República Federativa do Brasil
Ministério do Desenvolvimento, Indústria e do Comércio Exterior
Instituto Nacional da Propriedade Industrial

(21) **PI 1003590-7 A2**

BRPI1003590A2

(22) Data de Depósito: 17/09/2010
(43) Data da Publicação: 08/01/2013
(RPI 2192)

(51) Int.Cl.:
G07F 7/10

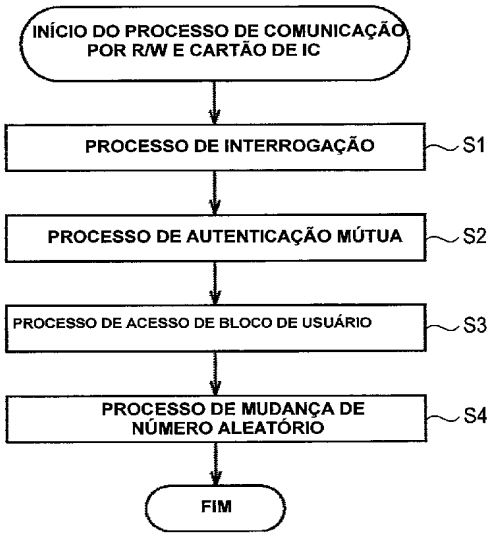
(54) Título: APARELHOS DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO PARA OPERAR UM APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, E, INSTRUÇÕES DE ARMAZENAMENTO DE DISPOSITIVO DE MEMÓRIA LEGÍVEL POR COMPUTADOR

(30) Prioridade Unionista: 25/09/2009 JP 2009-221300

(73) Titular(es): Sony Corporation

(72) Inventor(es): Mitsuhiro Nakamura, Toshimitsu Higashikawa, Yasumasa Nakatsugawa, Yinglin Zhu

(57) Resumo: APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO PARA OPERAR UM APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, E, INSTRUÇÕES DE ARMAZENAMENTO DE DISPOSITIVO DE MEMÓRIA LEGÍVEL POR COMPUTADOR. Em uma forma de realização exemplo, um aparelho de processamento de informação determina se uma ID alvo é uma ID única ou uma ID de aleatorização parcial, que inclui uma primeira parte sendo substituida por um diferente número e uma segunda parte sendo gerada com base na ID única. Em resposta à ID alvo sendo a ID de aleatorização parcial, o aparelho de processamento de informação gera uma chave de acesso com base na segunda parte da ID de aleatorização parcial e numa chave. O aparelho de processamento de informação executa um processo de autenticação mútua, usando a chave de acesso gerada.



"APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO PARA OPERAR UM APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, E, INSTRUÇÕES DE ARMAZENAMENTO DE DISPOSITIVO DE MEMÓRIA LEGÍVEL POR COMPUTADOR"

REFERÊNCIA A PEDIDOS RELACIONADOS

O presente pedido reivindica prioridade ao Pedido de Patente Japonesa No. JP 2009-221300, depositado no Escritório de Patente Japonês em 25 de setembro de 2009, cujo inteiro conteúdo está sendo incorporado aqui por referência.

FUNDAMENTOS

Na técnica relacionada, sistemas de comunicação sem-contato, representados por FeliCa (marca registrada da Sony Corporation) estão sendo amplamente sendo supridos.

O sistema de comunicação sem-contato inclui uma leitora/gravadora (a seguir abreviada como R/W) e um cartão de IC de comunicação sem contato (a seguir abreviado cartão de IC). O sistema de comunicação sem contato transmite informação usando ondas eletromagnéticas entre a R/W e o cartão de IC em um tipo sem contato. Antes de vários tipos de informação serem transmitidos, um processo mútuo de autenticação é executado. Em lugar do cartão de IC, um telefone móvel ou similar é usado, em que um chip IC, tendo a mesma função que o cartão de IC, foi construído.

Por exemplo, informação referente a uma pluralidade de serviços, tais como um serviço de dinheiro eletrônico, um serviço de bilhete de comutação para um trem elétrico ou similar e um serviço de cartão ID de empregado é capaz de ser montado no cartão de IC.

O direito de acesso ou método de acesso para dados de usuário dentro do cartão de IC é controlado em uma unidade de serviço. Há uma chave pela qual os dados do usuário para cada serviço são acessados. O

direito de acesso aos dados do usuário correspondendo a um serviço T9 é controlado pela chave acima descrita. Para cada serviço, um método de acesso é prescrito para uso em um método de gravação de dados de história ou um método de subtração de dinheiro eletrônico.

Para uma vez executar um processo de gravação de dados de história e um processo de subtração de dinheiro, é gerada uma chave (chave degenerada) das chaves de uma pluralidade de serviços. É possível acessar a pluralidade de serviços por um processo de autenticação mútuo usando-se a chave degenerada. A este respeito, é possível ter-se acesso executando-se um processo de autenticação mútuo, usando-se uma chave mantida para cada serviço, mesmo em serviços individuais.

A este respeito, um processo de autenticação mútua para cada serviço é necessário para utilizar uma pluralidade de diferentes serviços, isto é, para acessar informação referente a cada serviço. Quando o processo de autenticação mútua é executado usando-se uma diferente chave para cada serviço, o processo torna-se embaraçoso. Portanto, foi implementada uma técnica em que uma chave (chave degenerada) é gerada antecipadamente com base em uma pluralidade de chaves, respectivamente correspondendo a serviços, e a chave degenerada é comumente usada em mútuos processos de autenticação para os serviços (por exemplo, vide JP-A-10-327142).

Quando a chave degenerada acima descrita é usada, é possível reduzir o tempo que leva para o processo de autenticação mútua e é possível rapidamente acessar informação referente a um serviço desejado.

Entretanto, por exemplo, quando uma chave degenerada é vazada em uma situação onde uma pluralidade de cartões IC utiliza uma chave degenerada comum, é necessário mudar a chave degenerada comum mantida na pluralidade de cartões IC. Portanto, foi proposto um método para individualizar e utilizar uma chave degenerada para cada cartão de IC pela aplicação de informação de identificação única (a seguir referida como ID

única) de cada cartão de IC para uma chave degenerada sem diretamente utilizar a chave degenerada (por exemplo, vide JP-A-2008-99335).

SUMÁRIO DA INVENÇÃO

A presente descrição refere-se a um dispositivo de comunicação, um método de comunicação, um dispositivo de processamento de informação e, mais particularmente, a um dispositivo de comunicação, um método de comunicação um dispositivo de processamento de informação, um método de processamento de informação, um programa e um sistema de comunicação, que são adequados para uso no caso em que informação é transmitida em um tipo sem-contato.

Após individualização pela aplicação de uma ID única de um cartão de IC a uma chave degenerada, como descrito acima, o vazamento da própria chave degenerada pode ser evitado utilizando-se o resultado da individualização em um processo de autenticação mútua. Entretanto, neste caso, é difícil negar a possibilidade de que a ID única do cartão de IC possa vazada para terceiros em um processo de notificação, uma vez que é necessário que o cartão de IC notifique a R/W de sua própria ID única.

É necessário que a ID única do cartão de IC seja evitada de ser vazada, uma vez que há a possibilidade de que a ID única vazada do cartão de IC possa ser usada em um processo de rastreio de identificação não autorizado para um usuário do cartão de IC.

Assim, é desejável evitar que uma ID única de um cartão de IC seja vazada mesmo embora uma chave degenerada seja individualizada e usada.

A presente descrição provê um novo e inovativo aparelho de processamento de informação, método e dispositivo de memória legível por computador, para evitar uma que uma única ID seja vazada.

Em uma forma de realização exemplo, o aparelho de processamento de informação inclui um processador; uma seção de

comunicação, operativamente acoplada ao processador; e um dispositivo de memória operativamente acoplado ao processador, o dispositivo de memória armazenando instruções que fazem com que o processador, em cooperação com uma seção de comunicação e um dispositivo de memória: determine se uma ID alvo é uma ID única ou uma ID de aleatorização parcial, a ID de aleatorização parcial incluindo uma primeira parte sendo substituída por um diferente número e uma segunda parte sendo gerada com base na ID única: em resposta à ID alvo sendo a ID de aleatorização parcial, gera uma chave de acesso com base na segunda parte da ID de aleatorização parcial e numa chave; executa um processo de autenticação mútua usando a chave de acesso gerada.

Em uma forma de realização exemplo, o aparelho de processamento de informação é uma leitura/gravadora. Em outra forma de realização exemplo, o aparelho de processamento de informação é um cartão de comunicação sem contato. Em uma forma de realização exemplo, as instruções fazem com que o processador determine se a ID alvo é a única ID ou a ID de aleatorização parcial, com base em um sinalizador de aleatorização.

Em uma forma de realização exemplo, a ID alvo inclui um código. Nesta forma de realização exemplo, as instruções fazem com que o processador determine se a ID alvo é a única ID ou a ID de aleatorização parcial, com base no código.

Em uma forma de realização exemplo, o diferente número que substitui a primeira parte da ID de aleatorização parcial é aleatoriamente gerada. Em uma forma de realização exemplo, as instruções fazem com que o processador mude o número diferente aleatoriamente gerado.

Em uma forma de realização exemplo, a segunda parte da aleatorização parcial ID inclui uma parte da ID única.

Em uma forma de realização exemplo, em resposta à ID alvo

sendo a ID de aleatorização parcial, as instruções fazem com que o processador gere a chave acesso aplicando a segunda parte da ID de aleatorização parcial para a chave. Em uma forma de realização exemplo, a aplicação da segunda parte da ID de aleatorização parcial para chave inclui adicionar a segunda parte da ID de aleatorização parcial à chave.

Em uma forma de realização exemplo, em resposta à ID alvo sendo a única ID, as instruções fazem com que o processador gere a chave acesso aplicando a única ID à chave.

Em uma forma de realização exemplo, um método para operar um aparelho de processamento de informação incluindo instruções inclui: (a) fazer com que um processador execute as instruções para determinar se uma ID alvo é uma ID única ou uma ID de aleatorização parcial, a ID de aleatorização parcial ID incluindo: (i) uma primeira parte sendo substituída por um diferente número; e (ii) uma segunda parte sendo gerada com base na ID única; (b) fazer com que o processador execute as instruções para, em resposta à ID alvo sendo a ID de aleatorização parcial, gerar uma chave de acesso com base na segunda parte da ID de aleatorização parcial e em uma chave; e (c) fazer com que o processador execute as instruções para executar um processo de autenticação mútuo, usando a chave de acesso gerada.

Em uma forma de realização exemplo, o aparelho de processamento de informação é uma leitora/gravadora. Em outra forma de realização exemplo, o aparelho de processamento de informação é um cartão de IC de comunicação sem contato.

Em uma forma de realização exemplo, o método inclui fazer com que o processador execute as instruções para determinar se a ID alvo é a única ID ou a ID de aleatorização parcial com base em um sinalizador de aleatorização.

Em uma forma de realização exemplo, o método inclui: fazer com que o processador execute as instruções para determinar se a ID alvo

inclui um código; e fazer com que o processador execute as instruções para determinar se a ID alvo é a ID única ou a ID de aleatorização parcial com base no código.

Em uma forma de realização exemplo, o diferente número é aleatoriamente gerado. Em uma forma de realização exemplo, o método inclui fazer com que o processador execute as instruções para mudar o número diferente aleatoriamente gerado.

Em uma forma de realização exemplo, a segunda parte da ID de aleatorização parcial inclui uma parte da ID única.

Em uma forma de realização exemplo, o método inclui fazer com que o processador execute as instruções para, em resposta à ID alvo sendo a ID de aleatorização parcial, gere a chave de acesso pela aplicação da segunda parte da ID de aleatorização parcial à chave. Em uma forma de realização exemplo, aplicar a segunda parte da ID de aleatorização parcial à chave inclui adicionar a segunda parte da ID de aleatorização parcial à chave.

Em uma forma de realização exemplo, o método inclui fazer com que o processador execute as instruções para, em resposta à ID alvo sendo a única ID, gerar a chave de acesso pela aplicação da ID única à chave.

Em uma forma de realização, a memória legível por computador armazena instruções para fazer com que um aparelho de processamento de informação: (a) determine se uma ID alvo é a única ID ou uma ID de aleatorização parcial, a ID de aleatorização parcial incluindo: (i) uma primeira parte sendo substituída por um diferente número; e (ii) uma segunda parte sendo gerada com base na ID única; (b) em resposta à ID alvo sendo a ID de aleatorização parcial, gera uma chave de acesso com base na segunda parte da ID de aleatorização parcial e em uma chave; e (c) executar um processo de autenticação mútua usando a chave de acesso gerada.

Em uma forma de realização exemplo, o aparelho de processamento de informação é uma leitora/gravadora. Em outra forma de

realização exemplo, o aparelho de processamento de informação é um cartão de comunicação sem contato.

Em uma forma de realização exemplo, as instruções fazem com que o aparelho de processamento de informação determine se a ID alvo é a única ID ou a ID de aleatorização parcial ID com base em um sinalizador de aleatorização.

Em uma forma de realização exemplo, a ID alvo inclui um código. Em uma forma de realização exemplo, as instruções fazem com que o aparelho de processamento de informação determine se a ID alvo é a única ID ou a ID de aleatorização parcial com base no código.

Em uma forma de realização exemplo, o diferente número é aleatoriamente gerado. Em uma forma de realização exemplo, as instruções fazem com que o aparelho de processamento de informação mude a número diferente gerado aleatoriamente.

Em uma forma de realização exemplo, a segunda parte da ID de aleatorização inclui uma parte da ID única.

Aspectos e vantagens adicionais são descritos aqui e serão evidentes pela seguinte Descrição Detalhada e as figuras.

BREVE DESCRIÇÃO DAS FIGURAS

A Fig. 1 é um diagrama de blocos mostrando um exemplo de configuração de um sistema de comunicação sem contato, de acordo com uma forma de realização exemplar da presente descrição.

As Figs. 2A e 2B são diagramas de blocos mostrando exemplos de configuração funcional de uma R/W e um cartão de IC.

As Figs. 3A, 3B e 3C são diagramas mostrando as estruturas de dados de uma ID alvo.

A Fig. 4 é um diagrama ilustrando a individualização de uma chave degenerada.

A Fig. 5 é um fluxograma ilustrando um processo de

comunicação pela R/W e o cartão de IC das Figs. 2A e 2B.

A Fig. 6 é um fluxograma ilustrando um processo do cartão de IC da Fig. 2B.

A Fig. 7 é um fluxograma ilustrando um processo da R/W da Fig. 2A.

A Fig. 8 é um fluxograma ilustrando um processo de uma R/W da técnica relacionada.

DESCRIÇÃO DETALHADA

A seguir, serão descritas formas de realização da presente descrição em detalhes com referência aos desenhos.

1. Forma de realização

Exemplo de Configuração de Sistema de Comunicação Sem-Contato

A Fig. 1 mostra um exemplo de configuração de um sistema de comunicação sem contato, de acordo com uma forma de realização exemplar da presente descrição. Este sistema de comunicação sem contato 1 inclui uma R/W 10 e um cartão de IC 20. Quando um usuário move o cartão de IC em direção à R/W 10, força motriz é gerada dentro do cartão de IC 20.

A R/W 10 tem uma CPU 11 embutida, em que uma ROM 12, uma RAM 13, uma NVM (memória não volátil) 14 e um circuito de modulação/desmodulação 16 são conectados via um barramento 15. A CPU 11 controla cada elemento da R/W 10 executando um programa de controle pré-armazenado na ROM 12. A RAM 13 é usada como uma área de trabalho, quando a CPU 11 executa vários processos. Uma chave degenerada é mantida na NVM 14.

O circuito de modulação/desmodulação 16 modula uma portadora por informação, que é emitida pela CPU 11, introduzida via o barramento 15 e transmitida para o cartão de IC 20 e emite uma portadora modulada para uma antena 17. Também o circuito de

modulação/desmodulação 16 desmodula uma onda recebida pela antena 17 e emite informação quanto ao resultado da desmodulação do cartão de IC 20 para a CPU 11, via o barramento 15. A antena 17 transmite uma entrada de onda modulada do circuito de modulação/desmodulação 16. Também a antena 17 recebe uma onda modulada transmitida pelo cartão de IC 20 e emite a onda modulada para o circuito de modulação/desmodulação 16.

O cartão de IC 20 tem uma CPU 21 embutida, a que uma ROM 22, uma RAM 23, uma NVM 24 e um circuito de modulação/desmodulação 26 são conectados via um barramento 25. A CPU 21 controla cada elemento do cartão de IC 20 executando um programa de controle pré-armazenado na ROM 22. A RAM 23 é usada como uma área de trabalho, quando a CPU 21 executa vários processos. Na NVM 24, informação referente a uma chave degenerada ou vários serviços (um serviço de dinheiro eletrônico, um serviço de tíquete de comutação para um trem elétrico, um serviço de cartão ID de empregado e similares) é hierarquizado e armazenado para cada serviço.

O circuito de modulação/desmodulação 26 desmodula uma portadora recebida por uma antena 27 da R/W 10 e emite informação da R/W 10 como o resultado da desmodulação para a CPU 21, via o barramento 25. O circuito de modulação/desmodulação 26 modula uma portadora por informação, que é emitida pela CPU 21, introduzida via o barramento 25 e transmitida para a R/W 10 e emite a portadora modulada para a antena 27. A antena 27 recebe uma onda modulada transmitida pela R/W 10, emite a onda modulada para o circuito de modulação/desmodulação 26. Também a antena 27 transmite uma entrada de onda modulada pelo circuito de modulação/ desmodulação 26.

Em seguida, as Figs. 2A e 2B mostram diagramas de blocos funcionais a serem implementados pelos programas de controle respectivamente executados pela CPU 11 da R/W 10 e a CPU 21 do cartão de

IC 20.

Na R/W 10, uma seção de comunicação 51, uma seção de determinação de código alvo 52, uma seção de geração de chave de acesso 53, uma seção de controle de chave 54 e uma seção de processamento de dados 55 são implementadas.

A seção de comunicação 51 controla a comunicação com o cartão de IC 20. A seção de determinação de código alvo 52 lê um código alvo de uma ID alvo reportada pelo cartão de IC 20 e determina se a ID alvo é uma ID específica de cartão ou uma ID de aleatorização parcial.

A seção de geração de chave de acesso 53 gera uma chave de acesso pela individualização de uma chave degenerada com base no resultado da determinação da seção de determinação de código alvo 52. Um processo de individualização de chave degenerada será descrito com referência à Fig. 4.

A seção de controle de chave 54 controla uma chave degenerada pré-mantida e uma chave de acesso gerada. A seção de processamento de dados 55 executa um processo de autenticação mútua com o cartão de IC 20, usando a chave de avesso gerada via a seção de comunicação 51. A seção de processamento de dados 55 descriptografa informação criptografada transmitida pelo cartão de IC ou criptografa informação a ser transmitida para o cartão de IC 20, após o processo de autenticação mútua.

No cartão de IC 20, uma seção de comunicação 61, uma seção de saída de ID alvo 62, uma seção de retenção de sinalizador 63, uma seção de geração de número aleatório 64, uma seção de geração de chave de acesso 65, uma seção de controle de chave 66 e uma seção de processamento de dados são implementadas.

A seção de comunicação 61 controla a comunicação com a R/W 10. Em resposta ao estado de um sinalizador mantido pela seção de retenção de sinalizador 63, a seção de saída ID alvo 62 emite uma ID

específica de cartão ou uma ID de aleatorização parcial como uma ID alvo, em que a aleatorização ID parcial é gerada substituindo-se uma parte da ID específica de cartão com um número aleatório. A ID específica de cartão é pré-armazenada na NVM 24. A ID de aleatorização parcial é gerada pela seção de saída ID alvo 62 em um predeterminado instante e é armazenada na NVM 24. Um processo de geração de ID de aleatorização parcial será descrito com referência às Figs. 3A, 3B e 3C.

Na seção de retenção de sinalizador 63, um sinalizador de aleatorização ID alvo, indicando se usar diretamente uma ID específica de cartão da técnica relacionada ou usar uma ID de aleatorização parcial ID como a ID alvo, é pré-estabelecido. Em seguida, a ID específica de cartão ID é diretamente usada quando o sinalizador de aleatorização ID alvo é inválido e a ID de aleatorização parcial é usada quando o sinalizador de aleatorização ID alvo é válido.

Isto é, antes de o cartão de IC 20 ser provido para o usuário, é determinado se usar diretamente a ID específica de cartão ou usar a ID de aleatorização parcial como a ID alvo a ser reportada para a R/W 10.

A este respeito, a validade/invalidade do sinalizador de aleatorização ID alvo mantida na seção de retenção de sinalizador 63 pode ser comutada em resposta a um predeterminado comando da R/W 10.

Portanto, por exemplo, o sinalizador de aleatorização ID alvo é determinado ser inválido, de modo que a ID específica de cartão é reportada como a ID alvo, até a R/W 10, de acordo com uma forma de realização exemplar da presente descrição, ser amplamente suprida para a sociedade. O sinalizador de aleatorização ID alvo é restabelecido como válido, de modo que a ID de aleatorização parcial é reportada como a ID alvo após a R/W da técnica relacionada ser abolida e a R/W 10 ser amplamente suprida para a sociedade.

A seção de geração de número aleatório 64 gera um número

aleatório em resposta a uma solicitação da seção de saída de ID alvo 62. A seção de geração de chave de acesso 65 gera uma chave de acesso individualizando uma chave degenerada com base em um código alvo da ID alvo gerada em um predeterminado instante. A seção de controle de chave 66 controla a chave degenerada pré-mantida na NVM 24. Um processo de individualização de chave degenerada será descrito mais tarde com referência à Fig. 4.

A seção de processamento de dados 67 executa um processo de autenticação mútua com a R/W 10, utilizando a chave de acesso gerada via a seção de comunicação 61. Após o processo de autenticação mútua, a seção de processamento de dados 67 descriptografa a informação criptografada transmitida pela R/W 10 ou criptografa a informação a ser transmitida para a R/W 10.

Os blocos funcionais mostrados nas Figs. 2A e 2B são implementados por software (programas de controle) como descrito acima, porém podem ser instalados como hardware.

Em termos de ID de Aleatorização Parcial

As Figs. 3A, 3B e 3C são diagramas ilustrando um processo de gerar uma ID alvo pela seção de saída de ID alvo 62 do cartão de IC 20.

A Fig. 3A mostra uma estrutura de dados de uma ID específica de cartão pré-alocada ao cartão de IC 20 e armazenada na NVM 24 ou similar. Por exemplo, a ID específica de cartão tem uma quantidade de informação de 8 bytes D0 a D7, em que um número de sistema de 4-bits, um código de fabricante de 12-bits e um número de cartão de 6-bytes são gravados na ordem do lado do MSB (Bit Mais Significativo). Em cartões IC 20, manufaturados pelo mesmo fabricante, o número de sistema e o código de fabricante são comuns. Por conseguinte, o número de cartão de 6-bytes torna-se substancialmente informação única do cartão de IC 20.

A Fig. 3B mostra uma estrutura de dados de uma ID de

aleatorização parcial gerada pela seção de saída ID alvo 62. Isto é, a aleatorização parcial ID é obtida substituindo-se o código do fabricante da ID específica de cartão com um código IDr incluindo um valor predeterminado e substituindo-se n bytes predeterminados (4 bytes na Fig. 3B) no lado do MSB do número de cartão de 6-bytes com um número aleatório gerado pela seção de geração de número aleatório 64. Aqui, n é um inteiro que é igual a ou maior do que 1 e menor do que 6.

Portanto, quando a ID específica de cartão da Fig. 3A ou a ID de aleatorização parcial da Fig. 3B tiver sido reportada como a ID alvo do cartão de IC 20 para a R/W 10, é possível determinar se a ID alvo é a ID específica de cartão ou a ID de aleatorização parcial identificando-se os 12 bits subsequente ao número do sistema.

Como mostrado na Fig. 3C, 12 bits subsequentes ao número do sistema são referidos como um código alvo e 6 bytes D2 a D7 subsequentes a eles são referidos como os 6 bytes menos significativos da ID alvo.

Embora 4 bytes do alvo ID sejam substituídos com o número aleatório da forma de realização exemplar acima, o número de bytes que são substituídos pode ser diferente. Além disso, o código extra pode incluir informação indicativa de que byte e quantos bytes dos 6 bytes menos significativos do alvo ID (D2 – D7) são para ser substituídos pelo número aleatório. Por exemplo, pode ser arranjado que, quando 12 bits inferiores do código alvo forem "2FEh", então os 4 bytes dos 6 bytes menos significativos do alvo ID (D2 – D5) sejam substituídos pelo número aleatório e, como resultado, os 2 bytes menos significativos (D6 e D7) do alvo ID sejam os mesmos que os menos significantes 2 bytes do número de cartão. Também pode ser arranjado que, quando 12 bits inferiores do código extra sejam "2FFh", então 3 bytes dos 6 bytes menos significativos do ID alvo (D2 – D4) sejam substituídos pelo número aleatório e, como resultado, os 3 bytes menos

significativos (D5 e D7) do alvo ID sejam os mesmos que os menos significativos 3 bytes do número de cartão.

Em Termos de Individualização de Chave Degenerada

A Fig. 4 é um diagrama ilustrando a individualização chave degenerada a ser executada em cada uma da chave de geração de chave de acesso 53 da R/W 10 e da seção de geração de chave de acesso 65 do cartão de IC 20.

Como mostrado na Fig. 4, a individualização chave degenerada é executada aplicando-se um código de individualização para a chave degenerada, por exemplo, adicionando-se o código de individualização para a chave degenerada. A seguir, a chave degenerada individualizada como o resultado do processo de individualização é referida como uma chave de acesso.

Aqui, o código de individualização é gerado por um parâmetro de entrada do código de individualização. A este respeito, o parâmetro de entrada pode ser diretamente usado como o código de individualização.

Quando a ID alvo é a ID específica de cartão, os 6 bytes menos significativos da ID alvo, isto é, o total do número de cartão, tornam-se o parâmetro de entrada do código de individualização. Quando a ID alvo é a ID de aleatorização parcial, os (6-n) menos significativos bytes da ID alvo, isto é, os (6-n) bytes menos significativos do número de cartão excluindo uma parte de número aleatório dos 6 menos significativos bytes da ID alvo, tornam-se o parâmetro de entrada do código de individualização. Na Fig. 4, 2 bytes menos significativos D6 e D7 da ID alvo tornam-se o parâmetro de entrada do código de individualização, quando a ID alvo é a ID de aleatorização parcial.

Descrição da Operação do Sistema de Comunicação Sem-Contato 1

Em seguida, o resumo de um processo de comunicação pelo sistema de comunicação sem contato 1 será descrito. A Fig. 5 é um fluxograma ilustrando o processo de comunicação pelo sistema de

comunicação sem-contato 1.

Inicialmente, um processo de interrogação é executado na etapa S1. Isto é, quando a R/W 10 executa o processo de soldagem para pesquisar quanto ao cartão de IC 20 como um parceiro de comunicação, o cartão de IC 20 informa sua própria ID alvo (a aleatorização parcial ID ou a ID específica de cartão) para a R/W 10 em resposta.

Na etapa S2, um processo de autenticação mútua é executado. Isto é, a R/W 10 obtém uma chave de acesso como o resultado da execução de um processo de individualização em que um código de individualização é extraído da ID alvo informada pelo cartão de IC 20 e é aplicado à chave degenerada. Por outro lado, o cartão de IC 20 obtém uma chave de acesso como resultado da execução de um processo de individualização em que um código de individualização é extraído da ID alvo informada para a R/W 10 e é aplicado à chave degenerada. Desse modo, uma vez que a R/W 10 e o cartão de IC 20 obtêm a mesma chave de acesso, o processo de autenticação mútua é executado usando-se a mesma chave de acesso.

Na etapa S3, um processo de acesso de bloco de usuário é executado. Isto é, a R/W 10 executa um processo de leitura da informação gravada no cartão de IC 20, reescreve a gravação de informação no cartão de IC 20 ou grava nova informação no cartão de IC 20, de acordo com uma instrução de um controlador (não mostrado).

Na etapa S4, um processo de mudança de número aleatório é executado. O processo de mudança de número aleatório é executado pelo cartão de IC 20, de acordo com um predeterminado comando da R/W 10 somente quando o cartão de IC 20 é estabelecido para informar a aleatorização parcial ID como a ID alvo. Especificamente, um processo de atualização da ID de aleatorização parcial é executado mudando-se o número aleatório incluído na ID de aleatorização parcial como a ID alvo.

O processo de mudança do número aleatório da etapa S4 pode

não ser necessariamente executado toda vez quando o processo de comunicação é executado. Isto é, a R/W 10 faz com que o cartão de IC 20 execute a mudança do número aleatório, processando o comando predeterminado acima descrito quando necessário.

Descrição da Operação do Cartão de IC 20

Em seguida, o processo do cartão de IC 20 do processo de comunicação será descrito em detalhes. A Fig. 6 é um fluxograma ilustrando o processo do cartão de IC 20. Este processo é iniciado quando a força de acionamento foi gerada dentro do cartão de IC 20 pelo usuário movendo o cartão de IC 20 em direção à R/W 20.

No cartão de IC 20, a ID de aleatorização parcial já gerada pela seção de saída der ID alvo 62 é mantida na NVM 24.

Na etapa S11, a seção de comunicação 61 do cartão de IC 20 espera pela interrogação a ser recebida da R/W 10. Quando a interrogação foi recebida, o processo prossegue para a etapa S12.

Na etapa S12, a seção de saída ID alvo 62 determina o estado do sinalizador de aleatorização de ID alvo mantido pela seção de detenção de sinalizador 63. Aqui, quando o sinalizador de aleatorização ID alvo foi determinado como sendo válido, o processo prossegue para a etapa S13 e subsequentes etapas e a aleatorização parcial ID é informada como a ID alvo para a R/W 10.

Isto é, na etapa S13, a seção de saída ID alvo 62 lê a ID de aleatorização parcial gerada anteriormente, armazenada na NVM 24 e emite a ID lida para a seção de comunicação 61 e a seção de geração de chave de acesso 65. Aqui, é presumido que a ID de aleatorização parcial já está gerada. Entretanto, quando a ID de aleatorização parcial não está gerada por qualquer razão, é desejável gerar a ID de aleatorização parcial na etapa S13.

Na etapa S14, a seção de comunicação 61 provê a R/W 10 com a ID de aleatorização parcial como a entrada ID alvo da seção de saída ID

alvo 62.

Na etapa S15, a seção de geração de chave de acesso 65 gera a chave de acesso fazendo com que a seção de controle de chave 66 leia a chave degenerada e aplicando 2 bytes menos significativos do número de cartão da entrada ID de aleatorização da seção de saída ID alvo 62 para a chave degenerada lida.

Na etapa S16, a seção de processamento de dados 67 executa o processo de autenticação mútua com a R/W 10 usando a chave de acesso gerada via a seção de comunicação 61. Após o processo de autenticação mútua ter sido bem sucedido, a seção de processamento de dados 67 executa o processo de acesso de bloco de usuário da etapa S17. Isto é, a informação é lida da ou escrita na NVM 24, em resposta a uma solicitação da R/W 10.

Na etapa S18, a seção de saída ID alvo 62 determina se um comando de mudança de número aleatório foi transmitido da R/W 10. O processo prossegue para a etapa S19 ao mesmo tempo da determinação de que o comando de mudança de número aleatório foi transmitido. Na etapa S19, a seção de saída ID alvo 62 faz com que a seção de geração de número aleatório 64 gere um número aleatório e regenere uma aleatorização ID parcial substituindo uma parte de número aleatório da ID de aleatorização parcial atual pelo número aleatório gerado, e faz com que a NVM 24 armazene a ID de aleatorização parcial regenerada. Aqui, a aleatorização parcial regenerada ID é usada como a ID alvo transmitida do cartão de IC 20 para a R/W 10 na ocasião do processo de comunicação a seguir. Em seguida, o processo do cartão de IC 20 é terminado.

Por outro lado, quando o sinalizador de aleatorização da ID alvo foi determinado ser inválido na etapa S12, o processo prossegue para a etapa S22 e subsequentes etapas. A ID específica de cartão como a ID alvo é informada para a R/W 10.

Isto é, na etapa S20, a seção de saída de ID alvo 62 lê a ID

específica de cartão na NVM 24 e então emite a ID específica de cartão lida para a seção de comunicação 61 e a seção de geração de chave de acesso 65.

Na etapa S21, a seção de comunicação 61 provê a R/W 10 com a entrada ID específica de cartão da seção de saída ID alvo 62 como a ID alvo.

Na etapa S22, a seção de geração de chave de acesso 65 gera a chave de acesso fazendo com que a seção de controle de chave 66 leia a chave degenerada e aplicando o número de cartão de 6 bytes da entrada de ID específica de cartão da seção de saída de ID alvo 62 para a chave degenerada lida e emite a chave de acesso gerada para a seção de processamento de dados 67.

Na etapa S23, a seção de processamento de dados 67 executa o processo de autenticação mútua com a R/W 10, utilizando a chave de acesso gerada via a seção de comunicação 61. Após o processo de autenticação mútua ter sido bem sucedido, a seção de processamento de dados 67 executa o processo de acesso de bloco de usuário na etapa S17. Em seguida, o processo do cartão de IC 20 é terminado.

Em seguida, a descrição do processo do cartão de IC 20 é terminada.

Um processo de determinar se o sinalizador de aleatorização ID alvo é válido ou inválido toda vez quando a interrogação é recebida foi descrito acima. Alternativamente, o processo de determinação pode ser omitido por associação antecipada da aleatorização parcial ID ou da ID específica de cartão com a ID alvo.

Um processo de leitura e transmissão da ID de aleatorização parcial gerada e armazenada antecipadamente, quando a ID de aleatorização parcial, quando a ID alvo é relatado para a R/W 10, foi descrito acima. Alternativamente, o número aleatório pode ser gerado para gerar a ID de aleatorização parcial em cada relato.

Quando o sinalizador de aleatorização ID alvo mantido na seção de retenção de sinalizador 63 do cartão de IC 20 é determinado ser válido, como descrito acima, a ID de aleatorização parcial como a ID alvo é relatada pelo cartão de IC 20 para a R/W 10. Portanto, o vazamento da ID específica de cartão do cartão de IC 20 pode ser evitado.

Descrição da Operação de R/W 10

Em seguida, o processo da RW 10 no processo de comunicação será descrito em detalhes. A Fig. 7 é um fluxograma ilustrando o processo da R/W 10. Este processo é iniciado sob controle de um controlador (não mostrado).

Na etapa S51, a seção de comunicação 51 da R/W 10 realiza a interrogação. A ID alvo é adquirida do cartão de IC 20 movendo-se em direção à R/W 10. A ID alvo adquirida é emitida para a seção de determinação de código alvo 52.

Na etapa S52, a seção de determinação de código extra 52 determina se um código alvo da ID alvo é um código IDr ou um código de fabricante e relata a ID alvo para a seção de geração de chave de acesso 53 com o resultado da determinação. Aqui, quando o código alvo foi determinado ser o código IDr, o processo prossegue para a etapa S53. Neste caso, a ID alvo reportada pelo cartão de IC 20 é uma ID de aleatorização parcial.

Na etapa S53, a seção de geração de chave de acesso 53 gera uma chave de acesso fazendo com que a seção de controle de chave 54 leia uma chave degenerada e aplique 2 bytes menos significativos de um número de cartão da ID alvo (aleatorização ID parcial) como um parâmetro de entrada de um código de individualização para a chave degenerada lida e emite a chave de acesso gerada para a seção de processamento de dados 55.

Na etapa S54, a seção de processamento de dados 55 executa um processo de autenticação mútua com o cartão de IC 20 usando a chave de acesso gerada via a seção de comunicação 51. Após o processo de

autenticação mútua ter sido bem sucedido, a seção de processamento de dados 55 executa o processo de acesso de bloco do usuário da etapa S55. Isto é, a informação é lida do ou gravada no cartão de IC 20.

Na etapa S56, a seção de comunicação 56 transmite um comando de mudança de número aleatório para o cartão de IC 20. Em resposta ao comando de mudança de número aleatório, o cartão de IC 20 regenera a ID de aleatorização parcial. O processo da etapa S56 pode ser omitido. Alternativamente, por exemplo, o comando de mudança de número aleatório pode ser transmitido somente quando um processo de comunicação foi executado em uma faixa de tempo predeterminada. Em seguida, o processo da R/W 10 é terminado.

Na etapa S52, quando o código alvo foi determinado ser o código do fabricante, o processo prossegue para S57. Neste caso, a ID alvo do cartão de IC 20 é uma ID específica de cartão.

Na etapa S57, a seção de geração de chave de acesso 53 gera uma chave de acesso fazendo com que a seção de controle de chave 54 leia a chave degenerada e aplique 6 bytes do número de cartão da ID alvo (ID específica de cartão) como o parâmetro de entrada do código de individualização para a chave degenerada lida e emite a chave de acesso gerada para a seção de processamento de dados 55.

Na etapa S58, a seção de processamento de dados 55 executa o processo de autenticação mútua com o cartão de IC 20 usando a chave de acesso gerada via a seção de comunicação 51. Após o processo de autenticação mútua ter sido bem sucedido, a seção de processamento de dados 55 executa o processo de acesso de bloco do usuário S59. Isto é, a informação é lida do ou gravada no cartão de IC 20. Em seguida, o processo da R/W 10 é terminado.

Descrição para Operação de R/W da técnica Relacionada, que se Comunica com o Cartão de IC 20

Em seguida, o processo de uma R/W da técnica relacionada,

que se comunica com o cartão de IC 20, será descrito em detalhes. A Fig. 8 é um fluxograma ilustrando o processo da R/W da técnica relacionada. No cartão de IC 20 comunicável com a R/W da técnica relacionada, seu sinalizador de aleatorização ID alvo é presumido ser inválido.

Na etapa S71, a R/W da técnica relacionada realiza interrogação e uma ID alvo (ID específica de cartão) é adquirida do cartão de IC 20 movendo-se em direção à R/W da técnica relacionada.

Na etapa S72, a R/W da técnica relacionada gera uma chave de acesso aplicando 6 bytes de um número de cartão da ID alvo adquirida (ID específica de cartão) como um parâmetro de entrada de um código de individualização para uma chave degenerada mantida antecipadamente.

Na etapa S73, a R/W da técnica relacionada executa um processo de autenticação mútua com o cartão de IC 20, utilizando a chave de acesso gerada. Após o processo de autenticação mútua ter sido bem sucedido, um processo de acesso de bloco é executado na etapa S74. Em seguida o processo da R/W da técnica relacionada é terminado.

O cartão de IC 20 é também comunicável sem fio com a R/W da técnica relacionada, ajustando-se o sinalizador de aleatorização ID alvo do cartão de IC 20 para ser inválido como descrito acima.

O dispositivo de processamento de informação da forma de realização exemplar da presente execução é também aplicável a um telefone móvel ou similar, equipado com um chip IC equivalente ao cartão de IC 20, bem como o cartão de IC 20 desta forma de realização.

O sistema de comunicação da forma de realização exemplar da presente descrição é aplicável a qualquer sistema de comunicação que executa um processo de autenticação mútua, bem como o sistema de comunicação sem contato 1 nesta forma de realização.

Por outro lado, uma série de processos descritos acima pode ser executada por hardware e pode também ser executada por software.

Quando a série de processos é executada por software, um programa constituindo o software é instalado de um meio de gravação de programa em um computador embutido em hardware dedicado ou, por exemplo, um computador pessoal de fins gerais capaz de executar várias funções pela instalação de vários programas.

Um programa a ser executado pelo computador pode ser um programa a ser processado em uma maneira de série de tempo, de acordo com uma sequência descrita aqui ou pode ser um programa a ser processado em paralelo ou em uma ocasião quando invocado, por exemplo.

Um programa pode ser processado por um computador ou, alternativamente, pode ser processado por uma pluralidade de computadores por processamento distribuído. O programa pode também ser transferido para e executado por um computador remoto.

Neste relatório, o sistema representa a totalidade de um aparelho incluindo uma pluralidade de dispositivos.

Deve ser entendido que várias mudanças e modificações às formas de realização presentemente preferidas descritas aqui serão evidentes daqueles hábeis em tal técnica. Tais mudanças e modificações podem ser feitas sem desvio do espírito e escopo e sem diminuir suas vantagens pretendidas. É, portanto, pretendido que tais mudanças e modificações sejam cobertas pelas reivindicações anexas.

REIVINDICAÇÕES

1. Aparelho de processamento de informação, caracterizado pelo fato de compreender:

um processador;

uma seção de comunicação; e

um dispositivo de memória operativamente acoplado ao processador, o dispositivo de memória armazenando instruções que fazem com que o processador, em cooperação com a seção de comunicação e o dispositivo de memória:

(a) determine se uma ID alvo é uma ID única ou uma ID de aleatorização parcial, a ID de aleatorização parcial incluindo:

(i) uma primeira parte sendo substituída por um diferente número; e

(ii) uma segunda parte sendo gerada com base na ID única;

(b) em resposta à ID alvo sendo a ID de aleatorização parcial, gere uma chave de acesso com base na segunda parte da ID de aleatorização parcial e numa chave; e

(c) execute um processo de autenticação mútua usando a chave de acesso gerada.

2. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de ser uma leitora/gravadora.

3. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de ser um cartão de IC de comunicação sem contato.

4. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de as instruções fazerem com que o processador determine se a ID alvo é a única ID ou a ID de aleatorização parcial com base em um sinalizador de aleatorização.

5. Aparelho de processamento de informação de acordo com a

reivindicação 1, caracterizado pelo fato de:

(a) a ID alvo incluir um código; e

(b) as instruções fazerem com que o processador determine se a ID alvo é a única ID ou a ID de aleatorização parcial com base no código.

6. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de o diferente número ser aleatoriamente gerado.

7. Aparelho de processamento de informação de acordo com a reivindicação 6, caracterizado pelo fato de as instruções fazerem com que o processador mude o diferente número aleatoriamente gerado.

8. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de a segunda parte da ID de aleatorização parcial incluir uma parte da ID única.

9. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de as instruções fazerem com que o processador, em resposta à ID alvo sendo a ID de aleatorização parcial, gere a chave de acesso pela aplicação da segunda parte da ID de aleatorização parcial à chave.

10. Aparelho de processamento de informação de acordo com a reivindicação 9, caracterizado pelo fato de a aplicação da segunda parte da ID de aleatorização parcial à chave incluir adicionar a segunda parte da ID de aleatorização parcial ID à chave.

11. Aparelho de processamento de informação de acordo com a reivindicação 1, caracterizado pelo fato de as instruções fazerem com que o processador, em resposta à ID alvo sendo a ID única, gere a chave de acesso pela aplicação da ID única à chave.

12. Método para operar um aparelho de processamento de informação incluindo instruções, caracterizado pelo fato de compreender:

(a) fazer com que um processador execute as instruções para determinar se uma ID alvo é uma ID única ou uma ID de aleatorização

parcial, a ID de aleatorização parcial ID incluindo:

(i) uma primeira parte sendo substituída por um diferente número; e

(ii) uma segunda parte sendo gerada com base na ID única;

(b) fazer com que o processador execute as instruções para, em resposta à ID alvo sendo a ID de aleatorização parcial, gere uma chave de acesso com base na segunda parte da ID de aleatorização parcial e numa chave; e

(c) fazer com que o processador execute as instruções para executar um processo de autenticação mútua, usando a chave de acesso gerada.

13. Método de acordo com a reivindicação 12, caracterizado pelo fato de o aparelho de processamento de informação ser uma leitura/escritora.

14. Método de acordo com a reivindicação 12, caracterizado pelo fato de o aparelho de processamento de informação ser um cartão de IC de comunicação sem-contato.

15. Método de acordo com a reivindicação 12, caracterizado pelo fato de incluir fazer com que o processador execute as instruções para determinar se a ID alvo é a única ID ou a ID de aleatorização parcial com base em um sinalizador de aleatorização.

16. Método de acordo com a reivindicação 12, caracterizado pelo fato de incluir:

(a) fazer com que o processador execute as instruções para determinar se a ID alvo inclui um código; e

(b) fazer com que o processador execute as instruções para determinar se a ID alvo é a única ID ou a ID de aleatorização parcial com base no código.

17. Método de acordo com a reivindicação 12, caracterizado pelo fato de o diferente número ser aleatoriamente gerado.

18. Método de acordo com a reivindicação 17, caracterizado

pelo fato de incluir fazer com que o processador execute as instruções para mudar o diferente número aleatoriamente gerado.

19. Método de acordo com a reivindicação 12, caracterizado pelo fato de a segunda parte da ID de aleatorização parcial incluir uma parte da ID única.

20. Método de acordo com a reivindicação 12, caracterizado pelo fato de incluir fazer com que o processador execute as instruções para, em resposta à ID alvo sendo a ID de aleatorização parcial, gere a chave de acesso pela aplicação da segunda parte da ID de aleatorização parcial à chave.

21. Método de acordo com a reivindicação 20, caracterizado pelo fato de aplicar a segunda parte da ID de aleatorização parcial à chave incluir adicionar a segunda parte da ID de aleatorização parcial à chave.

22. Método de acordo com a reivindicação 12, caracterizado pelo fato de incluir fazer com que o processador execute as instruções, em resposta à ID alvo sendo a única ID, gerar a chave de acesso pela aplicação da ID única à chave.

23. Instruções de armazenamento de dispositivo de memória legível por computador, caracterizadas pelo fato de fazer com que um aparelho de processamento de informação:

(a) determine se uma ID alvo é uma ID única ou uma ID de aleatorização parcial, a ID de aleatorização parcial incluindo:

(i) uma primeira parte sendo substituída por um diferente número; e

(ii) uma segunda parte ser gerada com base na ID única;

(b) em resposta à ID alvo sendo a ID de aleatorização parcial, gere uma chave de acesso com base na segunda parte da ID de aleatorização parcial e numa chave; e

(c) execute um processo de autenticação mútua usando a chave de acesso gerada.

FIG.1

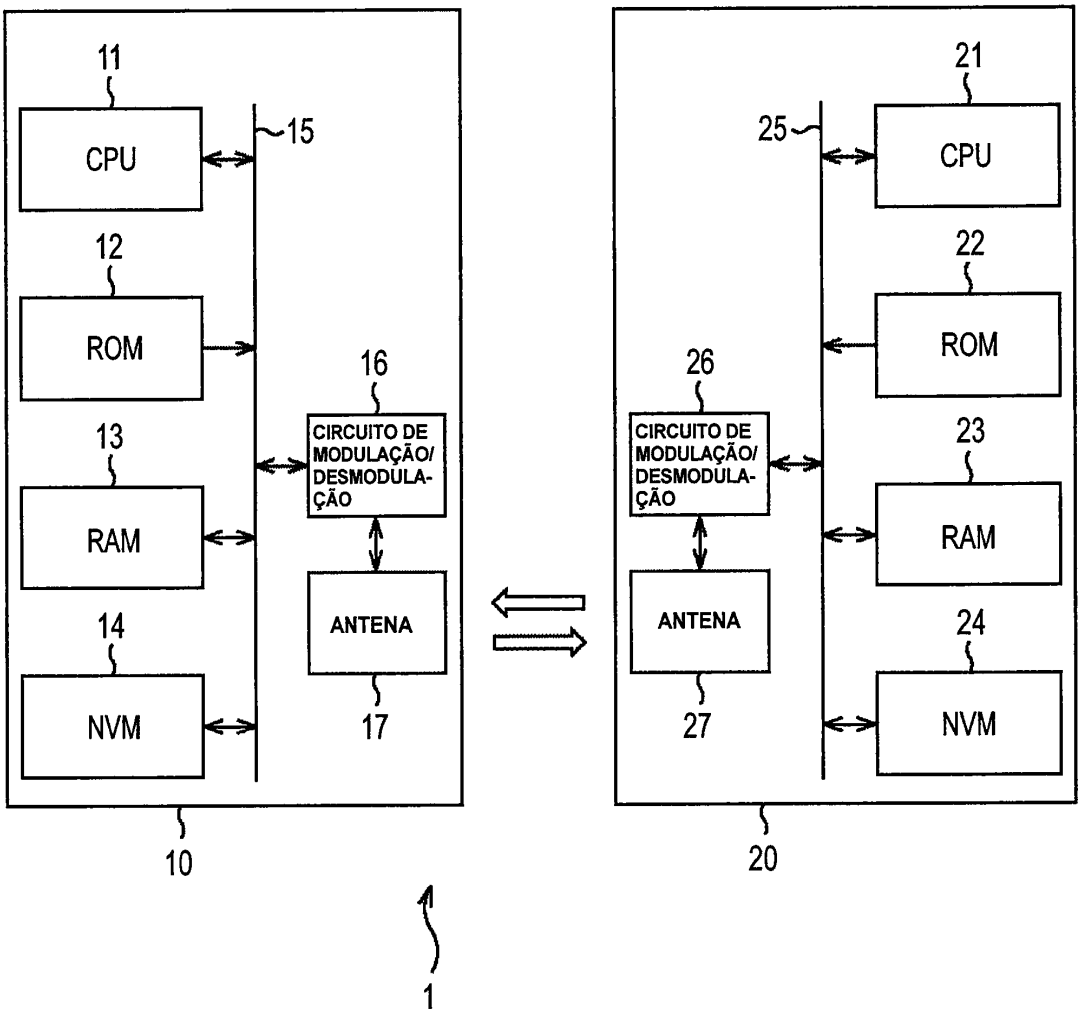

11
CPU
15
12
ROM
16
13
CIRCUITO DE MODULAÇÃO/ DESMODULA-ÇÃO
RAM
14
ANTENA
NVM
17
10
21
25
CPU
22
ROM
26
23
CIRCUITO DE MODULAÇÃO/ DESMODULA-ÇÃO
RAM
ANTENA
24
27
NVM
20
1

FIG.2A

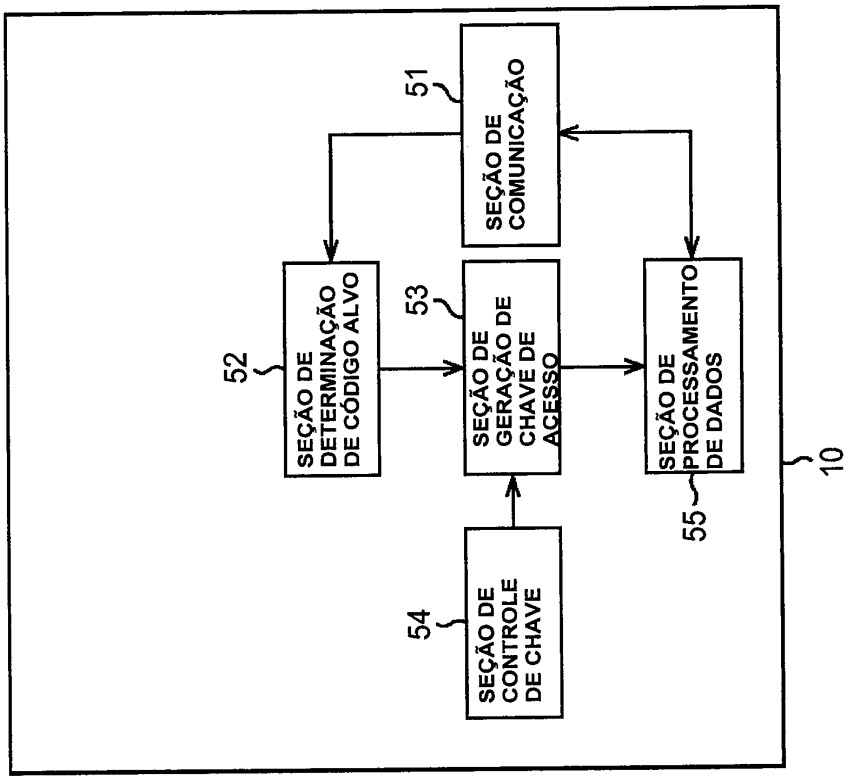

SEÇÃO DE COMUNICAÇÃO
51
SEÇÃO DE DETERMINAÇÃO DE CÓDIGO ALVO
52
SEÇÃO DE GERAÇÃO DE CHAVE DE ACESSO
53
SEÇÃO DE PROCESSAMENTO DE DADOS
55
SEÇÃO DE CONTROLE DE CHAVE
54
10

FIG.2B

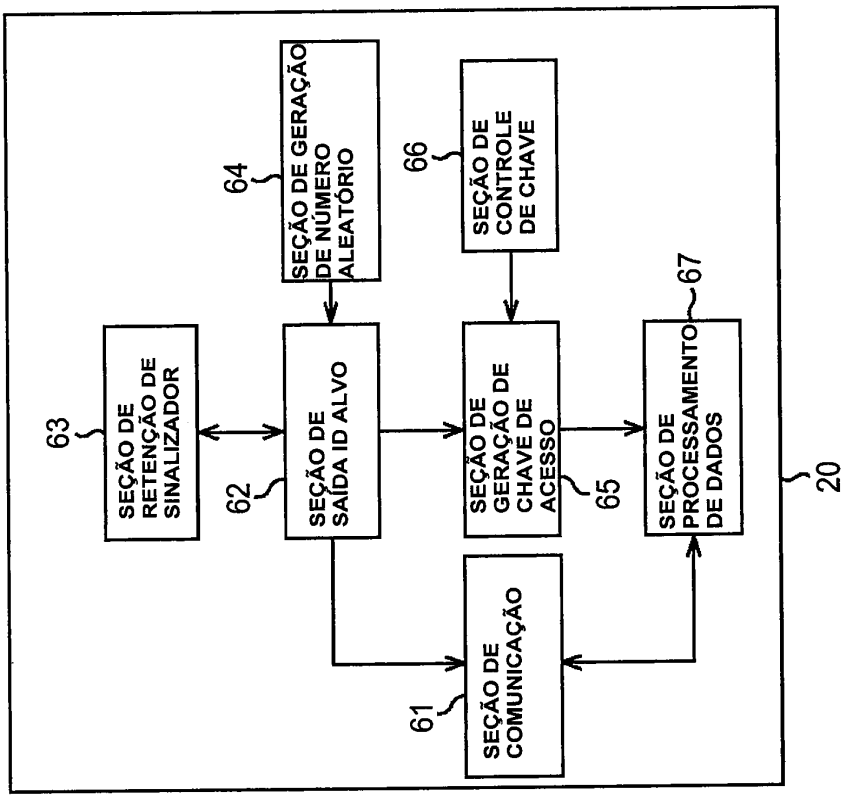

SEÇÃO DE RETENÇÃO DE SINALIZADOR
63
SEÇÃO DE SAÍDA ID ALVO
62
SEÇÃO DE GERAÇÃO DE NÚMERO ALEATÓRIO
64
SEÇÃO DE CONTROLE DE CHAVE
66
SEÇÃO DE GERAÇÃO DE CHAVE DE ACESSO
65
SEÇÃO DE PROCESSAMENTO DE DADOS
67
SEÇÃO DE COMUNICAÇÃO
61
20

FIG.3A

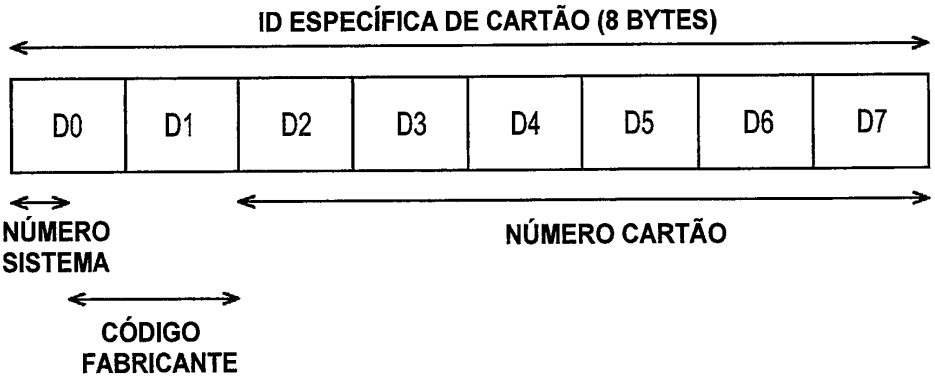


FIG.3B

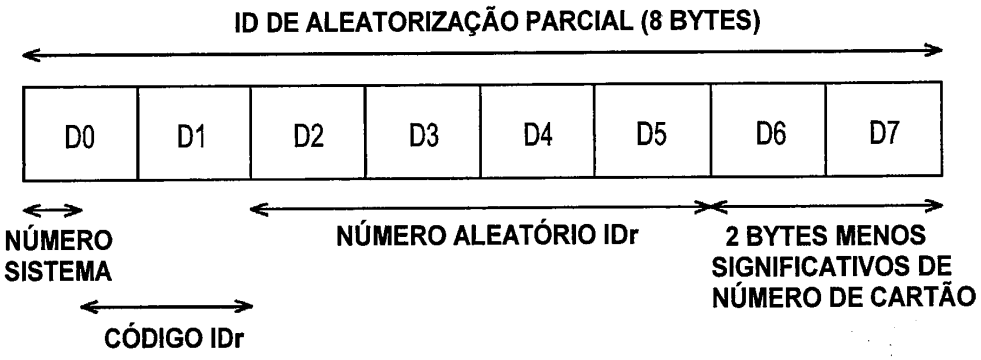


FIG.3C

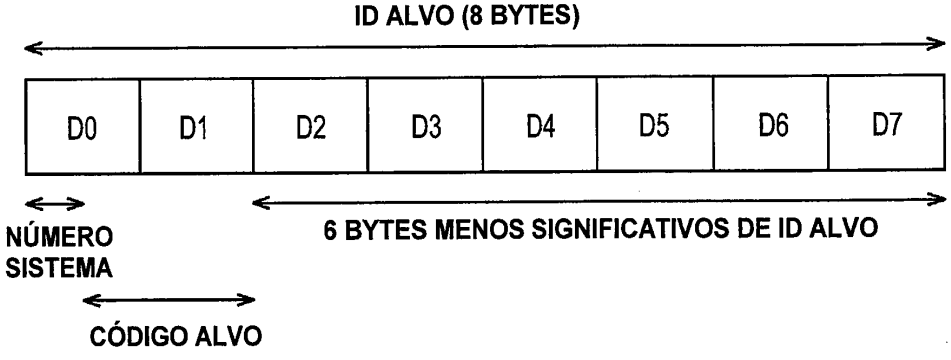


FIG.4

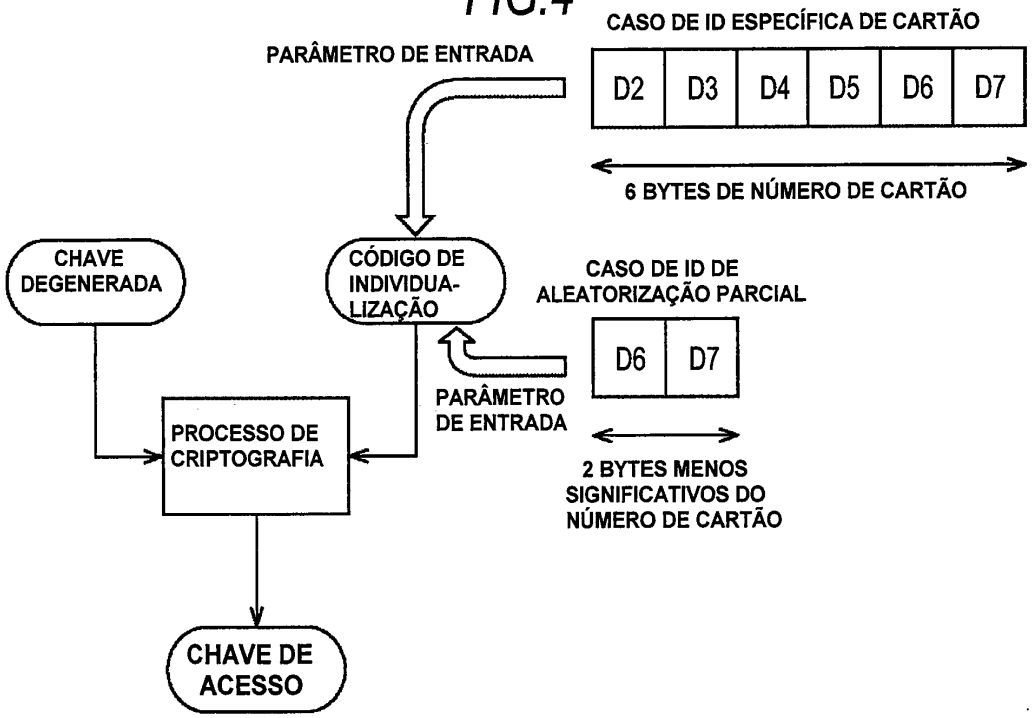

CASO DE ID ESPECÍFICA DE CARTÃO
PARÂMETRO DE ENTRADA
D2
D3
D4
D5
D6
D7
6 BYTES DE NÚMERO DE CARTÃO
CHAVE DEGENERADA
CÓDIGO DE INDIVIDUA-LIZAÇÃO
CASO DE ID DE ALEATORIZAÇÃO PARCIAL
D6
D7
PARÂMETRO DE ENTRADA
PROCESSO DE CRIPTOGRAFIA
2 BYTES MENOS SIGNIFICATIVOS DO NÚMERO DE CARTÃO
CHAVE DE ACESSO

FIG.5

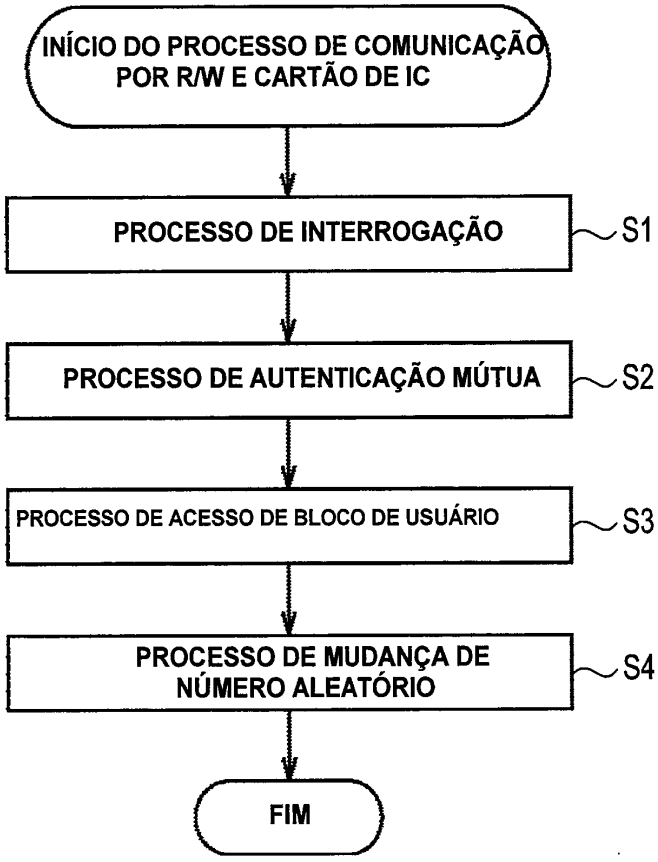

INÍCIO DO PROCESSO DE COMUNICAÇÃO POR R/W E CARTÃO DE IC
PROCESSO DE INTERROGAÇÃO
S1
PROCESSO DE AUTENTICAÇÃO MÚTUA
S2
PROCESSO DE ACESSO DE BLOCO DE USUÁRIO
S3
PROCESSO DE MUDANÇA DE NÚMERO ALEATÓRIO
S4
FIM

FIG.6

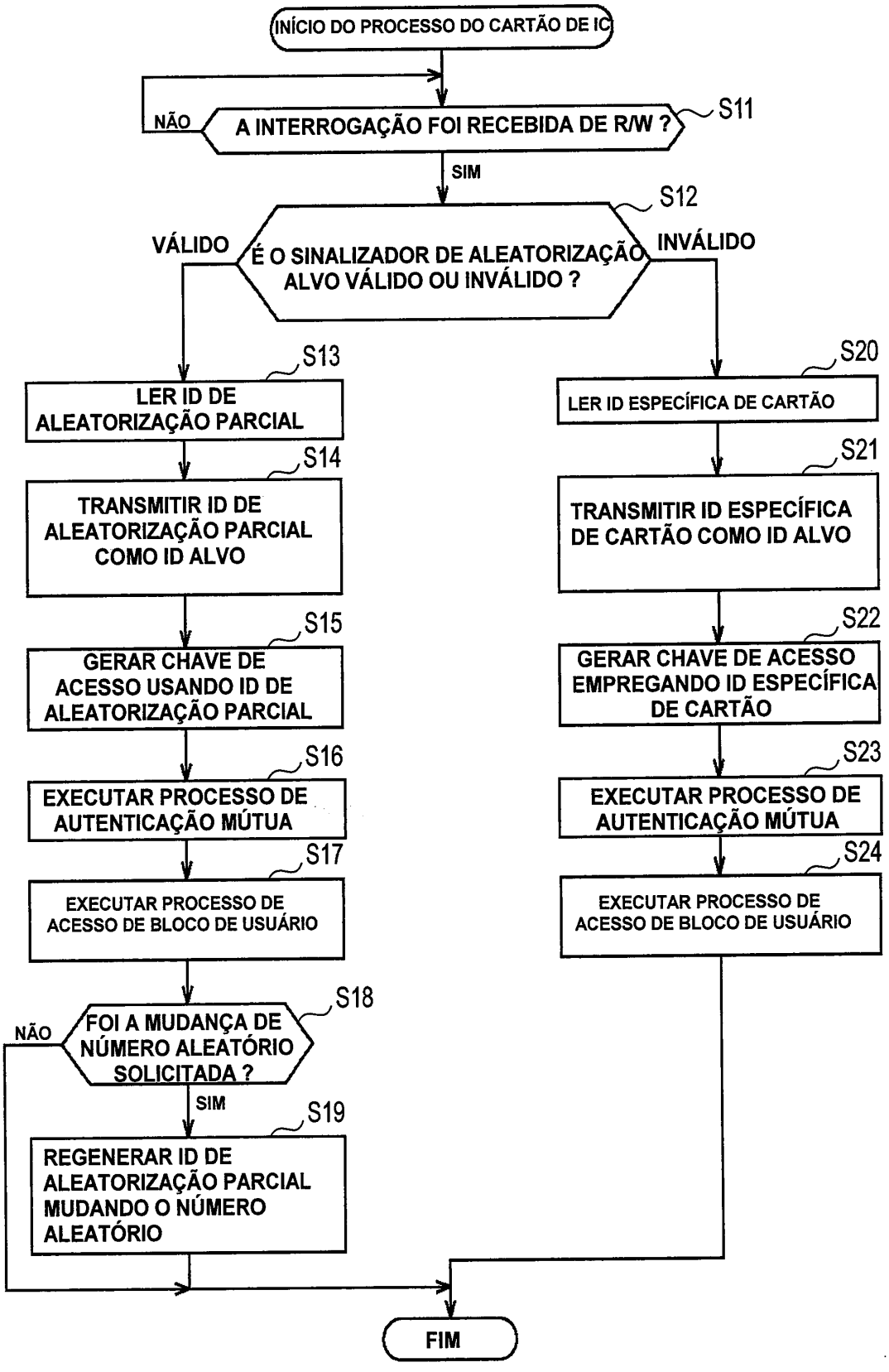

INÍCIO DO PROCESSO DO CARTÃO DE IC
NÃO
A INTERROGAÇÃO FOI RECEBIDA DE R/W ?
S11
SIM
S12
VÁLIDO
É O SINALIZADOR DE ALEATORIZAÇÃO ALVO VÁLIDO OU INVÁLIDO ?
INVÁLIDO
S13
LER ID DE ALEATORIZAÇÃO PARCIAL
S14
TRANSMITIR ID DE ALEATORIZAÇÃO PARCIAL COMO ID ALVO
S15
GERAR CHAVE DE ACESSO USANDO ID DE ALEATORIZAÇÃO PARCIAL
S16
EXECUTAR PROCESSO DE AUTENTICAÇÃO MÚTUA
S17
EXECUTAR PROCESSO DE ACESSO DE BLOCO DE USUÁRIO
S18
NÃO
FOI A MUDANÇA DE NÚMERO ALEATÓRIO SOLICITADA ?
SIM
S19
REGENERAR ID DE ALEATORIZAÇÃO PARCIAL MUDANDO O NÚMERO ALEATÓRIO
S20
LER ID ESPECÍFICA DE CARTÃO
S21
TRANSMITIR ID ESPECÍFICA DE CARTÃO COMO ID ALVO
S22
GERAR CHAVE DE ACESSO EMPREGANDO ID ESPECÍFICA DE CARTÃO
S23
EXECUTAR PROCESSO DE AUTENTICAÇÃO MÚTUA
S24
EXECUTAR PROCESSO DE ACESSO DE BLOCO DE USUÁRIO
FIM

FIG.7

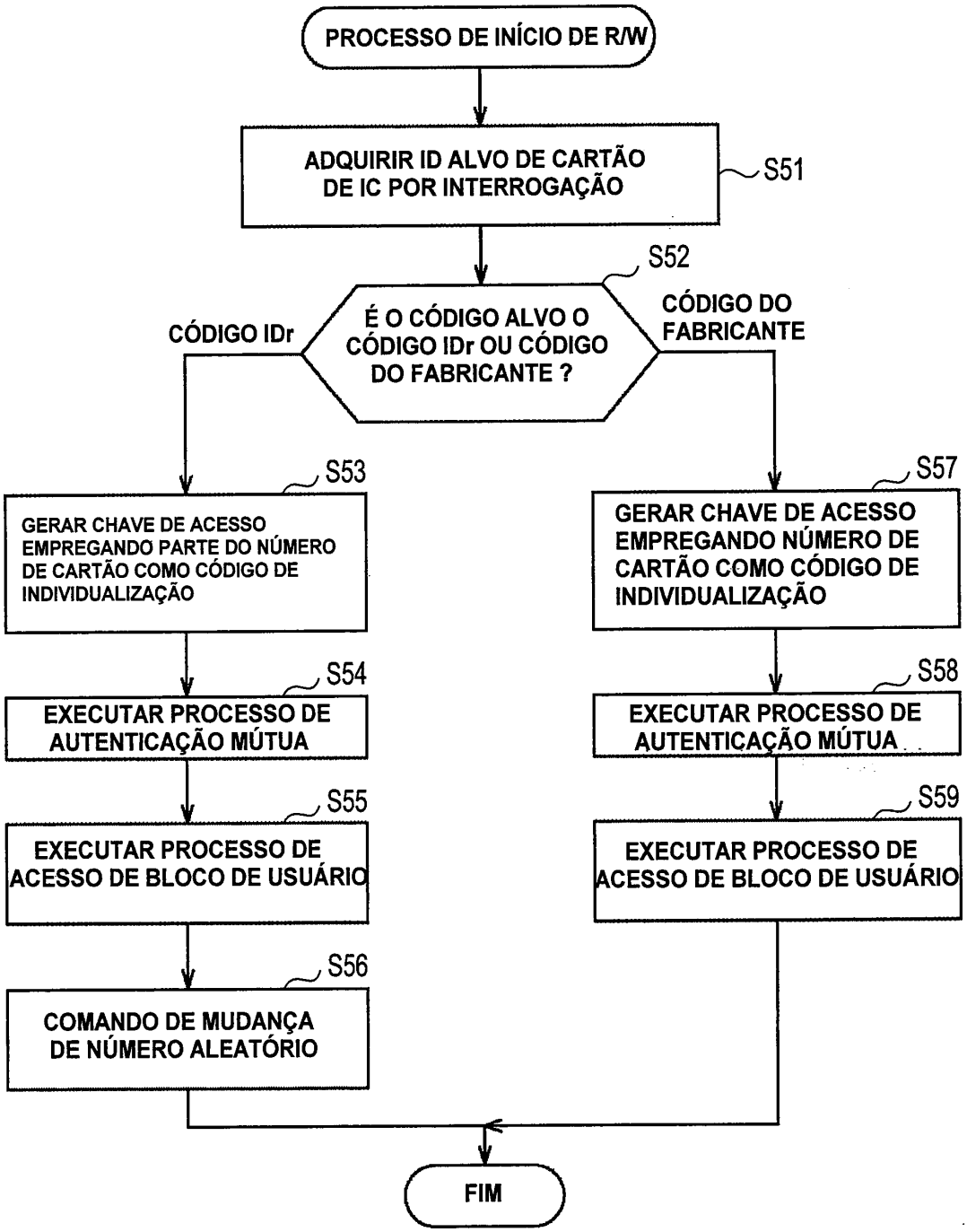
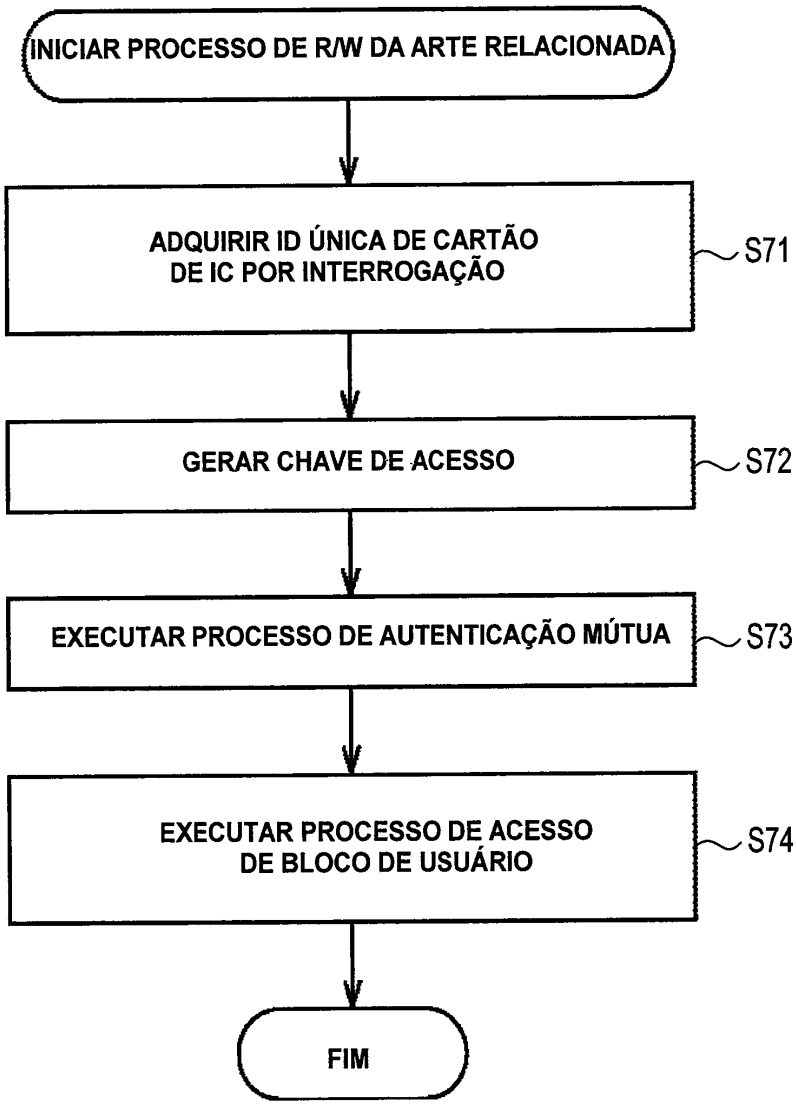

PROCESSO DE INÍCIO DE R/W
ADQUIRIR ID ALVO DE CARTÃO DE IC POR INTERROGAÇÃO
S51
S52
É O CÓDIGO ALVO O CÓDIGO IDr OU CÓDIGO DO FABRICANTE ?
CÓDIGO IDr
CÓDIGO DO FABRICANTE
S53
GERAR CHAVE DE ACESSO EMPREGANDO PARTE DO NÚMERO DE CARTÃO COMO CÓDIGO DE INDIVIDUALIZAÇÃO
S54
EXECUTAR PROCESSO DE AUTENTICAÇÃO MÚTUA
S55
EXECUTAR PROCESSO DE ACESSO DE BLOCO DE USUÁRIO
S56
COMANDO DE MUDANÇA DE NÚMERO ALEATÓRIO
S57
GERAR CHAVE DE ACESSO EMPREGANDO NÚMERO DE CARTÃO COMO CÓDIGO DE INDIVIDUALIZAÇÃO
S58
EXECUTAR PROCESSO DE AUTENTICAÇÃO MÚTUA
S59
EXECUTAR PROCESSO DE ACESSO DE BLOCO DE USUÁRIO
FIM

FIG.8


INICIAR PROCESSO DE R/W DA ARTE RELACIONADA
ADQUIRIR ID ÚNICA DE CARTÃO DE IC POR INTERROGAÇÃO
S71
GERAR CHAVE DE ACESSO
S72
EXECUTAR PROCESSO DE AUTENTICAÇÃO MÚTUA
S73
EXECUTAR PROCESSO DE ACESSO DE BLOCO DE USUÁRIO
S74
FIM

RESUMO

"APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, MÉTODO PARA OPERAR UM APARELHO DE PROCESSAMENTO DE INFORMAÇÃO, E, INSTRUÇÕES DE ARMAZENAMENTO DE DISPOSITIVO DE MEMÓRIA LEGÍVEL POR COMPUTADOR"

Em uma forma de realização exemplo, um aparelho de processamento de informação determina se uma ID alvo é uma ID única ou uma ID de aleatorização parcial, que inclui uma primeira parte sendo substituída por um diferente número e uma segunda parte sendo gerada com base na ID única. Em resposta à ID alvo sendo a ID de aleatorização parcial, o aparelho de processamento de informação gera uma chave de acesso com base na segunda parte da ID de aleatorização parcial e numa chave. O aparelho de processamento de informação executa um processo de autenticação mútua, usando a chave de acesso gerada.