



(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ  
(19) Cộng hòa xã hội chủ nghĩa Việt Nam (VN) (11)   
CỤC SỞ HỮU TRÍ TUỆ  
1-0047271  
(51)<sup>19</sup> G06F 13/00; G06K 7/10; H04B 1/59; (13) B  
G06K 19/07

---

(21) 1-2019-05499 (22) 30/03/2018  
(86) PCT/JP2018/013633 30/03/2018 (87) WO 2018/190154 18/10/2018  
(30) 2017-080289 14/04/2017 JP  
(45) 25/06/2025 447 (43) 30/01/2020 382A  
(73) SONY CORPORATION (JP)  
1-7-1, Konan, Minato-ku, Tokyo 1080075, Japan  
(72) NAKATSURU Tsutomu (JP); KAMINO Itsuki (JP); SUZUKI Yuki (JP); SAKABA  
Koji (JP).  
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

---

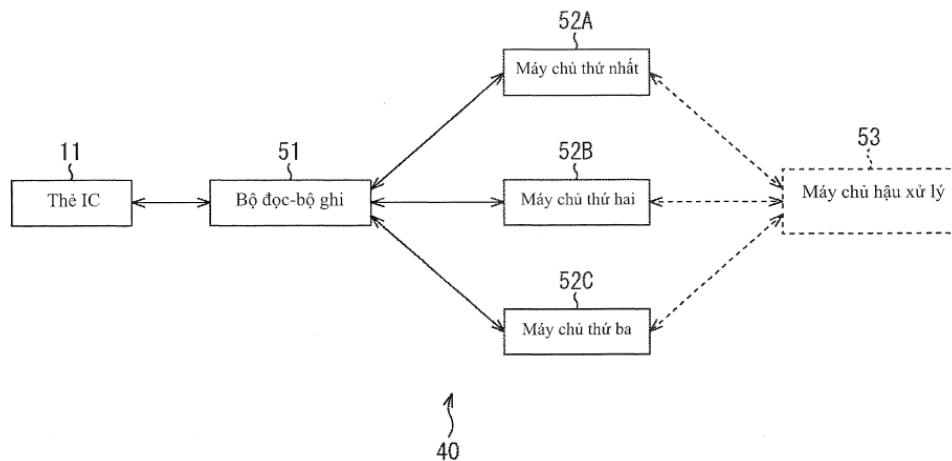
(54) THIẾT BỊ TRUYỀN THÔNG VÀ HỆ THỐNG XỬ LÝ DỮ LIỆU

(21) 1-2019-05499

(57) Sáng chế đề cập đến thiết bị truyền thông, thiết bị xử lý thông tin, và hệ thống xử lý dữ liệu mà có thể làm giảm trị số lớn nhất thời gian xử lý của toàn bộ hệ thống.

Bộ phận truyền thông của bộ đọc-bộ ghi truyền yêu cầu định trước đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thẻ mạch tích hợp (IC), và thu phản hồi tới yêu cầu từ các máy chủ. Bộ phận điều khiển của bộ đọc-bộ ghi thực hiện việc xử lý tiếp theo dựa vào phản hồi của một trong số các máy chủ, phản hồi đã thu được sớm nhất trong số các máy chủ. Sáng chế có thể được áp dụng tới hệ thống xử lý dữ liệu hoặc tương tự, chẳng hạn.

FIG. 3



**Lĩnh vực kỹ thuật được đề cập**

[0001]

Sáng chế đề cập đến thiết bị truyền thông, thiết bị xử lý thông tin, và hệ thống xử lý dữ liệu, và cụ thể là sáng chế đề cập đến thiết bị truyền thông, thiết bị xử lý thông tin, và hệ thống xử lý dữ liệu mà có thể làm giảm trị số lớn nhất thời gian xử lý của toàn bộ hệ thống.

**Tình trạng kỹ thuật của sáng chế**

[0002]

Trong hệ thống tiền điện tử, hệ thống an ninh, và tương tự, có sự xuất hiện rộng rãi thẻ mạch tích hợp (IC) được trang bị thiết bị ngoại vi mà có thể truyền thông với bộ đọc-bộ ghi. Hơn nữa, trong những năm gần đây, thiết bị đầu cuối di động mà được trang bị thiết bị ngoại vi không tiếp xúc, và có thể thực hiện sự truyền thông không tiếp xúc với bộ đọc-bộ ghi cũng đã trở nên phổ biến.

[0003]

Trong hệ thống sử dụng thẻ IC hoặc thiết bị đầu cuối di động như vậy, thông tin được trao đổi qua truyền thông được truyền đến máy chủ từ bộ đọc-bộ ghi, và được trải qua việc xử lý dữ liệu (ví dụ, tham khảo tài liệu sáng chế 1).

Tài liệu trích dẫn

Tài liệu sáng chế

[0004]

Tài liệu sáng chế 1: Công bố đơn xin cấp bằng sáng chế Nhật Bản số 2006-99509

Vấn đề cần được giải quyết bởi sáng chế

[0005]

Trong thời gian xử lý của toàn bộ hệ thống bao gồm thẻ IC, bộ đọc-bộ ghi, và máy chủ, có các độ biến thiên lớn về thời gian được cần đến cho việc truyền thông được thực hiện giữa bộ đọc-bộ ghi và máy chủ, và thời gian xử lý trong máy chủ do sự tắc nghẽn hoặc tương tự của đường truyền thông và yêu cầu xử lý. Kết quả là, thời gian xử lý của toàn bộ hệ thống đôi khi trở nên lớn.

#### **Bản chất kỹ thuật của sáng chế**

[0006]

Mục đích của sáng chế là được tạo ra dựa vào vấn đề nêu trên, và có thể làm giảm trị số lớn nhất thời gian xử lý của toàn bộ hệ thống.

Cách thức giải quyết vấn đề

[0007]

Thiết bị truyền thông theo khía cạnh thứ nhất của sáng chế bao gồm bộ phận truyền thông được tạo cấu hình để truyền yêu cầu định trước đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thiết bị ngoại vi, và thu phản hồi tới yêu cầu từ các máy chủ, và bộ phận điều khiển được tạo cấu hình để thực hiện việc xử lý tiếp theo dựa vào phản hồi của một trong số các

máy chủ, phản hồi đã thu được sớm nhất.

[0008]

Theo khía cạnh thứ nhất của sáng chế, yêu cầu định trước được truyền đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thiết bị ngoại vi, và phản hồi tới yêu cầu được thu từ các máy chủ, và việc xử lý tiếp theo được thực hiện dựa vào phản hồi của một trong số các máy chủ, phản hồi đã thu được sớm nhất.

[0009]

Thiết bị xử lý thông tin theo khía cạnh thứ hai của sáng chế bao gồm bộ phận truyền thông được tạo cấu hình để thu yêu cầu định trước từ thiết bị truyền thông được tạo cấu hình để truyền lệnh đến thiết bị ngoại vi, và truyền phản hồi bao gồm kết quả xử lý của việc xử lý được thực hiện đáp lại yêu cầu, đến thiết bị truyền thông, và bộ phận điều khiển được tạo cấu hình để thực hiện việc xử lý, mà trong đó kết quả xử lý được bao gồm trong phản hồi được mã hóa nhờ sử dụng khóa không thể giải mã được bởi thiết bị truyền thông.

[0010]

Theo khía cạnh thứ hai của sáng chế, yêu cầu định trước được thu từ thiết bị truyền thông được tạo cấu hình để truyền lệnh đến thiết bị ngoại vi, và việc xử lý được thực hiện đáp lại yêu cầu, và phản hồi bao gồm kết quả xử lý của việc xử lý được thực hiện được truyền đến thiết bị truyền thông. Kết quả xử lý được bao gồm trong phản hồi được mã hóa nhờ sử dụng khóa không thể giải mã được bởi thiết bị truyền thông.

[0011]

Hệ thống xử lý dữ liệu theo khía cạnh thứ ba của sáng chế bao gồm thiết bị truyền thông và các máy chủ, trong đó thiết bị truyền thông bao gồm bộ phận truyền thông thứ nhất được tạo cấu hình để truyền yêu cầu định trước đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thiết bị ngoại vi, và thu phản hồi tới yêu cầu từ các máy chủ, và bộ phận điều khiển thứ nhất được tạo cấu hình để thực hiện việc xử lý tiếp theo dựa vào phản hồi của một trong số các máy chủ, phản hồi đã thu được sớm nhất, mỗi trong số các máy chủ bao gồm bộ phận truyền thông thứ hai được tạo cấu hình để thu yêu cầu từ thiết bị truyền thông và truyền phản hồi bao gồm kết quả xử lý của việc xử lý được thực hiện đáp lại yêu cầu, đến thiết bị truyền thông, và bộ phận điều khiển thứ hai được tạo cấu hình để thực hiện việc xử lý, và kết quả xử lý được bao gồm trong phản hồi được mã hóa nhờ sử dụng khóa không thể giải mã được bởi thiết bị truyền thông.

[0012]

Theo khía cạnh thứ ba của sáng chế, thiết bị truyền thông và các máy chủ được bao gồm, trong thiết bị truyền thông, yêu cầu định trước được truyền đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thiết bị ngoại vi, và phản hồi tới yêu cầu được thu từ các máy chủ, và việc xử lý tiếp theo được thực hiện dựa vào phản hồi của một trong số các máy chủ, phản hồi đã thu được sớm nhất. Trong mỗi trong số các máy chủ, yêu cầu được thu từ thiết bị truyền thông và việc xử lý được thực hiện đáp lại yêu cầu, và phản hồi bao gồm

kết quả xử lý của việc xử lý được thực hiện được truyền đến thiết bị truyền thông. Kết quả xử lý được bao gồm trong phản hồi được mã hóa nhờ sử dụng khóa không thể giải mã được bởi thiết bị truyền thông.

[0013]

Thiết bị xử lý thông tin theo khía cạnh thứ tư của sáng chế bao gồm bộ phận truyền thông được tạo cấu hình để thu kết quả xử lý của việc xử lý xác thực được thực hiện trên thiết bị ngoại vi, và thông tin nhận dạng việc xử lý để nhận dạng việc xử lý, từ các thiết bị xử lý thông tin khác, và bộ phận điều khiển được tạo cấu hình để thực hiện việc xử lý liên quan đến các kết quả xử lý có cùng thông tin nhận dạng việc xử lý đã được thu từ các thiết bị xử lý thông tin khác, như là cùng kết quả xử lý xác thực.

[0014]

Theo khía cạnh thứ tư của sáng chế, kết quả xử lý của việc xử lý xác thực được thực hiện trên thiết bị ngoại vi, và thông tin nhận dạng việc xử lý để nhận dạng việc xử lý được thu từ các thiết bị xử lý thông tin khác, và việc xử lý liên quan đến các kết quả xử lý có cùng thông tin nhận dạng việc xử lý đã được thu từ các thiết bị xử lý thông tin khác, như cùng kết quả xử lý xác thực được thực hiện.

[0015]

Lưu ý rằng thiết bị truyền thông theo khía cạnh thứ nhất của sáng chế, thiết bị xử lý thông tin theo khía cạnh thứ hai của sáng chế, và thiết bị xử lý thông tin theo khía cạnh thứ tư của sáng chế có thể được thực hiện bằng cách

khuyến máy tính thực hiện các chương trình. Hơn nữa, các chương trình cần được thực hiện bởi máy tính có thể được cung cấp nhờ được truyền qua phương tiện truyền, hoặc nhờ được ghi tới phương tiện ghi.

[0016]

Thiết bị truyền thông theo khía cạnh thứ nhất, thiết bị xử lý thông tin theo khía cạnh thứ hai, và thiết bị xử lý thông tin theo khía cạnh thứ tư có thể là các thiết bị độc lập, hoặc có thể là các khối bên trong cấu thành một thiết bị.

Hiệu quả của sáng chế

[0017]

Theo khía cạnh thứ nhất đến khía cạnh thứ ba của sáng chế, trị số lớn nhất thời gian xử lý của toàn bộ hệ thống có thể được làm giảm.

[0018]

Hơn nữa, theo khía cạnh thứ tư của sáng chế, sự trùng lặp của cùng xử lý được thực hiện bởi các máy chủ có thể được loại trừ.

[0019]

Lưu ý rằng hiệu quả được nêu ở đây không nhất thiết được giới hạn, và có thể là hiệu quả bất kỳ được nêu theo sáng chế.

**Mô tả vắn tắt các hình vẽ**

[0020]

Fig.1 là sơ đồ khối minh họa ví dụ cấu hình chung của hệ thống xử lý dữ

liệu máy khách mỏng.

Fig.2 là lưu đồ minh họa ví dụ quy trình truyền thông trong hệ thống xử lý dữ liệu trên Fig.1.

Fig.3 là sơ đồ khối minh họa ví dụ cấu hình của hệ thống xử lý dữ liệu mà sáng chế được áp dụng.

Fig.4 là lưu đồ minh họa trường hợp mà ở đó cùng các quy trình truyền thông như các quy trình truyền thông trên Fig.2 được thực hiện bởi hệ thống xử lý dữ liệu trên Fig.3.

Fig.5 minh họa ví dụ trình tự của giao tác.

Fig.6 là hình vẽ minh họa ví dụ quy trình truyền thông mô tả vấn đề thứ nhất.

Fig.7 là hình vẽ minh họa ví dụ quy trình truyền thông mô tả vấn đề thứ nhất.

Fig.8 là lưu đồ minh họa các quy trình truyền thông được thực hiện bởi hệ thống xử lý dữ liệu trên Fig.3, mà trong đó vấn đề thứ nhất được giải quyết.

Fig.9 là lưu đồ minh họa các quy trình truyền thông được thực hiện bởi hệ thống xử lý dữ liệu trên Fig.3, mà trong đó vấn đề thứ nhất được giải quyết.

Fig.10 là lưu đồ minh họa các quy trình truyền thông được thực hiện trong trường hợp mà ở đó máy chủ hậu xử lý được bố trí.

Fig.11 là hình vẽ minh họa ví dụ quy trình truyền thông mô tả vấn đề thứ hai.

Fig.12 là lưu đồ minh họa các quy trình truyền thông được thực hiện bởi hệ thống xử lý dữ liệu trên Fig.3, mà trong đó vấn đề thứ hai được giải quyết.

Fig.13 là lưu đồ minh họa ví dụ sửa đổi về các quy trình truyền thông trên Fig.12.

Fig.14 là lưu đồ minh họa ví dụ về các quy trình truyền thông được thực hiện trong trường hợp mà ở đó máy chủ hậu xử lý không được sử dụng.

Fig.15 là sơ đồ khối minh họa các ví dụ cấu hình của thẻ IC và bộ đọc-bộ ghi.

Fig.16 là sơ đồ khối minh họa ví dụ cấu hình của thiết bị đầu cuối di động.

Fig.17 là sơ đồ khối minh họa ví dụ cấu hình của thiết bị máy chủ.

### **Mô tả chi tiết sáng chế**

[0021]

Dưới đây, cách thức để thực hiện sáng chế (dưới đây, được gọi là phương án) sẽ được mô tả. Lưu ý rằng phần mô tả sẽ được đưa ra theo thứ tự dưới đây.

1. Ví dụ cấu hình chung của hệ thống xử lý dữ liệu máy khách mỏng
2. Ví dụ cấu hình của hệ thống xử lý dữ liệu mà sáng chế được áp dụng
3. Vấn đề thứ nhất mà có thể được tạo ra trong cấu hình bao gồm các máy chủ, và biện pháp đối phó
4. Vấn đề thứ hai mà có thể được tạo ra trong cấu hình bao gồm các máy

chủ, và biện pháp đối phó

## 5. Ví dụ cấu hình phần cứng

[0022]

### <1. Ví dụ cấu hình chung của hệ thống xử lý dữ liệu máy khách mỏng>

Đối với hệ thống xử lý dữ liệu mà nó đọc dữ liệu định trước từ thẻ IC mà thực hiện sự truyền thông không tiếp xúc, thực hiện việc xử lý định trước, và sau đó, ghi dữ liệu được xử lý tới thẻ IC, có hệ thống máy khách mỏng mà nó tạo ra lệnh ở phía máy chủ.

[0023]

Fig.1 minh họa ví dụ cấu hình chung của hệ thống xử lý dữ liệu máy khách mỏng sử dụng thẻ IC mà thực hiện sự truyền thông không tiếp xúc.

[0024]

Hệ thống xử lý dữ liệu bao gồm thẻ IC 11, bộ đọc-bộ ghi 12, và máy chủ 13. Hơn nữa, một vài hệ thống xử lý dữ liệu còn bao gồm máy chủ hậu xử lý 14.

[0025]

Thẻ IC 11 là thẻ được trang bị chip IC, và là thiết bị ngoại vi mà có mặt ở phía bên ngoài khi được nhìn từ bộ đọc-bộ ghi 12. Bộ đọc-bộ ghi 12 đọc dữ liệu định trước được lưu trữ trong thẻ IC 11, từ thẻ IC 11, hoặc ghi dữ liệu định trước tới thẻ IC 11. Bằng cách đó người dùng sở hữu thẻ IC 11 được cung cấp dịch vụ định trước chẳng hạn như dịch vụ tiền điện tử, dịch vụ vé của giao thông vận tải chẳng hạn như đường sắt hoặc xe buýt, hoặc dịch vụ thẻ tín dụng. Các ví

dữ liệu bao gồm thông tin tiền điện tử liên quan đến hệ thống tiền điện tử, thông tin thẻ liên quan đến thẻ tín dụng, thông tin vé liên quan đến giao thông vận tải chẳng hạn như đường sắt hoặc xe buýt, thẻ ID duy nhất đối với thẻ IC 11, và tương tự.

[0026]

Thẻ IC 11 trao đổi dữ liệu định trước với bộ đọc-bộ ghi 12 nhờ truyền thông tầm gần (sự truyền thông không tiếp xúc) phù hợp với chuẩn ISO/IEC 14443 là chuẩn của hệ thống thẻ IC tầm gần, hoặc chuẩn ISO/IEC 18092 là chuẩn của giao diện và giao thức truyền thông trường gần (near field communication interface and protocol, viết tắt là NFCIP)-1. Sự truyền thông tầm gần hoặc sự truyền thông không tiếp xúc có nghĩa là sự truyền thông không tiếp xúc được cho phép khi khoảng cách giữa các thiết bị thực hiện việc truyền thông nằm trong khoảng vài chục centimét, và cũng bao gồm truyền thông được thực hiện ở trạng thái ở đó (vỏ của) các thiết bị thực hiện việc truyền thông tiếp xúc.

[0027]

Bộ đọc-bộ ghi 12 trao đổi dữ liệu định trước với máy chủ 13 nhờ truyền thông mạng được thực hiện qua mạng định trước. Các ví dụ về mạng định trước bao gồm Internet, mạng mạch điện thoại, mạng truyền thông vệ tinh, các mạng máy tính cục bộ (local area network, viết tắt là LAN) khác nhau bao gồm Ethernet (nhãn hiệu đã được đăng ký), mạng viễn thông diện rộng (wide area network, viết tắt là WAN), mạng mạch chuyên dụng chẳng hạn như mạng riêng

ảo-giao thức internet (internet protocol-virtual private network, viết tắt là IP-VPN), và tương tự.

[0028]

Phù hợp với yêu cầu từ bộ đọc-bộ ghi 12, máy chủ 13 thực hiện việc xử lý dữ liệu định trước liên quan đến dịch vụ được cung cấp bởi hệ thống xử lý dữ liệu đến người dùng. Ví dụ, máy chủ 13 thực hiện việc quản lý dữ liệu tiền điện tử, việc quản lý dữ liệu người dùng, và tương tự.

[0029]

Máy chủ hậu xử lý 14 thực hiện hậu xử lý tiếp theo việc xử lý dữ liệu được thực hiện bởi máy chủ 13.

[0030]

Fig.2 là lưu đồ minh họa ví dụ quy trình truyền thông trong hệ thống xử lý dữ liệu trên Fig.1.

[0031]

Ở bước S1, bộ đọc-bộ ghi 12 truyền lệnh 1, mà là một trong số các lệnh định trước, đến thẻ IC 11 được phát hiện với khoảng cách truyền thông của bộ đọc-bộ ghi 12.

[0032]

Ở bước S2, thẻ IC 11 truyền phản hồi 1 đến bộ đọc-bộ ghi 12 như trả lời đến lệnh 1 được thu từ bộ đọc-bộ ghi 12.

[0033]

Ở bước S3, bộ đọc-bộ ghi 12 thu phản hồi 1 từ thẻ IC 11, và truyền yêu cầu A để yêu cầu việc xử lý định trước, đến máy chủ 13 phù hợp với phản hồi 1 thu được.

[0034]

Ở bước S4, máy chủ 13 thu yêu cầu A từ bộ đọc-bộ ghi 12, và thực hiện việc xử lý định trước tương ứng với yêu cầu A thu được. Ở bước S5, dựa vào kết quả xử lý, máy chủ 13 truyền phản hồi A đang trả lời đến yêu cầu A, đến bộ đọc-bộ ghi 12. Như được minh họa trên Fig.2, theo quan điểm của bộ đọc-bộ ghi 12, thời gian xử lý của máy chủ 13 là thời gian từ khi yêu cầu A được truyền đến khi phản hồi A được thu, và bao gồm thời gian dành cho việc truyền thông được thực hiện giữa bộ đọc-bộ ghi 12 và máy chủ 13.

[0035]

Ở bước S6, bộ đọc-bộ ghi 12 thu phản hồi A từ máy chủ 13, và truyền lệnh 2 đến thẻ IC 11 như lệnh tiếp theo mà nó dựa vào phản hồi A.

[0036]

Ở bước S7, thẻ IC 11 truyền phản hồi 2 đến bộ đọc-bộ ghi 12 như trả lời đến lệnh 2 được thu từ bộ đọc-bộ ghi 12.

[0037]

Như được nêu trên, các lệnh và các phản hồi được trao đổi giữa thẻ IC 11 và bộ đọc-bộ ghi 12 nhờ truyền thông tầm gần. Các yêu cầu và các phản hồi được trao đổi giữa bộ đọc-bộ ghi 12 và máy chủ 13 nhờ truyền thông mạng.

[0038]

Trong hệ thống xử lý dữ liệu như vậy, thời gian xử lý được sử dụng trong thẻ IC 11, thời gian xử lý được sử dụng trong bộ đọc-bộ ghi 12, và thời gian dành cho việc truyền thông được thực hiện giữa thẻ IC 11 và bộ đọc-bộ ghi 12 là các thời gian ngắn, và các độ biến thiên (độ lệch chuẩn) về thời gian là nhỏ.

[0039]

Mặt khác, đối với thời gian xử lý được sử dụng trong máy chủ 13 và thời gian dành cho việc truyền thông được thực hiện giữa bộ đọc-bộ ghi 12 và máy chủ 13, các độ biến thiên (độ lệch chuẩn) về thời gian trở nên lớn trong một số trường hợp do lưu lượng của đường truyền thông, sự quá tải các yêu cầu xử lý từ số lượng bộ đọc-bộ ghi 12, hoặc tương tự.

[0040]

Do đó, để làm giảm trị số lớn nhất thời gian xử lý của toàn bộ hệ thống xử lý dữ liệu, cần phải rút ngắn thời gian trung bình dành cho việc xử lý được thực hiện giữa bộ đọc-bộ ghi 12 và máy chủ 13, và giảm bớt các biến.

[0041]

<2. Ví dụ cấu hình của hệ thống xử lý dữ liệu mà sáng chế được áp dụng>

Do đó, Fig.3 minh họa ví dụ cấu hình của hệ thống xử lý dữ liệu mà sáng chế được áp dụng tới, và nhằm để rút ngắn thời gian xử lý lớn nhất của toàn bộ hệ thống.

[0042]

Hệ thống xử lý dữ liệu 40 được minh họa trên Fig.3 bao gồm thẻ IC 11, bộ đọc-bộ ghi 51, và ba máy chủ 52 bao gồm máy chủ thứ nhất 52A, máy chủ thứ hai 52B, và máy chủ thứ ba 52C. Hơn nữa, tương tự như trường hợp trên Fig.1, một vài hệ thống xử lý dữ liệu 40 còn bao gồm máy chủ hậu xử lý 53.

[0043]

Như được thấy rõ từ Fig.3, hệ thống xử lý dữ liệu 40 khác nhiều với hệ thống xử lý dữ liệu trên Fig.1 ở chỗ các máy chủ 52 tương ứng với máy chủ 13 trên Fig.1 bao gồm các máy chủ. Thẻ IC 11 giống như thẻ IC trong hệ thống xử lý dữ liệu trên Fig.1.

[0044]

Cần lưu ý rằng, trong ví dụ trên Fig.3, cấu hình mà trong đó ba máy chủ 52 được bố trí được minh họa. Tuy nhiên, nó chỉ yêu cầu rằng các máy chủ 52 được bố trí. Do đó, số lượng các máy chủ 52 có thể là hai, hoặc bốn trở lên.

[0045]

Bộ đọc-bộ ghi 51 trao đổi dữ liệu định trước với thẻ IC 11 là thiết bị ngoại vi, nhờ truyền thông tầm gần (sự truyền thông không tiếp xúc) phù hợp với chuẩn ISO/IEC 14443 là chuẩn của hệ thống thẻ IC tầm gần, hoặc chuẩn ISO/IEC 18092 là chuẩn của NFCIP-1.

[0046]

Hơn nữa, bộ đọc-bộ ghi 51 trao đổi dữ liệu định trước với các máy chủ

52 nhờ truyền thông mạng được thực hiện qua mạng định trước. Các ví dụ về mạng định trước bao gồm Internet, mạng mạch điện thoại, mạng truyền thông vệ tinh, các mạng máy tính cục bộ khác nhau (local area network, viết tắt là LAN) bao gồm Ethernet (nhãn hiệu đã được đăng ký), mạng viễn thông diện rộng (wide area network, viết tắt là WAN), mạng mạch chuyên dụng chẳng hạn như mạng riêng ảo-giao thức internet (internet protocol-virtual private network, viết tắt là IP-VPN), và tương tự.

[0047]

Mỗi trong số các máy chủ 52 (từ máy chủ thứ nhất 52A đến máy chủ thứ ba 52C) thực hiện việc xử lý dữ liệu định trước liên quan đến dịch vụ được cung cấp bởi hệ thống xử lý dữ liệu 40 đến người dùng. Ví dụ, máy chủ 52 thực hiện việc quản lý dữ liệu tiền điện tử, việc quản lý dữ liệu người dùng, và tương tự.

[0048]

Máy chủ hậu xử lý 53 thực hiện hậu xử lý cho việc xử lý dữ liệu được thực hiện bởi các máy chủ 52 (từ máy chủ thứ nhất 52A đến máy chủ thứ ba 52C), chẳng hạn như, ví dụ, xử lý đối chiếu hoặc xử lý phát hiện bất thường đối với các kết quả xử lý nhận được bởi các máy chủ 52.

[0049]

Fig.4 là lưu đồ minh họa trường hợp mà ở đó các quy trình truyền thông giống như trình tự được minh họa trên Fig.2 được thực hiện bởi hệ thống xử lý dữ liệu 40 trên Fig.3.

[0050]

Ở bước S41, bộ đọc-bộ ghi 51 truyền lệnh 1, mà là một trong số các lệnh định trước, đến thẻ IC 11 được phát hiện trong khoảng cách truyền thông của bộ đọc-bộ ghi 51.

[0051]

Ở bước S42, thẻ IC 11 truyền phản hồi 1 đến bộ đọc-bộ ghi 51 như trả lời đến lệnh 1 được thu từ bộ đọc-bộ ghi 12.

[0052]

Ở bước S61, bộ đọc-bộ ghi 51 thu phản hồi 1 từ thẻ IC 11, và phù hợp với phản hồi 1 thu được, truyền yêu cầu A để yêu cầu việc xử lý định trước, đến ba máy chủ 52, nói cách khác, máy chủ thứ nhất 52A, máy chủ thứ hai 52B, và máy chủ thứ ba 52C.

[0053]

Mỗi trong số máy chủ thứ nhất 52A, máy chủ thứ hai 52B, và máy chủ thứ ba 52C bắt đầu (thực hiện) việc xử lý định trước tương ứng với yêu cầu A thu được, từ thời điểm tại đó yêu cầu A được thu từ bộ đọc-bộ ghi 51. Cụ thể là, ở bước S62, máy chủ thứ nhất 52A bắt đầu việc xử lý định trước tương ứng với yêu cầu A, ở bước S63, máy chủ thứ hai 52B bắt đầu việc xử lý định trước tương ứng với yêu cầu A, và ở bước S64, máy chủ thứ ba 52C bắt đầu việc xử lý định trước tương ứng với yêu cầu A.

[0054]

Sau đó, dựa vào kết quả xử lý, mỗi trong số máy chủ thứ nhất 52A, máy chủ thứ hai 52B, và máy chủ thứ ba 52C truyền, đến bộ đọc-bộ ghi 51, phản hồi A là trả lời đến yêu cầu A, tại thời điểm tại đó việc xử lý định trước tương ứng với yêu cầu A thu được kết thúc. Trong ví dụ trên Fig.4, thứ tự của thời gian kết thúc xử lý là máy chủ thứ hai 52B, máy chủ thứ ba 52C, và máy chủ thứ nhất 52A. Cụ thể hơn là, đầu tiên, ở bước S65, máy chủ thứ hai 52B truyền phản hồi A đến bộ đọc-bộ ghi 12, ở bước S66, máy chủ thứ ba 52C truyền phản hồi A đến bộ đọc-bộ ghi 12, và ở bước S67, máy chủ thứ nhất 52A truyền phản hồi A đến bộ đọc-bộ ghi 12.

[0055]

Các yêu cầu được truyền từ bộ đọc-bộ ghi 51 đến các máy chủ 52 bao gồm cùng nội dung, và các máy chủ 52 truyền, đến bộ đọc-bộ ghi 51, kết quả nhận được bằng cách thực hiện cùng xử lý cho cùng yêu cầu, như phản hồi. Do đó, các phản hồi cần được truyền từ các máy chủ 52 đến bộ đọc-bộ ghi 51 là các kết quả mà dựa vào cùng xử lý, tuy nhiên dữ liệu cần được truyền đôi khi khác nhau.

[0056]

Ví dụ, trong trường hợp mà ở đó các yêu cầu cần được truyền từ bộ đọc-bộ ghi 51 đến các máy chủ 52 là các yêu cầu cho khóa phiên, mỗi trong số các máy chủ 52 thực hiện việc xử lý tạo ra các số ngẫu nhiên làm khóa phiên, dựa vào yêu cầu. Bởi vì các số ngẫu nhiên cần được tạo ra bởi mỗi trong số các máy chủ 52 thường là các trị số khác nhau, các số ngẫu nhiên (các trị số) dùng làm

thông tin khóa phiên mà cần được truyền bởi mỗi trong số các máy chủ 52 đến bộ đọc-bộ ghi 51 làm khóa phiên là các số (các trị số) khác nhau.

[0057]

Bộ đọc-bộ ghi 51 truyền lệnh 2 tiếp theo đến thẻ IC 11 nhờ sử dụng dữ liệu của máy chủ 52 mà đã trả lời sớm nhất trong số các máy chủ 52 mà đã được truyền cùng yêu cầu. Trong ví dụ trên Fig.4, bởi vì phản hồi A được thu từ máy chủ thứ hai 52B sớm nhất, bộ đọc-bộ ghi 51 thu phản hồi A từ máy chủ thứ hai 52B, và sau đó, ở bước S43, truyền lệnh 2 đến thẻ IC 11 như lệnh tiếp theo mà nó dựa vào phản hồi A.

[0058]

Ở bước S44, thẻ IC 11 truyền phản hồi 2 đến bộ đọc-bộ ghi 51 như trả lời đến lệnh 2 được thu từ bộ đọc-bộ ghi 51.

[0059]

Như được nêu trên, trong hệ thống xử lý dữ liệu 40, bộ đọc-bộ ghi 51 truyền cùng yêu cầu A đến các máy chủ 52. Mỗi trong số các máy chủ 52 thu yêu cầu A từ bộ đọc-bộ ghi 51, thực hiện cùng xử lý, và khi kết thúc việc xử lý, truyền phản hồi A là trả lời đến yêu cầu A thu được, đến bộ đọc-bộ ghi 51. Do đó, các máy chủ 52 thực hiện một cách đồng thời cùng xử lý đối với yêu cầu A được truyền bởi bộ đọc-bộ ghi 51.

[0060]

Sau đó, bộ đọc-bộ ghi 51 thực hiện việc xử lý tiếp theo nhờ sử dụng dữ

liệu của máy chủ 52 mà đã được truyền phản hồi A sớm nhất trong số các máy chủ 52.

[0061]

Trên Fig.4, theo quan điểm của bộ đọc-bộ ghi 51, các thời gian xử lý dành cho yêu cầu A của máy chủ thứ nhất 52A, máy chủ thứ hai 52B, và máy chủ thứ ba 52C được biểu thị bởi T1, T2, và T3, và các độ dài của các thời gian xử lý này ở trong mối tương quan được thể hiện bởi  $T2 < T3 < T1$ .

[0062]

Do đó, trong ví dụ này, bộ đọc-bộ ghi 51 bắt đầu truyền lệnh 2 đến thẻ IC 11, ở thời điểm tại đó phản hồi được thu từ máy chủ thứ hai 52B.

[0063]

Trong hệ thống xử lý dữ liệu 40, trị số nhỏ nhất của các thời gian xử lý (bao gồm các thời gian truyền thông) được sử dụng bởi các máy chủ 52 trở thành thời gian xử lý của nhóm máy chủ theo quan điểm của bộ đọc-bộ ghi 51. Do đó, so với hệ thống xử lý dữ liệu bao gồm một máy chủ 13 mà được minh họa trên Fig.1, trung bình các thời gian xử lý trở nên ngắn hơn và độ biến thiên (độ lệch chuẩn) trở nên nhỏ hơn. Do đó, có thể làm giảm trị số lớn nhất thời gian xử lý của toàn bộ hệ thống xử lý dữ liệu.

[0064]

Hơn nữa, trong hệ thống xử lý dữ liệu 40, bởi vì các máy chủ 52 được bao gồm, ngay cả trong trường hợp mà ở đó một (ví dụ, máy chủ thứ hai 52B)

trong số các máy chủ 52 ngừng hoạt động, việc xử lý có thể được thực hiện nhờ sử dụng các máy chủ 52 khác (máy chủ thứ nhất 52A và máy chủ thứ ba 52C).

[0065]

Hơn thế nữa, bởi vì các đường truyền thông cũng được bố trí giữa các máy chủ 52 và bộ đọc-bộ ghi 51, ngay cả trong trường hợp mà ở đó sự tăng tải tạm thời hoặc sự mất kết nối của đường truyền thông định trước xuất hiện, việc xử lý có thể được thực hiện nhờ sử dụng các máy chủ 52 mà sử dụng các đường truyền thông khác. Ví dụ, trong trường hợp mà ở đó đường truyền thông giữa bộ đọc-bộ ghi 51 và máy chủ thứ nhất 52A là mạng công cộng, và đường truyền thông giữa bộ đọc-bộ ghi 51 và máy chủ thứ hai 52B là mạch chuyên dụng, nếu mạch chuyên dụng bị quá tải, việc xử lý mà sử dụng máy chủ thứ nhất 52A có thể được thực hiện nhờ sử dụng mạng công cộng.

[0066]

Do đó, theo hệ thống xử lý dữ liệu 40, tính khả dụng của toàn bộ hệ thống có thể được nâng cao và khả năng sử dụng được nâng cao.

[0067]

Cần lưu ý rằng, trong ví dụ nêu trên, ví dụ mà trong đó bộ đọc-bộ ghi 51 truyền các yêu cầu đến tất cả các máy chủ 52 được bao gồm trong hệ thống xử lý dữ liệu 40 được minh họa, tuy nhiên bộ đọc-bộ ghi 51 không phải lúc nào cũng truyền các yêu cầu đến tất cả các máy chủ 52, và bộ đọc-bộ ghi 51 có thể được tạo cấu hình để lựa chọn một cách thích hợp hai máy chủ 52 trở lên dựa vào điều kiện định trước, và truyền yêu cầu đến các máy chủ 52 được lựa chọn.

[0068]

Ví dụ, các phương pháp dưới đây có thể được sử dụng như phương pháp quyết định hai máy chủ 52 trở lên mà các yêu cầu cần được truyền đến, từ trong số các máy chủ 52 được bao gồm trong hệ thống xử lý dữ liệu 40.

(1) Bộ đọc-bộ ghi 51 quyết định các máy chủ 52 mà các yêu cầu cần được truyền đến, tùy thuộc vào loại của các yêu cầu cần được truyền.

(2) Bộ đọc-bộ ghi 51 quyết định các máy chủ 52 mà các yêu cầu cần được truyền đến, dựa vào các thời gian đến của các phản hồi được thu từ trước. Cụ thể là, bộ đọc-bộ ghi 51 lựa chọn các máy chủ 52 có các thời gian đến sớm hơn, hoặc loại trừ một hoặc nhiều máy chủ 52 có các thời gian đến sau.

[0069]

<3. Vấn đề thứ nhất mà có thể được tạo ra trong cấu hình bao gồm các máy chủ, và biện pháp đối phó>

Tiếp theo, vấn đề mà có thể được tạo ra trong trường hợp mà ở đó cấu hình bao gồm các máy chủ như trong hệ thống xử lý dữ liệu 40 được triển khai, và biện pháp đối phó đối với vấn đề mà được thực hiện trong hệ thống xử lý dữ liệu 40 sẽ được mô tả.

[0070]

Đầu tiên, vấn đề thứ nhất mà có thể được tạo ra trong cấu hình bao gồm các máy chủ, và biện pháp đối phó sẽ được mô tả.

[0071]

Trong trường hợp mà ở đó việc truyền thông được thực hiện giữa bộ đọc-bộ ghi 51 và các máy chủ 52 chỉ một lần, việc truyền thông dữ liệu của hệ thống xử lý dữ liệu 40 được thực hiện như theo trình tự được minh họa trên Fig.4, tuy nhiên giao tác (trình tự các quy trình) thường bao gồm các thời gian của việc truyền thông được thực hiện giữa bộ đọc-bộ ghi 51 và máy chủ 52.

[0072]

Fig.5 minh họa ví dụ trình tự của giao tác bao gồm các thời gian của việc truyền thông được thực hiện giữa bộ đọc-bộ ghi 51 và máy chủ 52.

[0073]

Đối với một giao tác, trao đổi của các lệnh và các phản hồi ở các bước từ S81 đến S86 được thực hiện lần lượt giữa thẻ IC 11 và máy chủ 52.

[0074]

Ở bước S81, lệnh để thu thẻ IC 11 (được gọi là lệnh hỏi vòng) và phản hồi thêm vào đó được truyền. Ở bước S82, lệnh để có được thông tin khóa dịch vụ tương ứng với dịch vụ định trước được cung cấp bởi thẻ IC 11, và phản hồi thêm vào đó được truyền. Ở bước S83, lệnh để xác thực thẻ IC 11 và phản hồi thêm vào đó được truyền. Ở bước S84, lệnh để xác thực bộ đọc-bộ ghi 51 và phản hồi thêm vào đó được truyền. Ở bước S85, lệnh để đọc dữ liệu được lưu trữ trong thẻ IC 11, và phản hồi thêm vào đó được truyền. Ở bước S86, lệnh để ghi dữ liệu định trước tới thẻ IC 11, và phản hồi thêm vào đó được truyền.

[0075]

Sau đó, phù hợp với các lệnh và các phản hồi được truyền ở các bước từ S81 đến S86, việc trao đổi các yêu cầu và các phản hồi được thực hiện lần lượt ở các bước từ S91 đến S96 giữa bộ đọc-bộ ghi 51 và máy chủ 52.

[0076]

Tại thời điểm này, ví dụ, trong phản hồi được truyền ở bước S91, thông tin được truyền từ máy chủ 52 đến bộ đọc-bộ ghi 51 đôi khi bao gồm thông tin cần thiết để trao đổi các yêu cầu và các phản hồi ở các bước tiếp theo từ S92 đến S96. Như ví dụ về thông tin như vậy, ví dụ, có thông tin khóa phiên là thông tin chỉ báo khóa phiên. Cụ thể là, ví dụ, ở bước S91, yêu cầu cho khóa phiên được yêu cầu, và máy chủ 52 tạo ra các số ngẫu nhiên định trước cần được sử dụng như khóa phiên, và trả lời các số ngẫu nhiên định trước đến bộ đọc-bộ ghi 51 như phản hồi. Ở các bước từ S92 đến S96, các yêu cầu và các phản hồi được trao đổi nhờ sử dụng khóa phiên được tạo ra ở bước S91.

[0077]

Theo cách này, trong trường hợp mà ở đó kết quả xử lý được xử lý bởi máy chủ tại thời điểm nhất định được yêu cầu trong việc xử lý tiếp theo, vấn đề không được tạo ra trong hệ thống xử lý dữ liệu có cấu hình bao gồm một máy chủ như trên Fig.1 bởi vì máy chủ 13 nhận dạng tất cả các phần thông tin đã được trao đổi cho đến giờ. Tuy nhiên, vấn đề (vấn đề thứ nhất) có thể được tạo ra trong trường hợp mà ở đó các máy chủ 52 được sử dụng như trong hệ thống xử lý dữ liệu 40 trên Fig.3.

[0078]

Fig.6 và Fig.7 minh họa các ví dụ quy trình truyền thông của vấn đề thứ nhất mà có thể được tạo ra trong hệ thống xử lý dữ liệu 40 có cấu hình bao gồm các máy chủ. Cần lưu ý rằng, trong phần mô tả tiếp theo Fig.6, bởi vì cấu hình bao gồm các máy chủ chỉ được yêu cầu bao gồm ít nhất hai máy chủ 52, máy chủ thứ ba 52C được bỏ qua.

[0079]

Ví dụ quy trình truyền thông trên Fig.6 minh họa ví dụ của trường hợp mà ở đó bộ đọc-bộ ghi 51 yêu cầu lần lượt mỗi trong số các máy chủ 52 thực hiện việc xử lý thứ nhất và việc xử lý thứ hai, và sử dụng kết quả xử lý thứ nhất cho kết quả xử lý thứ hai, và trường hợp mà ở đó các kết quả xử lý thứ nhất nhận được trong các máy chủ 52 là giống nhau.

[0080]

Đối với tiến trình chính của giao tác, bộ đọc-bộ ghi 51 trao đổi lệnh và phản hồi với thẻ IC 11 ba lần ở các bước từ S121 đến S123. Sau đó, ở bước S121, bộ đọc-bộ ghi 51 thu phản hồi 1 từ thẻ IC 11, và sau đó, truyền yêu cầu A đến mỗi trong số các máy chủ 52, yêu cầu việc xử lý thứ nhất, và thu phản hồi A từ mỗi trong số các máy chủ 52. Hơn nữa, bộ đọc-bộ ghi 51 thu phản hồi 2 từ thẻ IC 11 ở bước S122, và sau đó, truyền yêu cầu B đến mỗi trong số các máy chủ 52, yêu cầu việc xử lý thứ hai, và thu phản hồi B từ mỗi trong số các máy chủ 52.

[0081]

Bộ đọc-bộ ghi 51 truyền yêu cầu A để yêu cầu việc xử lý thứ nhất, đến

máy chủ thứ nhất 52A và máy chủ thứ hai 52B. Máy chủ thứ hai 52B thu yêu cầu A, thực hiện việc xử lý thứ nhất, và truyền phản hồi A mà nó dựa vào kết quả xử lý X1, đến bộ đọc-bộ ghi 51 như kết quả thực hiện, nhưng máy chủ thứ nhất 52A không thu được yêu cầu A bởi vì đường truyền thông không thể được sử dụng một cách tạm thời. Vì lý do này, máy chủ thứ nhất 52A không thực hiện việc xử lý thứ nhất, và kết quả xử lý X1 cần nhận được bằng cách thực hiện việc xử lý thứ nhất thất bại nhận được.

[0082]

Do đó, trong trường hợp mà ở đó máy chủ thứ nhất 52A và máy chủ thứ hai 52B thu yêu cầu B từ bộ đọc-bộ ghi 51 và thực hiện việc xử lý thứ hai, và trả lời kết quả xử lý như phản hồi B, bởi vì máy chủ thứ nhất 52A không biết kết quả xử lý X1, kết quả xử lý thứ hai hiệu chính thất bại nhận được.

[0083]

Ví dụ quy trình truyền thông trên Fig.7 minh họa ví dụ của trường hợp mà ở đó bộ đọc-bộ ghi 51 yêu cầu lần lượt mỗi trong số các máy chủ 52 thực hiện việc xử lý thứ nhất và việc xử lý thứ hai, và sử dụng kết quả xử lý thứ nhất cho kết quả xử lý thứ hai, và trường hợp mà ở đó các kết quả xử lý thứ nhất nhận được trong các máy chủ 52 là khác.

[0084]

Bộ đọc-bộ ghi 51 truyền yêu cầu A để yêu cầu việc xử lý thứ nhất, đến máy chủ thứ nhất 52A và máy chủ thứ hai 52B. Máy chủ thứ nhất 52A thu yêu cầu A, thực hiện việc xử lý thứ nhất, và truyền phản hồi A1 mà nó dựa vào kết

quả xử lý Y1, đến bộ đọc-bộ ghi 51 như kết quả thực hiện. Máy chủ thứ hai 52B thu yêu cầu A, thực hiện việc xử lý thứ nhất, và truyền phản hồi A2 mà nó dựa vào kết quả xử lý Y2, đến bộ đọc-bộ ghi 51 như kết quả thực hiện.

[0085]

Bởi vì bộ đọc-bộ ghi 51 thu phản hồi A1 từ máy chủ thứ nhất 52A trước đó trong số phản hồi A1 được truyền từ máy chủ thứ nhất 52A và phản hồi A2 được truyền từ máy chủ thứ hai 52B, bộ đọc-bộ ghi 51 chấp nhận phản hồi A1 mà nó dựa vào kết quả xử lý Y1 mà đã được truyền từ máy chủ thứ nhất 52A, và thực hiện quy trình truyền thông tiếp theo với thẻ IC 11.

[0086]

Sau đó, bộ đọc-bộ ghi 51 truyền yêu cầu B để yêu cầu việc xử lý thứ hai, đến máy chủ thứ nhất 52A và máy chủ thứ hai 52B, nhưng máy chủ thứ hai 52B không biết rằng bộ đọc-bộ ghi 51 đã chấp nhận kết quả xử lý Y1 của máy chủ thứ nhất 52A, và cũng không biết kết quả xử lý Y1. Do đó, máy chủ thứ hai 52B không thể nhận kết quả xử lý thứ hai hiệu chính.

[0087]

Theo cách này, trong trường hợp mà ở đó kết quả xử lý được xử lý bởi máy chủ tại thời điểm nhất định được yêu cầu trong việc xử lý tiếp theo, trong hệ thống xử lý dữ liệu 40 mà sử dụng các máy chủ 52, trong trường hợp mà ở đó việc truyền thông được thực hiện theo cách giống như hệ thống xử lý dữ liệu có cấu hình bao gồm một máy chủ, mà không thực hiện biện pháp đối phó bất kỳ, kết quả xử lý chính xác đôi khi thất bại nhận được khi xử lý toàn bộ giao tác.

[0088]

Do đó, để giải quyết vấn đề thứ nhất nêu trên, mỗi trong số các máy chủ 52 của hệ thống xử lý dữ liệu 40 truyền thông tin được yêu cầu trong việc xử lý tiếp theo trong mỗi trong số các máy chủ 52, được bao gồm trong phản hồi đến bộ đọc-bộ ghi 51, và bộ đọc-bộ ghi 51 của hệ thống xử lý dữ liệu 50 truyền thông tin được bao gồm trong yêu cầu cần được truyền đến mỗi trong số các máy chủ 52 tiếp theo.

[0089]

Như được nêu trên, trong trường hợp mà ở đó phản hồi được thu từ mỗi trong số các máy chủ 52, bởi vì việc xử lý tiếp theo được thực hiện nhờ sử dụng dữ liệu của máy chủ 52 mà đã được truyền phản hồi sớm nhất, bộ đọc-bộ ghi 51 truyền thông tin được bao gồm trong phản hồi mà là từ máy chủ 52 và đã thu được sớm nhất, được bao gồm trong yêu cầu cần được truyền đến mỗi trong số các máy chủ 52 tiếp theo.

[0090]

Fig.8 là lưu đồ minh họa các quy trình truyền thông được thực hiện bởi hệ thống xử lý dữ liệu 40, mà trong đó biện pháp đối phó đối với vấn đề thứ nhất được thực hiện trong cùng hoàn cảnh như Fig.6.

[0091]

Ở bước S121, việc trao đổi lệnh 1 và phản hồi 1 được thực hiện giữa thẻ IC 11 và bộ đọc-bộ ghi 51, và sau đó, ở bước S141, bộ đọc-bộ ghi 51 truyền yêu

cầu A đến các máy chủ 52.

[0092]

Tương tự như Fig.6, yêu cầu A không được gửi tới máy chủ thứ nhất 52A, và được gửi tới máy chủ thứ hai 52B.

[0093]

Ở bước S142, máy chủ thứ hai 52B thực hiện việc xử lý thứ nhất, và ở bước S143, truyền phản hồi A bao gồm kết quả xử lý X1, đến bộ đọc-bộ ghi 51. Kết quả xử lý X1 được mã hóa nhờ sử dụng khóa được dùng chung trong số các máy chủ 52, và sau đó, được truyền khi được được gán ký hiệu số hoặc mã xác thực tin nhắn.

[0094]

Ở bước S122, lệnh 2 và phản hồi 2 được truyền và được thu giữa thẻ IC 11 và bộ đọc-bộ ghi 51, và sau đó, ở bước S144, bộ đọc-bộ ghi 51 truyền yêu cầu B bao gồm kết quả xử lý X1 được thu ở bước S143, đến các máy chủ 52. Kết quả xử lý X1 được truyền tại thời điểm này cũng được mã hóa nhờ sử dụng khóa được dùng chung trong số các máy chủ 52, và được gán ký hiệu số hoặc mã xác thực tin nhắn.

[0095]

Mỗi trong số các máy chủ 52 mà đã thu được yêu cầu B bao gồm kết quả xử lý X1 thực hiện việc xử lý thứ hai nhờ sử dụng kết quả xử lý X1. Cụ thể là, ở bước S145, máy chủ thứ nhất 52A thực hiện việc xử lý thứ hai nhờ sử dụng kết

quả xử lý X1, và ở bước S147, máy chủ thứ hai 52B thực hiện việc xử lý thứ hai nhờ sử dụng kết quả xử lý X1.

[0096]

Sau khi kết thúc thực hiện việc xử lý thứ hai ở bước S145, ở bước S146, máy chủ thứ nhất 52A truyền kết quả xử lý của việc xử lý thứ hai đến bộ đọc-bộ ghi 51 như phản hồi B đến yêu cầu B. Sau khi kết thúc thực hiện việc xử lý thứ hai ở bước S147, ở bước S148, máy chủ thứ hai 52B truyền kết quả xử lý của việc xử lý thứ hai đến bộ đọc-bộ ghi 51 như phản hồi B đến yêu cầu B.

[0097]

Sau khi bộ đọc-bộ ghi 51 thu phản hồi B từ máy chủ thứ nhất 52A là phản hồi B được thu sớm nhất, ở bước S123, lệnh 3 và phản hồi 3 được truyền giữa thẻ IC 11 và bộ đọc-bộ ghi 51.

[0098]

Fig.9 là lưu đồ minh họa các quy trình truyền thông được thực hiện bởi hệ thống xử lý dữ liệu 40, mà trong đó biện pháp đối phó đối với vấn đề thứ nhất được thực hiện trong cùng hoàn cảnh như Fig.7.

[0099]

Ở bước S121, việc trao đổi lệnh 1 và phản hồi 1 được thực hiện giữa thẻ IC 11 và bộ đọc-bộ ghi 51, và sau đó, ở bước S161, bộ đọc-bộ ghi 51 truyền yêu cầu A đến các máy chủ 52.

[0100]

Mỗi trong số các máy chủ 52 mà đã thu được yêu cầu A đó thực hiện việc xử lý thứ nhất. Cụ thể là, Ở bước S162, máy chủ thứ nhất 52A thực hiện việc xử lý thứ hai, và ở bước S163, truyền phản hồi A1 bao gồm kết quả xử lý Y1 của việc xử lý thứ nhất, đến bộ đọc-bộ ghi 51. Tương tự, ở bước S164, máy chủ thứ hai 52B thực hiện việc xử lý thứ nhất, và ở bước S165, truyền phản hồi A2 bao gồm kết quả xử lý Y2 của việc xử lý thứ nhất, đến bộ đọc-bộ ghi 51. Các kết quả xử lý Y1 và Y2 cũng được mã hóa nhờ sử dụng khóa được dùng chung trong số các máy chủ 52, và được gán ký hiệu số hoặc mã xác thực tin nhắn.

[0101]

Bộ đọc-bộ ghi 51 thu phản hồi A1 từ máy chủ thứ nhất 52A ở bước S163 trước phản hồi A2 từ máy chủ thứ hai 52B ở bước S165.

[0102]

Ở bước S122, lệnh 2 và phản hồi 2 được truyền và được thu giữa thẻ IC 11 và bộ đọc-bộ ghi 51, và sau đó, ở bước S166, bộ đọc-bộ ghi 51 truyền yêu cầu B bao gồm kết quả xử lý Y1 được thu ở bước S163, đến các máy chủ 52. Kết quả xử lý Y2 cũng được mã hóa nhờ sử dụng khóa được dùng chung trong số các máy chủ 52, và được gán ký hiệu số hoặc mã xác thực tin nhắn.

[0103]

Mỗi trong số các máy chủ 52 mà đã thu được yêu cầu B bao gồm kết quả xử lý Y1 thực hiện việc xử lý thứ hai nhờ sử dụng kết quả xử lý Y1. Nói cách khác, ở bước S168, máy chủ thứ nhất 52A thực hiện việc xử lý thứ hai nhờ sử dụng kết quả xử lý Y1, và ở bước S167, máy chủ thứ hai 52B thực hiện việc xử

lý thứ hai nhờ sử dụng kết quả xử lý Y1.

[0104]

Sau khi kết thúc thực hiện việc xử lý thứ hai ở bước S167, ở bước S169, máy chủ thứ hai 52B truyền phản hồi B bao gồm kết quả xử lý của việc xử lý thứ hai, đến bộ đọc-bộ ghi 51. Sau khi kết thúc thực hiện việc xử lý thứ hai ở bước S168, ở bước S170, máy chủ thứ nhất 52A truyền phản hồi B bao gồm kết quả xử lý của việc xử lý thứ hai, đến bộ đọc-bộ ghi 51.

[0105]

Sau khi bộ đọc-bộ ghi 51 thu phản hồi B từ máy chủ thứ hai 52B là phản hồi B được thu sớm nhất, ở bước S123, lệnh 3 và phản hồi 3 được truyền giữa thẻ IC 11 và bộ đọc-bộ ghi 51.

[0106]

Như được nêu trên, mỗi trong số các máy chủ 52 của hệ thống xử lý dữ liệu 40 truyền thông tin được yêu cầu trong việc xử lý tiếp theo trong mỗi trong số các máy chủ 52, được bao gồm trong phản hồi đến bộ đọc-bộ ghi 51, và bộ đọc-bộ ghi 51 của hệ thống xử lý dữ liệu 40 truyền thông tin được bao gồm trong yêu cầu cần được truyền đến mỗi trong số các máy chủ 52 tiếp theo. Vấn đề thứ nhất như được mô tả trên Fig.6 và Fig.7 bằng cách này có thể được giải quyết.

[0107]

Hơn nữa, trong trường hợp mà ở đó thông tin cần được thu từ mỗi trong

số các máy chủ 52 và được yêu cầu bởi mỗi trong số các máy chủ 52 trong việc xử lý tiếp theo là thông tin mà không cần được biết đến bộ đọc-bộ ghi 51, máy chủ 52 chia sẻ thông tin trong số các máy chủ 52, mã hóa thông tin nhờ sử dụng khóa chưa biết đến bộ đọc-bộ ghi 51 (khóa không thể giải mã được bởi bộ đọc-bộ ghi 51), và sau đó, truyền thông tin được bao gồm trong phản hồi. Thông tin bằng cách này có thể được dùng chung với các máy chủ 52 khác không biết đến bộ đọc-bộ ghi 51.

[0108]

<Trường hợp bao gồm máy chủ hậu xử lý>

Trường hợp mà ở đó hệ thống xử lý dữ liệu 40 được bố trí có máy chủ hậu xử lý 53 sẽ được mô tả bổ sung.

[0109]

Trong trường hợp mà ở đó hệ thống xử lý dữ liệu 40 được bố trí có máy chủ hậu xử lý 53, khi mỗi trong số các máy chủ 52 thực hiện xử lý, mỗi trong số các máy chủ 52 cũng thực hiện xử lý truyền thông tin được yêu cầu cho việc xử lý của toàn bộ giao tác (thông tin được yêu cầu cho giao tác), đến máy chủ hậu xử lý 53.

[0110]

Máy chủ hậu xử lý 53 thu thông tin được yêu cầu cho giao tác được truyền từ mỗi trong số các máy chủ 52, và dựa vào thông tin được yêu cầu cho giao tác của mỗi trong số các máy chủ 52, thực hiện xử lý xác định kết quả của

toàn bộ giao tác (hậu xử lý). Các ví dụ về việc xử lý xác định kết quả của toàn bộ giao tác bao gồm việc xử lý bảo trì đối với thông tin số dư tiền điện tử được lưu trữ trong mỗi trong số các máy chủ 52, xử lý phát hiện bất thường, và tương tự, trong trường hợp mà ở đó hệ thống xử lý dữ liệu 40 là hệ thống tiền điện tử mà xử lý tiền điện tử.

[0111]

Fig.10 là lưu đồ minh họa việc xử lý mà trong đó các quy trình truyền thông của máy chủ hậu xử lý 53 được bổ sung vào các quy trình truyền thông của hệ thống xử lý dữ liệu 40 được minh họa trên Fig.8.

[0112]

Trong phần mô tả trên Fig.10, chỉ các quy trình được bổ sung mới vào các quy trình được mô tả trên Fig.8 sẽ được mô tả.

[0113]

Sau khi máy chủ thứ hai 52B thực hiện việc xử lý thứ nhất ở bước S142, ở bước S181, máy chủ thứ hai 52B truyền kết quả xử lý Z1 đến máy chủ hậu xử lý 53 như thông tin được yêu cầu cho giao tác. Trình tự của các quy trình ở các bước S181 và S143 không bị giới hạn.

[0114]

Sau khi máy chủ thứ nhất 52A thực hiện việc xử lý thứ hai ở bước S145, ở bước S182, máy chủ thứ nhất 52A truyền kết quả xử lý Z2 đến máy chủ hậu xử lý 53 như thông tin được yêu cầu cho giao tác. Trình tự của các quy trình ở

các bước S182 và S146 không bị giới hạn.

[0115]

Sau khi máy chủ thứ hai 52B thực hiện việc xử lý thứ hai ở bước S147, ở bước S183, máy chủ thứ hai 52B truyền kết quả xử lý Z2 đến máy chủ hậu xử lý 53 như thông tin được yêu cầu cho giao tác. Trình tự của các quy trình ở các bước S183 và S148 không bị giới hạn.

[0116]

Bởi vì việc xử lý thứ hai được thực hiện bởi máy chủ thứ nhất 52A và máy chủ thứ hai 52B là cùng xử lý, kết quả xử lý Z2 được truyền từ máy chủ thứ nhất 52A ở bước S182 và kết quả xử lý Z2 được truyền từ máy chủ thứ hai 52B ở bước S183 là giống nhau.

[0117]

Ở bước S184, máy chủ hậu xử lý 53 hợp nhất các phần thông tin được yêu cầu cho giao tác được truyền từ các máy chủ 52 trong các quy trình cấu thành giao tác, và xác định kết quả của toàn bộ giao tác. Hơn nữa, máy chủ hậu xử lý 53 thực hiện việc xử lý định trước mà đã được quyết định từ trước, dựa vào kết quả của toàn bộ giao tác.

[0118]

Trong việc hợp nhất các phần thông tin được yêu cầu cho giao tác, máy chủ hậu xử lý 53 thực hiện xử lý nhận dạng cùng các kết quả xử lý được truyền từ các máy chủ 52 như một kết quả xử lý, và loại bỏ sự trùng lặp trong các máy

chủ 52.

[0119]

Như được nêu trên, trong trường hợp mà ở đó hệ thống xử lý dữ liệu 40 có cấu hình bao gồm máy chủ hậu xử lý 53, mỗi trong số các máy chủ 52 truyền thông tin được yêu cầu cho việc xử lý của toàn bộ giao tác, đến máy chủ hậu xử lý 53 mà là thiết bị xử lý thông tin khác, dựa vào kết quả thực hiện của mỗi quy trình. Máy chủ hậu xử lý 53 hợp nhất các phần thông tin được yêu cầu cho giao tác được truyền từ các máy chủ 52 trong các quy trình cấu thành giao tác, và xác định kết quả của toàn bộ giao tác.

[0120]

<4. Vấn đề thứ hai mà có thể được tạo ra trong cấu hình bao gồm các máy chủ, và biện pháp đối phó>

Tiếp theo, vấn đề thứ hai mà có thể được tạo ra trong cấu hình bao gồm các máy chủ, và biện pháp đối phó sẽ được mô tả.

[0121]

Như đã thấy trong trình tự của giao tác được minh họa trên Fig.5, sự xác thực lẫn nhau mà trong đó bộ đọc-bộ ghi 51 xác thực thẻ IC 11 và thẻ IC 11 xác thực bộ đọc-bộ ghi 51 được thực hiện theo trình tự của các quy trình truyền thông. Đối với phương pháp bằng cách đó bộ đọc-bộ ghi 51 xác thực thẻ IC 11, phương pháp được gọi là phương pháp phản hồi đòi hỏi thường được sử dụng.

[0122]

Phương pháp phản hồi đòi hỏi sẽ được mô tả đơn giản như dưới đây.

[0123]

Đầu tiên, bộ đọc-bộ ghi 51 tạo ra các số ngẫu nhiên và truyền các số ngẫu nhiên được tạo ra hoặc trị số mà nó dựa vào các số ngẫu nhiên (dưới đây, trị số sẽ được gọi là yêu cầu ngẫu nhiên) đến thẻ IC 11. Thẻ IC 11 thực hiện việc tính toán cụ thể theo yêu cầu ngẫu nhiên nhờ sử dụng khóa riêng được giữ bởi thẻ IC 11, và truyền (trả lời) kết quả tính toán đến bộ đọc-bộ ghi 51. Bằng cách xác nhận kết quả tính toán của yêu cầu ngẫu nhiên (random challenge, viết tắt là RC) được truyền từ thẻ IC 11 (dưới đây, được gọi là kết quả tính toán RC), bộ đọc-bộ ghi 51 xác thực rằng thẻ IC 11 là đối tác truyền thông chính xác giữ khóa riêng.

[0124]

Trong hệ thống xử lý dữ liệu máy khách mỏng, bởi máy chủ 52 tạo ra yêu cầu ngẫu nhiên nêu trên và xác nhận kết quả tính toán RC, điều được xác nhận là thẻ IC 11 là đối tác truyền thông chính xác giữ khóa riêng.

[0125]

Trong trường hợp mà ở đó hệ thống xử lý dữ liệu 40 có cấu hình bao gồm các máy chủ như được nêu trên, bởi vì bộ đọc-bộ ghi 51 truyền kết quả tính toán RC đến các máy chủ 52, trạng thái ở đó việc xử lý xác thực đã được thực hiện nhiều lần có thể được tạo ra (vấn đề thứ hai).

[0126]

Các quy trình truyền thông cần được thực hiện trong trường hợp mà ở đó trạng thái ở đó việc xử lý xác thực đã được thực hiện nhiều lần có thể được tạo ra sẽ được mô tả dựa vào lưu đồ trên Fig.11.

[0127]

Đầu tiên, ở bước S201, một trong số các máy chủ 52, ví dụ, máy chủ thứ nhất 52A tạo ra yêu cầu ngẫu nhiên (dưới đây, được gọi là RC), và truyền RC được ký nhận được bằng cách gán cho RC được tạo ra ký hiệu số, đến bộ đọc-bộ ghi 51. Ký hiệu số là thông tin xác nhận rằng yêu cầu ngẫu nhiên (RC) đã được tạo ra bởi máy chủ 52 chính xác.

[0128]

Theo phương án hiện tại, một máy chủ 52 định trước của các máy chủ 52 được chuẩn bị được chỉ định như máy chủ 52 mà nó tạo ra RC, và máy chủ 52 được chỉ định tạo ra RC thường xuyên hoặc không thường xuyên, ví dụ, và truyền RC được tạo ra đến bộ đọc-bộ ghi 51. Lưu ý rằng máy chủ 52 chuyên dụng để tạo ra RC có thể được bố trí, hoặc máy chủ 52 có thể tạo ra RC chỉ khi yêu cầu cho việc tạo ra yêu cầu ngẫu nhiên được thu từ bộ đọc-bộ ghi 51.

[0129]

Ở bước S202, bộ đọc-bộ ghi 51 thu RC được ký từ máy chủ thứ nhất 52A và xác nhận rằng RC thu được đã được tạo ra bởi máy chủ thứ nhất 52A chính xác, và sau đó, truyền lệnh xác thực thẻ và RC đến thẻ IC 11.

[0130]

Ở bước S203, thẻ IC 11 thu lệnh xác thực thẻ và RC, thực hiện việc tính toán cụ thể theo RC, và truyền (trả lời) kết quả tính toán (kết quả tính toán RC) đến bộ đọc-bộ ghi 51.

[0131]

Ở bước S204, bộ đọc-bộ ghi 51 truyền kết quả tính toán RC được thu từ thẻ IC 11, đến mỗi trong số các máy chủ 52 cùng với RC được ký.

[0132]

Ở bước S205, máy chủ thứ nhất 52A thu RC được ký và kết quả tính toán RC từ bộ đọc-bộ ghi 51, và xác thực thẻ IC 11 bằng cách xác nhận kết quả tính toán RC nhờ sử dụng RC.

[0133]

Sau đó, ở bước S206, máy chủ thứ nhất 52A truyền kết quả xử lý nhận được bằng cách thực hiện việc xử lý xác thực, đến bộ đọc-bộ ghi 51.

[0134]

Tương tự ở phía máy chủ thứ hai 52B, ở bước S207, máy chủ thứ hai 52B thu RC được ký và kết quả tính toán RC từ bộ đọc-bộ ghi 51, và xác thực thẻ IC 11 bằng cách xác nhận kết quả tính toán RC nhờ sử dụng RC thu được.

[0135]

Sau đó, ở bước S208, máy chủ thứ hai 52B truyền kết quả xử lý nhận được bằng cách thực hiện việc xử lý xác thực, đến bộ đọc-bộ ghi 51.

[0136]

Như được nêu trên, trong hệ thống xử lý dữ liệu 40 bao gồm các máy chủ 52, trong trường hợp mà ở đó việc xử lý xác thực của thẻ IC 11 được thực hiện ở phía máy chủ, ví dụ, tình huống mà trong đó thẻ IC 11 tiếp xúc bộ đọc-bộ ghi 51 nhiều lần mặc dù thẻ IC 11 tiếp xúc bộ đọc-bộ ghi 51 chỉ một lần có thể được tạo ra.

[0137]

Ví dụ, trong trường hợp mà ở đó hệ thống xử lý dữ liệu 40 là hệ thống tiền điện tử mà nó quản lý số dư của tiền điện tử ở phía máy chủ, việc thanh toán có thể được thực hiện nhiều lần bằng cách thực hiện chạm chỉ một lần.

[0138]

Do đó, các quy trình truyền thông cần được thực hiện bởi hệ thống xử lý dữ liệu 40, mà trong đó biện pháp đối phó đối với vấn đề thứ hai được thực hiện sẽ được mô tả.

[0139]

Đối với biện pháp đối phó đối với vấn đề thứ hai, máy chủ thứ nhất 52A mà nó tạo ra RC cũng tạo ra giao tác ID (transaction ID, viết tắt là TID) là thông tin để nhận dạng giao tác, và truyền TID đến bộ đọc-bộ ghi 51. Bộ đọc-bộ ghi 51 truyền TID đến mỗi trong số các máy chủ 52 cùng với RC được ký và kết quả tính toán RC. Mỗi trong số các máy chủ 52 truyền kết quả xử lý của việc xử lý xác thực đến máy chủ hậu xử lý 53 cùng với TID. Sau đó, dựa vào TID thu được, máy chủ hậu xử lý 53 đối chiếu (so sánh) các kết quả xử lý xác thực được thu từ các máy chủ 52.

[0140]

Fig.12 là lưu đồ minh họa các quy trình truyền thông được thực hiện bởi hệ thống xử lý dữ liệu 40, mà trong đó biện pháp đối phó đối với vấn đề thứ hai được thực hiện.

[0141]

Đầu tiên, ở bước S221, một trong số các máy chủ 52, ví dụ, máy chủ thứ nhất 52A tạo ra RC và TID là thông tin để nhận dạng giao tác, và truyền RC được ký và TID được ký nhận được bằng cách gán cho RC và TID được tạo ra các ký hiệu số, đến bộ đọc-bộ ghi 51.

[0142]

Ở bước S222, bộ đọc-bộ ghi 51 thu RC được ký từ máy chủ thứ nhất 52A và xác nhận rằng RC và TID thu được đã được tạo ra bởi máy chủ 52 chính xác, và sau đó, truyền lệnh xác thực thẻ và RC đến thẻ IC 11.

[0143]

Ở bước S223, thẻ IC 11 thu lệnh xác thực thẻ và RC, thực hiện việc tính toán cụ thể theo RC, và truyền (trả lời) kết quả tính toán (kết quả tính toán RC) đến bộ đọc-bộ ghi 51.

[0144]

Ở bước S224, bộ đọc-bộ ghi 51 truyền kết quả tính toán RC được thu từ thẻ IC 11, đến mỗi trong số các máy chủ 52 cùng với RC được ký và TID được ký.

[0145]

Ở bước S225, máy chủ thứ nhất 52A thu RC được ký, TID được ký, và kết quả tính toán RC từ bộ đọc-bộ ghi 51, và xác nhận rằng RC và TID thu được đã được tạo ra bởi máy chủ thứ nhất 52A chính xác. Sau đó, máy chủ thứ nhất 52A xác thực thẻ IC 11 bằng cách xác nhận kết quả tính toán RC nhờ sử dụng RC. Ở bước S226, máy chủ thứ nhất 52A truyền kết quả xử lý nhận được bằng cách thực hiện việc xử lý xác thực, đến bộ đọc-bộ ghi 51.

[0146]

Sau đó, ở bước S227, máy chủ thứ nhất 52A truyền kết quả xử lý của việc xử lý xác thực, và TID được ký để nhận dạng việc xử lý xác thực, đến máy chủ hậu xử lý 53.

[0147]

Tương tự ở phía máy chủ thứ hai 52B, ở bước S231, máy chủ thứ hai 52B thu RC được ký, TID được ký, và kết quả tính toán RC từ bộ đọc-bộ ghi 51, và xác nhận rằng RC và TID thu được đã được tạo ra bởi máy chủ thứ nhất 52A chính xác. Sau đó, máy chủ thứ hai 52B xác thực thẻ IC 11 bằng cách xác nhận kết quả tính toán RC nhờ sử dụng RC. Ở bước S232, máy chủ thứ hai 52B truyền kết quả xử lý nhận được bằng cách thực hiện việc xử lý xác thực, đến bộ đọc-bộ ghi 51.

[0148]

Sau đó, ở bước S233, máy chủ thứ hai 52B truyền kết quả xử lý của việc

xử lý xác thực, và TID được ký để nhận dạng việc xử lý xác thực, đến máy chủ hậu xử lý 53.

[0149]

Ở bước S241, máy chủ hậu xử lý 53 thu các kết quả xử lý của việc xử lý xác thực và các TID được ký đã được truyền từ các máy chủ 52, và thực hiện xử lý đối chiếu mà nó dựa vào các TID. Cụ thể hơn là, máy chủ hậu xử lý 53 đối chiếu các TID được truyền từ các máy chủ 52, và xem các kết quả xử lý được gán cùng TID như cùng kết quả xử lý, bằng cách này thực hiện việc xử lý giả định rằng việc xử lý xác thực định trước đã được thực hiện chỉ một lần.

[0150]

Với cấu hình này, ví dụ, trong trường hợp mà ở đó hệ thống xử lý dữ liệu 40 là hệ thống tiền điện tử mà nó quản lý số dư của tiền điện tử ở phía máy chủ nhờ sử dụng thẻ ID là thông tin nhận dạng thẻ IC được giữ bởi thẻ IC 11, như khóa, việc xử lý thanh toán có cùng TID có thể được coi là cùng thanh toán.

[0151]

Như được nêu trên, máy chủ thứ nhất 52A mà nó tạo ra RC cũng tạo ra TID, và mỗi trong số các máy chủ 52 mà có việc xử lý xác thực được thực hiện truyền kết quả xử lý của việc xử lý xác thực đến máy chủ hậu xử lý 53 cùng với TID. Với cấu hình này, bởi vì máy chủ hậu xử lý 53 có thể loại bỏ sự trùng lặp của cùng xử lý dựa vào TID được phân bổ cho kết quả xử lý, có thể giải quyết vấn đề thứ hai mà có thể được tạo ra trong hệ thống xử lý dữ liệu 40 bao gồm các máy chủ 52.

[0152]

Cần lưu ý rằng, trong các quy trình truyền thông trên Fig.12, máy chủ thứ nhất 52A mà nó tạo ra RC đồng thời tạo ra RC và TID, và truyền RC và TID đến bộ đọc-bộ ghi 51, nhưng thời điểm tạo ra của TID và thời điểm truyền đến bộ đọc-bộ ghi 51 có thể là các thời điểm khác với thời điểm tạo ra và thời điểm truyền của RC.

[0153]

Hơn nữa, TID có thể được tạo ra bất kể RC, hoặc có thể được tạo ra bởi phép tính mà nó dựa vào trị số của RC.

[0154]

Hơn thế nữa, TID có thể được thay thế bởi RC (RC cũng có thể dùng làm TID). Trong trường hợp mà ở đó TID có thể được thay thế bởi RC, như được minh họa trên Fig.13, ở bước S221, dữ liệu cần được truyền đến bộ đọc-bộ ghi 51 bởi máy chủ thứ nhất 52A mà nó tạo ra RC trở thành chỉ RC được ký.

[0155]

Fig.13 là lưu đồ minh họa ví dụ sửa đổi về quy trình truyền thông được minh họa trên Fig.12. Bởi vì các bước của các quy trình trên Fig.12 và Fig.13 là giống nhau, trên Fig.13, cùng số bước như số bước trên Fig.12 được phân bổ.

[0156]

Ở bước S224, bộ đọc-bộ ghi 51 truyền RC được ký và kết quả tính toán RC được thu từ thẻ IC 11, đến mỗi trong số các máy chủ 52. Ở các bước S227

và S232, các kết quả xử lý của việc xử lý xác thực và các RC được ký được truyền đến máy chủ hậu xử lý 53. Ở bước S241, máy chủ hậu xử lý 53 thực hiện xử lý đối chiếu dựa vào các RC.

[0157]

Tiếp theo, biện pháp đối phó đối với vấn đề thứ hai mà trong đó máy chủ hậu xử lý 53 không được sử dụng sẽ được mô tả.

[0158]

Trong trường hợp mà ở đó cấu hình mà trong đó máy chủ hậu xử lý 53 không được sử dụng được triển khai, máy chủ thứ nhất 52A mà nó tạo ra RC thiết đặt khoảng thời gian hiệu lực của RC được tạo ra đến thời gian ngắn (ví dụ, vài giây), gán khoảng thời gian hiệu lực được thiết đặt ký hiệu số, và truyền khoảng thời gian hiệu lực đến bộ đọc-bộ ghi 51 cùng với RC được ký. Mỗi trong số các máy chủ 52 mà thực hiện việc xác thực dựa vào kết quả tính toán RC xác nhận khoảng thời gian hiệu lực của RC, và thực hiện việc xử lý xác thực trong trường hợp mà ở đó khoảng thời gian hiệu lực có hiệu lực (nghĩa là nằm trong khoảng thời gian hiệu lực).

[0159]

Fig.14 là lưu đồ minh họa ví dụ cụ thể về các quy trình truyền thông được thực hiện trong trường hợp mà ở đó máy chủ hậu xử lý 53 không được sử dụng.

[0160]

Đầu tiên, ở bước S241, một trong số các máy chủ 52, ví dụ, máy chủ thứ nhất 52A tạo ra RC và thiết đặt khoảng thời gian hiệu lực của RC, và truyền RC được ký và khoảng thời gian hiệu lực được ký nhận được bằng cách gán cho RC và TID được tạo ra các ký hiệu số, đến bộ đọc-bộ ghi 51.

[0161]

Ở bước S242, bộ đọc-bộ ghi 51 thu RC được ký và khoảng thời gian hiệu lực được ký từ máy chủ thứ nhất 52A và xác nhận rằng RC thu được đã được tạo ra bởi máy chủ 52 chính xác, và sau đó, truyền lệnh xác thực thẻ và RC đến thẻ IC 11.

[0162]

Ở bước S243, thẻ IC 11 thu lệnh xác thực thẻ và RC, thực hiện việc tính toán cụ thể theo RC, và truyền (trả lời) kết quả tính toán (kết quả tính toán RC) đến bộ đọc-bộ ghi 51.

[0163]

Ở bước S244, bộ đọc-bộ ghi 51 truyền kết quả tính toán RC được thu từ thẻ IC 11, đến mỗi trong số các máy chủ 52 cùng với RC được ký và khoảng thời gian hiệu lực được ký.

[0164]

Ở bước S245, máy chủ thứ nhất 52A thu RC được ký, khoảng thời gian hiệu lực được ký, và kết quả tính toán RC từ bộ đọc-bộ ghi 51, và xác nhận rằng RC thu được và khoảng thời gian hiệu lực đã được tạo ra bởi máy chủ thứ nhất

52A chính xác. Sau đó, máy chủ thứ nhất 52A xác thực thẻ IC 11 bằng cách xác nhận rằng khoảng thời gian hiệu lực có hiệu lực và còn xác nhận kết quả tính toán RC. Ở bước S246, máy chủ thứ nhất 52A truyền kết quả xử lý nhận được bằng cách thực hiện việc xử lý xác thực, đến bộ đọc-bộ ghi 51.

[0165]

Tương tự ở phía máy chủ thứ hai 52B, ở bước S251, máy chủ thứ hai 52B thu RC được ký, khoảng thời gian hiệu lực được ký, và kết quả tính toán RC từ bộ đọc-bộ ghi 51, và xác nhận rằng RC thu được và khoảng thời gian hiệu lực đã được tạo ra bởi máy chủ thứ nhất 52A chính xác. Sau đó, máy chủ thứ hai 52B xác thực thẻ IC 11 bằng cách xác nhận rằng khoảng thời gian hiệu lực có hiệu lực và còn xác nhận kết quả tính toán RC. Ở bước S252, máy chủ thứ hai 52B truyền kết quả xử lý nhận được bằng cách thực hiện việc xử lý xác thực, đến bộ đọc-bộ ghi 51.

[0166]

Bởi vì khoảng thời gian hiệu lực được thiết đặt đến thời gian cực ngắn, bộ đọc-bộ ghi 51 thực hiện xử lý liên quan đến các kết quả xử lý được truyền từ các máy chủ 52 trong khoảng thời gian hiệu lực, như cùng xử lý.

[0167]

Mặt khác, ví dụ, trong trường hợp mà ở đó RC được ký, khoảng thời gian hiệu lực được ký, và kết quả tính toán RC được truyền đến máy chủ 52 định trước (máy chủ thứ hai 52B trên Fig.14) từ bộ đọc-bộ ghi 51, trong khoảng thời gian sau khoảng thời gian hiệu lực như ở các bước từ S281 đến S283 trên

Fig.14, việc xử lý xác thực không thành công, và kết quả xử lý thất bại được trả lời đến bộ đọc-bộ ghi 51.

[0168]

Do đó, ví dụ, ngay cả trong trường hợp mà ở đó bộ đọc-bộ ghi giả mạo mạo danh bộ đọc-bộ ghi 51 thu và truyền RC được ký, khoảng thời gian hiệu lực được ký, và kết quả tính toán RC đến máy chủ 52 bất kỳ, việc xử lý xác thực không thành công, và việc xử lý sai có thể được ngăn ngừa.

[0169]

<5. Ví dụ cấu hình phần cứng>

<Các ví dụ cấu hình của thẻ IC và bộ đọc-bộ ghi>

Fig.15 là sơ đồ khối minh họa các ví dụ cấu hình của thẻ IC 11 và bộ đọc-bộ ghi 51.

[0170]

Bộ phận truyền thông RF 101 của bộ đọc-bộ ghi 51 quá tải các sóng điện từ định trước, và phát hiện thẻ IC 11 có tiếp cận hay không, dựa vào sự thay đổi về tải mà được tạo ra phù hợp với tắc nghẽn, và truyền và thu các loại dữ liệu khác nhau với thẻ IC 11 theo cách không tiếp xúc khi thẻ IC 11 tiếp cận, ví dụ.

[0171]

Bộ phận truyền thông RF 101 bao gồm anten, và thực hiện sự truyền thông tầm gần (sự truyền thông không tiếp xúc) phù hợp với chuẩn ISO/IEC 14443 hoặc chuẩn ISO/IEC 18092, ví dụ, với thẻ IC 11. Bộ phận truyền thông

RF 101 thực hiện việc điều biến khóa dịch vị biên độ (amplitude shift keying, viết tắt là ASK) của các sóng mang ở tần số định trước mà được cấp từ mạch dao động (oscillation circuit, viết tắt là OSC) (không được minh họa), ví dụ, dựa vào dữ liệu được cấp từ CPU 102, và đưa ra các sóng điều biến được tạo ra từ anten như các sóng điện từ. Hơn nữa, các sóng điều biến (các sóng điều biến ASK) thu được qua anten được giải điều biến và dữ liệu được giải điều biến được cấp đến CPU 102.

[0172]

Dựa vào sự điều khiển của CPU 102, bộ phận truyền thông RF 101 truyền lệnh đến thẻ IC 11 và thu phản hồi, nhờ sử dụng các sóng điện từ.

[0173]

Bộ xử lý trung tâm (CPU) 102 của bộ đọc-bộ ghi 51 là bộ phận điều khiển mà nó điều khiển toàn bộ hoạt động của bộ đọc-bộ ghi 51. CPU 102 thực hiện các loại xử lý khác nhau bằng cách tải các chương trình được lưu trữ trong bộ nhớ chỉ đọc (read only memory, viết tắt là ROM) 103, tới bộ nhớ truy cập ngẫu nhiên (random access memory, viết tắt là RAM) 104. Hơn nữa, các phần dữ liệu cần thiết để CPU 102 thực hiện các loại xử lý khác nhau, và tương tự cũng được lưu trữ một cách thích hợp trong RAM 104.

[0174]

CPU 102 được tạo cấu hình để mã hóa và giải mã dữ liệu dựa vào thuật toán mã hóa xác định trước bằng cách điều khiển bộ phận tính toán mã hóa 105. Dưới đây, thuật toán mã hóa của bộ phận tính toán mã hóa 105 là thuật toán mã

hóa chẳng hạn như chuẩn mã hóa dữ liệu (data encryption standard, viết tắt là DES), Triple DES, hoặc chuẩn mã hóa được cải tiến (advanced encryption standard, viết tắt là AES), và là thuật toán mã hóa của khóa riêng (khóa chung).

[0175]

Trong trường hợp mà ở đó việc mã hóa hoặc việc giải mã dữ liệu được thực hiện trong bộ đọc-bộ ghi 51, ví dụ, bởi CPU 102 cung cấp khóa riêng được lưu trữ trong bộ phận lưu trữ khóa riêng 106, đến bộ phận tính toán mã hóa 105 cùng với dữ liệu cần được mã hóa hoặc giải mã, việc mã hóa hoặc việc giải mã dữ liệu được cung cấp mà sử dụng khóa riêng được cung cấp được thực hiện bởi bộ phận tính toán mã hóa 105.

[0176]

Khóa riêng được lưu trữ trong bộ phận lưu trữ khóa riêng 106 được giả định là giống như khóa riêng được lưu trữ trong thẻ IC 11, và khóa riêng được lưu trữ trước chỉ trong bộ đọc-bộ ghi 51 mà hỗ trợ thẻ IC 11, và là bộ đọc-bộ ghi 51 được phép đọc thẻ ID là thông tin nhận dạng duy nhất đối với thẻ IC 11.

[0177]

Bộ phận truyền thông 107 trao đổi dữ liệu định trước với các máy chủ 52 nhờ truyền thông mạng được thực hiện qua mạng định trước, dựa vào sự điều khiển của CPU 102. Như được nêu trên, các ví dụ về mạng định trước bao gồm Internet, mạng mạch điện thoại, mạng truyền thông vệ tinh, các LAN khác nhau bao gồm Ethernet (nhãn hiệu đã được đăng ký), WAN, mạng mạch chuyên dụng chẳng hạn như IP-VPN, và tương tự. Loại của mạng định trước không bị giới

hạn.

[0178]

Bộ phận truyền thông RF 201 của thẻ IC 11 có cấu hình bao gồm anten cuộn và mạch LC bao gồm tụ điện, ví dụ, và thực hiện sự truyền thông tầm gần (sự truyền thông không tiếp xúc) phù hợp với chuẩn ISO/IEC 14443 hoặc chuẩn ISO/IEC 18092, ví dụ, với bộ đọc-bộ ghi 51.

[0179]

Bộ phận truyền thông RF 201 được tạo cấu hình để cộng hưởng với các sóng điện từ ở tần số định trước được quá tải từ bộ đọc-bộ ghi 51. Hơn nữa, bộ phận truyền thông RF 201 tinh chế từ trường dòng điện xoay chiều được kích thích trong anten, bằng cách giải điều biến ASK, ổn định từ trường dòng điện xoay chiều được tinh chế, và cung cấp từ trường dòng điện xoay chiều đến mỗi bộ phận như nguồn điện một chiều. Điện của các sóng điện từ được quá tải từ bộ đọc-bộ ghi 51 được điều chỉnh để tạo ra từ trường để cung cấp nguồn điện cần thiết cho thẻ IC 11.

[0180]

Hơn nữa, bộ phận truyền thông RF 201 giải điều biến các sóng điều biến (các sóng điều biến ASK) được thu qua anten, bằng cách thực hiện việc giải điều biến bao viền, thực hiện giải điều biến khóa dịch vị pha nhị phân (binary phase shift keying, viết tắt là BPSK) trên dữ liệu được giải điều biến, cung cấp dữ liệu kết quả đến CPU 202, và tạo ra tín hiệu đồng hồ có cùng tần số như tần số đồng hồ của tín hiệu thu được, và cung cấp tín hiệu đồng hồ đến CPU 202.

[0181]

Hơn thế nữa, trong trường hợp mà ở đó thông tin định trước được truyền đến bộ đọc-bộ ghi 51, bộ phận truyền thông RF 201 thực hiện việc điều biến ASK của dữ liệu được cung cấp từ CPU 202 và được trải qua điều biến BPSK, dựa vào sự biến thiên về tải của anten, ví dụ, và truyền thành phần điều biến đến bộ đọc-bộ ghi 51 qua anten.

[0182]

CPU 202 là bộ phận điều khiển mà nó điều khiển toàn bộ hoạt động của thẻ IC 11, và thực hiện các loại xử lý khác nhau bằng cách thực hiện các chương trình được lưu trữ trong ROM 203, ví dụ. Các bộ phận lưu trữ từ bộ phận lưu trữ khóa riêng 204 đến bộ phận lưu trữ dữ liệu 206 bao gồm bộ nhớ chỉ đọc có thể lập trình được xóa được bằng điện (electrically erasable programmable read-only memory, viết tắt là EEPROM) hoặc tương tự, ví dụ, và đều dùng làm một phần của vùng lưu trữ của EEPROM.

[0183]

CPU 202 được tạo cấu hình để mã hóa và giải mã dữ liệu dựa vào thuật toán mã hóa xác định trước bằng cách điều khiển bộ phận tính toán mã hóa 207. Dưới đây, thuật toán mã hóa của bộ phận tính toán mã hóa 207 được giả định là cùng thuật toán như thuật toán mã hóa của bộ phận tính toán mã hóa 105, và cũng được giả định là thuật toán mã hóa của phương pháp mã hóa khóa riêng (khóa chung).

[0184]

Trong trường hợp mà ở đó việc mã hóa hoặc việc giải mã dữ liệu được thực hiện trong thẻ IC 11, ví dụ, bởi CPU 202 cung cấp khóa riêng được lưu trữ trong bộ phận lưu trữ khóa riêng 204, đến bộ phận tính toán mã hóa 207 cùng với dữ liệu cần được mã hóa hoặc giải mã, việc mã hóa hoặc việc giải mã dữ liệu được cung cấp mà sử dụng khóa riêng được cung cấp được thực hiện bởi bộ phận tính toán mã hóa 207.

[0185]

Bộ phận lưu trữ ID 205 lưu trữ thẻ ID là thông tin nhận dạng duy nhất đối với thẻ IC 11.

[0186]

Bộ phận lưu trữ dữ liệu 206 lưu trữ dữ liệu ứng dụng để cung cấp các loại dịch vụ khác nhau và tương tự mà cần được thực hiện nhờ sử dụng thẻ IC 11, và tương tự, nếu cần thiết.

[0187]

Lưu ý rằng bộ phận tính toán mã hóa 105 và bộ phận tính toán mã hóa 207 cũng đều có thể được tạo nên như phần mềm.

[0188]

Bộ đọc-bộ ghi 51 và thẻ IC 11 có cấu hình nêu trên.

[0189]

Cần lưu ý rằng, phần mô tả nêu trên đã được đưa ra giả định rằng bộ đọc-bộ ghi 51 và thẻ IC 11 là các thiết bị tách rời, và bộ đọc-bộ ghi 51 thực hiện

sự truyền thông không tiếp xúc với thẻ IC 11 dùng làm thiết bị ngoại vi.

[0190]

Tuy nhiên, ví dụ, tương tự thiết bị đầu cuối di động đã biết như ví dụ động (nhãn hiệu đã được đăng ký) hoặc tương tự, cấu hình mà trong đó các chức năng của bộ đọc-bộ ghi 51 và thẻ IC 11 được bao gồm trong một thiết bị có thể được triển khai. Cụ thể là, như được minh họa trên Fig.16, thiết bị đầu cuối di động 70 bao gồm bộ đọc-bộ ghi 71 có chức năng của bộ đọc-bộ ghi 51, và chip IC 72 có chức năng của thẻ IC 11. Cũng trong trường hợp này, chip IC 72 là thiết bị ngoại vi mà có mặt ở phía bên ngoài khi được nhìn từ bộ đọc-bộ ghi 71. Do đó, thiết bị ngoại vi trong bản mô tả này có thể có mặt trong cùng vỏ.

[0191]

Bộ đọc-bộ ghi 71 và chip IC 72 mà tồn tại bên trong cùng vỏ được kết nối bởi dây dẫn kim loại, thiết bị đầu cuối đầu vào-đầu ra, hoặc tương tự, và lệnh và phản hồi được trao đổi giữa bộ đọc-bộ ghi 71 và chip IC 72 nhờ truyền thông nối dây. Hơn nữa, chip IC 72 cũng có cấu hình của bộ phận truyền thông RF 201 trên Fig.15, và có thể cũng thực hiện sự truyền thông không tiếp xúc với bộ đọc-bộ ghi (thiết bị truyền thông) khác có cấu hình giống như bộ đọc-bộ ghi 51.

[0192]

<Ví dụ cấu hình của thiết bị máy chủ>

Fig.17 là sơ đồ khối minh họa ví dụ cấu hình của thiết bị máy chủ được

sử dụng như mỗi trong số các máy chủ 52 hoặc máy chủ hậu xử lý 53.

[0193]

Trong thiết bị máy chủ 300, bộ xử lý trung tâm (CPU) 301, bộ nhớ chỉ đọc (read only memory, viết tắt là ROM) 302, và bộ nhớ truy cập ngẫu nhiên (random access memory, viết tắt là RAM) 303 được kết nối đến nhau qua bus 304.

[0194]

Giao diện đầu vào-đầu ra 305 còn được kết nối đến bus 304. Bộ phận đầu vào 306, bộ phận đầu ra 307, bộ phận lưu trữ 308, bộ phận truyền thông 309, và ổ đĩa 310 được kết nối đến giao diện đầu vào-đầu ra 305.

[0195]

Bộ phận đầu vào 306 bao gồm bàn phím, chuột, micrô, bảng cảm ứng, thiết bị đầu cuối đầu vào, và tương tự. Bộ phận đầu ra 307 bao gồm màn hình, loa, thiết bị đầu cuối đầu ra, và tương tự. Bộ phận lưu trữ 308 bao gồm đĩa cứng, đĩa RAM, bộ nhớ không khả biến, và tương tự. Bộ phận truyền thông 309 bao gồm giao diện mạng và tương tự. Ổ đĩa 310 điều khiển phương tiện ghi tháo lắp được 311 chẳng hạn như đĩa từ, đĩa quang, đĩa quang từ tính, hoặc bộ nhớ bán dẫn.

[0196]

Trong thiết bị máy chủ 300 có cấu hình nêu trên, trình tự các quy trình nêu trên được thực hiện bởi CPU 301 tải các chương trình được lưu trữ trong, ví

dụ, bộ phận lưu trữ 308, đến RAM 303 qua giao diện đầu vào-đầu ra 305 và bus 304, và thực hiện các chương trình. CPU 301 là bộ phận điều khiển mà nó điều khiển toàn bộ hoạt động của thiết bị máy chủ 300. Hơn nữa, các phần dữ liệu cần thiết để CPU 301 thực hiện các loại xử lý khác nhau, và tương tự cũng được lưu trữ một cách thích hợp trong RAM 303.

[0197]

Trong thiết bị máy chủ 300, các chương trình có thể được thiết đặt trên bộ phận lưu trữ 308 qua giao diện đầu vào-đầu ra 305 bằng cách gắn phương tiện ghi tháo lắp được 311 vào ổ đĩa 310. Hơn nữa, các chương trình có thể được thu qua phương tiện truyền nối dây hoặc không dây chẳng hạn như mạng máy tính cục bộ, Internet, và vệ tinh kỹ thuật số phát rộng bởi bộ phận truyền thông 309 và được thiết đặt trên bộ phận lưu trữ 308. Theo cách khác nữa, chương trình có thể được thiết đặt trước trên ROM 302 và bộ phận lưu trữ 308.

[0198]

Trong bản mô tả này, cần hiểu rằng các bước được mô tả trong các lưu đồ được thực hiện theo thứ tự thời gian phù hợp với thứ tự được mô tả trong một số trường hợp. Trong các trường hợp khác, các bước không cần được xử lý theo thứ tự thời gian, và có thể được thực hiện một cách đồng thời, hoặc được thực hiện tại thời điểm được yêu cầu chẳng hạn như thời điểm khi cuộc gọi được thực hiện, ví dụ.

[0199]

Trong bản mô tả này, hệ thống có nghĩa là tập các thành phần cấu thành

(các thiết bị, các môđun (các bộ phận), và tương tự), và không quan trọng việc tất cả thành phần cấu thành được cung cấp trong cùng vỏ hoặc không. Do đó, các thiết bị được lưu trữ trong các vỏ riêng và được kết nối qua mạng, và một thiết bị mà trong đó các môđun được lưu trữ trong một vỏ đều được coi là các hệ thống.

[0200]

Phương án của sáng chế không bị giới hạn ở phương án nêu trên, và các sự thay đổi khác nhau có thể được thực hiện mà không trệch khỏi phạm vi bảo hộ của sáng chế.

[0201]

Trong ví dụ nêu trên, thẻ IC 11 và bộ đọc-bộ ghi 51 trao đổi dữ liệu định trước nhờ truyền thông tầm gần (sự truyền thông không tiếp xúc) phù hợp với chuẩn ISO/IEC 14443 hoặc chuẩn ISO/IEC 18092, tuy nhiên kỹ thuật truyền thông khác với các cách trên có thể được sử dụng.

[0202]

Ví dụ, chế độ bao gồm chỉ một phần chức năng của phương án nêu trên có thể được triển khai.

[0203]

Ví dụ, sáng chế có thể triển khai cấu hình của điện toán đám mây mà trong đó một chức năng được dùng chung bởi các thiết bị và được xử lý kết hợp với nhau, qua mạng.

[0204]

Hơn nữa, thay vì được thực hiện trong một thiết bị, mỗi bước được mô tả trong các lưu đồ được mô tả ở trên có thể được thực hiện bởi các thiết bị theo cách được dùng chung.

[0205]

Hơn thế nữa, trong trường hợp mà ở đó các xử lý được bao gồm trong một bước, các xử lý được bao gồm trong một bước có thể được thực hiện bởi các thiết bị theo cách được dùng chung, thay vì được thực hiện trong một thiết bị.

[0206]

Lưu ý rằng các hiệu quả được mô tả trong bản mô tả này chỉ là các ví dụ, và không bị giới hạn, và các hiệu quả khác các hiệu quả được mô tả trong bản mô tả này có thể được tạo ra.

[0207]

Lưu ý rằng sáng chế cũng có thể triển khai các cấu hình dưới đây.

(1) Thiết bị truyền thông bao gồm:

bộ phận truyền thông được tạo cấu hình để truyền yêu cầu định trước đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thiết bị ngoại vi, và thu phản hồi tới yêu cầu từ các máy chủ; và

bộ phận điều khiển được tạo cấu hình để thực hiện việc xử lý tiếp theo dựa vào phản hồi của một trong số các máy chủ, phản hồi đã thu được sớm nhất.

(2) Thiết bị truyền thông theo điểm (1) nêu trên,

trong đó bộ phận truyền thông truyền thông tin được bao gồm trong phản hồi của máy chủ, phản hồi đã thu được sớm nhất, đến các máy chủ.

(3) Thiết bị truyền thông theo điểm (2) nêu trên,

trong đó thông tin được bao gồm trong phản hồi của máy chủ, phản hồi đã thu được sớm nhất, được mã hóa nhờ sử dụng khóa không thể giải mã được bởi thiết bị truyền thông, và

bộ phận truyền thông truyền thông tin được mã hóa nhờ sử dụng khóa, đến các máy chủ.

(4) Thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ (1) đến (3) nêu trên,

trong đó bộ phận truyền thông thu yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi, và truyền yêu cầu ngẫu nhiên, và kết quả tính toán của yêu cầu ngẫu nhiên mà đã thu được từ thiết bị ngoại vi, đến các máy chủ.

(5) Thiết bị truyền thông theo điểm (4) nêu trên,

trong đó yêu cầu ngẫu nhiên được gán ký hiệu số.

(6) Thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ (1) đến (3) nêu trên,

trong đó bộ phận truyền thông thu yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi, và thông tin nhận dạng giao tác để nhận dạng giao tác, và truyền yêu cầu ngẫu nhiên và thông tin nhận dạng giao tác, và kết quả tính toán của yêu cầu ngẫu nhiên mà đã thu được từ thiết bị ngoại vi, đến các máy chủ.

(7) Thiết bị truyền thông theo điểm (6) nêu trên,

trong đó yêu cầu ngẫu nhiên và thông tin nhận dạng giao tác được gán các ký hiệu số.

(8) Thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ (1) đến (3) nêu trên,

trong đó bộ phận truyền thông thu yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi, và thông tin khoảng thời gian hiệu lực chỉ báo khoảng thời gian hiệu lực của yêu cầu ngẫu nhiên, và truyền yêu cầu ngẫu nhiên và thông tin khoảng thời gian hiệu lực, và kết quả tính toán của yêu cầu ngẫu nhiên mà đã thu được từ thiết bị ngoại vi, đến các máy chủ.

(9) Thiết bị truyền thông theo điểm (8) nêu trên,

trong đó yêu cầu ngẫu nhiên và thông tin khoảng thời gian hiệu lực được gán các ký hiệu số.

(10) Thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ (1) đến (9) nêu trên, thiết bị còn bao gồm

bộ phận truyền thông không tiếp xúc được tạo cấu hình để truyền lệnh đến thiết bị ngoại vi nhờ truyền thông không tiếp xúc.

(11) Thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ (1) đến (9) nêu trên, thiết bị còn bao gồm

bộ phận truyền thông nối dây được tạo cấu hình để truyền lệnh đến thiết bị ngoại vi nhờ truyền thông nối dây.

(12) Thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ (1) đến (11) nêu trên,

trong đó bộ phận điều khiển quyết định hai máy chủ trở lên mà yêu cầu cần được truyền đến, từ trong số các máy chủ, và

bộ phận truyền thông truyền yêu cầu đến hai máy chủ trở lên được quyết định bởi bộ phận điều khiển.

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

bộ phận truyền thông được tạo cấu hình để thu yêu cầu định trước từ thiết bị truyền thông được tạo cấu hình để truyền lệnh đến thiết bị ngoại vi, và truyền phản hồi bao gồm kết quả xử lý của việc xử lý được thực hiện đáp lại yêu cầu, đến thiết bị truyền thông; và

bộ phận điều khiển được tạo cấu hình để thực hiện việc xử lý,

trong đó kết quả xử lý được bao gồm trong phản hồi được mã hóa nhờ sử dụng khóa không thể giải mã được bởi thiết bị truyền thông.

(14) Thiết bị xử lý thông tin theo điểm (13) nêu trên,

trong đó bộ phận truyền thông còn truyền thông tin được yêu cầu cho việc xử lý của toàn bộ giao tác, đến thiết bị xử lý thông tin khác, dựa vào kết quả thực hiện của việc xử lý.

(15) Thiết bị xử lý thông tin theo điểm (13) hoặc điểm (14) nêu trên,

trong đó bộ phận truyền thông còn truyền yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi đến thiết bị truyền thông, và

bộ phận điều khiển còn thực hiện việc xử lý tạo ra yêu cầu ngẫu nhiên.

(16) Thiết bị xử lý thông tin theo điểm bất kỳ trong số các điểm từ (13) đến (15) nêu trên,

trong đó bộ phận truyền thông thu kết quả tính toán của yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi mà nhận được bởi thiết bị ngoại vi, từ thiết bị truyền thông cùng với yêu cầu ngẫu nhiên,

bộ phận điều khiển thực hiện việc xử lý xác thực dựa vào kết quả tính toán của yêu cầu ngẫu nhiên, và

bộ phận truyền thông truyền kết quả xử lý của việc xử lý xác thực và yêu cầu ngẫu nhiên đến thiết bị xử lý thông tin khác.

(17) Thiết bị xử lý thông tin theo điểm (15) hoặc điểm (16) nêu trên,

trong đó yêu cầu ngẫu nhiên được gán ký hiệu số.

(18) Thiết bị xử lý thông tin theo điểm (13) hoặc điểm (14) nêu trên,

trong đó bộ phận truyền thông còn truyền yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi, và thông tin nhận dạng giao tác để nhận dạng giao tác, đến thiết bị truyền thông, và

bộ phận điều khiển còn thực hiện việc xử lý tạo ra yêu cầu ngẫu nhiên và thông tin nhận dạng giao tác.

(19) Thiết bị xử lý thông tin theo điểm (13) hoặc điểm (18) nêu trên,

trong đó bộ phận truyền thông thu kết quả tính toán của yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi mà nhận được bởi thiết bị ngoại vi,

yêu cầu ngẫu nhiên, và thông tin nhận dạng giao tác để nhận dạng giao tác, từ thiết bị truyền thông,

bộ phận điều khiển thực hiện việc xử lý xác thực dựa vào kết quả tính toán của yêu cầu ngẫu nhiên, và

bộ phận truyền thông truyền kết quả xử lý của việc xử lý xác thực và thông tin nhận dạng giao tác đến thiết bị xử lý thông tin khác.

(20) Thiết bị xử lý thông tin theo điểm (18) hoặc điểm (19) nêu trên,

trong đó yêu cầu ngẫu nhiên và thông tin nhận dạng giao tác được gán các ký hiệu số.

(21) Thiết bị xử lý thông tin theo điểm (13) hoặc điểm (14) nêu trên,

trong đó bộ phận truyền thông còn truyền yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi, và thông tin khoảng thời gian hiệu lực chỉ báo khoảng thời gian hiệu lực của yêu cầu ngẫu nhiên, đến thiết bị truyền thông, và

bộ phận điều khiển còn thực hiện việc xử lý tạo ra yêu cầu ngẫu nhiên và thiết đặt khoảng thời gian hiệu lực.

(22) Thiết bị xử lý thông tin theo điểm (13) hoặc điểm (14) nêu trên,

trong đó bộ phận truyền thông thu kết quả tính toán của yêu cầu ngẫu nhiên theo phương pháp phản hồi đòi hỏi mà nhận được bởi thiết bị ngoại vi, yêu cầu ngẫu nhiên, và thông tin khoảng thời gian hiệu lực chỉ báo khoảng thời gian hiệu lực của yêu cầu ngẫu nhiên, từ thiết bị truyền thông, và

bộ phận điều khiển thực hiện việc xử lý xác thực dựa vào kết quả tính

toán của yêu cầu ngẫu nhiên, trong trường hợp mà ở đó khoảng thời gian hiệu lực có hiệu lực.

(23) Thiết bị xử lý thông tin theo điểm (21) hoặc điểm (22) nêu trên, trong đó yêu cầu ngẫu nhiên và thông tin khoảng thời gian hiệu lực được gán các ký hiệu số.

(24) Hệ thống xử lý dữ liệu bao gồm:

thiết bị truyền thông; và

các máy chủ,

trong đó thiết bị truyền thông bao gồm

bộ phận truyền thông thứ nhất được tạo cấu hình để truyền yêu cầu định trước đến các máy chủ dựa vào kết quả nhận được bằng cách truyền lệnh đến thiết bị ngoại vi, và thu phản hồi tới yêu cầu từ các máy chủ, và

bộ phận điều khiển thứ nhất được tạo cấu hình để thực hiện việc xử lý tiếp theo dựa vào phản hồi của một trong số các máy chủ, phản hồi đã thu được sớm nhất, và

mỗi trong số các máy chủ bao gồm

bộ phận truyền thông thứ hai được tạo cấu hình để thu yêu cầu từ thiết bị truyền thông và truyền phản hồi đến thiết bị truyền thông, và

bộ phận điều khiển thứ hai được tạo cấu hình để thực hiện việc xử lý để trả lời đến yêu cầu như là phản hồi.

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

bộ phận truyền thông được tạo cấu hình để thu kết quả xử lý của việc xử lý xác thực được thực hiện trên thiết bị ngoại vi, và thông tin nhận dạng việc xử lý để nhận dạng việc xử lý, từ các thiết bị xử lý thông tin khác; và

bộ phận điều khiển được tạo cấu hình để thực hiện việc xử lý liên quan đến các kết quả xử lý có cùng thông tin nhận dạng việc xử lý đã được thu từ các thiết bị xử lý thông tin khác, như cùng kết quả xử lý xác thực.

(26) Thiết bị xử lý thông tin theo điểm (25) nêu trên,

trong đó bộ phận truyền thông còn thu thông tin cần cho việc xử lý của toàn bộ giao tác, từ các thiết bị xử lý thông tin khác, và

bộ phận điều khiển xác định kết quả của toàn bộ giao tác dựa vào thông tin được yêu cầu cho việc xử lý của toàn bộ giao tác.

Danh mục các số chỉ dẫn

[0208]

- 11 Thẻ IC
- 40 Hệ thống xử lý dữ liệu
- 51 Bộ đọc-bộ ghi
- 52A Máy chủ thứ nhất
- 52B Máy chủ thứ hai

|     |                           |
|-----|---------------------------|
| 52C | Máy chủ thứ ba            |
| 53  | Máy chủ hậu xử lý         |
| 70  | Thiết bị đầu cuối di động |
| 70  | Bộ đọc-bộ ghi             |
| 72  | Chip IC                   |
| 101 | Bộ phận truyền thông RF   |
| 102 | CPU                       |
| 107 | Bộ phận truyền thông      |
| 201 | Bộ phận truyền thông RF   |
| 300 | Thiết bị máy chủ          |
| 301 | CPU                       |
| 302 | ROM                       |
| 303 | RAM                       |
| 306 | Bộ phận đầu vào           |
| 307 | Bộ phận đầu ra            |
| 308 | Bộ phận lưu trữ           |
| 309 | Bộ phận truyền thông      |
| 310 | Ổ đĩa                     |

## YÊU CẦU BẢO HỘ

### 1. Thiết bị truyền thông (51) bao gồm:

bộ phận truyền thông (107) được tạo cấu hình để truyền lệnh đến thiết bị ngoại vi, truyền yêu cầu định trước đến các máy chủ (52) trên cơ sở kết quả thu được bằng cách truyền lệnh đến thiết bị ngoại vi (11), và thu phản hồi đối với yêu cầu từ các máy chủ; và

bộ phận điều khiển (102) được tạo cấu hình để thực hiện quy trình xử lý tiếp theo trên cơ sở phản hồi của một trong các máy chủ, phản hồi đã được thu sớm nhất;

trong đó bộ phận truyền thông truyền thông tin được bao gồm trong phản hồi của máy chủ, phản hồi đã được thu sớm nhất, đến các máy chủ.

### 2. Thiết bị truyền thông theo điểm 1, trong đó thông tin được bao gồm trong phản hồi của máy chủ, phản hồi đã được thu sớm nhất, được mã hóa sử dụng khóa không giải mã được bởi thiết bị truyền thông, và

bộ phận truyền thông truyền thông tin được mã hóa sử dụng khóa, đến các máy chủ.

### 3. Thiết bị truyền thông theo điểm 1 hoặc điểm 2,

trong đó bộ phận truyền thông thu thử thách ngẫu nhiên trong phương pháp phản hồi thử thách, và truyền thử thách ngẫu nhiên, và kết quả tính toán của thử thách ngẫu nhiên mà đã được thu từ thiết bị ngoại vi, đến các máy chủ.

### 4. Thiết bị truyền thông theo điểm 3, trong đó bộ phận truyền thông cũng thu một trong số thông tin nhận dạng giao tác để nhận dạng giao tác, và thông tin khoảng thời gian hiệu lực chỉ báo khoảng thời gian hiệu lực của thử thách ngẫu nhiên, và truyền một trong số thông tin nhận dạng giao tác, thông tin khoảng thời gian hiệu lực đến các máy chủ.

### 5. Hệ thống xử lý dữ liệu bao gồm:

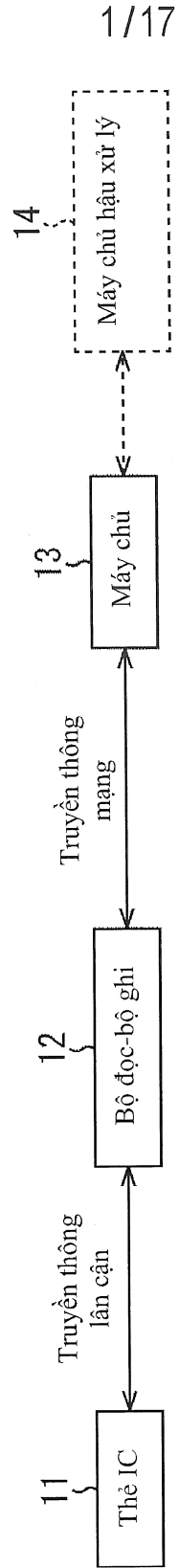
thiết bị truyền thông theo điểm bất kỳ trong số các điểm từ 1 đến 4, và các máy chủ (52A, 52B, 52C), trong đó mỗi trong số các máy chủ bao gồm bộ phận truyền thông thứ hai (309) được tạo cấu hình để thu yêu cầu từ thiết bị truyền

thông và truyền phản hồi bao gồm kết quả xử lý của việc xử lý được thực hiện phản hồi lại yêu cầu, đến thiết bị truyền thông, và

bộ phận điều khiển thứ hai (301) được tạo cấu hình để thực hiện quy trình xử lý, và

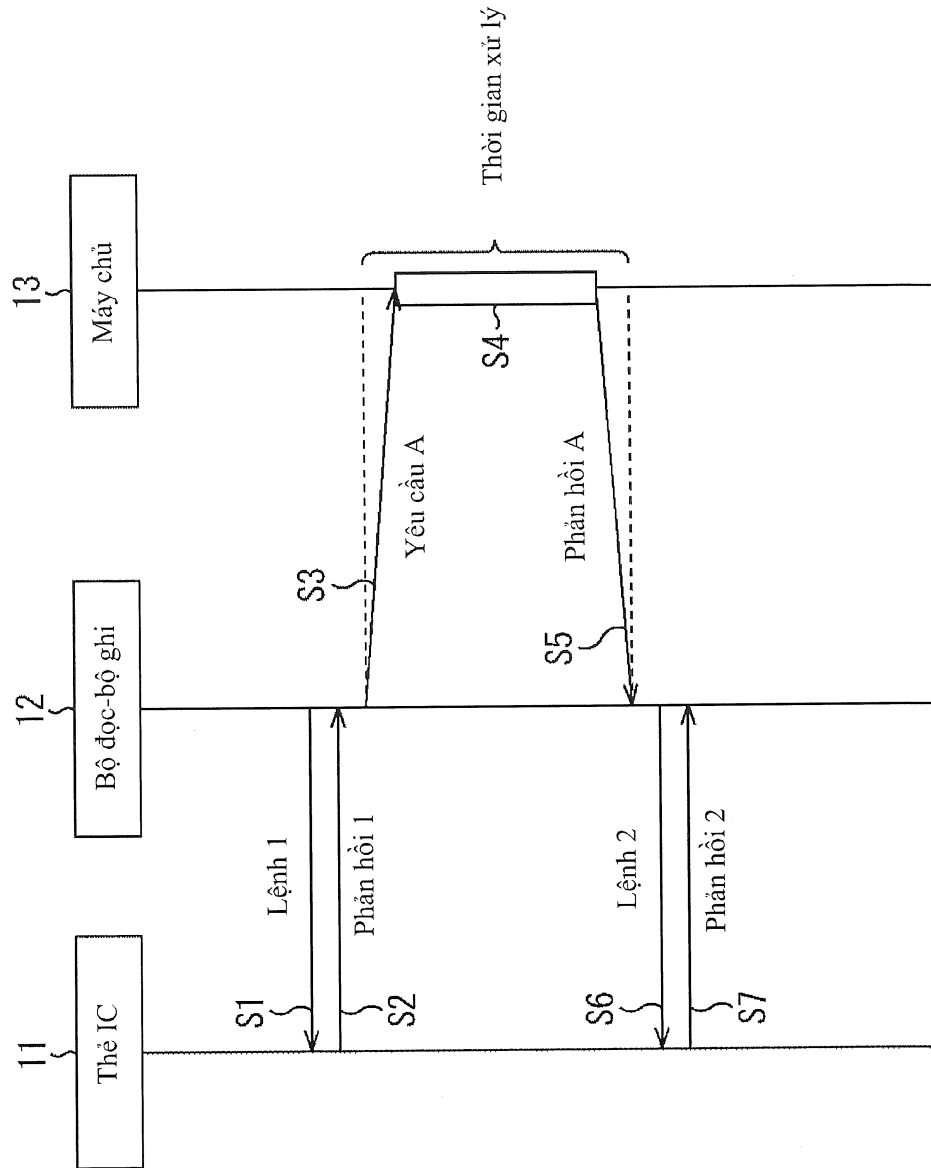
kết quả xử lý được bao gồm trong phản hồi được mã hóa nhờ sử dụng khóa không giải mã được bởi thiết bị truyền thông.

FIG. 1



2/17

FIG. 2



3/17

FIG. 3

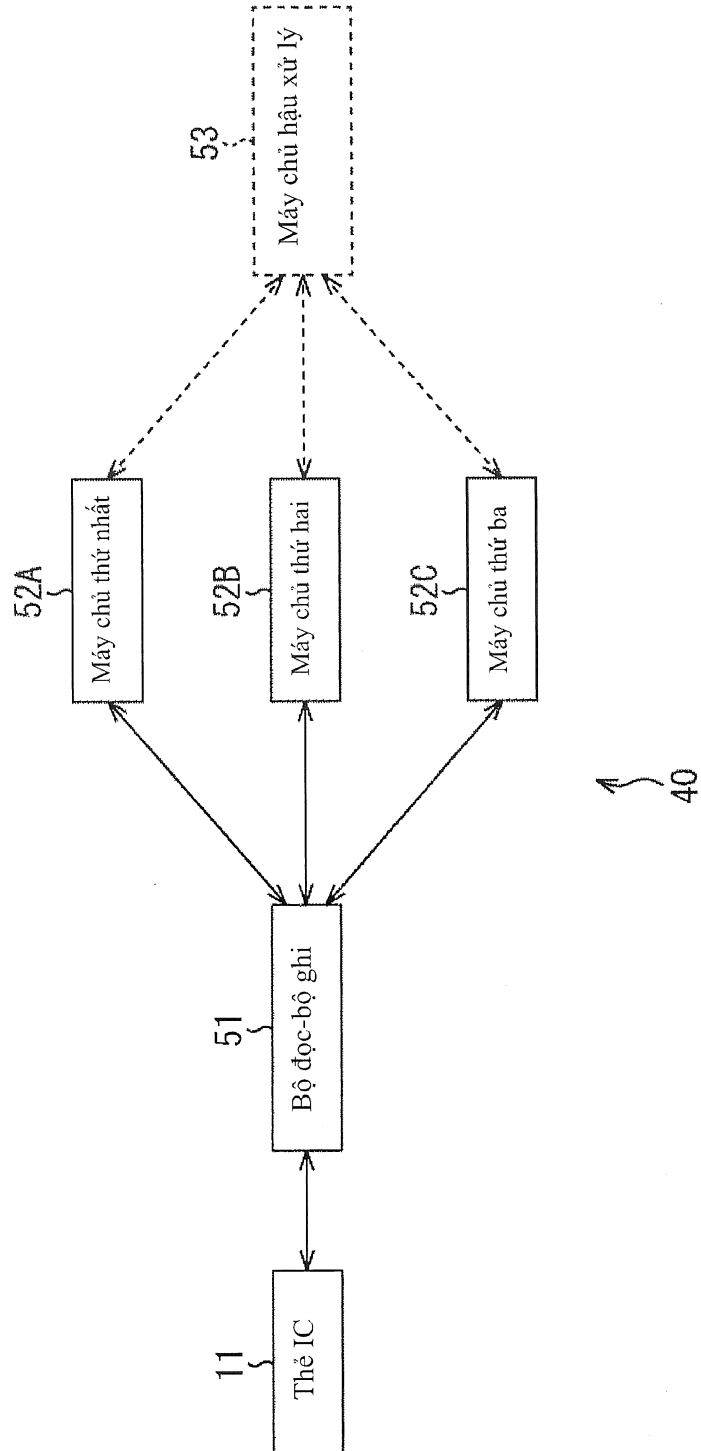
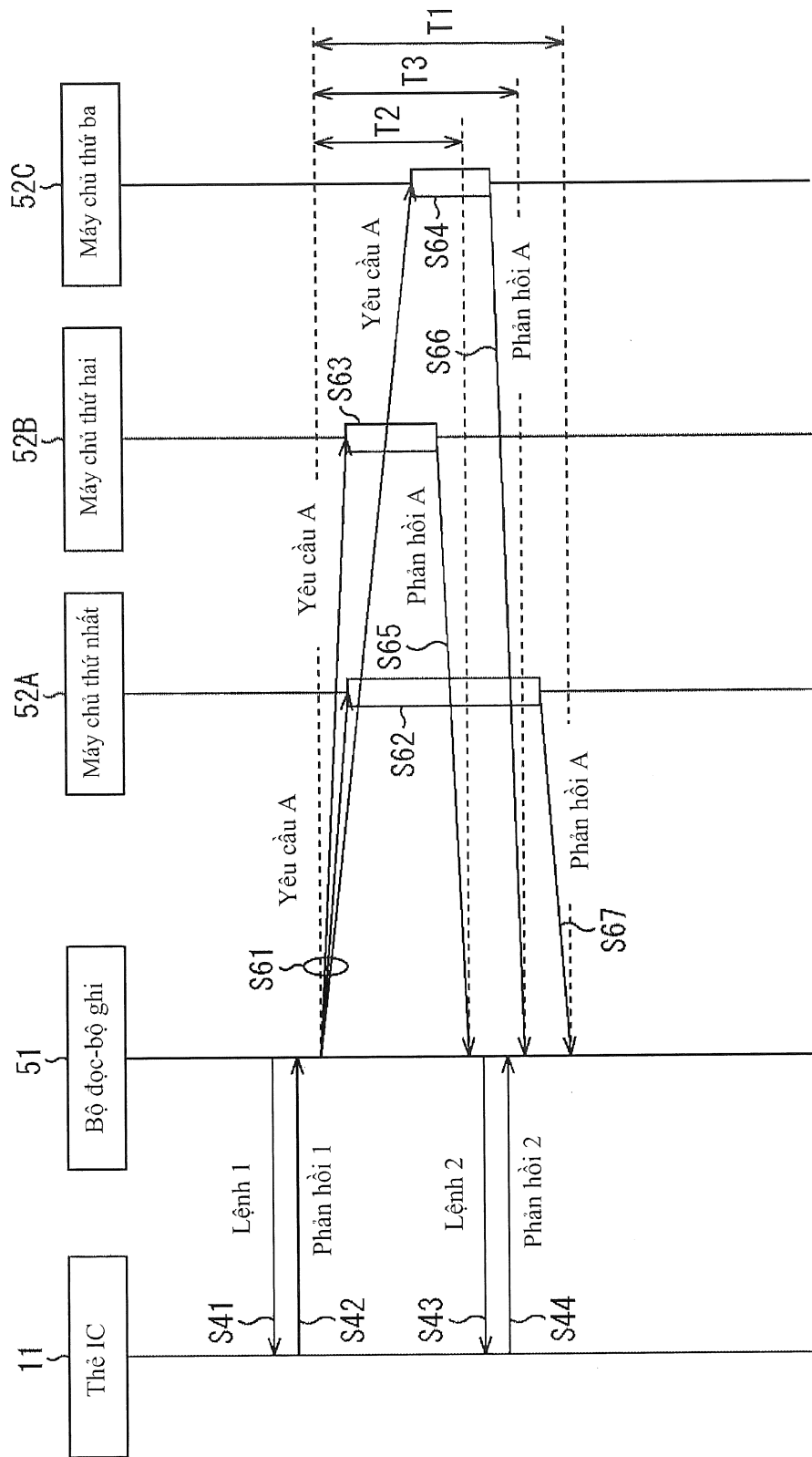
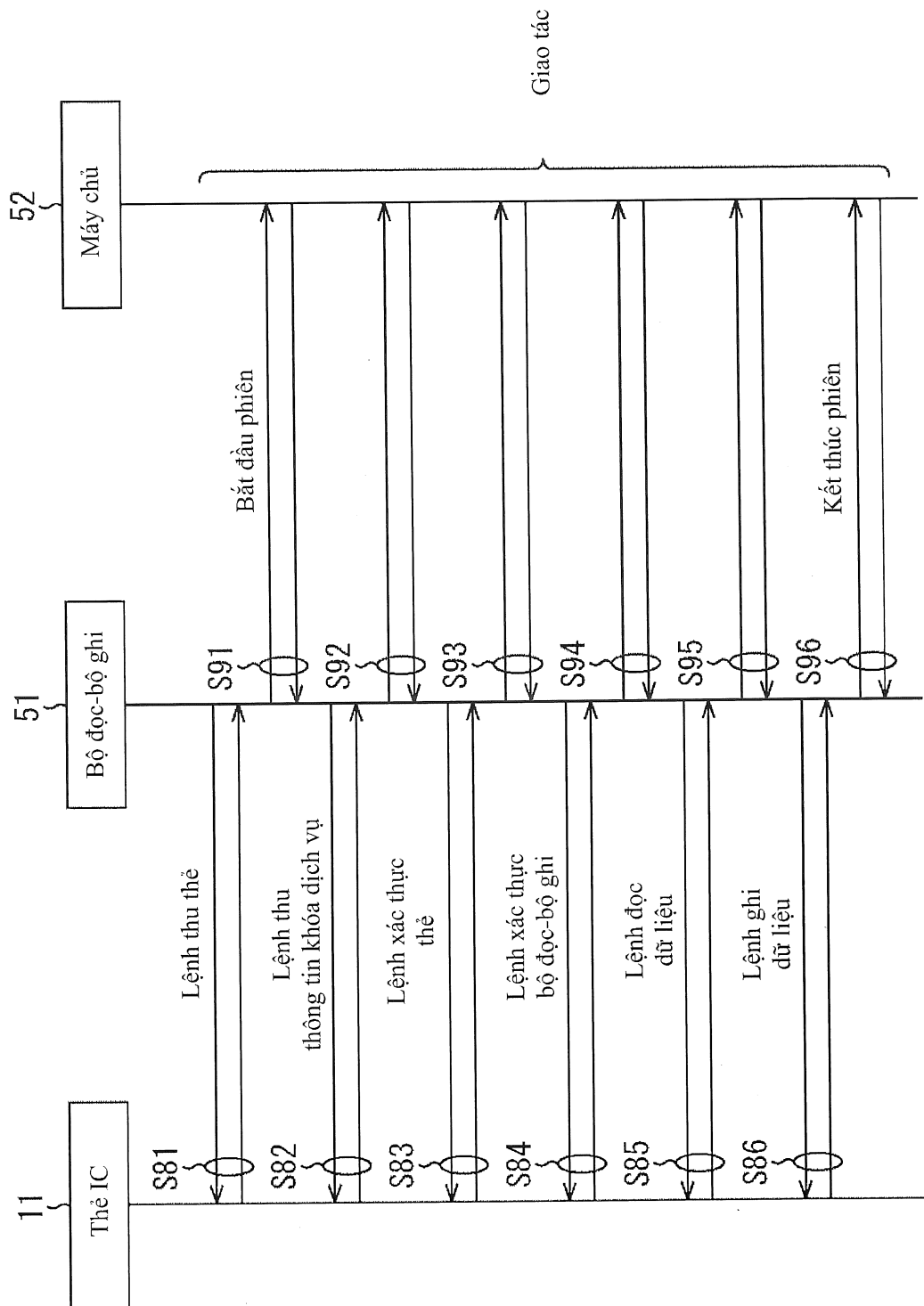


FIG. 4



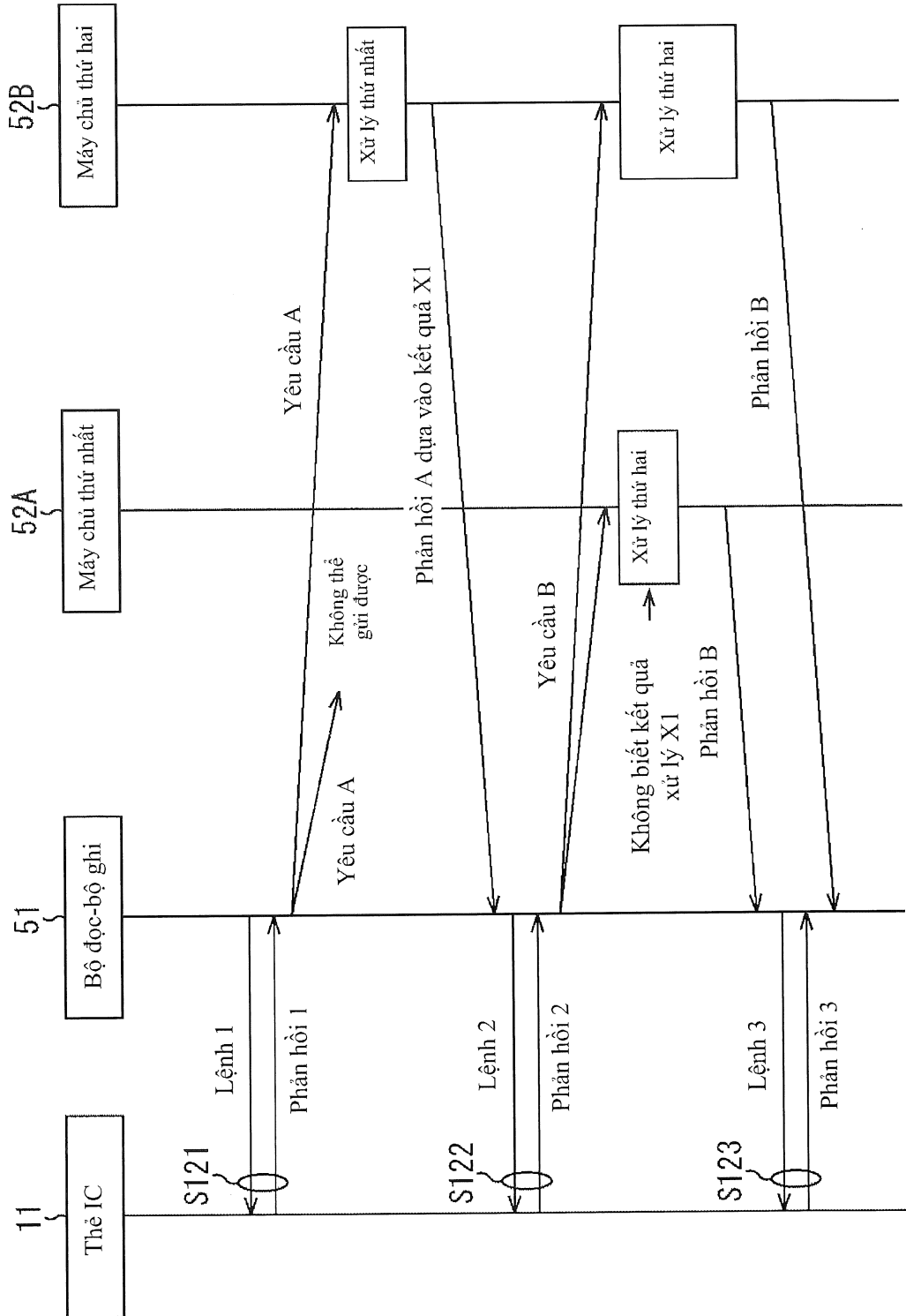
5/17

FIG. 5



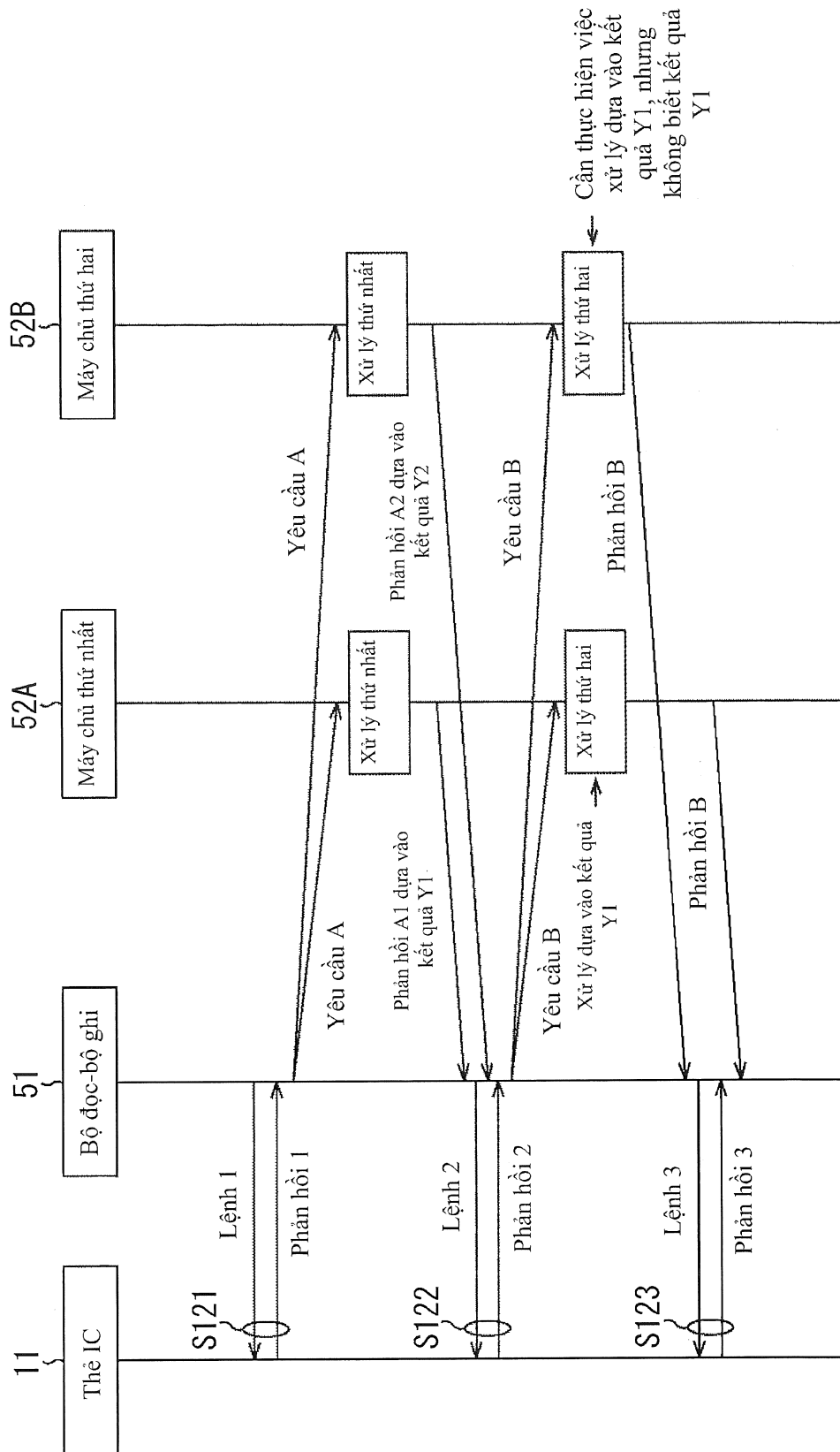
6/17

FIG. 6



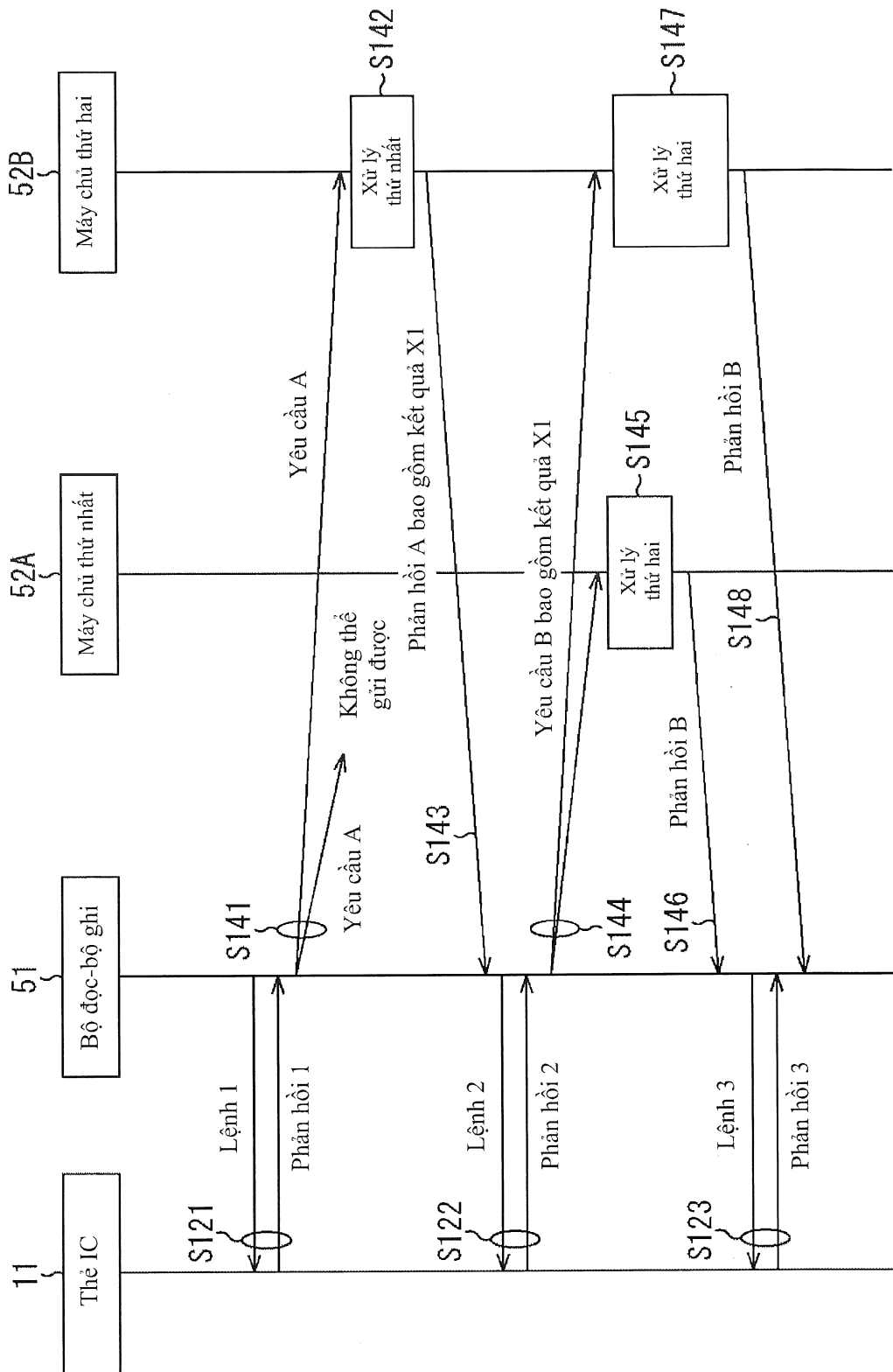
7/17

FIG. 7



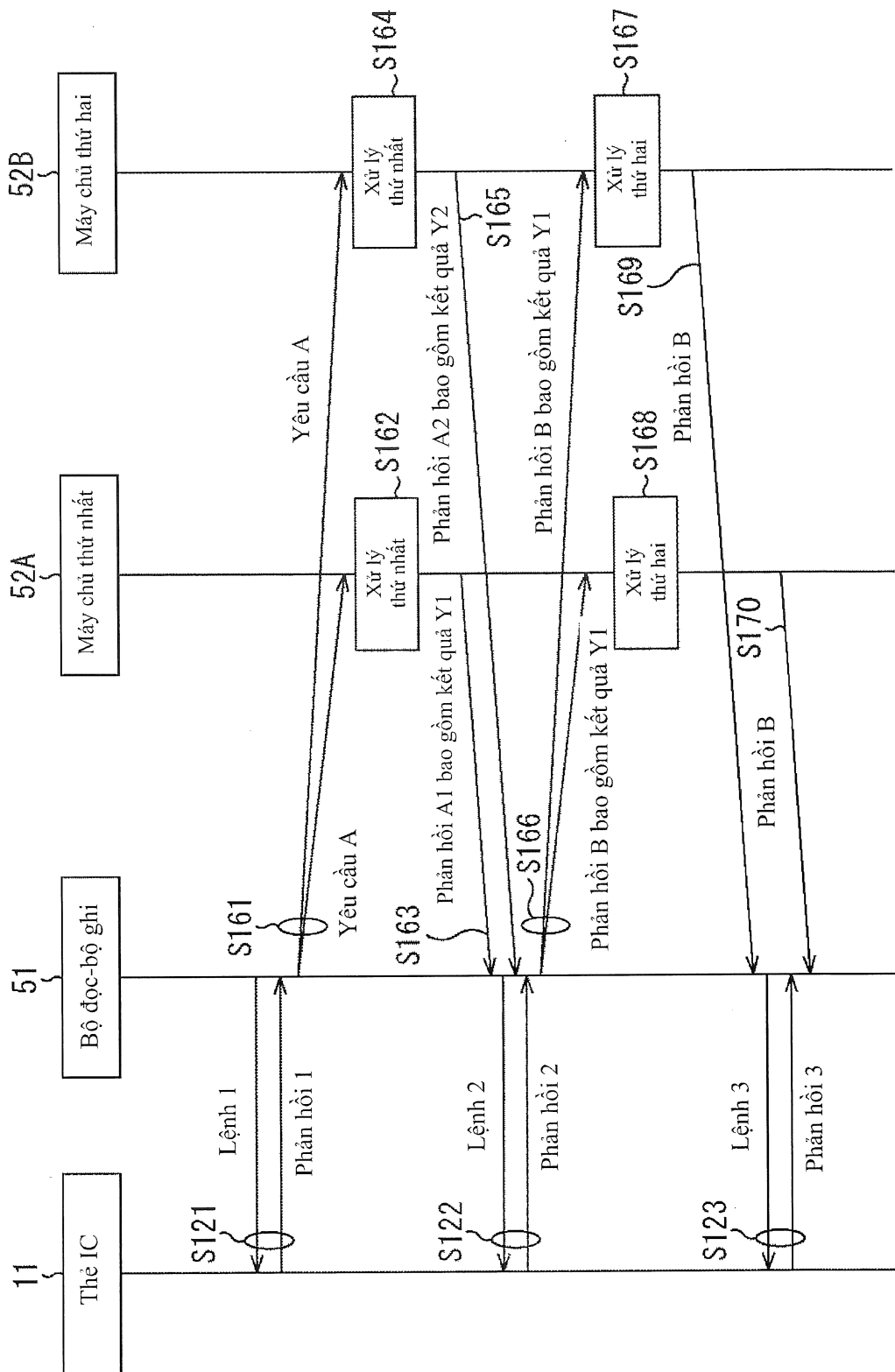
8/17

FIG. 8



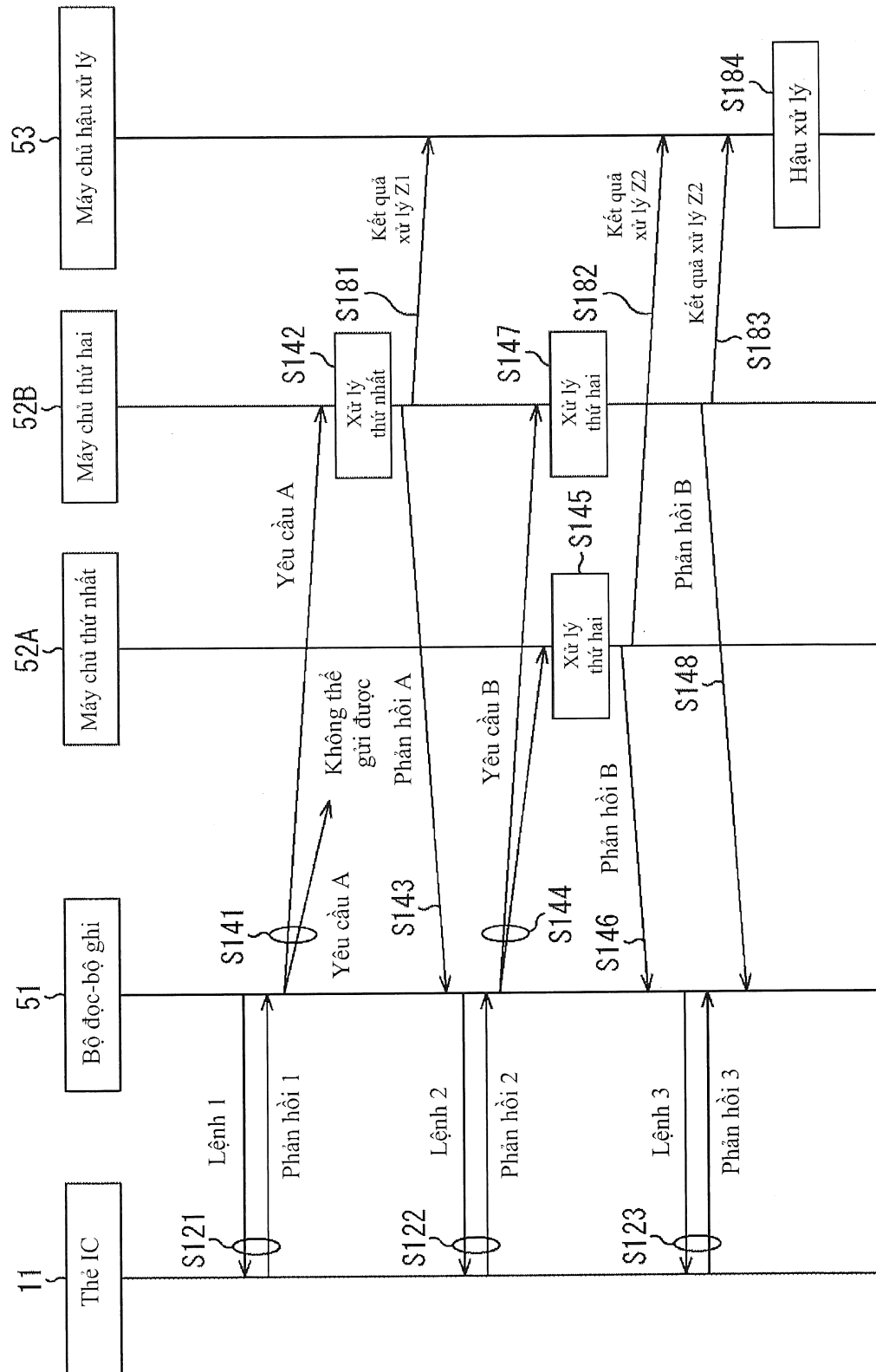
9/17

FIG. 9



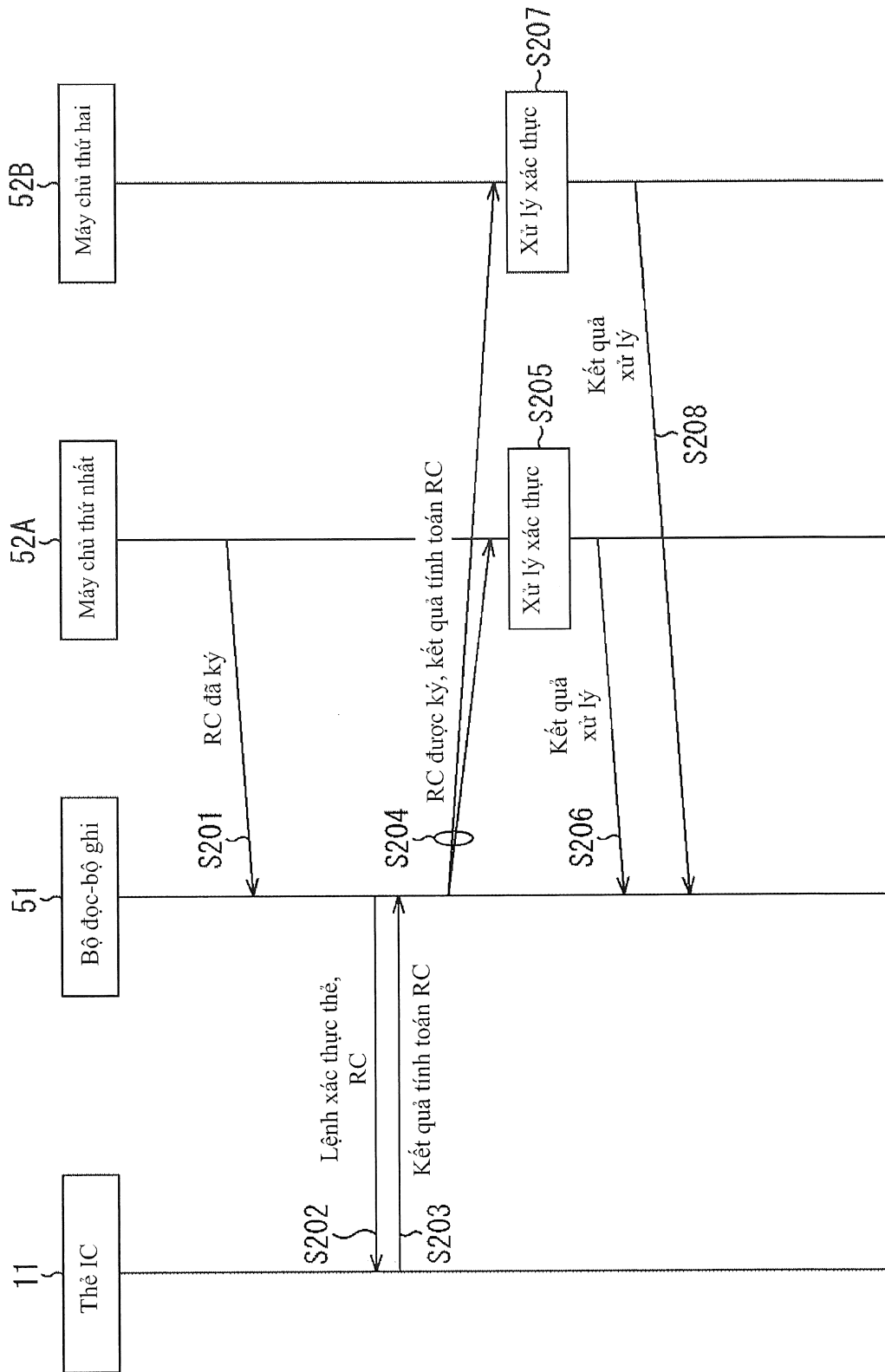
10/17

FIG. 10



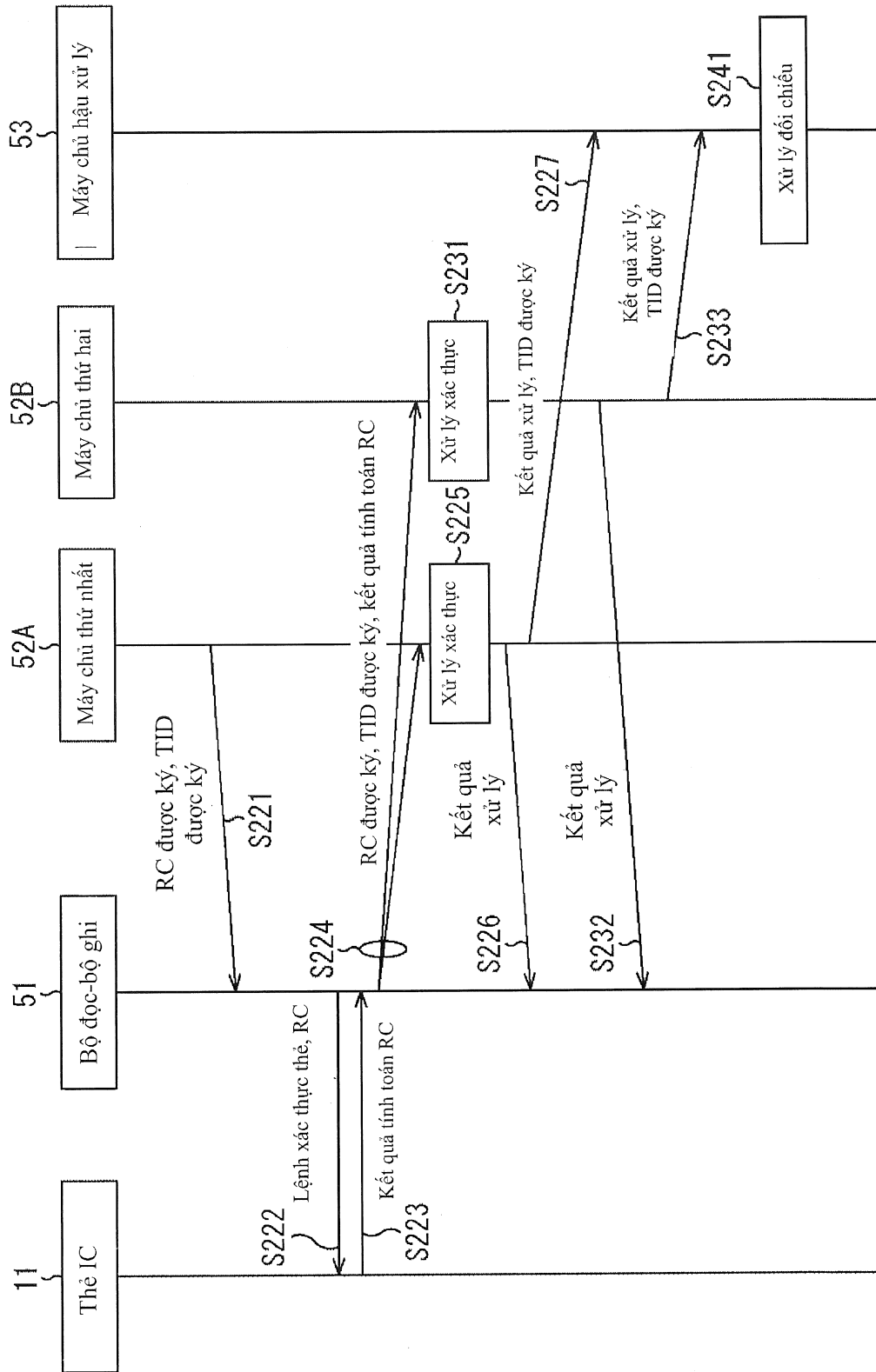
11/17

FIG. 11



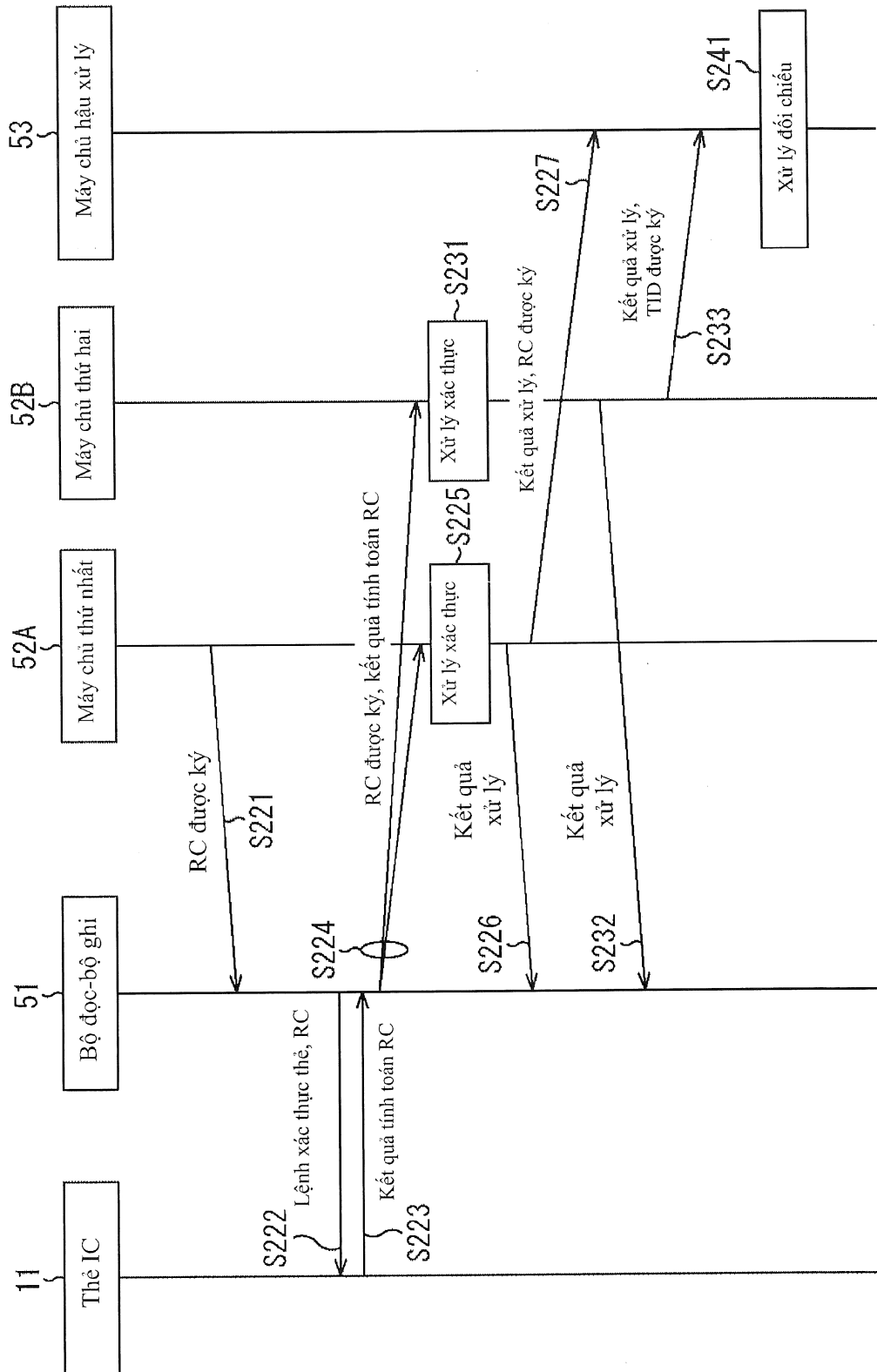
12/17

FIG. 12



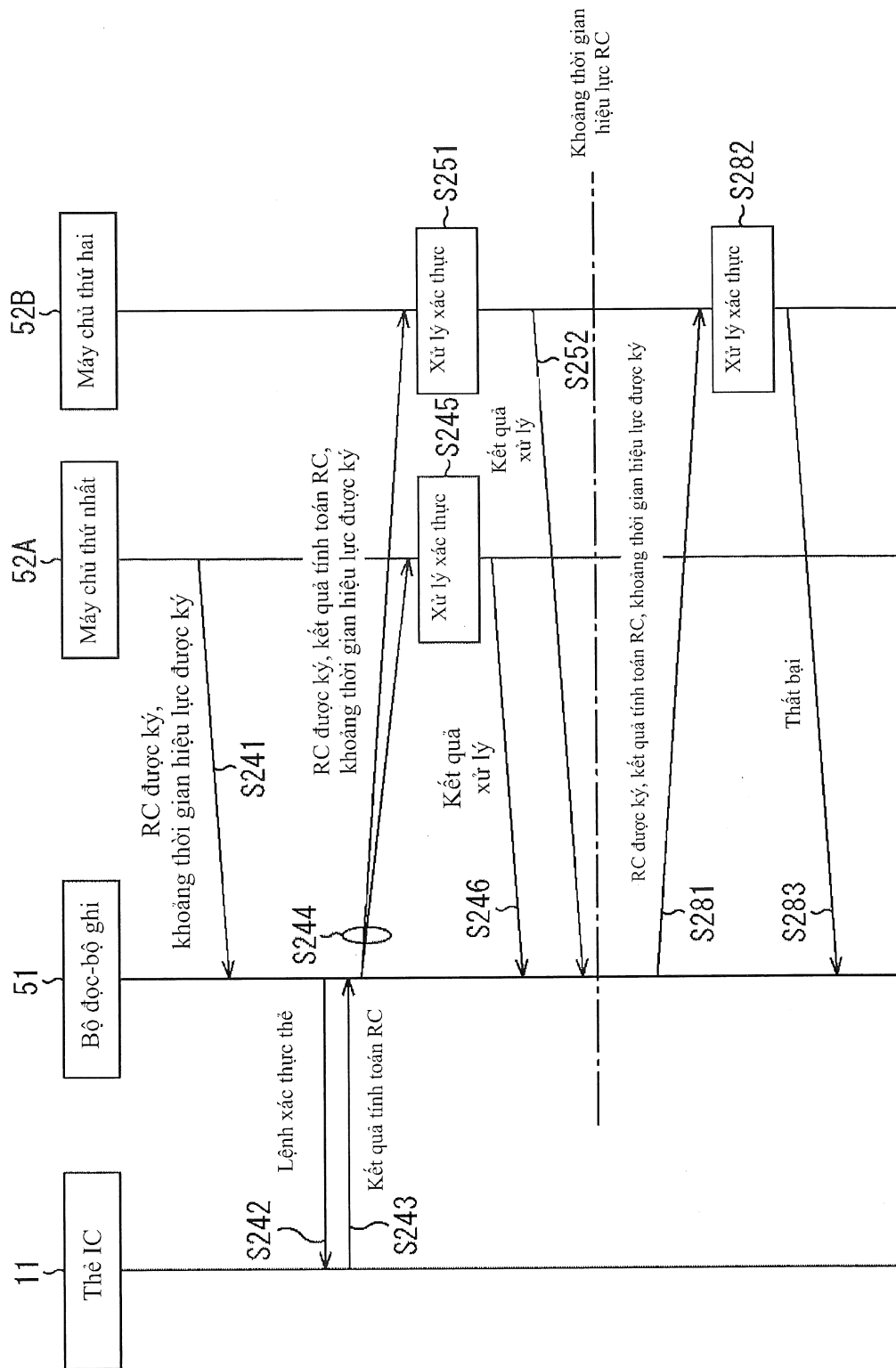
13/17

FIG. 13



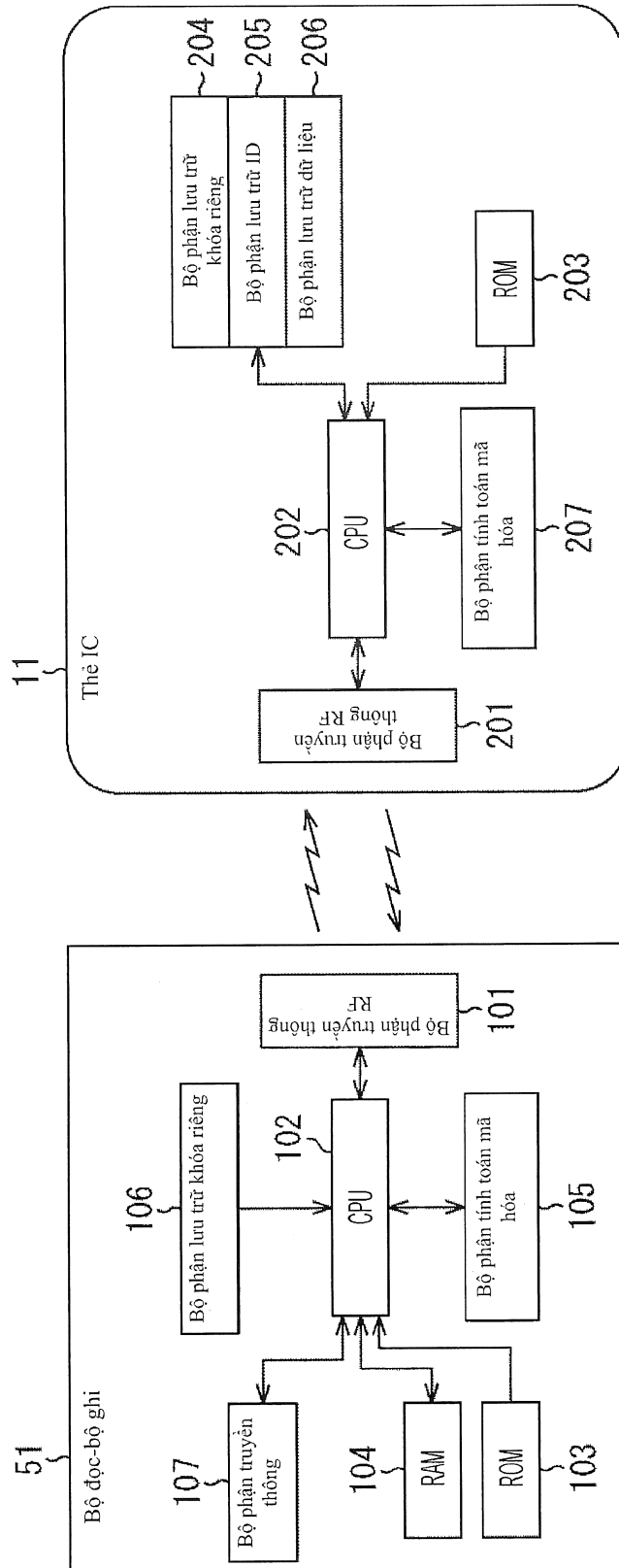
14/17

FIG. 14

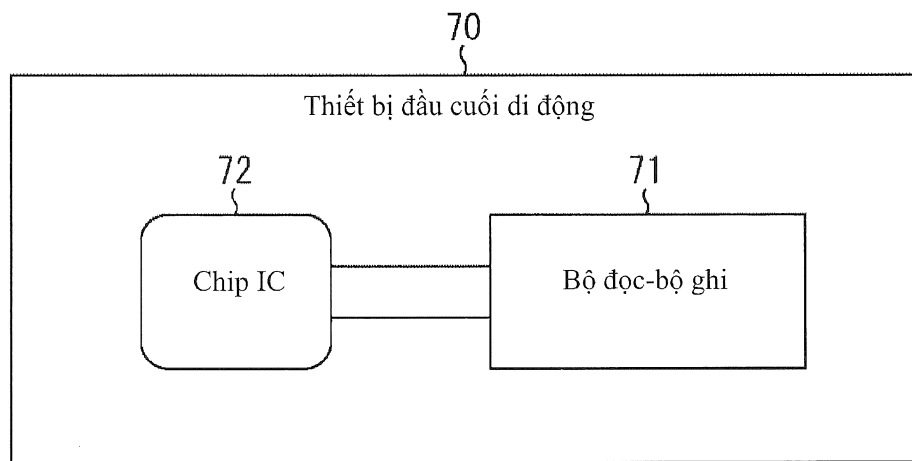


15/17

FIG. 15



16/17

*FIG. 16*

17/17

FIG. 17

