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

(11) PI 0710622-0 B1

(22) Data do Depósito: 17/04/2007

(45) Data de Concessão: 14/02/2018

(54) Título: SISTEMA DE COMUNICAÇÕES

(51) Int.Cl.: G08B 13/14

(30) Prioridade Unionista: 17/04/2006 US 11/405,011

(73) Titular(es): AMTECH SYSTEMS LLC

(72) Inventor(es): KELLY GRAVELLE; DALE L. SCOTT; ZHENPING TAN

Relatório Descritivo da Patente de Invenção para **"SISTEMA DE COMUNICAÇÕES".**

Campo da Invenção

A presente invenção refere-se em geral a sistemas de identificação de rádiofreqüência (RFID), e mais particularmente, a métodos e dispositivos para proteger a segurança de comunicações entre etiquetas e leitoras de RFID.

Antecedentes da Invenção

Nos termos mais básicos, os sistemas de RFID consistem em uma etiqueta de RFID implementada para fornecer informação armazenada na etiqueta pertencente à identidade e talvez aspectos ou características de um objeto no qual a etiqueta é afixada, e comunicar esta informação por meio de um sinal de RF para uma leitora de RFID em resposta a um sinal de interrogação de RF recebido pela etiqueta a partir da leitora. Na maioria dos casos de uso corrente, uma única leitora é usada para começar as seções de comunicação individual ou transações com uma multiplicidade de etiquetas.

Tipicamente, os objetos que portam as etiquetas são passados pela localização fixa da leitora, que é afastada das etiquetas mas dentro da faixa de comunicação, ou faixa de resposta, de cada etiqueta na medida em que a etiqueta atravessa a posição da leitora. Um exemplo de tal aplicação de um sistema de RFID é um sistema de recolhimento de pedágio de rodovia em que veículos autorizados – isto é, veículos que portam uma etiqueta que designa o uso permitido sob a autoridade de uma agência de governo – são consultados ou comandados por uma leitora de RFID posicionada em uma pista designada da área de recolhimento de pedágio para se identificar quando passam "sem se deter" pela leitora. O recolhimento remoto de identidades dos veículos permite que a autoridade de governo cobre ou debite o valor de cada proprietário de veículo individual quando registrado em conjunto com uma correspondência auxiliada por computador ou outro sistema de notificação. Tais sistemas representam não somente um vasto aperfeiçoamento em controle de tráfego, mas na eficiência de recolhimento de pedágio

e redução em operações trabalhosas também. Isto deve ser contrastado com o recolhimento físico do pedágio em cabinas com pessoas (um cobrador de pedágio) ou sem pessoas (por exemplo, através de recolhimento de moedas) em pistas abertas onde cada veículo deve parar ou pelo menos diminuir o movimento através da pista.

Outro exemplo de uma aplicação de sistema de RFID onde a leitora é fixada e o objeto que porta a etiqueta passa pela leitora, é um em que a segurança deve ser mantida tanto para permitir a passagem do objeto (por exemplo, uma pessoa usando um crachá que incorpora a etiqueta) em uma parte de segurança de uma instalação, ou para anunciar ou impedir a passagem do objeto (por exemplo, mercadorias nas quais a etiqueta é de segurança) de uma localização de saída de uma instalação, como soando um alarme ou trancando a saída.

Mas dependendo da aplicação particular do sistema de RFID, a leitora pode ser móvel de modo a obter informação armazenada de objetos relativamente imóveis, tal como em aplicações de cadeia de suprimento onde mercadorias comuns são temporariamente mantidas em caixas ou em estrados portando a etiqueta de RFID em um depósito de inventário. As caixas inventariadas ou estrados podem ser varridos ocasional ou periodicamente por uma leitora de RFID manual para obter a informação de identidade da mercadoria a partir das etiqueta(s). Em ainda outras aplicações, ambas as etiquetas e a leitora podem ser móveis durante o processo de varredura, tal como durante a varredura rápida de objetos com etiquetas de RFID em uma correia transportadora se movendo por uma leitora de RFID sendo transportada em uma direção oposta àquela da correia se movendo. De qualquer maneira, em cada aplicação de um sistema de RFID, a leitora e a etiqueta devem estar relativamente posicionadas dentro de uma faixa adequada para a comunicação de RF ocorrer entre elas; isto é, a faixa de comunicação de leitora e etiqueta, ou faixa de resposta da etiqueta.

Em sua forma mais simples, a etiqueta de RFID convencional consiste em um transponder e uma antena. Algumas vezes, a etiqueta de RFID propriamente dita é referida como um transponder. De qualquer manei-

ra, a etiqueta é fornecida com capacidade de armazenamento de dados, usualmente na forma de memória de leitura (ROM) ou memória de leitura/gravação (R/W) (tal como ROM programável eletricamente apagável, ou EEPROM) incorporada no circuito integrado (IC) de um chip semicondutor (algumas vezes chamado de um microchip). O conjunto de circuitos eletrônicos, integrado no microchip da etiqueta de RFID, junto com ou sem o conjunto de circuitos de correspondência de impedância que acopla os eletrônicos e a antena da etiqueta, pode ser denominado um RFIC (circuito integrado de RF) ou um ASIC (IC de aplicação específica).

Etiquetas de RFID podem tanto ser passivas quanto ativas. Uma etiqueta de RFID passiva precisa de um suprimento de energia autosuficiente interna, por exemplo, uma bateria, e conta, em vez disto, com a consulta de RF que entra pela leitora para produzir energia suficiente no conjunto de circuitos internos da etiqueta para permitir que a etiqueta transmita uma resposta. Em essência, a consulta induz uma corrente elétrica muito pequena na antena interna da etiqueta, que serve como a fonte de energia que permite uma resposta refletida ou retrodispersada. Conseqüentemente, uma etiqueta de RFID passiva é bastante limitada com respeito à quantidade de dados que pode ser fornecida em sua resposta para uma consulta da leitora, consistindo normalmente somente informação invariável fixa armazenada na etiqueta, por exemplo, um número de ID e talvez uma pequena quantidade de dados adicionais. Mas a ausência de uma bateria leva a certas vantagens, primeiramente que uma etiqueta passiva pode ser fabricada a um custo muito menor e em tamanho menor que uma etiqueta ativa.

Dentre outros usos, as etiquetas de RFID passivas são projetadas para substituir eventualmente o código de produto universal ubíquo (UPC), ou código de barra impresso, tira encontrada em grande quantidade de produtos na tendência de comércio, a tira exigindo uma linha de varredura ótica visual para obter uma leitura do UPC de identificação. A leitura pode então ser usada, por exemplo, para recuperar a informação de preço computadorizada para o produto, e para produzir uma exibição e/ou impressão do

preço comum do produto, em um ponto de venda (por exemplo, localização da caixa registradora) para o produto.

A bateria a bordo, ou no chip, de uma etiqueta de RFID ativa pode fornecer à etiqueta uma faixa de resposta maior, com maior precisão, confiabilidade e capacidade de armazenamento de dados, mas a etiqueta ativa tem as desvantagens acima mencionadas de custo e tamanho maiores com relação à etiqueta passiva. A bateria propriamente dita pode ser bastante pequena, mas não o suficiente para superar a desvantagem de tamanho.

Uma leitora de etiqueta de RFID convencional típica emprega um transceptor, uma unidade de controle e uma antena para se comunicar com a etiqueta a uma freqüência de RF designada dentre várias alocadas para este propósito. Uma interface adicional tal como RS 232, RS 485, ou outra, pode ser fornecida com a leitora para permitir que dados recebidos da etiqueta sejam enviados para outro sistema.

Em muitas aplicações, pode ser importante assegurar a privacidade da informação transferida entre a etiqueta e a leitora, particularmente informação armazenada na etiqueta. Considere, por exemplo, um veículo que porta uma ou mais etiquetas de RFID cuja memória R/W é continuamente ou periodicamente atualizada com a milhagem percorrida, localização corrente, rotina de operação diária, carga corrente, identidade do proprietário, motorista(s) autorizado (s), e outra informação que o proprietário do veículo pode querer que seja mantida confidencial. Existem considerações, no entanto, sobre a perda potencial de privacidade e furto de informação de identidade pessoal como resultado do uso crescente de etiquetas de RFID.

Tentativas foram feitas para proteger e para mitigar as considerações quanto à privacidade e segurança de dados armazenados em etiquetas. Em geral, estas tentativas foram direcionadas para os protocolos e esquemas para impedir o acesso à informação secreta, confidencial, privada armazenada em etiquetas de RFID através de interrogação ou intercepção por leitoras não-autorizadas, algumas vezes chamadas leitoras nocivas, leitoras ilegítimas, intrusos, atacantes, interceptores ou adversários. Estas apelações e similares são coletivamente referidas aqui como "leitora não-

autorizada".

Uma solução proposta é encontrada em um artigo por I. Vajda e outros, intitulado "Lightweight Authentication Protocols for Low-Cost RFID Tags", Budapest University of Technology and Economics, Hungary, 5 de agosto de 2003. No artigo de Vajda, o desejo de fornecer segurança em etiquetas de RFID de baixo custo é vista como desafio devido à natureza altamente restringida de recurso das etiquetas, e sua inabilidade de suportar criptografia forte. Uma necessidade expressa para algoritmos leves especiais que levam em conta as limitações de etiquetas de RFDI e a corrida precipitada na direção de desdobramento universal de sistemas de RFID é tratada através de uma listagem de certos protocolos de autenticação de etiqueta previamente apresentados por outros.

No entanto, Vajda apresenta a complexidade de exigir dois estados ou modos de operação das etiquetas, e a possibilidade distinta que uma leitora não-autorizada poderia penetrar em uma defesa da etiqueta contra a aquisição de sua data de segurança para atingir a entrada através do modo de ID mais aberto apesar de sua designação como o estado travado. Em adição, o uso de Vajda de uma lista de pseudônimos tem problemas no número de mensagens relativamente grande exigido, bem como o fato de custo associado com a atualização freqüente destas listas de pseudônimos e chaves secretas, e confiança excessiva na premissa que uma leitora não-autorizada pode somente observar um número limitado de execuções consecutivas do protocolo.

Outra tentativa de proteger dados armazenados em etiquetas é discutida em um artigo por D. Molnar e outros, intitulado "Privacy and Security in Library RFID Issues, Practices and Architecture", CCS'04, October 25-29, 2004, Washington, DC. Molnar trata a leitora e autenticação de etiqueta antes da comunicação de informação de etiqueta ser permitida, especificamente no contexto de etiquetas de rastreamento em um regime de etiquetagem de RFID aplicado no registro de saída e de entrada de livros de biblioteca. Tal rastreamento de livros de biblioteca etiquetados eleva o espectro de vigilância de clientes de biblioteca e seus hábitos de leitura.

Como um assunto prático, os produtos de RFID operando em freqüências designadas até freqüência ultra-alta (UHF) tinham necessidade relativamente mínima para verificação de sessão desde que a maioria das transações baseadas em comércio foram realizadas com dispositivos passivos. Mas onde uma etiqueta de RFID é ativa, e acionada por uma bateria também, é relativamente fácil de remover a etiqueta de RFID acionada por bateria a partir da vizinhança de uma leitora. Portanto, se torna incumbente do ponto de vista de segurança proporcionar proteção contra a etiqueta sendo removida por um atacante de faixa de comunicação com uma leitora de RFID autorizada durante uma sessão autenticada, e então posicionar dentro da faixa de uma leitora não-autorizada (ou posicionar a leitora não-autorizada na faixa de resposta de etiqueta). Tal ação permitiria acesso aberto amplo para as localizações de memória protegida da etiqueta pela leitora não-autorizada.

Consideração sobre violações de segurança e privacidade de comunicações entre a leitora autorizada e a etiqueta pode também estar presente com uma etiqueta passiva, mas a habilidade de montar o equipamento que mantém a energia na etiqueta por meio de energia de RF todas as vezes é muito mais difícil, embora possível.

Seria desejável fornecer um protocolo simples e ainda eficiente ou método para assegurar a privacidade e segurança de uma sessão de comunicação entre uma leitora de RFID autorizada e uma etiqueta de RFID, especialmente uma etiqueta ativa.

Sumário da Invenção

É um objetivo principal da presente invenção fornecer um método relativamente simples ou protocolo para obter autenticação mútua de uma etiqueta de RFID e uma leitora de RFID autorizada antecipada e por toda uma sessão de comunicação entre elas.

De acordo com a invenção, é permitido ocorrer uma sessão de comunicação a ser protegida como segura ou privada, somente depois que a leitora e a etiqueta autenticaram uma a outra de acordo com um protocolo da invenção. Uma vez que a autenticação mútua foi realizada com sucesso, a

etiqueta e a leitora continuam a verificar comunicações subseqüentes para confirmar que ambos os dispositivos são autênticos. Em um protocolo preferido, isto é, obtido por códigos de redundância cíclica de cifragem (CRC's) que são enviados da leitora para a etiqueta e vice-versa.

É bem-conhecido que o CRC é uma técnica de detecção de erro pretendida para assegurar que os dados de mensagem recebida foram corrompidos no curso da transmissão de mensagem. Para este fim, um valor (uma soma de teste, tipicamente constituindo um algoritmo de CRC) é construído no transmissor de uma função da mensagem, e é anexada na mensagem. O receptor usa a mesma função para calcular a soma de teste anexada à mensagem pelo transmissor para confirmar (ou questionar) se a mensagem foi corretamente recebida.

No protocolo preferido da invenção, a leitora de RFID autorizada envia um comando com um CRC criptografado e a etiqueta RFID decodifica o CRC para assegurar que o CRC codificado está correto. Similarmente, a etiqueta envia uma resposta ao comando da leitora com um CRC codificado e a leitora decodifica o CRC para ter certeza que este CRC codificado está também correto. Se ambos estão corretos, uma sessão de comunicação ou transação é começada, mas a verificação contínua de autenticação mútua é exigida a fim de que a transação seja permitida continuar. Se cada codificação/decodificação não é correta, a leitora e etiqueta devem abortar a transação, e é exigida que a autenticação mútua seja repetida do início. O uso do campo de CRC, que está no fluxo de dados tipicamente anexado a cada comando e resposta, permite que a máquina de estado desempenhe como designado. Não existe necessidade de estados especiais durante a sessão de autenticação ou qualquer tempo adicional para obter isto.

Os princípios da presente invenção são aplicáveis a ambas as etiquetas de RFID passivo e ativo, embora a questão de autenticidade é um pouco maior que as etiquetas ativas devido à remoção relativamente fácil acima mencionada de uma etiqueta ativa de uma sessão de comunicações com uma leitora autorizada.

Outro objetivo da invenção é fornecer um método de assegurar a

privacidade de comunicações entre uma etiqueta de RFID ativa ou passiva e uma leitora de RFID autorizada remota dentro da faixa de comunicação da etiqueta, para impedir o acesso aos dados armazenados na etiqueta por uma leitora não-autorizada, em que o método inclui realizar a autenticação mútua da etiqueta e a leitora autorizada como um pré-requisito a uma transição de comunicação entre as duas; e depois disto verificar continuamente a autenticação mútua como um pré-requisito em cada comunicação subseqüente durante a transação.

Um objetivo relacionado é fornecer um protocolo para salvaguardar a segurança de comunicações de RFID entre uma leitora autorizada de RFID e uma etiqueta de RFID dentro de uma faixa de resposta de RF da leitora, de modo a fornecer proteção de leitura para pelo menos uma parte da memória da etiqueta contra a intrusão por uma leitora não-autorizada, incluindo conduzir um processo de autenticar mutuamente a etiqueta e a leitora autorizada como sendo autorizados para participar de uma série de transações envolvendo uma leitura de dados da parte protegida de leitura da memória da etiqueta, e verificar separadamente a autenticidade da leitora como tendo esta autoridade antes de cada transação nas séries.

Breve Descrição dos Desenhos

Os objetivos acima e ainda objetivos adicionais, alvos, aspectos, características e vantagens conseqüentes da invenção se tornarão claros para aqueles versados na técnica a partir de uma consideração da descrição detalhada seguinte do melhor modo presentemente considerado para realizar os princípios da invenção, tomada em conjunto com as figuras seguintes.

A figura 1 é um diagrama de bloco de uma etiqueta e leitora de acordo com a modalidade preferida da invenção; e

a figura 2 ilustra o protocolo preferido como uma seqüência de eventos que devem ocorrer antes de uma sessão de comunicação entre uma leitora de RFID autorizada e uma etiqueta de RFID, e cada verificação de autenticação mútua pode começar.

Descrição Detalhada da Modalidade Preferida da Invenção

Ao descrever um método preferido ou protocolo da invenção i-

lustrada nas figuras, certa terminologia específica será usada em benefício da clareza. No entanto, a invenção não pretende ser limitada a esta terminologia específica, e deve ser entendido que a terminologia inclui todos os equivalentes técnicos que realizam em uma maneira similar para realizar o mesmo resultado ou similar.

Referindo-se aos desenhos, a figura 1 mostra um sistema total 9 tendo uma leitora e uma ou mais etiquetas 20. Como mostrado, a leitora 10 tem um processador 14 para controlar a operação da leitora 10, memória 16 para armazenar dados, um gerador de números randômico 18 para gerar números randômicos, e um gerador de código de autenticação 19 para gerar códigos de autenticação. A etiqueta 20 contém um processador 24 para controlar a operação da etiqueta 20, a memória 26 para armazenar dados, um gerador de números randômicos 28 para gerar números randômicos, e um gerador de código de autenticação 29 para gerar códigos de autenticação. A etiqueta 10 e a leitora 20 incluem outros elementos que não são mostrados, incluindo um transmissor e receptor para comunicar um com o outro.

Sem limitação para a invenção ou reivindicações, uma sessão autêntica é considerada para ser em geral uma sessão que começa uma vez que a etiqueta e a leitora foram autenticadas, isto é, cada uma validou as credenciais da outra. Como tal, comandos subseqüentes e respostas e/ou seus CRCs então se tornam codificados e decodificados. A codificação e decodificação devem corresponder para cada comunicação, ou a sessão será terminada pela leitora ou etiqueta.

Deve ser notado que a autenticação mútua é especialmente importante para a aplicação na qual um usuário definiu uma certa área de memória como sendo suficientemente importante para exigir proteção. Se proteção é importante, então um bit de controle é determinado e este força uma condição autenticada ser verdadeira antes que as transações possam ocorrer. Uma implementação pode usar este bit de controle para proteger contra leitoras não-autorizadas escrevendo em páginas na memória da etiqueta 26, mas não para controlar uma habilidade da leitora em ler estas áreas de memória. No entanto, implementação similar poderia ser feita para proteção de

leitura.

A figura 2 ilustra a seqüência de eventos que devem ocorrer antes de uma sessão de comunicação e cada verificação de autenticação mútua pode começar. A leitora 10 e a etiqueta 20 operam sob controle dos processadores 14, 24. Embora os processadores 14, 24 sejam mostrados como componentes separados, os geradores de números randômicos 18, 28 e os geradores de código de autenticação 19, 29 podem ser operações sem os processadores 14, 24.

Como mostrado, a leitora de RFID autorizada 10 deve primeiro solicitar, etapa 1, e obter, etapa 2, a ID de etiqueta de RFID 20 com a qual a sessão de comunicação deve ser mantida. A ID da etiqueta é armazenada na memória de etiqueta 26. Uma vez que a ID da etiqueta é conhecida, a leitora obtém a Chave Privada K. Usando a ID da etiqueta, a leitora 10 obtém a Chave Privada K de sua memória 16, ou alternativamente de uma base de dados externa sobre uma conexão segura. A Chave Privada K é de preferência não obtida da etiqueta 20 desde que não é uma conexão segura. Tendo obtido a Chave Privada, a leitora 10 emite um comando para a etiqueta 20 para solicitar um Número Randômico RND1, etapa 3, a partir da etiqueta 20. A etiqueta 20 gera um número randômico RND1, usando seu gerador de número randômico 28, e envia este número randômico RND1 para a leitora 10, etapa 4.

Na recepção do Número Randômico RND1, a leitora 10 usa seu gerador de número randômico 18 para criar um segundo Número Randômico RND2. A leitora 10 então usa ambos os Números Randômicos RND1, RND2 e a Chave Privada K para gerar o Código de Autenticação f' da leitora. O Código de Autenticação f' da leitora é determinado pelo gerador de código de autenticação da leitora 19 baseado em um primeiro algoritmo ou função, que é baseado naquelas três variáveis. A leitora 10 envia o Número Randômico RND2 e seu Código de Autenticação de leitora f' para a etiqueta 20 na etapa 5.

A etiqueta 20 recupera sua Chave Privada K, que é armazenada em uma área protegida de sua memória 26, e o Número Randômico RND1

que foi enviado ao leitor 10. O gerador de autenticação de etiqueta 29 então realiza a mesma primeira função de autenticação que o gerador de autenticação da leitora 19 realizou usando as mesmas variáveis (isto é, a Chave Privada K e os números randômicos RND1, RND2), e verifica se ou não o Código de Autenticação da leitora f' recebido da leitora 10 é o mesmo que o Código de Autenticação da leitora f que foi determinado na etiqueta 20. Se os dois códigos não correspondem, é determinado que o Código de Autenticação da leitora f está incorreto, e a autenticação mútua falha.

Se o Código de Autenticação f' da leitora está correto (isto é, o código de autenticação f determinado pela etiqueta 20 corresponde com o código de autenticação f' gerado pela leitora 10), então a leitora 10 provou sua autenticidade para a etiqueta 20. O gerador de código de autenticação da etiqueta 29 então usa uma segunda função de autenticação para gerar um Código de Autenticação de etiqueta g baseado nas variáveis K, RND1, e RND2. A etiqueta 20 transmite seu código de Autenticação g para a leitora 10 para validação, etapa 6. O gerador de código de autenticação 19 da leitora 10 então determina se ou não o Código de Autenticação g da etiqueta está correto usando a mesma segunda função de autenticação que a etiqueta 20 realizada com as mesmas variáveis (isto é, a Chave Privada K e os números randômicos RND1, RND2). Se o Código de Autenticação g da etiqueta está correto (isto é, o código de autenticação de etiqueta determinado pela leitora 10 corresponde com o código de autenticação de etiqueta gerado pela etiqueta 20), então a etiqueta 20 provou sua autenticidade à leitora 10, e o processo de autenticação mútua está completo.

Uma vez que este processo de autenticação mútua está completo, começa a verificação de sessão. Todos os comandos subseqüentes que são enviados para a etiqueta 20 a partir da leitora 10 têm um CRC codificado, diferente para cada comando, anexado ao comando respectivo. Este CRC codificado muda e é baseado na seqüência que ocorreu durante o processo de autenticação mútua. De preferência, a codificação da CRC é baseada pelo menos em parte em uma ou mais das variáveis RND1, RND2 e K. A etiqueta 20 recebe cada comando e o CRC codificado anexado a ela e

prossegue decodificando-o. Se a decodificação está correta, a etiqueta 20 valida, isto é, verifica, que a leitora previamente autenticada 10 é de fato a leitora que enviou o comando respectivo.

De acordo com a modalidade preferida, os geradores de código de autenticação de etiqueta e leitora 19, 29 geram as primeira e segunda funções de autenticação utilizando um registrador de deslocamento com realimentação linear. Igualmente, a codificação do CRC é também baseada em um registrador de deslocamento com realimentação linear. Qualquer função adequada pode ser implementada sem se afastar do espírito e escopo da presente invenção. No entanto, a função preferida é obtida através do uso de um registrador de deslocamento com realimentação linear, tal como descrito em "Linear Feedback Shift Registers", que foi publicado em http://www-math.cudenver.edu/~wcherowi/courses/m5410/m5410fsr.html, os conteúdos da qual são incorporados aqui por referência.

Quando a etiqueta 20 envia de volta sua resposta para cada comando respectivo, o CRC que acompanha a resposta é codificado e a leitora 10 prossegue decodificando-o. Se a decodificação está correta, a leitora valida que a etiqueta previamente autenticada é a etiqueta que enviou a resposta. Este processo continuará até que a sessão esteja terminada por um CRC incorreto, uma perda de energia, ou um comando especial da leitora para a etiqueta

É bem-conhecido que o CRC é uma técnica de detecção de erro pretendida para assegurar que os dados de mensagem recebida não foram corrompidos no curso da transmissão da mensagem. Para este fim, um valor (uma soma de teste, tipicamente constituindo um algoritmo de CRC) é construído no transmissor a partir de uma função da mensagem, e é anexado à mensagem. O receptor usa esta mesma função para calcular a soma de teste da mensagem recebida e comparar com a soma de teste anexada à mensagem pelo transmissor para confirmar (ou questionar) se a mensagem foi recebida corretamente.

No protocolo preferido da invenção, a leitora de RFID autorizada envia um comando com um CRC codificado e a etiqueta de RFID decodifica

o CRC para assegurar-se que o CRC codificado está correto. Similarmente, a etiqueta envia uma resposta ao comando da leitora com um CRC codificado e a leitora decodifica o CRC para ter certeza que este CRC codificado também está correto. Se ambos estão corretos, uma sessão de comunicação ou transação é começada, mas a verificação contínua de autenticação mútua é exigida a fim de que a transação seja permitida continuar. Se cada codificação/decodificação não está correta, a leitora e a etiqueta devem abortar a transação, e é exigido que a autenticação mútua seja repetida do início. O uso do campo de CRC, que está no fluxo de dados tipicamente acrescentado a cada comando e resposta, permite que a máquina de estado desempenhe como designado. Não existe necessidade de estados especiais durante a sessão de autenticação ou qualquer tempo adicional para obter isto.

Este protocolo é descomplicado e extremamente eficiente. Inicialmente, antes que uma sessão de comunicação possa ser entrada na qual os dados armazenados na memória da etiqueta ou uma parte designada de memória é lida ou alterada pela leitora, a leitora e a etiqueta engatam no processo de autenticação mútua. Mas este sozinho não é considerado ser suficiente para proteger contra a possibilidade de que uma leitora não-autorizada busque fazer-se passar pela leitora autorizada (e autenticada) e ser bem-sucedida em recuperar dados designados como privados da etiqueta. Em vez disto, para cada comando da leitora para a etiqueta e cada resposta da etiqueta para a leitora, a autenticação prévia é verificada através de um processo de codificação e decodificação dos CRCs que acompanham cada comando e resposta. A falha em verificar a autenticação do emissor em qualquer ponto na seqüência constitui a causa para abortar a sessão de comunicação.

A descrição precedente e o desenho anexo devem ser considerados como ilustrativos somente dos princípios da invenção. A invenção pode ser configurada em uma variedade de maneiras, e não pretende ser limitada pelas modalidades preferidas ou métodos. Numerosas aplicações da invenção ocorrerão facilmente àqueles versados na técnica a partir de uma

consideração da descrição precedente. Portanto, é desejado que a invenção não é limitada ao exemplo específico descrito ou à construção e operação mostradas e descritas. Em vez disto, todas as modificações e os equivalentes adequados podem ser escolhidos, estando dentro do escopo da invenção.

REIVINDICAÇÕES

1. Sistema de comunicações (9), **caracterizado** pelo fato de que compreende:

uma etiqueta de identificação de rádiofreqüência (RFID) (20) compreendendo uma memória de etiqueta (26) armazenando uma chave privada e uma identificação de etiqueta (ID), um gerador de número randômico de etiqueta (28) para gerar um primeiro número randômico, um gerador de código de autenticação de etiqueta (29), e um processador de etiqueta (24) para fazer a ID da etiqueta ser transmitida; e

uma leitora de RFID (10) compreendendo um gerador de número randômico de leitora (18) para gerar um segundo número randômico, uma memória de leitora (16) armazenando chaves privadas de etiquetas e IDs de etiquetas, cada chave privada associada com uma das IDs de etiquetas, um processador de leitora (14) para receber a ID de etiqueta transmitida da etiqueta de RFID e recuperar da dita memória de leitora a chave privada de etiqueta associada com a ID de etiqueta recebida, um gerador de código de autenticação de leitora (19) para receber o primeiro número randômico, o segundo número randômico, e a chave privada de etiqueta recuperada, o dito gerador de código de autenticação de leitora gerando um código de autenticação de leitora baseado na chave privada, o primeiro número randômico, e o segundo número randômico,

onde o dito processador de leitora (14) faz o primeiro código de autenticação de leitora a ser transmitido para a dita etiqueta (20);

onde o dito gerador de código de autenticação de etiqueta (29) ainda gera um código de autenticação de leitora baseado na chave privada, o primeiro número randômico, e o segundo número randômico, e o dito processador de etiqueta (24) determina se a leitora (10) é autêntica, baseado em uma comparação do código de autenticação de leitora transmitido pela leitora (10), e o código de autenticação de leitora gerado pelo gerador de código de autenticação de etiqueta (29).

2. Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de que a dita etiqueta (20) aceita comunicações da dita leitora (10) se o

dito processador de etiqueta (24) determina que a leitora (10) é autêntica.

3. Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito processador de etiqueta (24) determina que a leitora (10) é autêntica se o código de autenticação da leitora transmitido pela leitora (10) corresponde ao código de autenticação de leitora gerado pelo gerador de código de autenticação de etiqueta (29).

4. Sistema, de acordo com a reivindicação 1, **caracterizado** pelo fato de que o dito gerador de código de autenticação de etiqueta (29) ainda gera um código de autenticação da etiqueta baseado na chave privada, o primeiro número randômico, e o segundo número randômico, e o dito processador de etiqueta (24) faz o dito código de autenticação da etiqueta ser transmitido para a dita leitora (10), e ainda onde o dito gerador de código de autenticação de leitora (19) gera um código de autenticação da etiqueta baseado na chave privada, o primeiro número randômico, e o segundo número randômico, e o dito processador de leitora (14) determina se a etiqueta (20) é autêntica com base na comparação do código de autenticação da etiqueta transmitido pela etiqueta (20) e do código de autenticação da etiqueta gerado pela leitora.

5. Sistema, de acordo com a reivindicação 4, **caracterizado** pelo fato de que a dita etiqueta (20) aceita as comunicações da dita leitora (10) se o dito processador de etiqueta (24) determina que a leitora (10) é autêntica, e a dita leitora (10) aceita comunicações da dita etiqueta (20) se o dito processador de leitora (14) determina que a etiqueta (20) é autêntica.

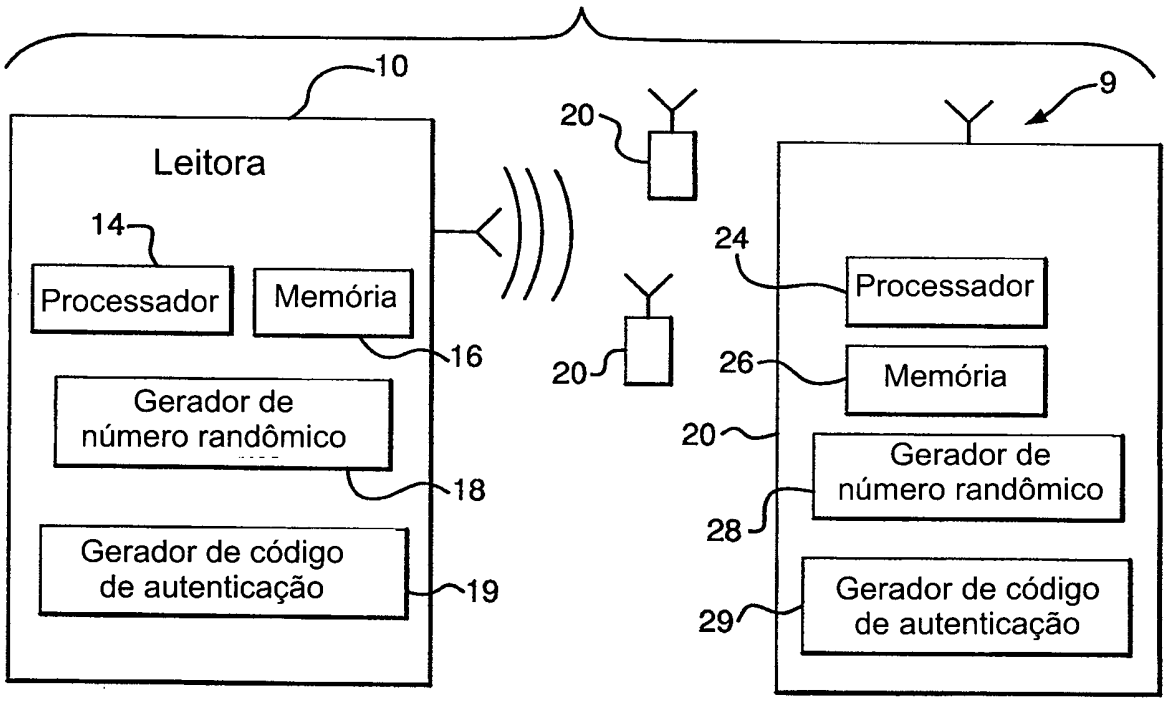
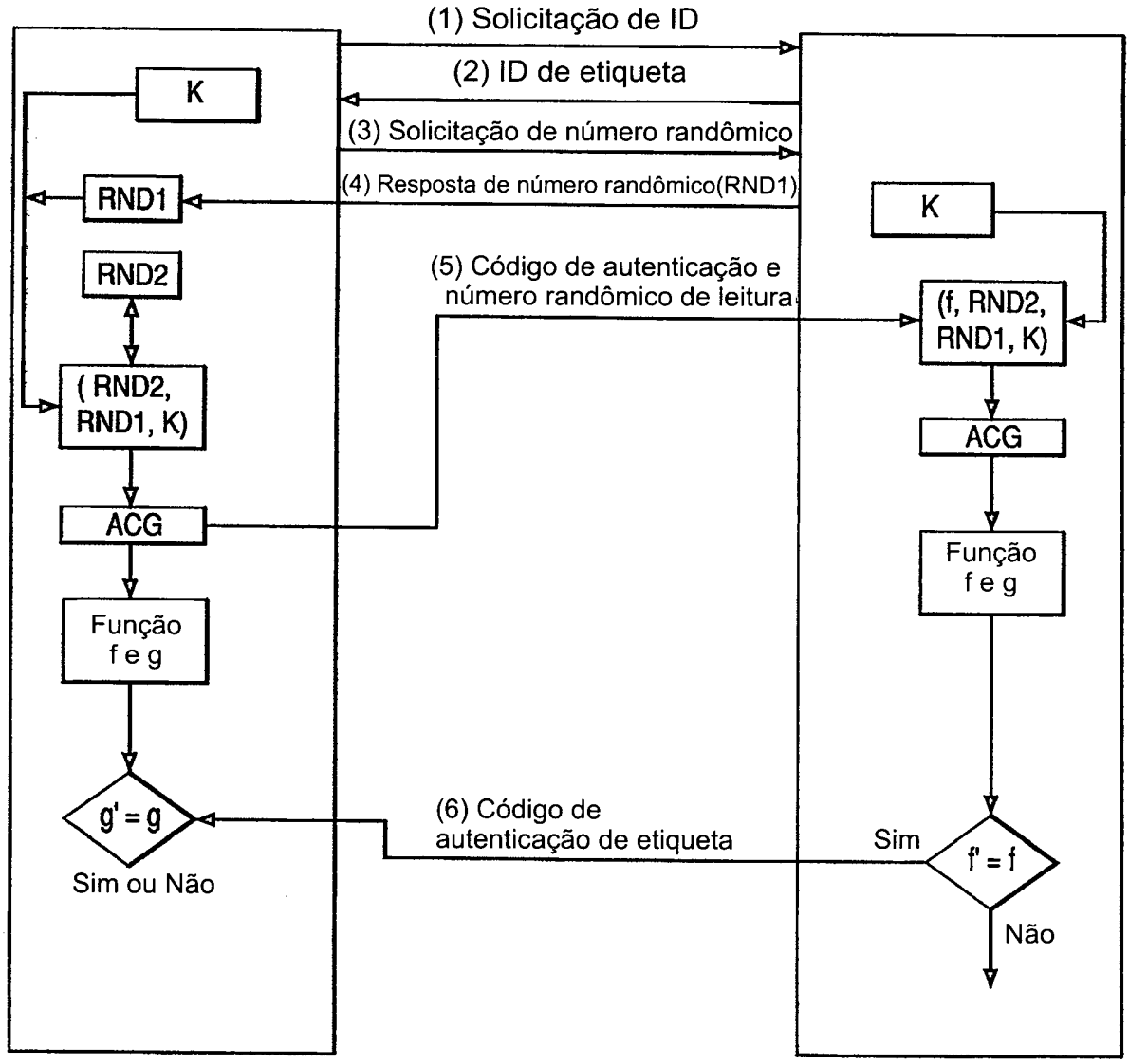

10
Leitora
14
Processador
Memória
16
Gerador de
número randômico
18
Gerador de código
de autenticação
19
20
20
9
24
Processador
26
Memória
20
Gerador de
número randômico
28
29
Gerador de código
de autenticação

FIG. 1



ACG - Gerador de código de autenticação

FIG. 2