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

(21) **PI 0712152-0 A2**

BRPI0712152A2

(22) Data de Depósito: 11/06/2007
(43) Data da Publicação: 22/02/2012
(RPI 2146)

(51) Int.Cl.:
H04L 9/00

(54) Título: MÉTODO E APARELHO PARA PROVER AUTETENTICAÇÃO E PRIVACIDADE COM DISPOSITIVOS DE BAIXA COMPLEXIDADE

(30) Prioridade Unionista: 09/06/2006 US 60/812,386

(73) Titular(es): Verisign, Inc.

(72) Inventor(es): David M'Raihi, Joseph A. Adler

(74) Procurador(es): Dannemann ,Siemsen, Bigler & Ipanema Moreira

(86) Pedido Internacional: PCT US2007070916 de 11/06/2007

(87) Publicação Internacional: WO 2008/033590de 20/03/2008

(57) Resumo: MÉTODO E APARELHO PARA PROVER AUTENTICAÇÃO E PRIVACIDADE COM DISPOSITIVOS DE BAIXA COMPLEXIDADE. A presente invenção refere-se a um método e aparelho para prover um protocolo criptográfico para uma autenticação, privacidade, e anonimato. O protocolo, em uma modalidade, é projetado para ser implementado em um pequeno número de portas lógicas, executadas rapidamente em dispositivos simples, e prover uma segurança de grau militar.

Relatório Descritivo da Patente de Invenção para **"MÉTODO E APARELHO PARA PROVER AUTENTICAÇÃO E PRIVACIDADE COM DISPOSITIVOS DE BAIXA COMPLEXIDADE".**

Casos Relacionados

O presente pedido de patente reivindica a prioridade do Pedido de Patente Provisório U.S. N. de Série 60/812 386, depositado em 09 de junho de 2006.

Campo da Invenção

A presente invenção refere-se à criptografia e autenticação e, mais particularmente, à criptografia e autenticação em dispositivos de baixa complexidade.

Antecedentes da Invenção

As etiquetas de identificação por radiofreqüência (RFID) estão se tornando cada vez mais comuns. As mesmas são usadas no rastreamento de produtos e outros objetos. De modo geral, quando um marcador de identificação RFID é consultada, a mesma supre a sua identidade, que pode ser, então, usada para pesquisar dados sobre o objeto ao qual a etiqueta de identificação RFID se encontra fixada.

No entanto, algumas entidades querem ser capazes de usar a etiqueta de identificação RFID sem a apresentação dos dados de identificação RFID às consultas de terceiras partes. Por exemplo, o governo norte-americano quer embutir chips de identificação RFID em documentos, tais como, passaportes, ou em cartões do tamanho de um cartão de crédito a fim de ajudar a expedir um processamento de documentos de identificação nos limites de fronteira dos Estados Unidos.

As atuais soluções de uma identificação RFID ostentam quatro vulnerabilidades básicas. Primeiramente, a etiqueta de identificação RFID de modo geral não provê autenticação. Em segundo lugar, uma parte não-autorizada poderia consultar um dispositivo e aprender os dados do chip de identificação RFID, que, no caso de um passaporte, poderia incluir dados suficientes sobre a identidade de seu portador a fim de possibilitar a identificação de um roubo. Em terceiro lugar, um agressor poderia de forma consis-

tente rastrear uma pessoa utilizando um único identificador no chip de identificação RFID.

Sumário da Invenção

É descrito um método e aparelho para prover um protocolo criptográfico para a obtenção de autenticação, privacidade, e anonimato em um dispositivo de baixa complexidade. O protocolo, em uma modalidade, é projetado de modo a ser implementado em um pequeno número de portas lógicas, executado rapidamente em dispositivos simples, e prover uma segurança de grau militar.

Breve Descrição dos Desenhos

A presente invenção é ilustrada, à guisa de exemplo e não à guisa de limitação, nas figuras dos desenhos em anexo, nas quais os numerais de referência similares referem-se a elementos similares, e nas quais:

A figura 1 é um diagrama de rede de uma modalidade dos componentes do serviço criptográfico de acordo com a presente invenção.

A figura 2 é um diagrama em blocos de uma modalidade do servidor e cliente que pode implementar o protocolo criptográfico da presente invenção.

A figura 3 é um fluxograma resumido de uma modalidade de utilização do protocolo criptográfico.

As figuras 4A e 4B são fluxogramas de sinais de uma modalidade de inicialização de uma leitora e de um marcador de acordo com a presente invenção.

A figura 5 é uma fluxograma de sinais de uma modalidade de utilização de um protocolo de identificação ID de etiqueta para a criptografia, autenticação e privacidade.

A figura 6 é um fluxograma de sinais de uma modalidade de utilização de um protocolo de identificação ID de etiqueta para privacidade e rastreamento.

A figura 7 é um fluxograma de sinais de uma modalidade de utilização de um protocolo de identificação ID de etiqueta para a criptografia e não-rastreamento.

A figura 8 é um diagrama em blocos de uma modalidade de um sistema computacional que pode ser usado com a presente invenção.

Descrição Detalhada

O método e aparelho descrito é um protocolo criptográfico para dispositivos de baixa potência que refere-se a um número de exigências de segurança. O protocolo criptográfico também preserva as características de desempenho do presente pedido. Em particular, o dispositivo que inclui este protocolo criptográfico pode ser construído de uma forma relativamente econômica por meio do uso de tecnologias-padrão. O mesmo não requer um grande número de portas lógicas na sua implementação, e, deste modo, pode ser implementado em dispositivo de baixa potência, como, por exemplo, nos chips de identificação RFID passivos. Finalmente, o protocolo permite que um grande número de dispositivos sejam simultaneamente consultados.

Este protocolo inclui a capacidade de prover um ou mais dentre os recursos criptográficos a seguir:

- autenticação. O protocolo pode incluir informações para a verificação criptográfica da autenticidade de um marcador.

- privacidade. O protocolo pode proteger o identificador da etiqueta de modo que uma parte não autorizada não poderá conhecer o identificador da etiqueta.

- não-rastreamento / Ofuscação. O protocolo de uma modalidade nunca retorna exatamente ao mesmo valor. Isto significa que, se uma leitora não sabe qual é a chave para conhecer o identificador de um marcador, a leitora não poderá nem mesmo informar que está se comunicando com a mesma etiqueta.

Em uma modalidade, a autenticação é provida através de uma Criptografia de Curva Elíptica (ECC), e, mais especificamente, um processo de criptografia de curva elíptica que usa um par de chaves pública / privada. Em uma modalidade, a privacidade é provida por meio da criptografia do identificador da etiqueta. Em uma modalidade, a criptografia é feita usando-se um mecanismo baseado em Diffie - Helman a fim de derivar uma chave de criptografia para o identificador de etiqueta, e a criptografia do identifica-

dor de etiqueta com esta chave. Em uma modalidade, um não-rastreamento é provido por meio da geração de um número aleatório para cada troca usada na produção da chave de criptografia.

Em uma modalidade, o presente pedido pode ser implementado usando-se computações sobre um campo de números primos (prime field). Para fins de simplicidade, alguns exemplos apenas mostram a criptografia de curva elíptica (ECC) ou o problema de Diffie - Helman para os campos de números primos. No entanto, uma pessoa versada na técnica entenderia que tanto este método, como uma combinação dos dois métodos, podem ser usados pela presente invenção.

Observa-se que, embora os exemplos do presente pedido descrevam um sistema implementado usando uma leitora e etiqueta de identidade de radiofreqüência (RFID), a presente invenção pode ser usada com qualquer dispositivo de baixa complexidade.

A figura 1 é um diagrama de rede de uma modalidade dos componentes do serviço criptográfico de acordo com a presente invenção. O sistema de identificação RFID 120, em uma modalidade, inclui uma leitora para ler uma ou mais etiquetas de identificação RFID criptografadas 110A, 110B, 110C. Em uma modalidade, o sistema de identificação RFID 120 é capaz de ler múltiplas etiquetas de identificação RFID 110A a 110C simultaneamente. Em uma outra modalidade, cada etiqueta é interrogada por vez. O sistema de identificação RFID 120, em uma modalidade, inclui um sistema criptográfico. Em uma outra modalidade, o sistema de identificação RFID 120 pode ser ligado a um sistema criptográfico a fim de realizar as funções criptográficas descritas no presente documento em associação à leitora.

A leitora 120 solicita a identificação ID de etiqueta de um marcador de identificação RFID criptografada 110A. Em uma modalidade, a solicitação inclui um desafio. A leitora retorna uma resposta criptografada. A resposta criptografada pode se descriptografada por um sistema 120 que possui as chaves apropriadas. Um sistema zombador (spoofer) 130, independentemente de com que freqüência envia uma solicitação de identificação ID de etiqueta, não receberá respostas consistentes (uma vez que as respostas

estarão criptografadas e ofuscadas). Sendo assim, o sistema zombador 130 não será capaz de identificar a identificação ID de etiqueta da etiqueta de identificação RFID criptografada 110A, e, deste modo, não conseguirá pesquisar os dados associados à etiqueta de identificação RFID 110A.

Em uma modalidade, após a descriptografia da resposta de etiqueta e a obtenção da identificação ID da etiqueta, o sistema de identificação RFID 120 pesquisa uma chave pública associada à identificação ID da etiqueta. Em uma modalidade, a pesquisa de chave pública pode ser feita por um sistema remoto 160 acessível via a rede 150. De maneira alternativa, a pesquisa de chave pode ser um sistema local ou incorporada no próprio sistema de identificação RFID 120. Em uma modalidade, o servidor de pesquisa pública 160 pode estar local ao sistema de identificação RFID 120. Em uma modalidade, o servidor de pesquisa pública 160 pode ser um servidor privado não-acessível ao público.

Em uma modalidade, o registro no banco de dados 170 para cada etiqueta de identificação RFID inclui o identificador de etiqueta (ID de etiqueta) e a chave pública de etiqueta Q. Em uma modalidade, o registro pode incluir ainda uma estampa de hora ("time stamp") indicando quando a identificação RFID foi criada. Observa-se, portanto, que estes dados não incluem a chave privada da etiqueta, a qual nunca é armazenada fora da própria etiqueta.

A figura 2 é um diagrama em blocos de uma modalidade do sistema de processamento de baixa potência (LPPS) e seu sistema de comunicação associado. O sistema LPPS pode ser um marcador de identificação RFID, enquanto o sistema de comunicação pode ser uma leitora de identificação RFID.

A etiqueta de identificação RFID 110 inclui um transceptor 250, ou, de maneira alternativa, lógicas de recepção e transmissão separadas. Em uma modalidade, o transceptor 250 é um transceptor de identificação RFID. Em uma modalidade, o sistema LPPS 210 pode ser de uma potência suficientemente baixa, fazendo com que o transceptor 250 seja ativado pelos sinais entrantes, recebidos do sistema 220.

Durante a inicialização, a criptológica 255 calcula uma chave privada para a etiqueta 110, que fica armazenada na memória 260. Observa-se que o termo chave privada no presente relatório descritivo pode se referir a um ponto sobre uma curva elíptica ou a um número primo grande utilizado nos problemas de Diffie - Helman. Uma chave pública é a função ou valor que provê o par de chave para a chave privada.

A etiqueta de identificação RFID 110 recebe uma chave pública, ou, em outra modalidade, múltiplas chaves públicas do sistema de identificação RFID 120. A etiqueta de identificação RFID 110 também recebe o seu identificador de etiqueta (ID de etiqueta) do sistema 120, e armazena o manso na memória 260. Em uma modalidade, a chave privada tem um valor igual ao comprimento da ordem de E(F), e é aleatoriamente gerada. A criptológica 255 da etiqueta 110 calcula ainda a chave pública da etiqueta de identificação RFID com base na chave privada da etiqueta. Esta chave pública, em uma modalidade assinada por uma autoridade de certificação, é usada para a autenticação do sistema LPPS 210.

A memória 260 é usada para armazenar a chave privada (um número aleatório a, gerado dentro da etiqueta), assim como o identificador ID da etiqueta e as chaves públicas da leitora (recebidas durante a inicialização). O número de portas requerido para armazenar a chave privada, as chaves públicas, e o identificador ID da etiqueta, e computar a função de autenticação é proporcional ao comprimento das chaves. Sendo assim, a minimização do tamanho da chave, ao mesmo tempo garantindo a segurança, é de interesse. Portanto, em uma modalidade, o sistema utiliza um campo ternário como F, que permite a redução do tamanho da palavra de 163 em um campo binário para 107 em um campo ternário, uma redução de aproximadamente 35 % no tamanho da palavra, sem diminuir a segurança do sistema. Isto significa que, ao se usar portas lógicas ternárias ao invés de portas lógicas binárias, menos portas lógicas serão necessárias, e que algumas operações (como, por exemplo, de multiplicação) podem ficar mais rápidas.

Em uma modalidade, o sistema inclui uma lógica de adulteração

265. A lógica de adulteração 265 oferece resistência à adulteração. Em uma modalidade, a etiqueta como um todo é inviolável. Em uma outra modalidade, apenas a memória 260, ou a porção da memória que armazena a chave privada é inviolável. Em uma modalidade, a resistência à adulteração pode incluir uma lógica que apaga a memória caso o sistema detecte uma tentativa de ler a memória, invadir o barramento, etc. Isto pode ser implementado, em uma modalidade, usando fusíveis.

Durante o uso para autenticação, a criptológica 255 recebe um desafio, e calcula uma resposta para o desafio. A resposta ao desafio é uma resposta criptografada, autenticada, e ofuscada, que garante que a resposta da etiqueta de identificação RFID 110 seja sempre diferente, mesmo que um desafio igual seja enviado repetidas vezes. Os cálculos, em uma modalidade, são feitos sobre as curvas elípticas selecionadas sobre os campos finitos selecionados. Conforme notado acima, este campo, em uma modalidade, é um campo binário conhecido.

O sistema de identificação RFID 220 inclui uma leitora de identificação RFID 210, que envia um desafio para a etiqueta de identificação RFID 210. O desafio é gerado pelo calculador de desafio 220, com base em um número aleatório criado pelo gerador de número aleatório 215. Em uma modalidade, o número aleatório é um número de uma ordem similar em magnitude à ordem de E.

Quando a etiqueta de identificação RFID 210 responde ao desafio, a resposta inclui o identificador ID de etiqueta criptografado e a resposta do desafio. O criptocalculador 230 é usada para descriptografar a resposta criptografada, e obter o identificador ID de etiqueta a partir da resposta. A lógica de pesquisa de chave pública 225 usa o identificador ID de etiqueta para pesquisar a chave pública da etiqueta em um banco de dados. Conforme notado acima, o banco de dados pode fazer parte do sistema de identificação RFID 120, local, ou remoto, e acessível via uma rede.

O criptocalculador 230 assume o número aleatório e usando a chave pública calcula o valor da chave pública. O valor da chave pública deve ser igual à resposta do desafio retornada pela etiqueta de identificação

RFID. Sendo assim, a lógica de comparação 235 faz uma comparação entre a resposta de desafio retornada pela etiqueta de identificação RFID 210 e o resultado do cálculo. Quando os valores são idênticos, o sistema de identificação RFID 120 certifica a etiqueta de identificação RFID 210. Em uma modalidade, a lógica de validação 240 emite as informações apropriadas indicando que a etiqueta de identificação RFID 110 foi validade. Em uma modalidade, o sistema de identificação RFID 120 tem um mecanismo de saída para indicar se a etiqueta de identificação RFID 110 é válida.

A figura 3 é um fluxograma resumido de uma modalidade de utilização do protocolo criptográfico. O processo começa com a inicialização.

No bloco 310, os dados comuns são compartilhados entre um marcador e a leitora. A etiqueta pode ser qualquer dispositivo de processamento de baixa complexidade, por exemplo, um marcador de identificação (RFID) por radiofreqüência. A leitora pode ser qualquer dispositivo projetado para fazer interface com a etiqueta, como, por exemplo, uma leitora de identificação RFID. Em uma modalidade, o termo "leitora" refere-se ao sistema que interagem com a etiqueta, assim como o sistema que provê serviços criptográficos. No entanto, em uma modalidade, estas funções podem ser representadas por dispositivos separados acoplados através de uma conexão de rede ou de outra forma. Os dados comuns definem as curvas elípticas, campos, e pontos necessários a uma criptografia elíptica, ou os geradores e números primos grandes para uma criptografia tradicional. O termo "originador" é utilizado na presente patente de modo a se referir ao gerador para um número primo grande e ao ponto em um campo elíptico utilizado para uma criptografia de curva elíptica.

No bloco 315, as chaves são compartilhadas entre a etiqueta e a leitora. Em uma modalidade, as chaves incluem um ou mais pares de chave públicos / privados, que podem utilizar a criptografia elíptica ou a criptografia de números primos grandes tradicional. Em uma modalidade, três pares de chave são criados, cada qual para autenticação, criptografia, e ofuscação. Em uma modalidade, a etiqueta cria suas próprias chaves.

Quando chaves privadas e as chaves públicas apropriadas são

armazenadas, no bloco 320, a inicialização se completa. Em uma modalidade, a etiqueta armazena a chave pública da leitora e sua própria chave privada e identificação (n), e a leitora armazena a sua própria chave privada. Em uma modalidade, a chave pública da etiqueta e a identificação (n) são armazenadas em um diretório de chaves públicas separadas.

Os processos abaixo fazem parte da obtenção da chave pública da etiqueta para fins de identificação. O processo abaixo, além de prover um identificador ID de etiqueta autenticado, provê ainda o identificador ID de etiqueta de uma maneira a criptografar o identificador ID de etiqueta, e obscurecer o seu valor. Isto garante que se uma leitora zombadora tentar discernir a criptografia enviando os mesmos tempos múltiplos de desafio, os dados retornados não serão idênticos.

No bloco 325, a leitora computa um desafio para a etiqueta. O desafio é projetado de modo a deduzir as informações que permitam a leitora determinar o identificador ID de etiqueta da etiqueta. O desafio, em uma modalidade, é um valor aleatório. Em uma modalidade, o desafio é um valor aleatório ao longo da curva elíptica sobre o campo finito selecionado.

No bloco 330, a etiqueta computa uma resposta para o desafio. A resposta ao desafio, em uma modalidade, é a chave privada da etiqueta vezes o desafio.

No bloco 335, a etiqueta computa os dados de retorno, que vêm a ser uma combinação da resposta ao desafio e três valores aleatórios criptografados com três chaves, uma para a criptografia, uma para a autenticação, e uma para a privacidade. Em uma modalidade, a etiqueta gera dois valores aleatórios (s e u), e criptografa cada qual com uma chave correspondente (de criptografia e de ofuscação, respectivamente). A chave de autenticação é criptografada com a chave pública da leitora. A etiqueta em seguida retorna um valor concatenado incluindo todos os quatro valores aleatórios. Em uma modalidade, o valor retornado inclui o identificador de etiqueta (n).

No bloco 340, a leitora, que recebe os dados de retorno da etiqueta, utiliza a sua chave privada para computar n (ID de etiqueta) a partir

dos dados de retorno.

No bloco 345, a leitora pesquisa a chave pública da etiqueta, usando o identificador ID de etiqueta.

No bloco 350, a leitora verifica se os dados retornados incluem a resposta ao desafio assinada. Caso positivo, conforme verificado no bloco 355, a leitora conhece o identificador ID da etiqueta (n) e sabe se este identificador ID foi autenticado pela resposta ao desafio. A leitora pode então, no bloco 360, utilizar o identificador ID de etiqueta a fim de realizar outras atividades. Por exemplo, o identificador ID de etiqueta pode ser usado para pesquisar dados em um outro banco de dados, verificar a autorização para a etiqueta, etc. O processo em seguida finaliza, no bloco 365.

As figuras 4A e 4B são fluxogramas de sinais de uma modalidade de inicialização de uma leitora e um marcador de acordo com a presente invenção. O sistema pode usar a criptografia de curva elíptica (ECC) ou usar os tradicionais parâmetros de criptografia de chave pública.

No bloco 405, a etiqueta e a leitora são inicializadas com parâmetros criptográficos. Quando o sistema criptográfico usado no sistema de curva elíptica é o sistema de curva elíptica, em uma modalidade, os seguintes valores são definidos:

1. Uma primeira curva elíptica E_A e um campo finito $\mathfrak{F}_A$ para a autenticação (de etiqueta).

2. Um primeiro ponto $P_A = (x_A, y_A)$ sobre a primeira curva elíptica E_A ($\mathfrak{F}_A$) para a autenticação (de etiqueta).

3. Uma segunda curva elíptica E_E e um campo finito $\mathfrak{F}_A$ para a criptografia (de identificador ID de etiqueta).

4. Um segundo ponto $P_E = (x_E, y_E)$ sobre a segunda curva elíptica E_E ($\mathfrak{F}_A$) para a criptografia (de identificador ID de etiqueta).

5. Uma terceira curva elíptica E_O e um campo finito $\mathfrak{F}_O$ para a ofuscação (de identificador ID de etiqueta).

6. Um terceiro ponto $P_O = (x_O, y_O)$ sobre a terceira curva elíptica E_O ($\mathfrak{F}_A$) para a ofuscação (de identificador ID de etiqueta).

Para cada um dos pontos, o conjunto de todos os pontos que

podem ser gerados por meio da multiplicação de $P_{A/E/O}$ por inteiros deve ser similar em tamanho ao número total de pontos sobre a curva elíptica no campo. Mais formalmente, a ordem do conjunto $\{P_i \mid \exists\ x$ de tal modo que $P = P_A^x\}$ deve ser similar à ordem de E_A ($\mathcal{F}_A$).

Em uma modalidade, os recursos da autenticação, da criptografia, e da ofuscação podem utilizar curvas elípticas separadas, campos finitos, e/ou pontos sobre as curvas elípticas, conforme descrito acima. Em uma outra modalidade, os campos definidos, as curvas, e/ou os pontos podem ser idênticos. Em uma modalidade, a mesma curva elíptica, campo, e pontos são usados para todos os três aspectos criptográficos (autenticação, criptografia, e ofuscação). Estes aspectos E_A, E_E, E_O, $\mathcal{F}_A$, $\mathcal{F}_A$, $\mathcal{F}_A$, e P_A, P_E, P_O são usados para inicializar a etiqueta e a leitora. A função de uma via para a criptografia ECC é: f(a, B) = a . B, na qual o operador de ponto significa a multiplicação de ponto. Por exemplo, a. B significa "multiplique o ponto B pelo inteiro de a".

Para um método tradicional de criptografia, a criptografia que utiliza computações em um grande campo de números primos, em uma modalidade, os seguintes valores são definidos:

1. Escolher um número primo de Q_A para a autenticação (de etiqueta).

2. Escolher um gerador $g_A \in [2, Q_A - 1]$ para a autenticação (de etiqueta).

3. Escolher um número primo de Q_E para a criptografia (de identificador ID de etiqueta).

4. Escolher um gerador $g_E \in [2, Q_E - 1]$ para a criptografia (de identificador ID de etiqueta).

5. Escolher um número primo de Q_O para a ofuscação (de identificador ID de etiqueta).

6. Escolher um gerador $g_O \in [2, Q_O - 1]$ para a ofuscação (de identificador ID de etiqueta).

Em uma modalidade, os geradores e números primos podem ser idênticos para cada um dos valores (autenticação, criptografia, e ofuscação).

A função de uma via para as computações sobre um campo de números primos é:

$$f(a, B) = B^a \bmod p.$$

Os geradores $g_{A/E/O}$ e os pontos $P_{A/E/O}$ podem ser coletivamente referidos como os originadores $O_{A/E/O}$.

Como acima, estes geradores criptográficos são usados para inicializar a etiqueta e a leitora. Observa-se que uma leitora / etiqueta usará um tipo de criptografia. Neste caso, a criptografia elíptica e as computações sobre um campo de números primos grandes são descritas. No entanto, as funções criptográficas que geram pares de chaves de criptografia e descriptografia seguras podem ser usadas.

A inicialização pode ocorrer de diversas maneiras. Em uma modalidade, todos os componentes de sistema são programados anteriormente com os mesmos parâmetros, de modo que nenhum acordo seja necessário. Em uma outra modalidade, cada componente de sistema receberá uma descrição completa de quais parâmetros usar para comunicação. Ainda em uma outra modalidade, os dois lados especificarão quais parâmetros usar a partir de um conjunto de parâmetros padrão com nomes bem conhecidos. Por exemplo, vide a seção 5.1.1 do padrão RFC 4492 http://www.faqs.org/rfcs/rfc4492.html, que especifica identificadores de 16 bits para algumas curvas elípticas e campos-padrão. em uma outra modalidade, os dois lados selecionarão os parâmetros de um conjunto de parâmetros acordados ou predeterminados. Podem ser usadas formas alternativas de se garantir que ambos os componentes apresentem estes parâmetros.

No bloco 410, a leitora coleta um valor aleatório r como a sua chave de criptografia. No bloco 415, a leitora computa a chave correspondente $R = f(r, P_E)$, que vem a ser a chave pública associada à chave de criptografia r, a fim de criar um par de chaves (R, r).

No bloco 420, a leitora coleta um segundo valor aleatório j como a chave de ofuscação. No bloco 430, o par de chaves de ofuscação (J, j) é computado pelo cálculo $J = f(j, P_O)$. Sendo assim, a leitora gera um par de chaves (R, r) para criptografia, e um segundo par de chaves (J, j) para a o-

fuscação da identidade da etiqueta. Em uma modalidade, R = J e r = j. Os valores de r e j são armazenados na leitora.

No bloco 440, a leitora envia as chaves públicas (R e J) juntamente com o identificador ID de etiqueta (n) para a etiqueta, dizendo para a etiqueta se inicializar. Em uma modalidade, o sistema de identificação RFID seleciona n para ser um número aleatório. Em uma modalidade, o valor n do identificador ID de etiqueta é selecionado para ser menor que o comprimento das chaves (R e J). Em uma modalidade, o processo de inicialização pode ser feito simultaneamente com um número de etiquetas.

No bloco 445, os valores de n, R, e J são salvos em uma memória interna da etiqueta. Conforme notado acima, a memória interna é uma memória segura. Em uma modalidade, a memória interna não pode ser acessada sem passar pelo processo criptográfico sem destruir a etiqueta.

No bloco 450, um valor aleatório a é selecionado pela etiqueta como a sua chave privada, e salvo na memória interna da etiqueta. A memória interna, em uma modalidade, é a memória segura. Em uma modalidade, apenas o identificador ID de etiqueta e a chave privada da etiqueta são armazenados na memória segura.

No bloco 455, a etiqueta computa uma chave público Q - f (a, P_A). No bloco 460, o valor Q é enviado para a leitora / sistema. Em uma modalidade, a leitora / sistema encaminha a chave pública da etiqueta para um diretório de chave pública (bloco 465). O diretório de chave pública armazena o valor de Q em associação ao valor n (o identificador ID de etiqueta) no bloco 470. No bloco 475, o diretório de chave pública reconhece que os valores foram armazenados de maneira bem-sucedida.

A figura 5 é um fluxograma de sinais de uma modalidade de uso de um protocolo de identificador ID de etiqueta para criptografia, autenticação e ofuscação. Este processo é inicializado quando o sistema de identificação RFID deseja obter os dados de um marcador. Em uma modalidade, o sistema de identificação RFID pode realizar o mesmo processo em paralelo com mais de um marcador de identificação RFID.

No bloco 510, o sistema de identificação RFID coleta um valor

aleatório c. No bloco 515, o sistema de identificação RFID computa o desafio C = f (c, PA). O desafio C é o par de valor aleatório C. Em uma modalidade, a função de criptografia E assume o XOR do texto simples e a chave para gerar o texto cifrado. Para uma mensagem n e um ponto P_i, este texto seria c - E (m, Pi) = m ⊕ bin (Pi). Para esta opção de função criptográfica, a descriptografia funcionaria da mesma maneira: m = D (c, P_i) = c ⊕ bin (P_i). No bloco 520, o sistema envia uma mensagem solicitando a identidade da etiqueta e a resposta da etiqueta para o desafio C. A mensagem inclui o desafio C.

No bloco 525, a etiqueta computa A = f (a, C). O valor a é a chave privada da etiqueta de identificação RFID.

No bloco 530, a etiqueta gera um valor aleatório s. O valor aleatório s, em uma modalidade, é gerado usando um gerador de número aleatório. Em uma outra modalidade, o valor é gerado usando uma função física não copiável (PUF). No bloco 535, em uma modalidade, S = f (s, P_E) é calculado. Conforme previamente notado, PE = (x_E, y_E) é um ponto sobre a segunda curva elíptica (E_E ($\mathbb{F}_A$) para criptografia (identificador ID de etiqueta).

O sistema, no bloco 540, computa o valor k_E = f (s, R). R é uma das chaves públicas do sistema de identificação RFID, enquanto s é o número aleatório gerado acima. No bloco 542, a etiqueta de identificação RFID computa B = E (n, k_E). O valor n é o identificador ID de etiqueta, enquanto k_E = f (s, R), conforme notado acima.

Em uma modalidade, o sistema no bloco 545, coleta um segundo número aleatório u. No bloco 550, a etiqueta computa U = f (u, Po). Conforme notado acima, Po = (x_O, y_O) é um ponto sobre a terceira curva elíptica E_O ($\mathbb{F}_A$) para ofuscação (identificador ID de etiqueta). No bloco 555, o sistema computa k_O = f (u, J), no qual é o segundo número aleatório e J é a segunda chave pública da leitora de identificação RFID.

No bloco 565, a etiqueta computa G = f (A, k_O). A = f (a, C) e é uma função da chave privada da etiqueta e do desafio, enquanto k_O = f (u, J).

No bloco 570, a etiqueta retorna os valores S, U, B, e G, sendo

que $S = f(s, P_E)$, $U = (u, P_O)$, $B = E(n, k_E)$, $G = f(A, k_O)$. Em uma modalidade, a etiqueta retorna uma concatenação destes valores. Uma das propriedades deste protocolo é que a etiqueta retorna toda vez uma resposta diferente (e então um marcador não pode ser monitorada, mas um chaveiro (key holder) (leitora autorizada) poderá determinar a identidade da etiqueta com base nos dados retornados.

A leitora em seguida faz os seguintes cálculos:

- computar $k_E = f(r, S)$ usando a chave privada r e valor S provido

- computar k_O - f (j, U) usando a chave privada j e valor U provido

- computar $n = D(B, k_E)$ usando o valor k_E computado e valor B provido.

O valor n é o identificador ID de etiqueta, usado no bloco 580 para solicitar a chave pública para a etiqueta n do diretório de chave pública. No bloco 585, o diretório de chave pública retorna a chave pública da etiqueta Q. A leitora em seguida computa (590) $A = D(G, k_O)$, usando o valor G provido, e o valor k_O computado, e verifica que $A = f(c, Q) = f(a, C)$. Quando a verificação é correta, a leitora sabe que a etiqueta é autêntica, e o identificador ID de etiqueta é exato, e pode usar o identificador ID de etiqueta para várias funções, tais como pesquisa, certificação, ou outras.

Observa-se que, embora este exemplo descreva as funções sobre uma curva elíptica, o protocolo criptográfico descrito poderá utilizar, em seu lugar, números primos grandes. Nos números primos grandes, cada f (x, P) é substituído por f (x, g), em que g é um gerador para um número primo grande.

A figura 6 é um fluxograma de sinais de uma modalidade usando um protocolo de identificador ID de etiqueta menor para criptografia e ofuscação. Este processo menor simplifica alguns cálculos, ao definir pontos com o mesmo valor. No bloco 610, o sistema de identificação RFID coleta um valor aleatório c. No bloco 615, o sistema de identificação RFID computa o desafio $C = f(c, P_A)$. O desafio C é o par de valores aleatórios c. No bloco 620, o sistema envia uma mensagem solicitando a identidade da etiqueta,

incluindo o desafio C.

No bloco 625, a etiqueta computa A = f (a, C). O valor a é a chave privada da etiqueta de identificação RFID.

No bloco 630, a etiqueta gera um valor aleatório s. Em uma modalidade, o valor aleatório s pode ser gerado usando um gerador de número aleatório. Em uma outra modalidade, o valor aleatório s pode ser gerado usando uma função fisicamente não copiável (PUF). No bloco 635, S = f (s, P_E) é calculado. Conforme previamente notado, $P_E = (x_E, y_E)$ é um ponto sobre a segunda curva elíptica (E_E ($\mathcal{F}_A$) para criptografia (identificador ID de etiqueta).

No bloco 640, T = f (s, R) é calculado. R é uma das chaves públicas do sistema de identificação RFID, enquanto s é o número aleatório gerado acima. No bloco 645, a etiqueta computa k_E, k_O = g (T). A função g() computa uma cadeia longa o suficiente para XOR com n | A. A função g:k - > k_1, k_2 é usada para gerar dois valores de comprimento / a partir de uma entrada de comprimento /. Os valores são pseudo-aleatórios, em uma modalidade, e é melhor usar algo criptograficamente seguro como uma função g().

No bloco 650, a etiqueta de identificação RFID computa B = E (n, k_E). O valor n é o identificador ID de etiqueta, enquanto k_E = f (s, R), conforme notado acima. No bloco 655, a etiqueta computa G = f (A, k_O). A = f (a, C) e é uma função da chave privada da etiqueta e do desafio.

No bloco 660, a etiqueta retorna os valores S, B, e G. Em uma modalidade, a etiqueta retorna uma concatenação destes valores. S = f (s, P_E), B = E (n, k_E), G = f (A, k_O).

A leitora em seguida realiza os seguintes cálculos:

- computar T = f (r, S) usando a chave privada r e o valor S provido

- computar k_E . k_O = g (T)

- computar n = D (B, k_E) usando o valor k_E computado e o valor B provido.

- computar A = D (G, k_O) usando o valor G provido, e o valor k_O computado.

O valor n é o identificador ID de etiqueta, usado no bloco 670 para solicitar a chave pública para a etiqueta n do diretório de chave pública. No bloco 675, o diretório de chave pública retorna a chave pública da etiqueta Q. A leitora em seguida verifica se A = f (c, Q) = f (a, C), no bloco 680. Quando a verificação é correta, a leitora sabe que a etiqueta é autêntica, e o identificador ID de etiqueta é exato, e pode usar o identificador ID de etiqueta para várias funções, tais como pesquisa, certificação, ou outras.

A figura 7 é um fluxograma de sinais de uma modalidade de uso de um protocolo de identificador ID de etiqueta simplificado para privacidade e não-rastreamento. Este protocolo criptográfico provê privacidade e não-rastreamento, mas não-autenticação. No bloco 710, o sistema envia uma mensagem solicitando a identidade da etiqueta.

No bloco 715, a etiqueta seleciona o valor aleatório s.

No bloco 720, a etiqueta computa S = f (s, P_E). Conforme previamente notado, PE = (x_E, y_E) é um ponto sobre a segunda curva elíptica (E_E (□$_E$) para criptografia (identificador ID de etiqueta).

No bloco 725, a etiqueta computa k_E = f (s, R). R é a chave pública da leitora, enquanto s é o valor aleatório.

No bloco 730, a etiqueta computa B = E (n, k_E). O valor n é o identificador ID de etiqueta, enquanto k_E = f (s, R), conforme notado acima. No bloco 735, a etiqueta retorna os valores S e B para a leitora. Observa-se que, uma vez que tanto S como B são pelo menos em parte uma função do número s aleatório, estes valores são diferentes para cada resposta.

A leitora em seguida realiza os seguintes cálculos:

(740) k_E = f (r, S), em que r é a chave privada da leitora, e S é recebido da etiqueta

(745) Computar n = D (B, k_E) usando o valor k_E computado e o valor B provido

O valor n é o identificador ID de etiqueta, que pode então ser usado para pesquisar dados sobre os objetos associados à etiqueta. Observa-se que este processo não provê a autenticação da etiqueta. No entanto, provê o não-rastreamento e a privacidade.

A figura 8 é um diagrama em blocos de uma modalidade de um sistema computacional que pode ser usado com a presente invenção. a figura 8 é uma modalidade de um sistema computacional que pode ser usado com a presente invenção. Contudo, tornar-se-á aparente àqueles versados na técnica que outros sistemas alternativos de várias arquiteturas de sistema poderão ser também usados.

O sistema de processamento de dados ilustrado na figura 8 inclui um barramento ou outro meio de comunicação interno, e um processador 810 acoplado ao barramento 815 para o processamento de informações. O sistema compreende ainda uma memória de acesso aleatório (RAM) ou outro dispositivo de armazenamento volátil 850 (referido como memória), acoplado ao barramento 815 para o armazenamento de informações e instruções a serem executadas pelo processador 810. A memória principal 850 pode ainda ser usada para o armazenamento de variáveis temporárias ou outras informações intermediárias durante a execução de instruções por parte do processador 810. O sistema compreende ainda uma memória de leitura (ROM) e/ou um dispositivo de armazenamento estático 820 acoplado ao barramento 815 para o armazenamento de informações e instruções estáticas para o processador 810, e um dispositivo de armazenamento de dados 825, como, por exemplo, um disco magnético ou disco ótico e sua correspondente unidade de disco. O dispositivo de armazenamento de dados 825 é acoplado ao barramento 815 para o armazenamento de informações e instruções.

O sistema pode ainda ser acoplado a um dispositivo de imagem 870, como, por exemplo, um tubo de raios catódicos (CRT) ou uma tela de cristal líquido (LCD) acoplado ao barramento 815 através do barramento 865 para a exibição de informações a um usuário de computador. Um dispositivo de entrada alfanumérico 875, incluindo chaves alfanuméricas e outras chaves, pode também ser acoplado ao barramento 815 através do barramento 865 para a comunicação de informações e seleções de comandos a um processador 810. Um dispositivo de entrada de usuário adicional é o dispositivo de controle de cursor 860, como, por exemplo, um mouse, um trackball, uma

caneta, ou as chaves de direção de cursor acopladas ao barramento 815 através do barramento 865 para a comunicação de informações de direção e para as seleções de comandos a um processador 810, e para o controle do movimento do cursor no dispositivo de imagem 870.

Um outro dispositivo, que pode opcionalmente ser acoplado ao sistema comunicação 800 é um dispositivo de comunicação 890 para o acesso aos demais nós de um sistema distribuído via uma rede. O dispositivo de comunicação 890 pode incluir qualquer número de dispositivos periféricos de rede comercialmente disponíveis, como, por exemplo, os utilizados para o acoplamento a uma Ethernet, "token ring", internet, ou uma rede de longa distância. O dispositivo de comunicação 890 pode ainda ser uma conexão de modem nulo, ou qualquer outro mecanismo que provenha conectividade entre o sistema computacional 800 e o mundo exterior. Observa-se que qualquer ou todos os componentes do sistema ilustrado na figura 8 e hardware associado podem ser usados em diferentes modalidades da presente invenção.

Será apreciado por aqueles versados simples na técnica que qualquer configuração do sistema pode ser usada para várias finalidades de acordo com a implementação em particular. A lógica ou software de controle que implementa a presente invenção pode ser armazenada na memória principal 850, no dispositivo de armazenamento de massa 825, ou outro meio de armazenamento local ou remotamente acessível ao processador 310.

Ficará aparente àqueles versados na técnica que o sistema, método, e processo descritos no presente documento podem ser implementados como um software armazenado na memória principal 850 ou na memória de leitora 820 e executados pelo processador 810. Esta lógica ou software de controle pode também estar residente em um artigo de fabricação, compreendendo um meio legível em computador tendo um código de programa legível em computador incorporado no mesmo e sendo legível pelo dispositivo de armazenamento de massa 825 e de modo a fazer com que o processador 810 opere de acordo com os métodos e ensinamentos do pre-

sente documento.

A presente invenção pode ser ainda incorporada em um dispositivo portátil ou manual contendo um subconjunto dos componentes de hardware de computador descritos acima. Por exemplo, o dispositivo portátil pode ser configurado de modo a conter apenas o barramento 815, o processador 810, e a memória 850 e/ou 825. O dispositivo portátil pode ainda ser configurado de modo a incluir um conjunto de botões ou componentes de sinalização de entrada com os quais um usuário poderá selecionar dentre um conjunto de opções disponíveis. O dispositivo portátil pode ainda ser configurado de modo a incluir uma aparelho de saída, como, por exemplo, uma tela de cristal líquido (LCD) ou matriz de elemento de imagem para a exibição de informações a um usuário do dispositivo portátil. Podem ser usados métodos convencionais a fim de implementar tal dispositivo portátil. A implementação da presente invenção para tal dispositivo seria aparente a uma pessoa versada na técnica dada a apresentação da presente invenção conforme provida no presente documento.

A presente invenção pode ainda ser incorporada em um aparelho de uso especial, incluindo um subconjunto de componentes de hardware de computador descritos acima. Por exemplo, o aparelho pode incluir um processador 810, um dispositivo de armazenamento de dados 825, um barramento 815, e uma memória 850, e apenas mecanismos de comunicação rudimentares, tais como uma pequena tela sensível ao toque que permite ao usuário se comunicar de uma maneira básica com o dispositivo. Em geral, quanto mais o dispositivo for de uso especial, menos elementos precisam estar presentes para o dispositivo funcionar. Em alguns dispositivos, a comunicação com o usuário pode ser através de uma tela sensível ao toque ou mecanismo similar.

Será apreciado pelos versados na técnica que qualquer configuração do sistema pode ser usada para diversas finalidades de acordo com a implementação em particular. A lógica ou software de controle que implementa a presente invenção pode ser armazenada em qualquer meio legível em máquina local ou remotamente acessível ao processador 810. Um meio

legível em máquina inclui qualquer mecanismo para o armazenamento e transmissão de informações em uma forma legível por uma máquina (por exemplo, um computador). Por exemplo, um meio legível em máquina inclui a memória de leitora (ROM), uma memória de acesso aleatório (RAM), um meio de armazenamento em disco magnético, dispositivos de memória flash, sinais elétricos, ópticos, acústicos, ou outras formas de sinais propagados (por exemplo, ondas portadoras, sinais infravermelhos, sinais digitais, etc.).

No relatório descritivo acima, a presente invenção foi descrita com referência a modalidades exemplares específicas da mesma. No entanto, ficará evidente que várias modificações e alterações podem ser feitas à invenção sem se afastar do espírito e âmbito de aplicação da presente invenção conforme apresentada nas reivindicações em apenso. O relatório descritivo e os desenhos devem, portanto, ser considerados em um sentido ilustrativo ao invés de um sentido restritivo.

REIVINDICAÇÕES

1. Método para prover um protocolo criptográfico, compreendendo:

- uma autenticação baseada no uso de uma chave privada de um sistema de processamento de baixa potência (LPPS);

- privacidade no sentido de proteger um identificador de etiqueta (ID de etiqueta) de modo que uma parte não autorizada não possa aprender o identificador da etiqueta;

- não-rastreamento de modo a garantir que um valor diferente seja retornado em resposta a um desafio, pelo que um leitor não poderá identificar o sistema LPPS por meio da resposta.

2. Método, de acordo com a reivindicação 1, no qual o protocolo criptográfico compreende uma criptografia de curva elíptica.

3. Método, de acordo com a reivindicação 1, no qual a autenticação compreende:

- a utilização de uma chave privada do sistema LPPS e o cálculo de uma função da chave privada e um desafio recebido no sistema LPPS.

4. Método, de acordo com a reivindicação 1, no qual o não-rastreamento compreende:

- a provisão de um valor criptográfico adicional concatenado com um valor de autenticação.

5. Método, de acordo com a reivindicação 1, no qual a privacidade compreende:

- a criptografia do ID de etiqueta com uma chave pública de uma leitora.

6. Método, de acordo com a reivindicação 1, compreendendo ainda:

- a troca dos parâmetros iniciais entre a leitora e o sistema LPPS.

7. Método, de acordo com a reivindicação 6, no qual os parâmetros iniciais incluem: um ID de etiqueta, e uma curva elíptica e um ponto sobre a curva elíptica para a autenticação, a privacidade, e a ofuscação.

8. Método, de acordo com a reivindicação 7, no qual a curva elíptica e o ponto são iguais para a autenticação, a privacidade, e a ofuscação.

9. Método, de acordo com a reivindicação 6, no qual a leitora provê os parâmetros iniciais ao sistema LPPS.

10. Método de utilização de um marcador de RFID:

- que recebe um desafio de uma leitora;

- que calcula $S = f(s, O_E)$, $U = f(u, O_O)$, $B = E(n, k_E)$, $G = f(A, K_O)$, em que:

A é uma função do desafio e uma chave privada da etiqueta de RFID;

s e u são números aleatórios gerados pela etiqueta de RFID,

n é o ID da etiqueta,

K_E e K_O são funções de uma primeira chave pública e de uma segunda chave pública da leitora, respectivamente, e

O_E e O_O são originadores, providos pela leitora; e

- que retorna S, U, B e G para a leitora, os dados retornados incluindo uma resposta de desafio e o ID de etiqueta, e sendo únicos para cada resposta, mesmo ao responder a um desafio idêntico.

11. Método, de acordo com a reivindicação 10, no qual os originadores O_E e O_O são pontos sobre uma curva elíptica.

12. Método, de acordo com a reivindicação 10, no qual os originadores O_E e O_O são geradores de grandes números primos.

13. Método, de acordo com a reivindicação 10, compreendendo ainda a inicialização da etiqueta de RFID, no qual a inicialização compreende o recebimento por parte da leitora:

- da primeira chave pública de um primeiro par de chaves para privacidade;

- da segunda chave pública de um segundo par de chaves para ofuscação; e

- um ID de etiqueta.

14. Método, de acordo com a reivindicação 13, no qual a iniciali-

zação compreende ainda:

- a seleção de um terceiro par de chaves para autenticação; e

- o envio de uma chave pública do terceiro par de chaves para a leitora.

15. Método, de acordo com a reivindicação 13, no qual a inicialização compreende ainda:

- o recebimento a partir da leitora de uma chave privada de um terceiro par de chaves para autenticação, a chave privada do terceiro par de chaves armazenado somente pela etiqueta de RFID.

16. Sistema de processamento de baixa potência compreendendo:

- um transceptor para transmitir e receber dados, o transceptor para receber um desafio de um sistema de leitora;

- uma criptológica a fim de realizar cálculos criptográficos, a criptológica para calcular $S = f(s, o_{E)}, U = F(u, O_{O)}, B = E(n, k_{E)}, G = f(A, k_{O)}$, no qual:

A é uma função do desafio e uma chave privada do sistema LPPS,

s e u são números aleatórios,

n é um identificador do sistema LPPS,

K_E e k_O são funções de uma primeira chave pública e de uma segunda chave pública da leitora, respectivamente, e

O_E e O_O são originadores, providos pela leitora;

- o transceptor ainda para retornar S, U, B e G para o sistema de leitora, os dados retornados incluindo uma resposta de desafio e o ID de etiqueta, e sendo únicos para cada resposta, mesmo ao responder a um desafio idêntico.

17. Sistema, de acordo com a reivindicação 14, compreendendo ainda uma memória segura para armazenar a chave privada do sistema LPPS e um identificador do sistema LPPS.

18. Sistema, de acordo com a reivindicação 16, no qual a criptológica é ainda para a geração dos números aleatórios s e u.

19. Sistema, de acordo com a reivindicação 16, compreendendo ainda:

- uma memória para armazenar dados de inicialização, os dados de inicialização incluindo as chaves públicas da leitora e o ID de etiqueta.

20. Sistema, de acordo com a reivindicação 16, no qual os originadores O_E e O_O são pontos sobre uma curva elíptica, e no qual os originadores O_E e O_O estão no mesmo ponto sobre a mesma curva elíptica.

21. Sistema de processamento de baixa potência (LPPS) projetado para ser seguramente interrogado por um sistema de leitora, o sistema LPPS compreendendo:

- um transceptor para receber um desafio do sistema de leitora;

- uma criptológica para calcular uma resposta ao desafio, a resposta compreendendo uma chave privada do sistema LPPS;

- a criptológica para calcular um dado de retorno para retorno para o sistema de leitora, os dados de retorno sendo uma combinação da resposta ao desafio e da chave de criptografia, uma chave de autenticação e uma chave de ofuscação.

22. Sistema, de acordo com a reivindicação 21, no qual a chave criptográfica deve gerar dois números aleatórios, e ainda criptografar um primeiro número aleatório com uma chave de criptografia, e criptografar o segundo número aleatório com uma chave de ofuscação, e criptografar uma chave de autenticação com a chave pública da leitora.

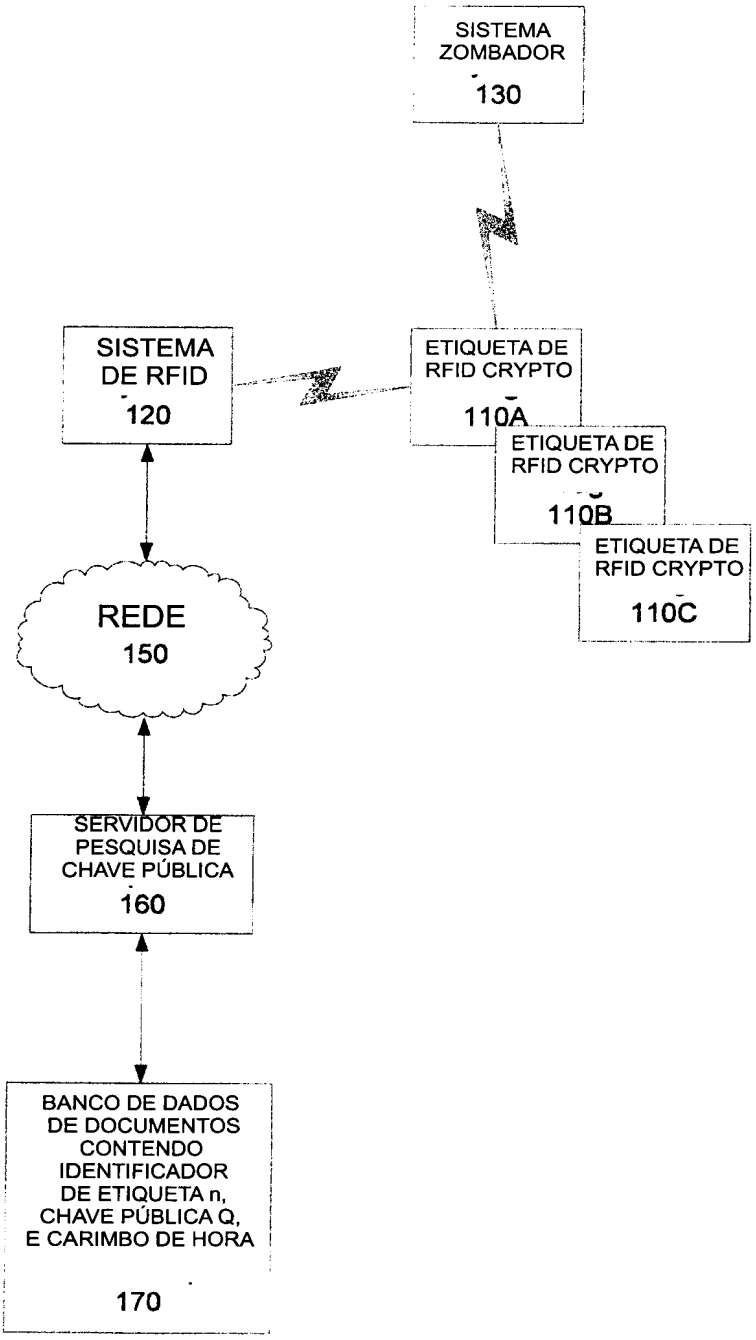
SISTEMA ZOMBADOR
130
SISTEMA DE RFID
120
ETIQUETA DE RFID CRYPTO
110A
ETIQUETA DE RFID CRYPTO
110B
ETIQUETA DE RFID CRYPTO
110C
REDE
150
SERVIDOR DE PESQUISA DE CHAVE PÚBLICA
160
BANCO DE DADOS DE DOCUMENTOS CONTENDO IDENTIFICADOR DE ETIQUETA n, CHAVE PÚBLICA Q, E CARIMBO DE HORA
170

Fig. 1

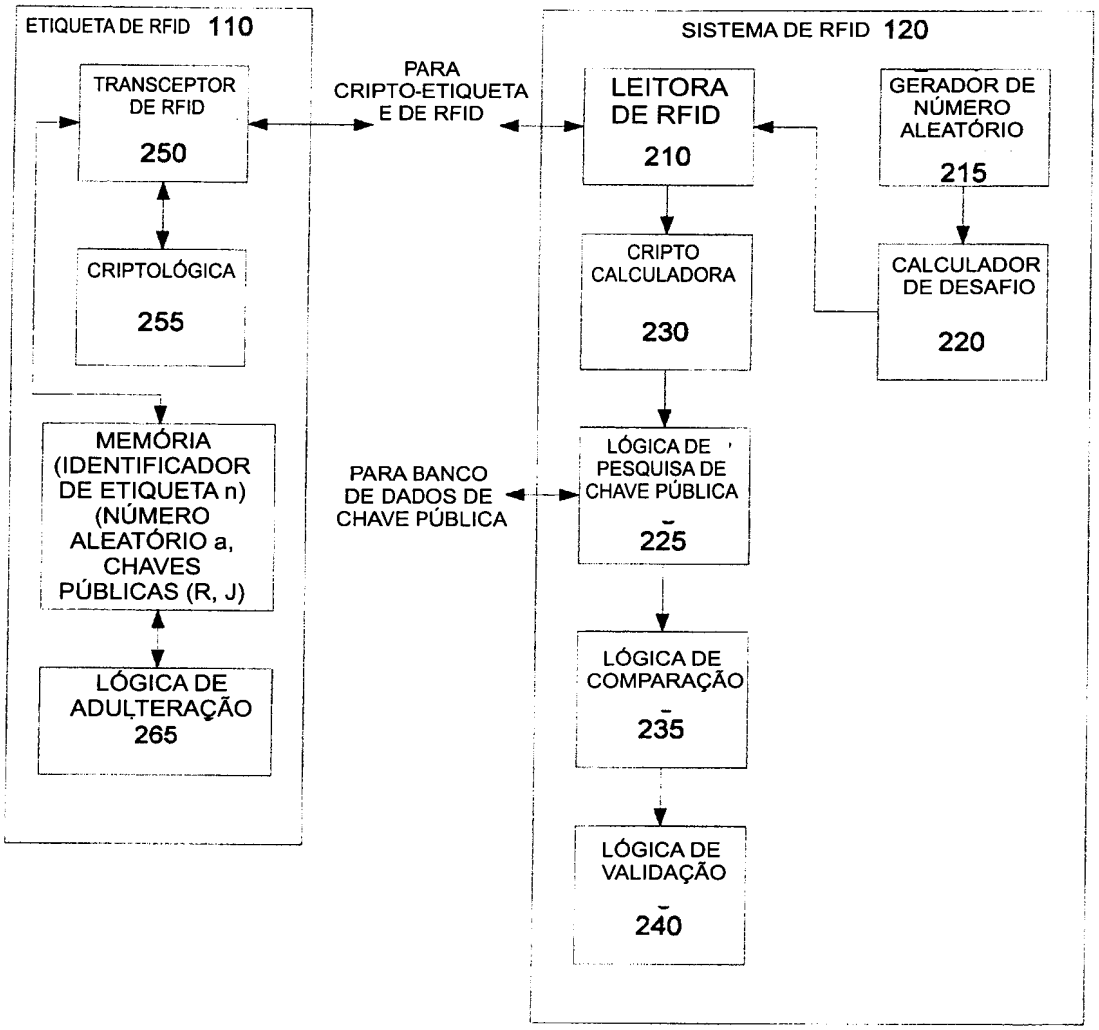
ETIQUETA DE RFID 110
TRANSCEPTOR DE RFID 250
CRIPTOLÓGICA 255
MEMÓRIA (IDENTIFICADOR DE ETIQUETA n) (NÚMERO ALEATÓRIO a, CHAVES PÚBLICAS (R, J)
LÓGICA DE ADULTERAÇÃO 265
PARA CRIPTO-ETIQUETA E DE RFID
PARA BANCO DE DADOS DE CHAVE PÚBLICA
SISTEMA DE RFID 120
LEITORA DE RFID 210
GERADOR DE NÚMERO ALEATÓRIO 215
CRIPTO CALCULADORA 230
CALCULADOR DE DESAFIO 220
LÓGICA DE PESQUISA DE CHAVE PÚBLICA 225
LÓGICA DE COMPARAÇÃO 235
LÓGICA DE VALIDAÇÃO 240

Fig. 2

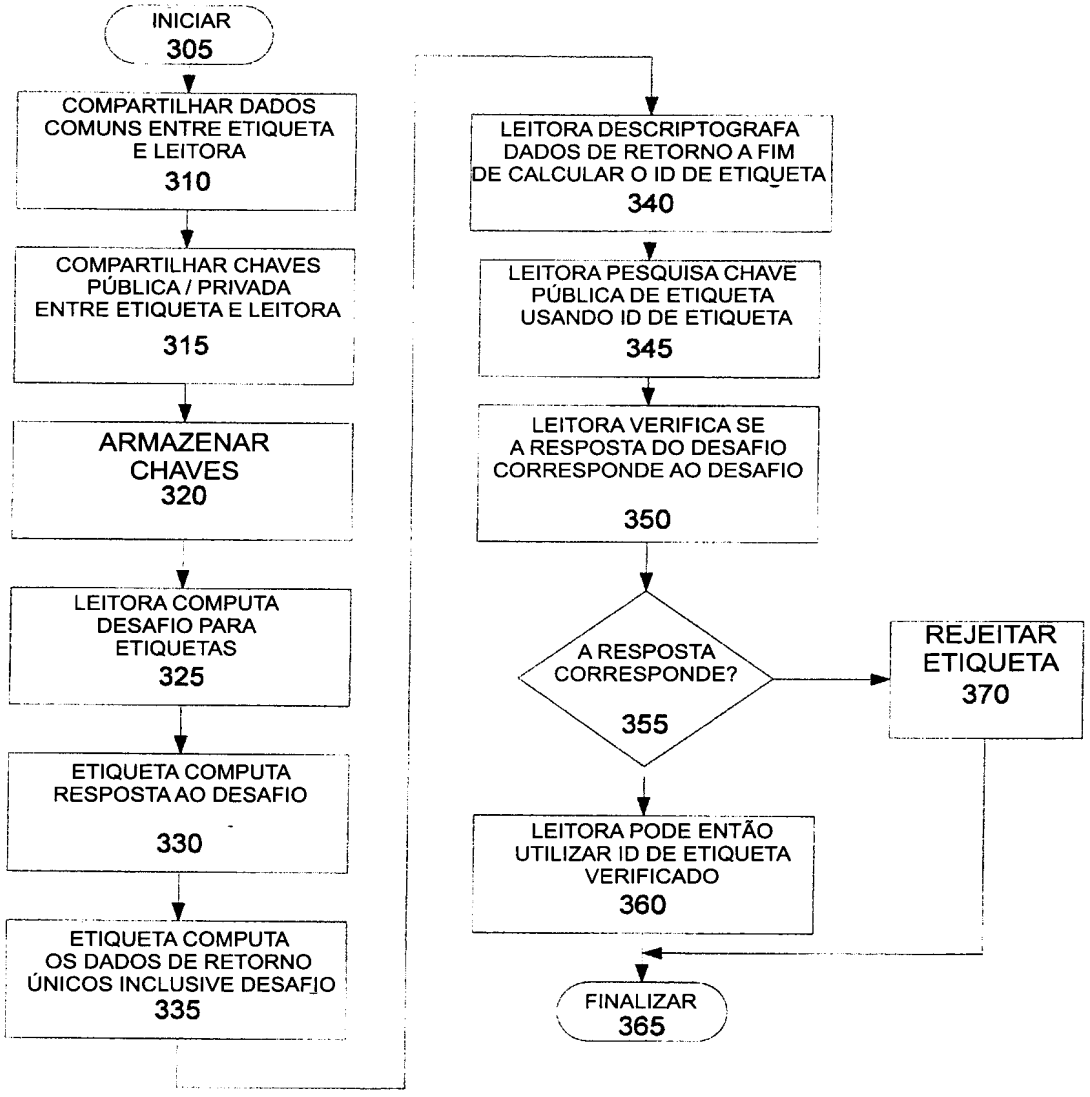
INICIAR
305
COMPARTILHAR DADOS COMUNS ENTRE ETIQUETA E LEITORA
310
COMPARTILHAR CHAVES PÚBLICA / PRIVADA ENTRE ETIQUETA E LEITORA
315
ARMAZENAR CHAVES
320
LEITORA COMPUTA DESAFIO PARA ETIQUETAS
325
ETIQUETA COMPUTA RESPOSTA AO DESAFIO
330
ETIQUETA COMPUTA OS DADOS DE RETORNO ÚNICOS INCLUSIVE DESAFIO
335
LEITORA DESCRIPTOGRAFA DADOS DE RETORNO A FIM DE CALCULAR O ID DE ETIQUETA
340
LEITORA PESQUISA CHAVE PÚBLICA DE ETIQUETA USANDO ID DE ETIQUETA
345
LEITORA VERIFICA SE A RESPOSTA DO DESAFIO CORRESPONDE AO DESAFIO
350
A RESPOSTA CORRESPONDE?
355
REJEITAR ETIQUETA
370
LEITORA PODE ENTÃO UTILIZAR ID DE ETIQUETA VERIFICADO
360
FINALIZAR
365

Fig. 3

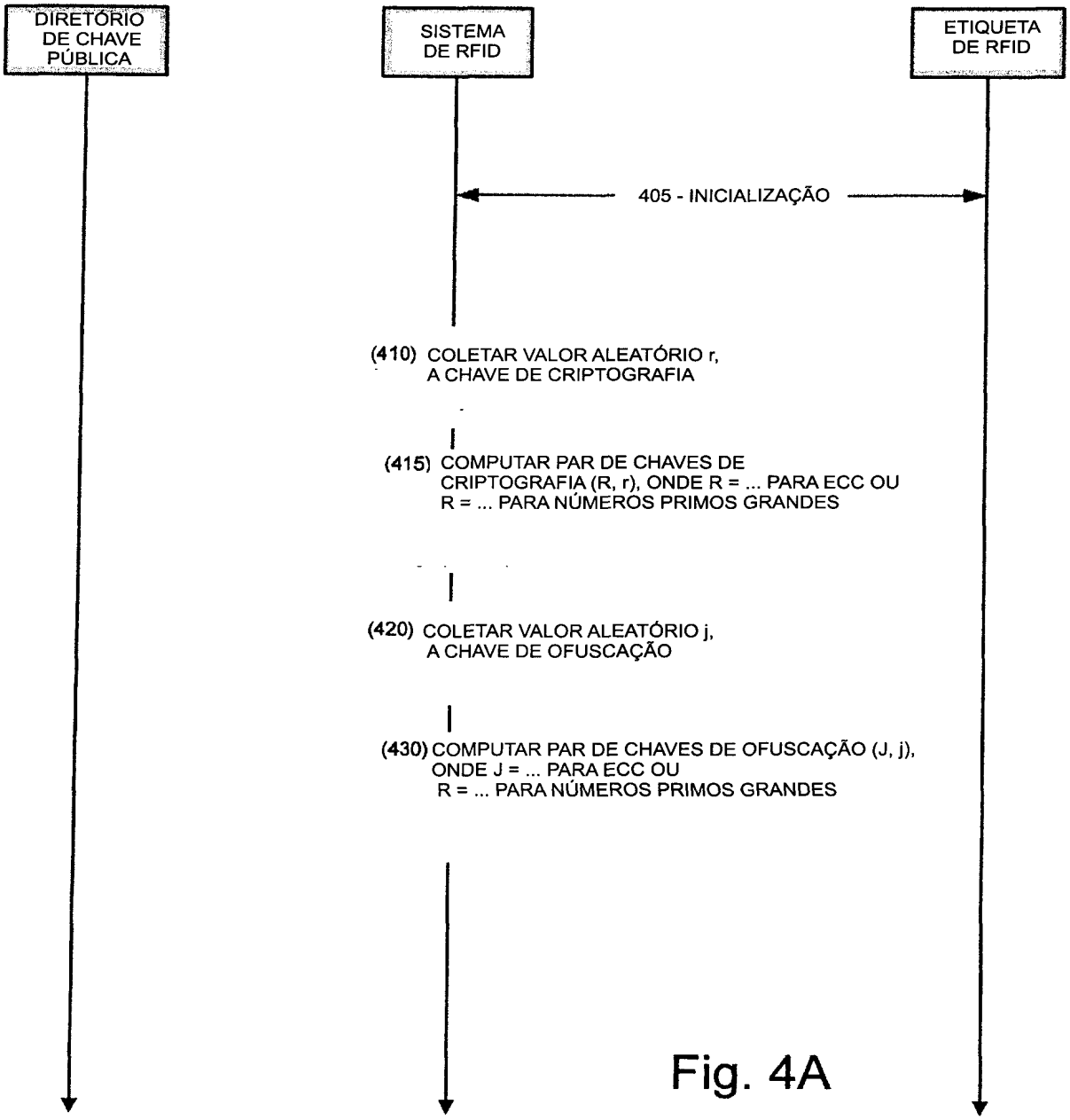

Fig. 4A

NOTAS:

1.TODAS AS COMPUTAÇÕES SÃO FEITAS SOBRE CURVAS ELÍPTICAS EM CAMPOS FINITOS (CONFORME DESCRITO NA SEÇÃO DE PRÉ-REQUISITOS)

2.O VALOR DE ID DE ETIQUETA n DEVE SER MENOR QUE O COMPRIMENTO DAS CHAVES

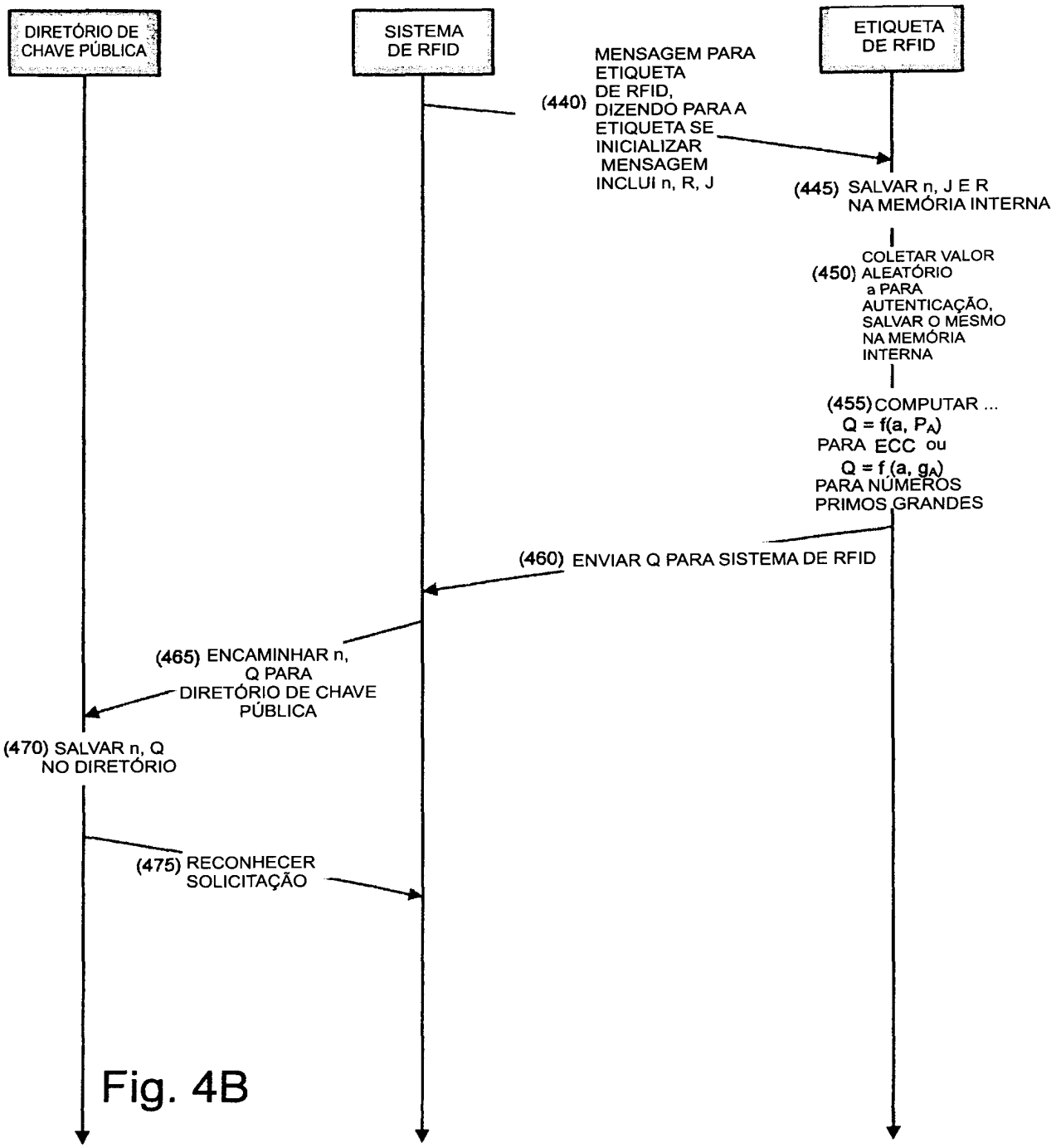
DIRETÓRIO DE CHAVE PÚBLICA
SISTEMA DE RFID
ETIQUETA DE RFID
(440) MENSAGEM PARA ETIQUETA DE RFID, DIZENDO PARA A ETIQUETA SE INICIALIZAR MENSAGEM INCLUI n, R, J
(445) SALVAR n, J E R NA MEMÓRIA INTERNA
(450) COLETAR VALOR ALEATÓRIO a PARA AUTENTICAÇÃO, SALVAR O MESMO NA MEMÓRIA INTERNA
(455) COMPUTAR ... Q = f(a, P_A) PARA ECC ou Q = f (a, g_A) PARA NÚMEROS PRIMOS GRANDES
(460) ENVIAR Q PARA SISTEMA DE RFID
(465) ENCAMINHAR n, Q PARA DIRETÓRIO DE CHAVE PÚBLICA
(470) SALVAR n, Q NO DIRETÓRIO
(475) RECONHECER SOLICITAÇÃO

Fig. 4B

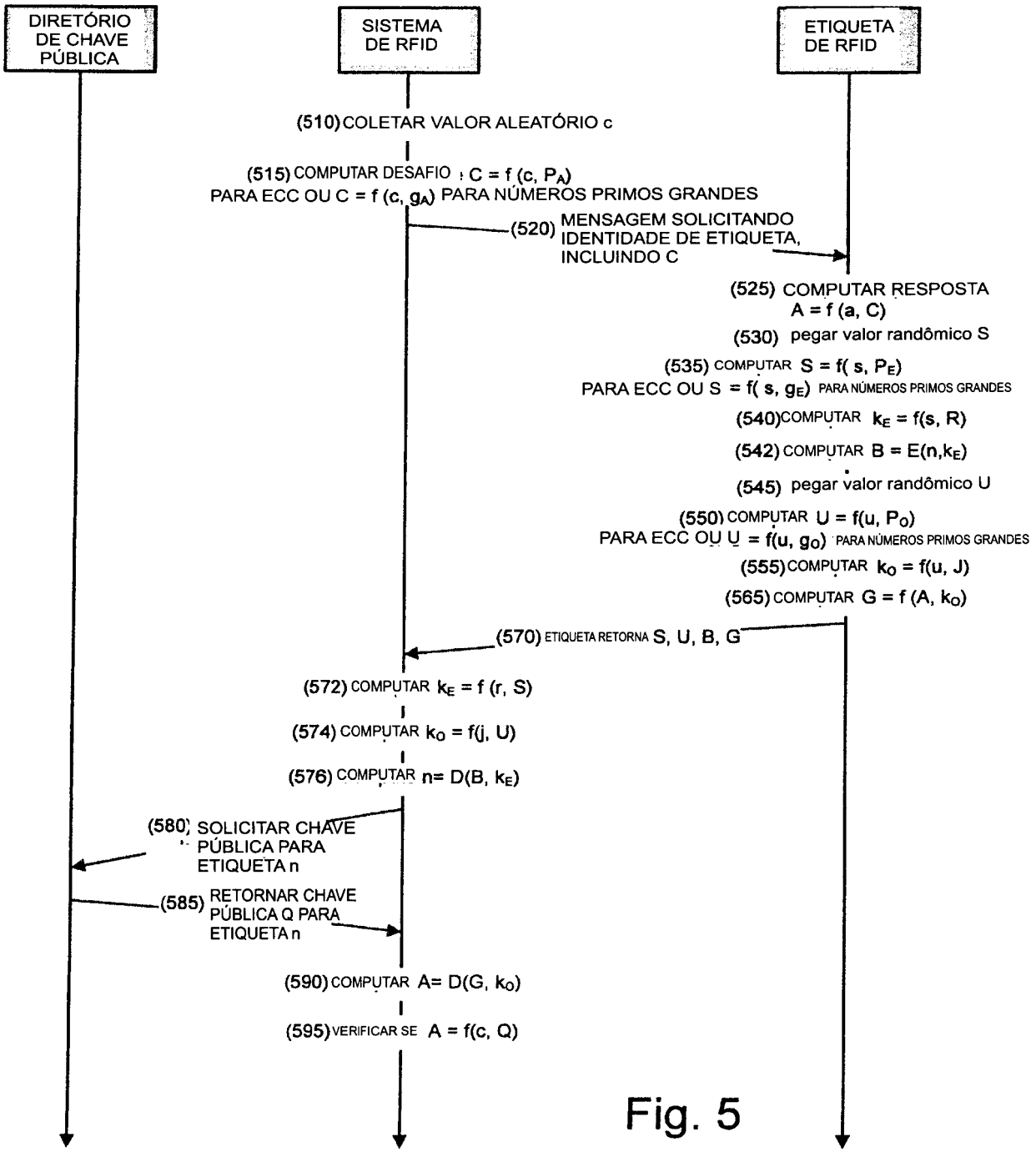
DIRETÓRIO DE CHAVE PÚBLICA
SISTEMA DE RFID
ETIQUETA DE RFID
(510) COLETAR VALOR ALEATÓRIO c
(515) COMPUTAR DESAFIO : C = f (c, P_A) PARA ECC OU C = f (c, g_A) PARA NÚMEROS PRIMOS GRANDES
(520) MENSAGEM SOLICITANDO IDENTIDADE DE ETIQUETA, INCLUINDO C
(525) COMPUTAR RESPOSTA A = f (a, C)
(530) pegar valor randômico S
(535) COMPUTAR S = f(s, P_E) PARA ECC OU S = f(s, g_E) PARA NÚMEROS PRIMOS GRANDES
(540) COMPUTAR k_E = f(s, R)
(542) COMPUTAR B = E(n,k_E)
(545) pegar valor randômico U
(550) COMPUTAR U = f(u, P_O) PARA ECC OU U = f(u, g_O) PARA NÚMEROS PRIMOS GRANDES
(555) COMPUTAR k_O = f(u, J)
(565) COMPUTAR G = f (A, k_O)
(570) ETIQUETA RETORNA S, U, B, G
(572) COMPUTAR k_E = f (r, S)
(574) COMPUTAR k_O = f(j, U)
(576) COMPUTAR n= D(B, k_E)
(580) SOLICITAR CHAVE PÚBLICA PARA ETIQUETA n
(585) RETORNAR CHAVE PÚBLICA Q PARA ETIQUETA n
(590) COMPUTAR A= D(G, k_O)
(595) VERIFICAR SE A = f(c, Q)

Fig. 5

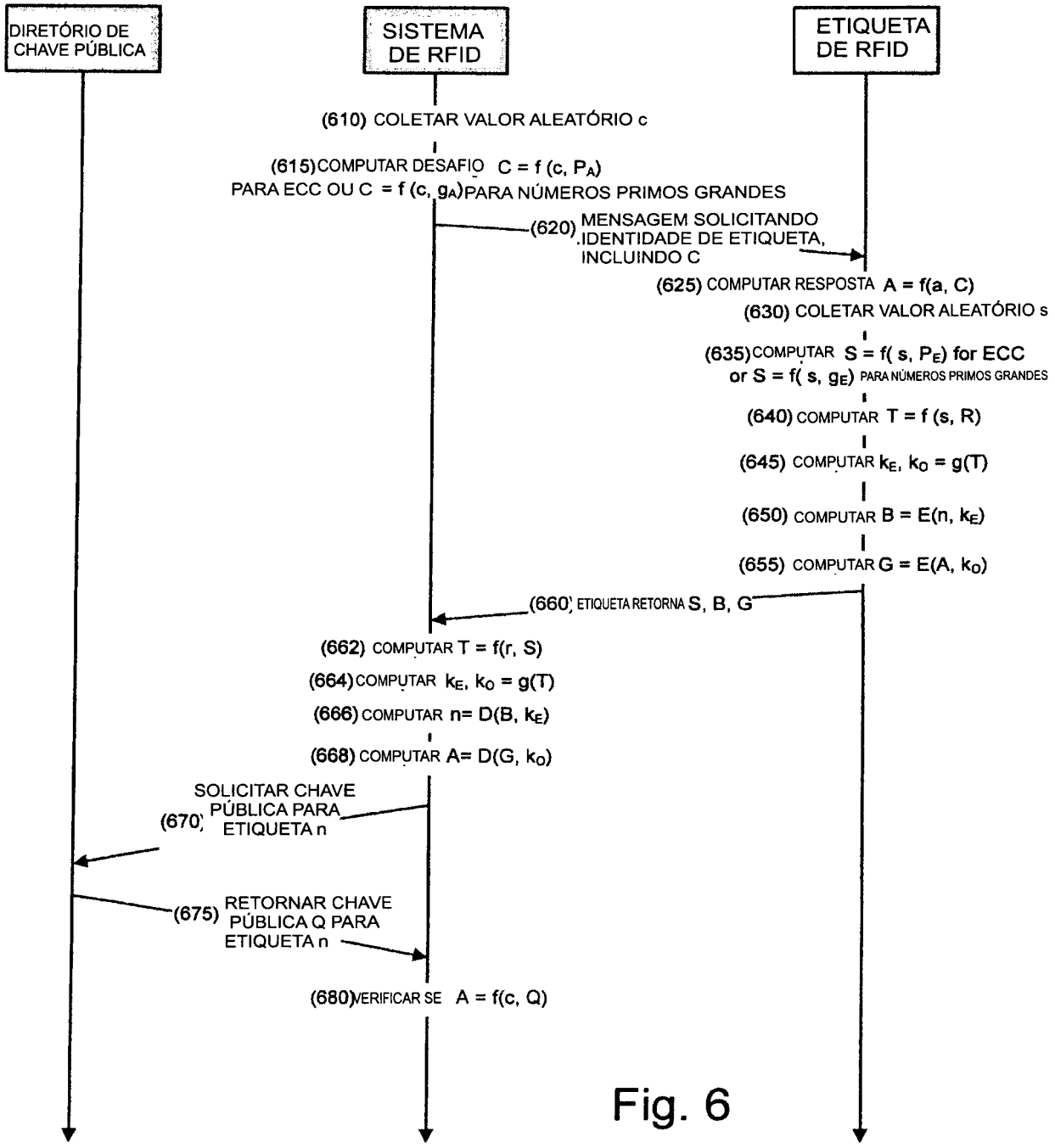
DIRETÓRIO DE CHAVE PÚBLICA
SISTEMA DE RFID
ETIQUETA DE RFID
(610) COLETAR VALOR ALEATÓRIO c
(615) COMPUTAR DESAFIO C = f (c, P_A) PARA ECC OU C = f (c, g_A) PARA NÚMEROS PRIMOS GRANDES
(620) MENSAGEM SOLICITANDO IDENTIDADE DE ETIQUETA, INCLUINDO C
(625) COMPUTAR RESPOSTA A = f(a, C)
(630) COLETAR VALOR ALEATÓRIO s
(635) COMPUTAR S = f(s, P_E) for ECC or S = f(s, g_E) PARA NÚMEROS PRIMOS GRANDES
(640) COMPUTAR T = f (s, R)
(645) COMPUTAR k_E, k_O = g(T)
(650) COMPUTAR B = E(n, k_E)
(655) COMPUTAR G = E(A, k_O)
(660) ETIQUETA RETORNA S, B, G
(662) COMPUTAR T = f(r, S)
(664) COMPUTAR k_E, k_O = g(T)
(666) COMPUTAR n= D(B, k_E)
(668) COMPUTAR A= D(G, k_O)
(670) SOLICITAR CHAVE PÚBLICA PARA ETIQUETA n
(675) RETORNAR CHAVE PÚBLICA Q PARA ETIQUETA n
(680) VERIFICAR SE A = f(c, Q)

Fig. 6

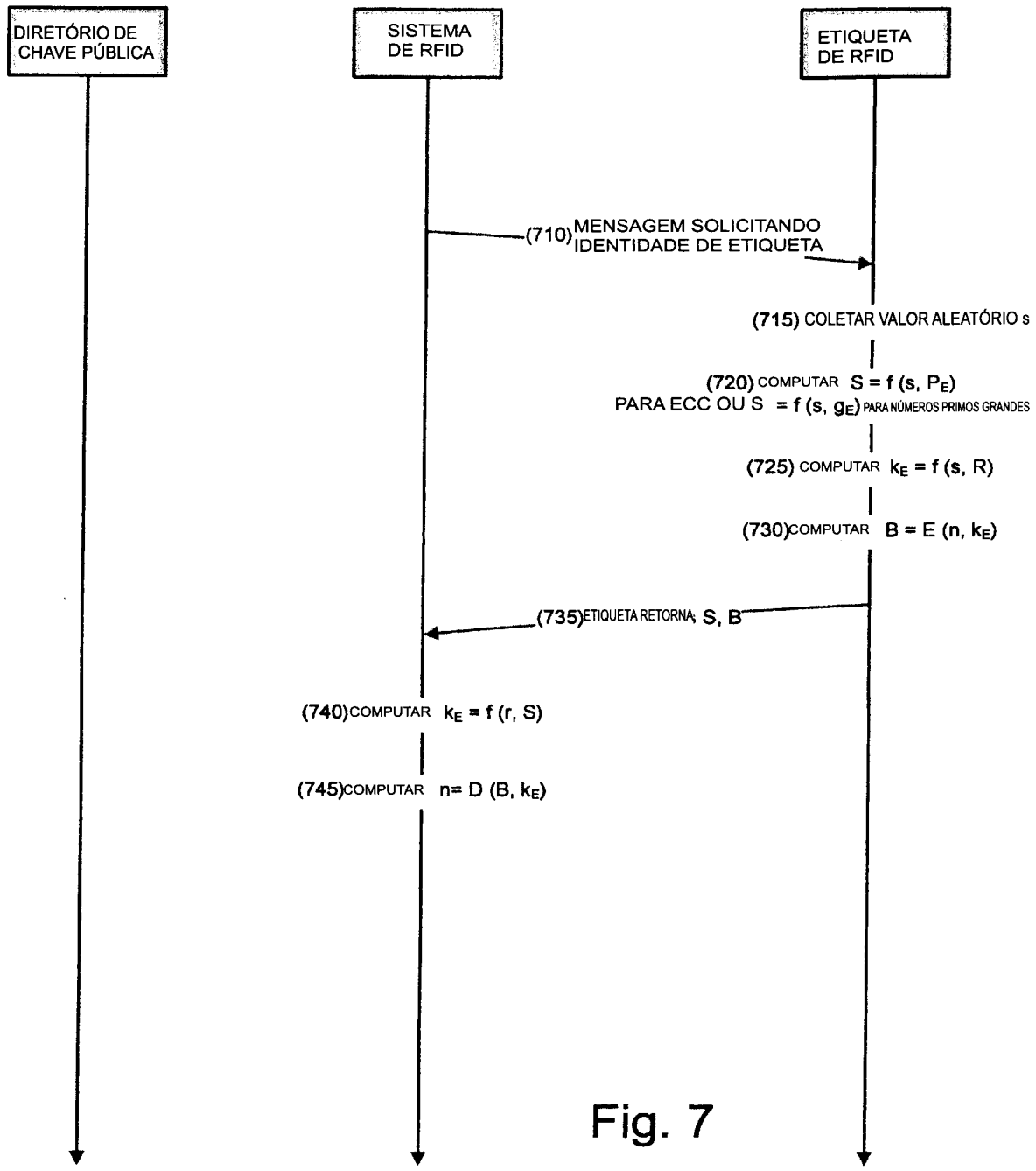

Fig. 7

NOTAS:

1.TODAS AS COMPUTAÇÕES SÃO FEITAS DENTRO DE UMA CURVA ELÍPTICA BEM CONHECIDA E POR UM CAMPO FINITO BEM CONHECIDO ...

2. O OPERADOR SIGNIFICA O RESULTADO DA REALIZAÇÃO DE UM EXCLUSIVO OU (XOR) NOS DOIS MODOS DE OPERAÇÃO.

3.A CHAVE PÚBLICA X NÃO PRECISA SER TRANSMITIDA COMO PARTE DO PROTOCOLO, MAS SIM UM IDENTIFICADOR PARA A CHAVE PÚBLICA PODE SER TRANSMITIDO

4.O VALOR n DE ID DE ETIQUETA DEVE SER MENOR QUE O COMPRIMENTO DAS CHAVES

5.A FUNÇÃO G0 COMPUTA UMA CADEIA LONGA O SUFICIENTE PARA XOR COM n | A

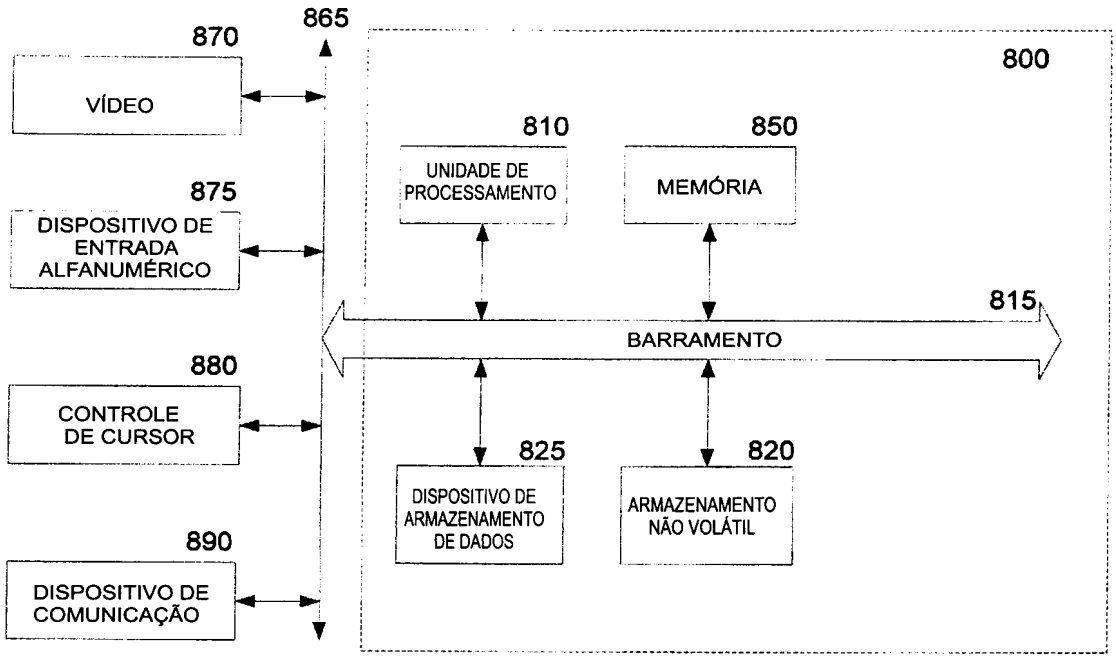
865
870
VÍDEO
875
DISPOSITIVO DE ENTRADA ALFANUMÉRICO
880
CONTROLE DE CURSOR
890
DISPOSITIVO DE COMUNICAÇÃO
800
810
UNIDADE DE PROCESSAMENTO
850
MEMÓRIA
815
BARRAMENTO
825
DISPOSITIVO DE ARMAZENAMENTO DE DADOS
820
ARMAZENAMENTO NÃO VOLÁTIL

Fig. 8

RESUMO

Patente de Invenção: **"MÉTODO E APARELHO PARA PROVER AUTENTICAÇÃO E PRIVACIDADE COM DISPOSITIVOS DE BAIXA COMPLEXIDADE".**

A presente invenção refere-se a um método e aparelho para prover um protocolo criptográfico para uma autenticação, privacidade, e anonimato. O protocolo, em uma modalidade, é projetado para ser implementado em um pequeno número de portas lógicas, executadas rapidamente em dispositivos simples, e prover uma segurança de grau militar.