặc các khóa dịch vụ, và việc xác thực được thực hiện nhờ sử dụng khóa suy biến

Ở đây, trong trường hợp trong đó khóa suy biến khác với khóa vùng và khóa dịch vụ được sử dụng trong việc xác thực như trong kỹ thuật được bộc lộ trong tài liệu sáng chế 1, do khó để lưu trữ chỉ khóa suy biến trong bộ đọc/bộ ghi, tính bảo mật của toàn bộ hệ thống được cải thiện.

Tuy nhiên, trong trường hợp trong đó việc xác thực được thực hiện nhờ sử dụng khóa suy biến theo kỹ thuật được bộc lộ trong tài liệu sáng chế 1, dịch vụ có thể truy nhập được trong thiết bị bị giới hạn ở dịch vụ tương ứng với khóa dịch vụ được sử dụng để tạo ra khóa suy biến. Ngoài ra, trong trường hợp trong đó việc xác thực sử dụng khóa suy biến theo kỹ thuật được bộc lộ trong tài liệu sáng chế 1 được thực hiện hai lần hoặc nhiều hơn, chỉ dịch vụ tương ứng với khóa suy biến được sử dụng trong việc xác thực cuối cùng có thể truy nhập được.

Ngoài ra, nói chung, nhà điều hành kinh doanh (nhà điều hành kinh doanh bộ đọc/bộ ghi) mà phát triển và lắp đặt bộ đọc/bộ ghi thu nhận sự bộc lộ của khóa suy biến từ nhà quản trị (nhà cung cấp dịch vụ) của khóa vùng và khóa dịch vụ. Sau đó, trong trường hợp trong đó bộ đọc/bộ ghi thực hiện việc ghi tới các dịch vụ lần lượt được quản lý bởi các nhà cung cấp dịch vụ, do số lượng khóa suy biến là hai hoặc nhiều hơn, việc xác thực được thực hiện hai lần hoặc nhiều hơn.

Ở đây, trong số các thiết bị mà hỗ trợ NFC như thẻ IC, có các thiết bị mà có thể thực hiện việc ghi tới nhiều dịch vụ tại cùng thời điểm để phản hồi lại lệnh ghi đơn và có đặc tính mà có thể đảm bảo tính nguyên tố của các xử lý. Tuy nhiên, trong kỹ thuật hiện này, trong trường hợp trong đó nhiều khóa suy biến được tạo ra, và việc xác thực được thực hiện nhiều lần, việc ghi mà có tính

nguyên tố không thể được thực hiện.

Liên quan đến việc này, thiết bị xử lý thông tin 100 mà phương pháp xử lý thông tin theo phương án thứ hai được áp dụng cho tạo ra khóa suy biến được tổng hợp (khóa suy biến thứ hai. Sau đây được gọi là “khóa suy biến lại”) thu được bằng cách tổng hợp nhiều khóa suy biến (các khóa suy biến thứ nhất) thành một khóa suy biến. Ngoài ra, thiết bị xử lý thông tin 100 thực hiện xử lý xác thực nhờ sử dụng khóa suy biến lại làm khóa xác thực.

Do khóa suy biến lại là khóa trong đó nhiều suy biến được tổng hợp, việc xác thực nhờ sử dụng khóa suy biến lại tương ứng với “việc xác thực sử dụng khóa suy biến của nguồn tổng hợp được thực hiện nhiều lần”.

Do đó, khi việc xác thực sử dụng khóa suy biến lại theo phương pháp xử lý thông tin theo phương án thứ hai được thực hiện, tất cả dịch vụ tương ứng với khóa suy biến của nguồn tổng hợp trở nên có thể truy nhập được.

Ngoài ra, do việc xác thực sử dụng khóa suy biến lại tương ứng với “việc xác thực sử dụng khóa suy biến của nguồn tổng hợp được thực hiện nhiều lần”, việc ghi mà có tính nguyên tố có thể được thực hiện bởi việc xác thực đơn sử dụng khóa suy biến lại.

Do đó, theo thiết bị xử lý thông tin 100 mà phương pháp xử lý thông tin theo phương án thứ hai được áp dụng cho có thể cải thiện sự thuận tiện của việc xác thực nhờ sử dụng khóa xác thực.

(2-2-2) Xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 theo phương án thứ hai

Tiếp theo, ví dụ về xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 theo phương án thứ hai sẽ được mô tả.

Thiết bị xử lý thông tin 100 tạo ra khóa xác thực cần được sử dụng trong xử

lý xác thực.

Cụ thể hơn, thiết bị xử lý thông tin 100 tạo ra các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi. Khóa suy biến thứ nhất được tạo ra, ví dụ, bằng cách thực hiện tuần tự việc mã hóa nhờ sử dụng mỗi khóa trên giá trị làm cơ sở như số ngẫu nhiên.

Ở đây, các phương pháp mã hóa được hỗ trợ bởi các khóa suy biến thứ nhất có thể giống nhau hoặc khác nhau. Nói cách khác, các phương pháp mã hóa có thể được chứa trong các phương pháp mã hóa được hỗ trợ bởi các khóa suy biến thứ nhất.

Sau đó, thiết bị xử lý thông tin 100 tạo ra khóa suy biến lại (khóa suy biến thứ hai) thu được bằng cách tổng hợp các suy biến thứ nhất được tạo ra như là khóa xác thực. Khóa suy biến lại được tạo ra, ví dụ, bằng cách thực hiện việc mã hóa nhờ sử dụng các khóa suy biến thứ nhất. Ngoài ra, các xử lý liên quan đến việc tạo ra của khóa suy biến lại không bị giới hạn ở ví dụ được mô tả ở trên, và xử lý tính toán nghịch đảo tùy ý mà có thể tổng hợp các khóa suy biến thứ nhất và thu nhận một khóa suy biến lại có thể được sử dụng.

Fig.11 là sơ đồ giải thích minh họa ví dụ tạo ra khóa xác thực theo phương pháp xử lý thông tin theo phương án thứ hai.

Thiết bị xử lý thông tin 100 tạo ra khóa suy biến 1 (ví dụ về khóa suy biến thứ nhất) bằng cách thực hiện tuần tự việc mã hóa sử dụng các khóa (khóa vùng 1, khóa dịch vụ 2, và khóa dịch vụ 3 được minh họa trên Fig.11) được gán cho vùng 1 của phương tiện ghi trên số ngẫu nhiên (ví dụ về giá trị mà đóng vai trò là cơ sở) (S400).

Thiết bị xử lý thông tin 100 tạo ra khóa suy biến 2 (ví dụ khác của khóa suy biến thứ nhất) bằng cách thực hiện tuần tự việc mã hóa sử dụng các khóa (khóa

vùng 4, khóa dịch vụ 4, và khóa dịch vụ 6 được minh họa trên Fig.11) được gán cho vùng 4 của phương tiện ghi trên số ngẫu nhiên (ví dụ về giá trị mà đóng vai trò là cơ sở) (S402).

Thiết bị xử lý thông tin 100 thực hiện việc tính toán sử dụng khóa suy biến 1 được tạo ra trong bước S400 và khóa suy biến 2 được tạo ra trong bước S402 và tạo ra khóa suy biến lại (khóa suy biến thứ hai) (S404). Trong ví dụ được minh họa trên Fig.11, khóa suy biến lại được tạo ra trong xử lý của bước S404 tương ứng với khóa xác thực.

Ví dụ, như được minh họa trên Fig.11, thiết bị xử lý thông tin 100 tạo ra các khóa suy biến thứ nhất và tạo ra khóa suy biến lại như là khóa xác thực bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra.

Ngoài ra, ví dụ tạo ra khóa xác thực theo phương án thứ hai không bị giới hạn ở ví dụ được minh họa trên Fig.11.

Chẳng hạn, ví dụ được minh họa trên Fig.11 minh họa ví dụ trong đó hai khóa suy biến thứ nhất được tạo ra, nhưng thiết bị xử lý thông tin 100 có thể tạo ra ba khóa suy biến thứ nhất hoặc nhiều hơn và tạo ra khóa suy biến lại.

Nếu khóa suy biến lại (khóa suy biến thứ hai) được tạo ra như là khóa xác thực, thiết bị xử lý thông tin 100 thực hiện xử lý xác thực nhờ sử dụng khóa suy biến lại.

Ngoài ra, sẽ được hiểu rằng thiết bị xử lý thông tin 100 có thể thực hiện xử lý xác thực nhờ sử dụng khóa riêng biệt như khóa vùng hoặc khóa dịch vụ làm khóa xác thực và thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thứ nhất làm khóa xác thực.

(2-3) Phương pháp xử lý thông tin theo phương án thứ ba

(2-3-1) Tổng quát của hệ thống xử lý thông tin 1000 mà phương pháp xử lý

thông tin theo phương án thứ ba được áp dụng cho

Như được mô tả trong phương pháp xử lý thông tin theo phương án thứ hai, trong trường hợp trong đó việc xác thực sử dụng khóa suy biến liên quan đến kỹ thuật được bộc lộ trong tài liệu sáng chế 1 được thực hiện nhiều lần, chỉ dịch vụ tương ứng với khóa suy biến được sử dụng trong việc xác thực cuối cùng có thể truy nhập được. Ngoài ra, như được mô tả trong phương pháp xử lý thông tin theo phương án thứ hai, trong trường hợp trong đó việc xác thực nhờ sử dụng các khóa suy biến được thực hiện nhiều lần trong kỹ thuật hiện tại, việc ghi mà có tính nguyên tố không thể được thực hiện.

Liên quan đến việc này, thiết bị xử lý thông tin 100 mà phương pháp xử lý thông tin theo phương án thứ ba được áp dụng cho điều khiển xử lý liên quan đến dịch vụ có thể được thực hiện trong trường hợp trong đó việc xử lý xác thực được thực hiện nhờ sử dụng khóa suy biến làm khóa xác thực.

Cụ thể hơn, ví dụ, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, thiết bị xử lý thông tin 100 làm cho xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể được thực hiện.

Do đó, trong trường hợp trong đó việc xác thực theo phương pháp xử lý thông tin theo phương án thứ ba được thực hiện, ngay cả khi việc xác thực sử dụng khóa suy biến được thực hiện nhiều lần, tất cả dịch vụ tương ứng với khóa suy biến được sử dụng trong các việc xác thực có thể truy nhập được.

Ngoài ra, do tất cả dịch vụ tương ứng với khóa suy biến được sử dụng trong các việc xác thực có thể truy nhập được, việc ghi mà có tính nguyên tố có thể được thực hiện.

Do đó, thiết bị xử lý thông tin 100 mà phương pháp xử lý thông tin theo

phương án thứ ba được áp dụng cho có thể cải thiện sự thuận tiện của việc xác thực nhờ sử dụng khóa xác thực.

(2-2-2) Xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 theo phương án thứ ba

Tiếp theo, ví dụ về xử lý theo phương pháp xử lý thông tin trong thiết bị xử lý thông tin 100 theo phương án thứ ba sẽ được mô tả. Thiết bị xử lý thông tin 100 thực hiện xử lý xác thực nhờ sử dụng khóa suy biến làm khóa xác thực. Ngoài ra, sẽ được hiểu rằng thiết bị xử lý thông tin 100 có thể thực hiện xử lý xác thực nhờ sử dụng khóa riêng biệt như khóa vùng hoặc khóa dịch vụ làm khóa xác thực.

Ngoài ra, thiết bị xử lý thông tin 100 điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực. Thiết bị xử lý thông tin 100 điều khiển việc thực hiện xử lý liên quan đến dịch vụ, ví dụ, bằng cách thay đổi dịch vụ có thể truy nhập được theo kết quả xác thực.

Ví dụ, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, thiết bị xử lý thông tin 100 làm cho xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể được thực hiện.

Ở đây, các phương pháp mã hóa được hỗ trợ bởi các khóa suy biến được sử dụng trong các xử lý xác thực mà được thực hiện nhiều lần có thể giống hoặc khác nhau. Nói cách khác, các phương pháp mã hóa có thể được chứa trong các phương pháp mã hóa được hỗ trợ bởi các khóa suy biến theo phương án thứ ba, tương tự các khóa suy biến thứ nhất theo phương án thứ hai.

Fig.12 là sơ đồ giải thích để mô tả xử lý theo phương pháp xử lý thông tin theo phương án thứ ba.

Thiết bị xử lý thông tin 100 tạo ra khóa suy biến 1 bằng cách thực hiện tuần

tự việc mã hóa nhờ sử dụng các khóa (khóa vùng 1, khóa dịch vụ 2, và khóa dịch vụ 3 được minh họa trên Fig.12) được gán cho vùng 1 của phương tiện ghi trên số ngẫu nhiên (ví dụ về giá trị mà đóng vai trò là cơ sở) (S500).

Sau đó, thiết bị xử lý thông tin 100 thực hiện việc xác thực nhờ sử dụng khóa suy biến 1 (S502). Do khóa suy biến 1 là khóa suy biến mà được dựa trên khóa dịch vụ 2 tương ứng với dịch vụ 2 và khóa dịch vụ 3 tương ứng với dịch vụ 3, dịch vụ 2 và dịch vụ 3 trở nên có thể truy nhập được bởi việc xác thực sử dụng khóa suy biến 1 trong bước S502.

Thiết bị xử lý thông tin 100 tạo ra khóa suy biến 2 bằng cách thực hiện tuần tự việc mã hóa nhờ sử dụng các khóa (khóa vùng 4, khóa dịch vụ 5, và khóa dịch vụ 6 được minh họa trên Fig.12) được gán cho vùng 4 của phương tiện ghi trên số ngẫu nhiên (ví dụ về giá trị mà đóng vai trò là cơ sở) (S504).

Sau đó, thiết bị xử lý thông tin 100 thực hiện việc xác thực nhờ sử dụng khóa suy biến 2 (S506).

Ở đây, do khóa suy biến 2 là khóa suy biến mà được dựa trên khóa dịch vụ 5 tương ứng với dịch vụ 5 và khóa dịch vụ 6 tương ứng với dịch vụ 6, dịch vụ 5 và dịch vụ 6 là các dịch vụ mà trở nên có thể truy nhập được bởi việc xác thực sử dụng khóa suy biến 2 trong bước S506. Ngoài ra, dịch vụ 2 và dịch vụ 3 trở nên có thể truy nhập được bằng việc xác thực sử dụng khóa suy biến 1 trong bước S502.

Do đó, trong ví dụ được minh họa trên Fig.12, trong trường hợp trong đó việc xác thực sử dụng khóa suy biến 2 được thực hiện trong bước S506, tất cả dịch vụ (dịch vụ 2, dịch vụ 3, dịch vụ 5, và dịch vụ 6) mà trở nên có thể truy nhập được bằng việc xác thực sử dụng khóa suy biến 1 và việc xác thực sử dụng khóa suy biến 2 trở thành các dịch vụ có thể truy nhập được trong thiết bị xử lý

thông tin 100.

Trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể được thực hiện trong thiết bị xử lý thông tin 100, ví dụ, như được minh họa trên Fig.12.

Ngoài ra, xử lý theo phương pháp xử lý thông tin theo phương án thứ ba không bị giới hạn ở ví dụ được mô tả ở trên.

Ví dụ, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, thiết bị xử lý thông tin 100 có thể thay đổi xử lý liên quan đến dịch vụ được làm cho có thể được thực hiện trên cơ sở của tham số của lệnh thu được từ thiết bị phía ngoài trước khi xử lý xác thực được thực hiện.

Cụ thể, thiết bị xử lý thông tin 100 thay đổi xử lý liên quan đến dịch vụ được làm cho có thể được thực hiện thành “xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực” như trong ví dụ được minh họa trên Fig.12 hoặc “xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực mà được thực hiện gần nhất” như trong trường hợp trong đó kỹ thuật hiện tại được sử dụng trên cơ sở của tham số của lệnh.

Nói cách khác, trong hệ thống xử lý thông tin 1000 mà phương pháp xử lý thông tin theo phương án thứ ba được áp dụng, có thể được chỉ định rằng dịch vụ có thể truy nhập được được tăng lên hay được thay thế thông qua tham số lệnh tại thời điểm xác thực.

(2-4) Phương pháp xử lý thông tin theo các phương án khác

Xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế không bị giới hạn ở các xử lý theo phương pháp xử lý thông tin theo các phương án thứ nhất đến thứ ba.

Ví dụ, xử lý theo phương pháp xử lý thông tin theo phương án của sáng chế có thể là xử lý thu được bằng cách kết hợp hai xử lý hoặc nhiều hơn theo phương pháp xử lý thông tin theo các phương án thứ nhất đến thứ ba.

(Chương trình theo phương án của sáng chế)

Đối với chương trình mà làm cho hệ thống máy tính thực hiện chức năng là thiết bị xử lý thông tin theo phương án của sáng chế (ví dụ, chương trình mà có thể thực hiện một vài hoặc tất cả chức năng của bộ xử lý 110 mà thực hiện xử lý theo phương pháp xử lý thông tin theo phương án thứ nhất, chức năng của bộ xử lý 110 mà thực hiện xử lý theo phương pháp xử lý thông tin theo phương án thứ hai, và chức năng của bộ xử lý 110 mà thực hiện xử lý theo phương pháp xử lý thông tin theo phương án thứ ba) được thực hiện bởi bộ xử lý hoặc loại tương tự trong hệ thống máy tính, sự tiện lợi của việc xác thực nhờ sử dụng khóa xác thực có thể được cải thiện. Ở đây, một máy tính hoặc nhiều máy tính có thể được sử dụng làm hệ thống máy tính theo phương án của sáng chế. Một loạt xử lý được thực hiện bởi hệ thống máy tính theo phương án của sáng chế.

Ngoài ra, đối với chương trình mà làm cho hệ thống máy tính thực hiện chức năng là thiết bị xử lý thông tin theo phương án của sáng chế được thực hiện bởi bộ xử lý hoặc loại tương tự trong hệ thống máy tính, các hiệu quả thu được bởi xử lý theo phương pháp xử lý thông tin theo của các phương án tương ứng được mô tả ở trên có thể thu được.

Người có hiểu biết trung bình trong lĩnh vực kỹ thuật sẽ hiểu rằng các cải biến, kết hợp, kết hợp phụ và thay đổi khác nhau có thể diễn ra phụ thuộc vào các yêu cầu thiết kế và các yếu tố khác miễn là chúng nằm trong phạm vi của yêu cầu bảo hộ đi kèm hoặc các phân tương đương của chúng.

Chẳng hạn, ví dụ (chương trình máy tính) trong đó chương trình này làm

cho hệ thống máy tính thực hiện chức năng là thiết bị xử lý thông tin theo phương án của sáng chế được đề xuất đã được mô tả ở trên, nhưng trong phương án này, phương tiện ghi mà có chương trình được lưu trữ trong đó có thể được đề xuất cùng nhau.

Cấu hình nêu trên chỉ báo ví dụ về phương án của sáng chế, và điều này rõ ràng thuộc về phạm vi kỹ thuật của sáng chế.

Ngoài ra, các hiệu quả được mô tả trong bản mô tả này chỉ nhằm mục đích minh họa hoặc các hiệu quả ví dụ, và không bị giới hạn. Tức là, ngoài các hiệu quả nêu trên, kỹ thuật theo sáng chế có thể đạt được các hiệu quả khác mà là rõ ràng với chuyên gia trong lĩnh vực kỹ thuật từ phân mô tả của bản mô tả này.

Ngoài ra, kỹ thuật của sáng chế cũng có thể được tạo cấu hình như dưới đây.

(1) Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực,

trong đó bộ xử lý tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử dụng trong việc tính toán.

(2) Thiết bị xử lý thông tin theo mục (1), trong đó bộ xử lý thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với khóa được sử dụng trong việc tính toán mỗi lần việc tính toán sử dụng khóa được thực hiện.

(3) Thiết bị xử lý thông tin theo mục (1), trong đó bộ xử lý thực hiện việc tính toán sử dụng các trị số chuyển đổi tương ứng với các khóa sau khi việc tính

toán sử dụng khóa được thực hiện.

(4) Thiết bị xử lý thông tin theo mục (1), trong đó bộ xử lý thực hiện việc tính toán nhờ sử dụng trị số tổng hợp thu được bằng cách tổng hợp các trị số chuyển đổi tương ứng với các khóa sau khi việc tính toán sử dụng khóa được thực hiện.

(5) Thiết bị xử lý thông tin theo mục bất kỳ trong số các mục từ (1) đến (4), trong đó bộ xử lý chỉ rõ phương pháp chuyển đổi được kết hợp với mỗi khóa trên cơ sở của thông tin thiết lập được kết hợp với vùng.

(6) Thiết bị xử lý thông tin theo mục bất kỳ trong số các mục (1) đến (5), trong đó phương pháp chuyển đổi bao gồm không chuyển đổi thông tin dành riêng cho thiết bị, và

trong trường hợp trong đó phương pháp chuyển đổi được kết hợp với một khóa chỉ báo rằng thông tin dành riêng cho thiết bị không được chuyển đổi, bộ xử lý không thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với một khóa.

(7) Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để tạo ra khóa xác thực được sử dụng trong xử lý xác thực và thực hiện xử lý xác thực nhờ sử dụng khóa xác thực đã được tạo ra,

trong đó bộ xử lý

tạo ra các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi,

tạo ra khóa suy biến thứ hai thu được bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra, và

thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thứ hai làm khóa xác thực.

(8) Thiết bị xử lý thông tin theo mục (7), trong đó, trong bộ xử lý, các phương pháp mã hóa được hỗ trợ bởi các khóa suy biến thứ nhất là đồng nhất với nhau.

(9) Thiết bị xử lý thông tin theo (7), trong đó, trong bộ xử lý, các phương pháp mã hóa được chứa trong các phương pháp mã hóa được hỗ trợ bởi các khóa suy biến thứ nhất.

(10) Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi làm khóa xác thực và điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực,

trong đó, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, bộ xử lý là cho xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể được thực hiện.

(11) Thiết bị xử lý thông tin theo mục (10), trong đó, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, bộ xử lý thay đổi xử lý liên quan đến dịch vụ để được làm cho có thể thực hiện được trên cơ sở của tham số của lệnh thu được từ thiết bị phía ngoài trước khi xử lý xác thực được thực hiện.

(12) Thiết bị xử lý thông tin theo mục (11), trong đó bộ xử lý thay đổi xử lý liên quan đến dịch vụ để được làm cho có thể thực hiện được thành xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực hoặc xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực mà đã được thực hiện gần nhất trên cơ sở của tham số của lệnh.

(13) Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước:

thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực,

trong đó, trong bước tạo ra khóa xác thực, khóa xác thực được tạo ra bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử dụng trong việc tính toán.

(14) Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước:

tạo ra khóa xác thực được sử dụng trong xử lý xác thực; và

thực hiện xử lý xác thực nhờ sử dụng khóa xác thực đã được tạo ra,

trong đó, trong bước tạo ra khóa xác thực,

các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi được tạo ra, và

khóa suy biến thứ hai thu được bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra, và

trong bước thực hiện xử lý xác thực, xử lý xác thực được thực hiện nhờ sử dụng khóa suy biến thứ hai làm khóa xác thực.

(15) Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước:

thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi làm khóa xác

thực; và

điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực,

trong đó, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, trong bước điều khiển việc thực hiện, xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực được làm cho có thể được thực hiện.

(16) Chương trình khiến máy tính thực hiện:

chức năng để thực hiện việc tính toán nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi và tạo ra khóa xác thực,

trong đó, chức năng để tạo khóa xác thực bao gồm tạo ra khóa xác thực bằng cách thực hiện việc tính toán nhờ sử dụng các trị số chuyển đổi tương ứng với các khóa, các trị số chuyển đổi thu được bằng cách chuyển đổi thông tin dành riêng cho thiết bị nhờ sử dụng các phương pháp chuyển đổi được kết hợp với các khóa được sử dụng trong việc tính toán.

(17) Chương trình khiến máy tính thực hiện:

chức năng để tạo ra khóa xác thực được sử dụng trong xử lý xác thực; và

chức năng để thực hiện xử lý xác thực nhờ sử dụng khóa xác thực đã được tạo ra,

trong đó chức năng tạo ra bao gồm các bước

tạo ra các khóa suy biến thứ nhất thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi, và

tạo ra khóa suy biến thứ hai thu được bằng cách tổng hợp nhiều khóa suy biến thứ nhất đã được tạo ra, và

chức năng để thực hiện xử lý xác thực bao gồm thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thứ hai làm khóa xác thực.

(18) Chương trình khiến máy tính thực hiện:

chức năng để thực hiện xử lý xác thực nhờ sử dụng khóa suy biến thu được bằng cách tổng hợp nhiều khóa được gán cho các vùng của phương tiện ghi làm khóa xác thực; và

chức năng để điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực,

trong đó, trong trường hợp trong đó việc xử lý xác thực được thực hiện nhiều lần, chức năng để điều khiển việc thực hiện bao gồm làm cho xử lý liên quan đến dịch vụ được xác thực trong xử lý bất kỳ trong số các xử lý xác thực có thể được thực hiện.

Danh mục các số chỉ dẫn

100	thiết bị xử lý thông tin
200	bộ đọc/bộ ghi
300	máy chủ
102	bộ truyền thông thứ nhất
104	bộ truyền thông thứ hai
106	bộ điều khiển
110	bộ xử lý
1000	hệ thống xử lý thông tin

YÊU CẦU BẢO HỘ

1. Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để:

thực hiện việc tính toán thứ nhất nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi;

tạo ra trị số tổng hợp dựa trên sự tổng hợp của các trị số chuyển đổi tương ứng với các khóa, trong đó các trị số chuyển đổi thu được dựa trên sự chuyển đổi của thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với mỗi trong số các khóa;

thực hiện việc tính toán thứ hai dựa trên đầu ra của việc tính toán thứ nhất và trị số tổng hợp; và

tạo ra khóa xác thực dựa trên đầu ra của việc tính toán thứ hai.

2. Thiết bị xử lý thông tin theo điểm 1, trong đó bộ xử lý còn được tạo cấu hình để chỉ rõ phương pháp chuyển đổi được kết hợp với mỗi khóa dựa trên thông tin thiết lập được kết hợp với nhiều vùng.

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

phương pháp chuyển đổi còn bao gồm phương pháp dựa trên sự không chuyển đổi của thông tin dành riêng cho thiết bị, và

bộ xử lý còn được tạo cấu hình để không thực hiện việc tính toán nhờ sử dụng trị số chuyển đổi tương ứng với khóa cụ thể khi phương pháp chuyển đổi được kết hợp với khóa cụ thể chỉ báo rằng thông tin dành riêng cho thiết bị không được chuyển đổi.

4. Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để:

tổng hợp nhiều khóa được gán cho nhiều vùng của phương tiện ghi;

tạo ra nhiều khóa suy biến dựa trên sự tổng hợp của nhiều khóa;
tổng hợp nhiều khóa suy biến đã được tạo ra;
tạo ra khóa suy biến lại dựa trên sự tổng hợp của nhiều khóa suy biến đã
được tạo ra; và

thực hiện xử lý xác thực dựa trên khóa suy biến lại đã được tạo ra, trong đó
khóa suy biến lại được sử dụng làm khóa xác thực trong việc xử lý xác thực.

5. Thiết bị xử lý thông tin theo điểm 4, trong đó, trong bộ xử lý, các phương
pháp mã hóa được hỗ trợ bởi nhiều khóa suy biến thứ nhất giống hệt nhau.

6. Thiết bị xử lý thông tin theo điểm 4, trong đó, trong bộ xử lý, nhiều phương
pháp mã hóa được chứa trong các phương pháp mã hóa được hỗ trợ bởi nhiều
khóa suy biến.

7. Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để:

tổng hợp nhiều khóa thứ nhất được gán cho các vùng của phương tiện ghi;
tạo ra, như là khóa xác thực, khóa suy biến thứ nhất dựa trên sự tổng hợp
của nhiều khóa thứ nhất;

tổng hợp nhiều khóa thứ hai được gán cho các vùng của phương tiện ghi;
tạo ra, như là khóa xác thực, khóa suy biến thứ hai dựa trên sự tổng hợp
của nhiều khóa thứ hai, trong đó khóa suy biến thứ hai được tạo ra sau khóa suy
biến thứ nhất;

điều khiển việc thực hiện xử lý xác thực thứ nhất dựa trên khóa suy biến
thứ nhất;

điều khiển việc thực hiện xử lý xác thực thứ hai dựa trên khóa suy biến thứ
hai; và

điều khiển việc thực hiện xử lý thứ nhất liên quan đến dịch vụ thứ nhất được xác thực trong xử lý xác thực thứ nhất, trong đó

xử lý thứ nhất liên quan đến dịch vụ thứ nhất còn được xác thực trong xử lý bất kỳ của xử lý xác thực thứ hai, dựa trên việc thực hiện xử lý xác thực thứ nhất.

8. Thiết bị xử lý thông tin theo điểm 7, trong đó bộ xử lý còn được tạo cấu hình để điều khiển việc thực hiện xử lý thứ nhất liên quan đến dịch vụ thứ nhất dựa trên tham số của lệnh thu được từ thiết bị phía ngoài trước khi thực hiện mỗi trong số xử lý xác thực thứ nhất và xử lý xác thực thứ hai.

9. Thiết bị xử lý thông tin theo điểm 8, trong đó bộ xử lý còn được tạo cấu hình để thay đổi xử lý thứ nhất liên quan đến dịch vụ thứ nhất thành xử lý thứ hai liên quan đến dịch vụ thứ hai được xác thực trong xử lý xác thực thứ hai, trong đó xử lý xác thực thứ hai được thực hiện sau xử lý xác thực thứ nhất, và xử lý xác thực thứ hai được thực hiện dựa trên tham số của lệnh.

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

thực hiện việc tính toán thứ nhất nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi;

tạo ra trị số tổng hợp dựa trên sự tổng hợp của các trị số chuyển đổi tương ứng với các khóa, trong đó các trị số chuyển đổi thu được dựa trên sự chuyển đổi của thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với mỗi trong số các khóa;

thực hiện việc tính toán thứ hai dựa trên đầu ra của việc tính toán thứ nhất và trị số tổng hợp; và

tạo ra khóa xác thực dựa trên đầu ra của việc tính toán thứ hai.

11. Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước:

tổng hợp nhiều khóa được gán cho nhiều vùng của phương tiện ghi;

tạo ra nhiều khóa suy biến dựa trên sự tổng hợp của nhiều khóa;

tổng hợp nhiều khóa suy biến đã được tạo ra;

tạo ra khóa suy biến lại dựa trên sự tổng hợp của nhiều khóa suy biến đã được tạo ra; và

thực hiện xử lý xác thực dựa trên khóa suy biến lại đã được tạo ra, trong đó khóa suy biến lại được sử dụng làm khóa xác thực trong việc xử lý xác thực.

12. Phương pháp xử lý thông tin được thực hiện bởi thiết bị xử lý thông tin, phương pháp này bao gồm các bước:

tổng hợp nhiều khóa thứ nhất được gán cho các vùng của phương tiện ghi;

tạo ra, như là khóa xác thực, khóa suy biến thứ nhất dựa trên sự tổng hợp của nhiều khóa thứ nhất;

tổng hợp nhiều khóa thứ hai được gán cho các vùng của phương tiện ghi;

tạo ra, như là khóa xác thực, khóa suy biến thứ hai dựa trên sự tổng hợp của nhiều khóa thứ hai, trong đó khóa suy biến thứ hai được tạo ra sau khóa suy biến thứ nhất;

điều khiển việc thực hiện xử lý xác thực thứ nhất dựa trên khóa suy biến thứ nhất;

điều khiển việc thực hiện xử lý xác thực thứ hai dựa trên khóa suy biến thứ hai; và

điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực thứ nhất, trong đó

xử lý liên quan đến dịch vụ còn được xác thực trong xử lý xác thực thứ hai, dựa trên việc thực hiện xử lý xác thực thứ nhất.

13. Phương tiện đọc được bởi máy tính không tạm thời có lưu trữ trên đó, các lệnh thực hiện được bởi máy tính mà, khi được thực hiện bởi bộ xử lý, khiến bộ xử lý thực hiện các thao tác, các thao tác bao gồm:

thực hiện việc tính toán thứ nhất nhờ sử dụng các khóa được gán cho nhiều vùng của phương tiện ghi;

tạo ra trị số tổng hợp dựa trên sự tổng hợp của các trị số chuyển đổi tương ứng với các khóa, trong đó các trị số chuyển đổi thu được dựa trên sự chuyển đổi của thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với mỗi trong số các khóa;

thực hiện việc tính toán thứ hai dựa trên đầu ra của việc tính toán thứ nhất và trị số tổng hợp; và

tạo ra khóa xác thực dựa trên đầu ra của việc tính toán thứ hai.

14. Phương tiện đọc được bởi máy tính không tạm thời có lưu trữ trên đó, các lệnh thực hiện được bởi máy tính mà, khi được thực hiện bởi bộ xử lý, khiến bộ xử lý thực hiện các thao tác, các thao tác bao gồm:

tổng hợp nhiều khóa được gán cho nhiều vùng của phương tiện ghi;

tạo ra nhiều khóa suy biến dựa trên sự tổng hợp của nhiều khóa;

tổng hợp nhiều khóa suy biến đã được tạo ra;

tạo ra khóa suy biến lại dựa trên sự tổng hợp của nhiều khóa suy biến đã được tạo ra; và

thực hiện xử lý xác thực dựa trên khóa suy biến lại đã được tạo ra, trong đó khóa suy biến lại được sử dụng làm khóa xác thực trong việc xử lý xác thực.

15. Phương tiện đọc được bởi máy tính không tạm thời có lưu trữ trên đó, các

lệnh thực hiện được bởi máy tính mà, khi được thực hiện bởi bộ xử lý, khiến bộ xử lý thực hiện các thao tác, các thao tác bao gồm:

tổng hợp nhiều khóa thứ nhất được gán cho các vùng của phương tiện ghi;
tạo ra, như là khóa xác thực, khóa suy biến thứ nhất dựa trên sự tổng hợp của nhiều khóa thứ nhất;

tổng hợp nhiều khóa thứ hai được gán cho các vùng của phương tiện ghi;
tạo ra, như là khóa xác thực, khóa suy biến thứ hai dựa trên sự tổng hợp của nhiều khóa thứ hai, trong đó khóa suy biến thứ hai được tạo ra sau khóa suy biến thứ nhất;

điều khiển việc thực hiện xử lý xác thực thứ nhất dựa trên khóa suy biến thứ nhất;

điều khiển việc thực hiện xử lý xác thực thứ hai dựa trên khóa suy biến thứ hai; và

điều khiển việc thực hiện xử lý liên quan đến dịch vụ được xác thực trong xử lý xác thực thứ nhất, trong đó

xử lý liên quan đến dịch vụ còn được xác thực trong xử lý xác thực thứ hai, dựa trên việc thực hiện xử lý xác thực thứ nhất.

16. Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để:

thực hiện việc tính toán thứ nhất dựa trên khóa thứ nhất, của nhiều khóa, được gán cho vùng thứ nhất của nhiều vùng của phương tiện ghi;

thực hiện việc tính toán thứ hai dựa trên sự tổng hợp của việc tính toán thứ nhất và trị số chuyển đổi thứ nhất tương ứng với khóa thứ nhất, trong đó trị số chuyển đổi thứ nhất thu được dựa trên sự chuyển đổi của thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với khóa thứ

nhất;

thực hiện việc tính toán thứ ba dựa trên sự tổng hợp của việc tính toán thứ hai và khóa thứ hai của nhiều khóa;

thực hiện việc tính toán thứ tư dựa trên sự tổng hợp của việc tính toán thứ ba và trị số chuyển đổi thứ hai tương ứng với khóa thứ hai, trong đó trị số chuyển đổi thứ hai thu được dựa trên sự chuyển đổi của thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với khóa thứ hai; và

tạo ra khóa xác thực dựa trên đầu ra của việc tính toán thứ tư.

17. Thiết bị xử lý thông tin bao gồm:

bộ xử lý được tạo cấu hình để:

thực hiện việc tính toán thứ nhất nhờ sử dụng nhiều khóa được gán cho nhiều vùng của phương tiện ghi; và

thực hiện việc tính toán thứ hai dựa trên nhiều trị số chuyển đổi tương ứng với nhiều khóa, trong đó

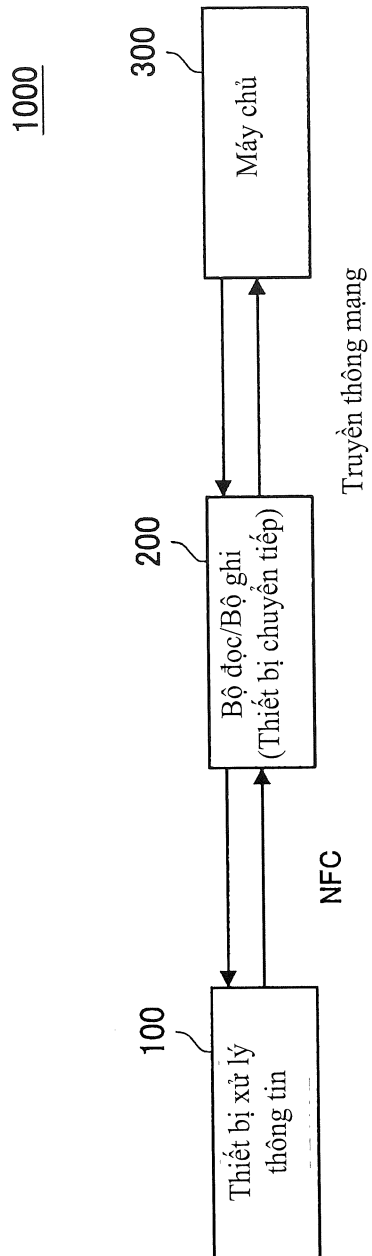
việc tính toán thứ hai được thực hiện sau việc tính toán thứ nhất nhờ sử dụng mỗi khóa trong số nhiều khóa, và

nhiều trị số chuyển đổi thu được dựa trên sự chuyển đổi của thông tin dành riêng cho thiết bị nhờ sử dụng phương pháp chuyển đổi được kết hợp với khóa; và

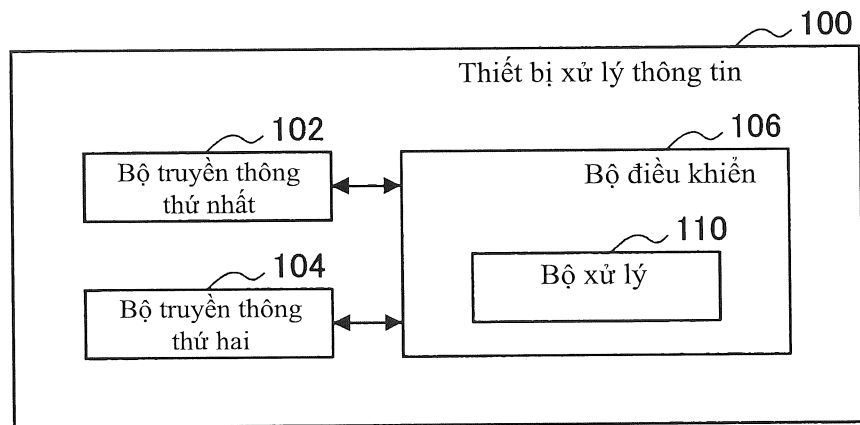
tạo ra khóa xác thực dựa trên đầu ra của việc tính toán thứ hai.

1/12

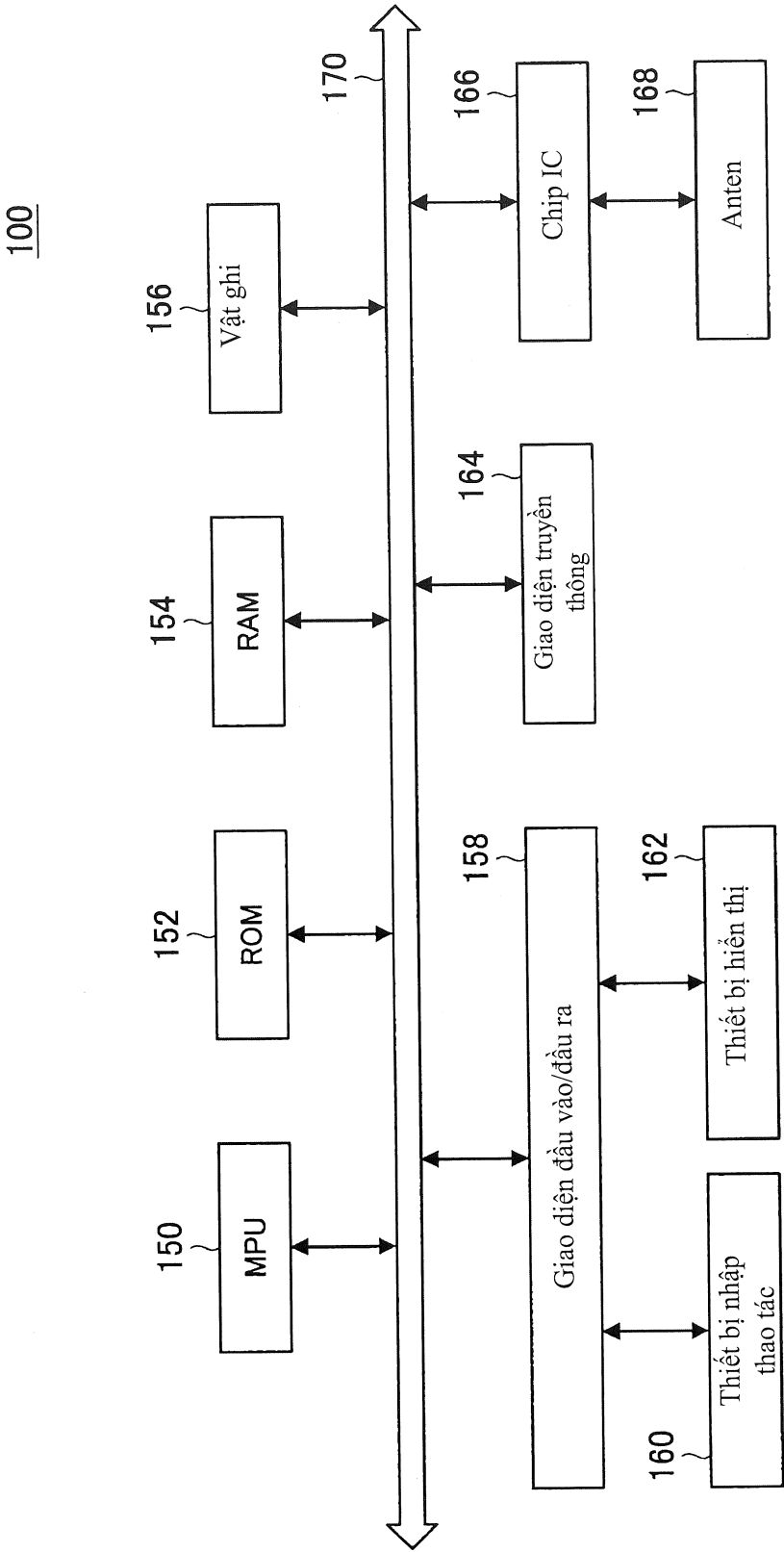
[Fig. 1]



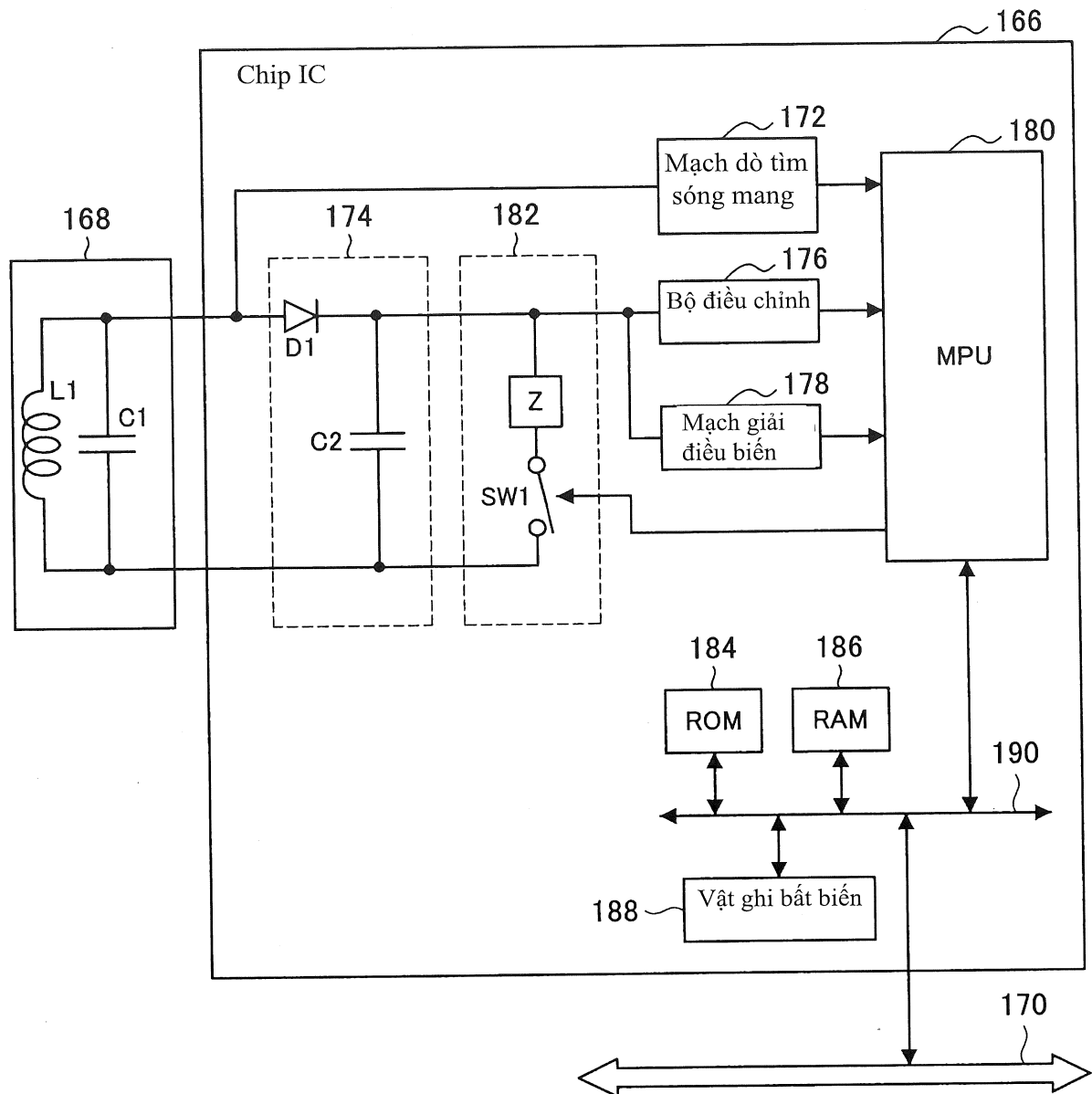
[Fig. 2]



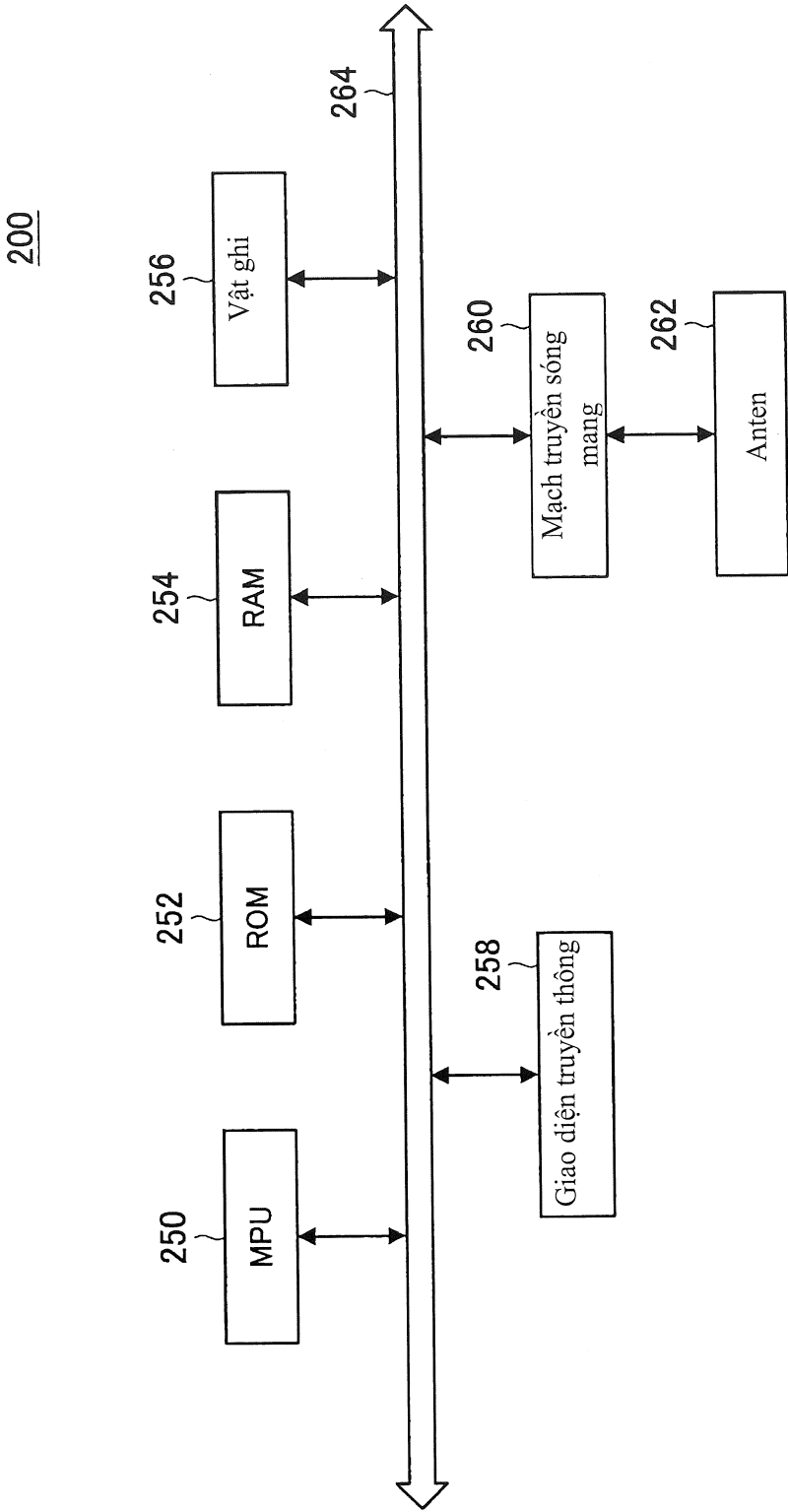
[Fig. 3]



[Fig. 4]

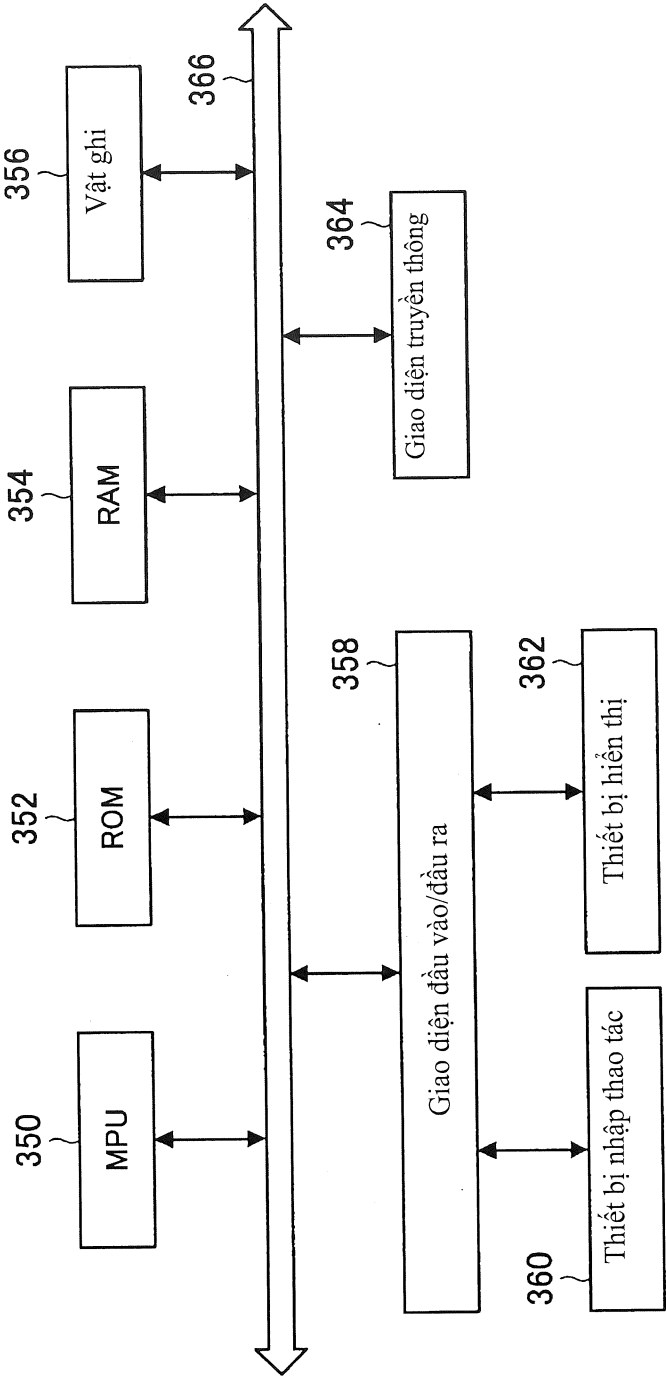


[Fig. 5]



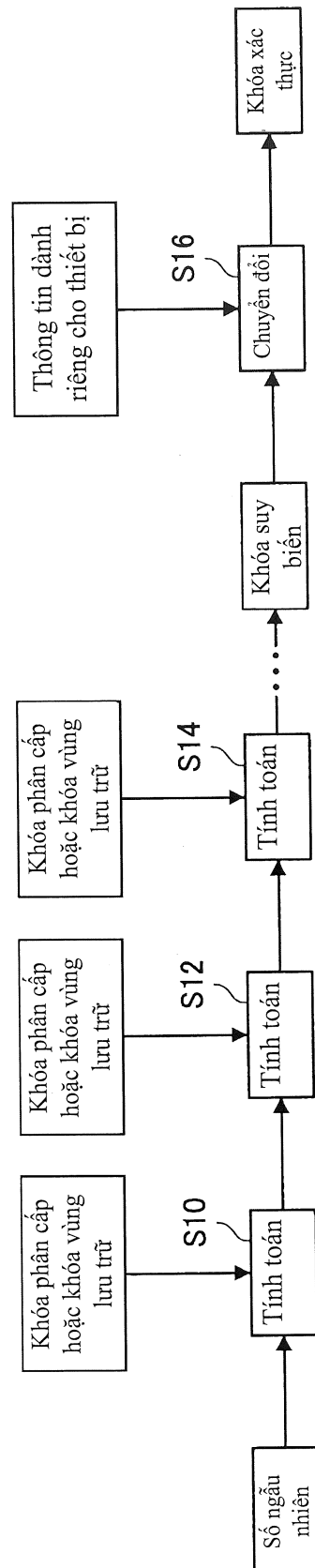
[Fig. 6]

300



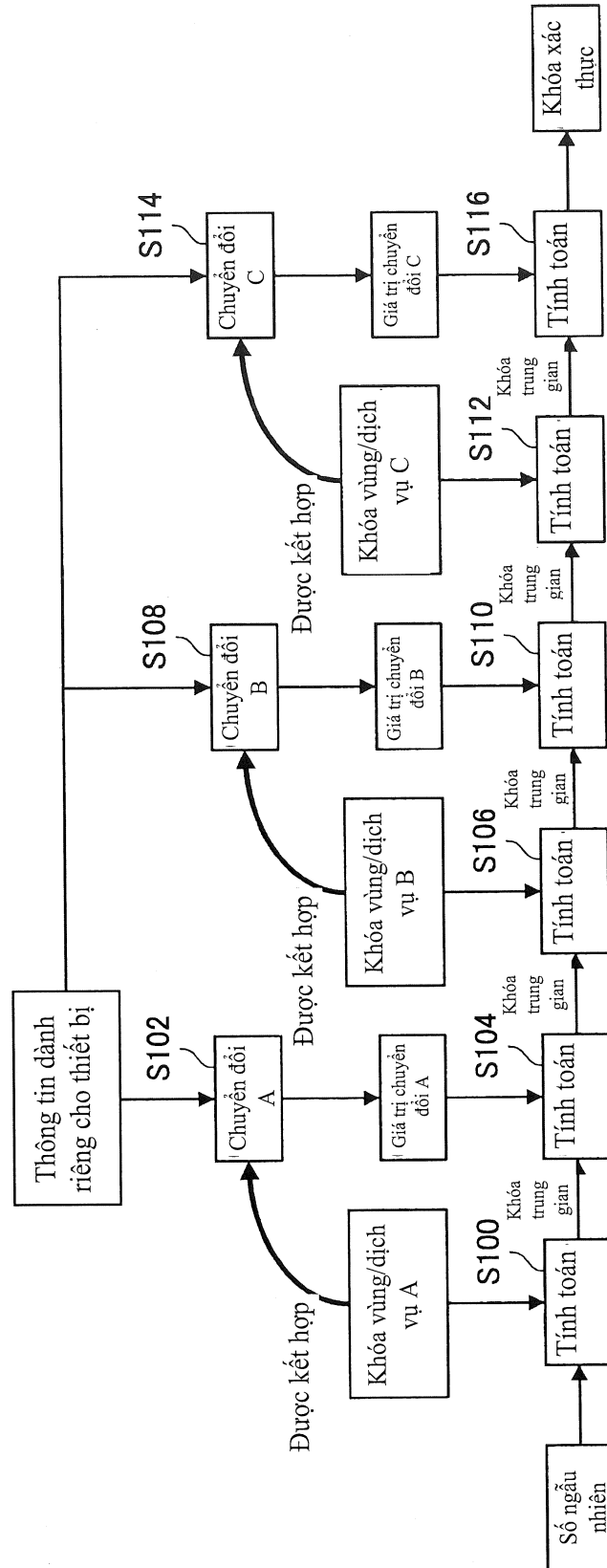
7/12

[Fig. 7]



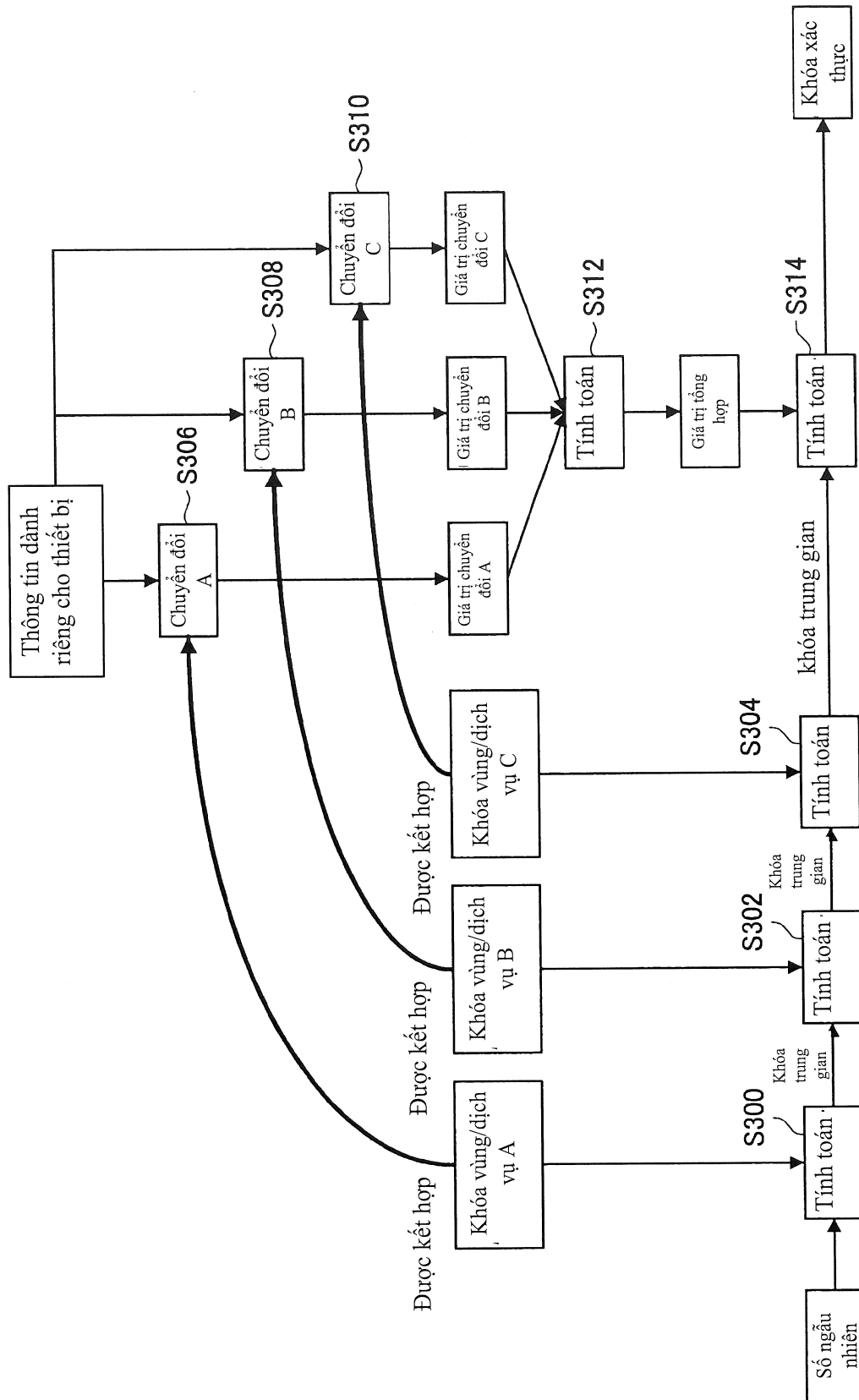
8/12

[Fig. 8]



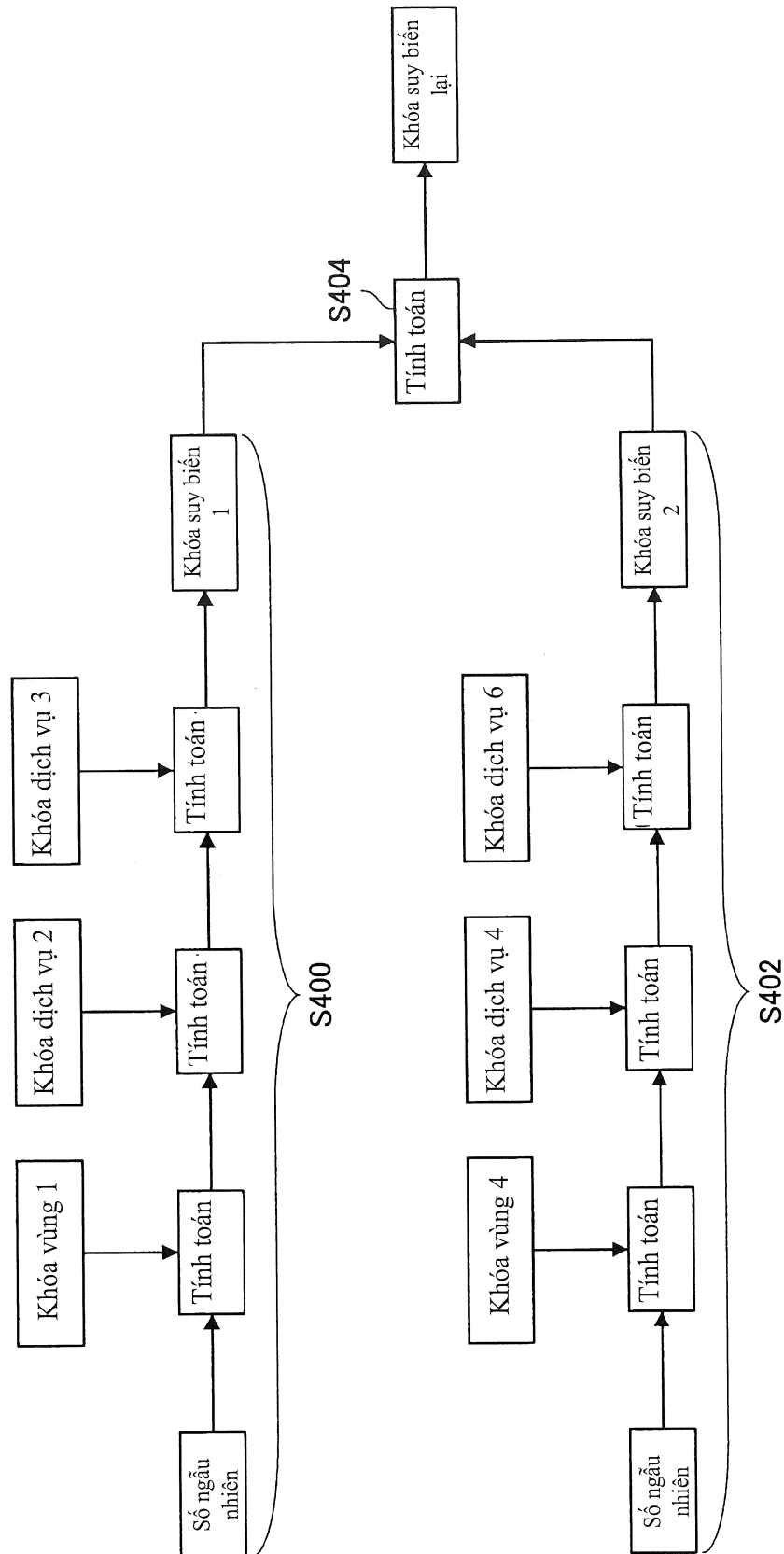
10/12

[Fig. 10]



11/12

[Fig. 11]



12/12

[Fig. 12]

