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

(11) **PI 0212117-4 B1**

BRPI0212117B1

(22) Data do Depósito: 22/08/2002

(45) Data de Concessão: 24/05/2016

(RPI 2368)

(54) Título: APARELHO DE AUTENTIFICAÇÃO DE ARTIGO, ARTIGO PARA AUTENTICAÇÃO E SISTEMA DE PROCESSAMENTO

(51) Int.Cl.: H04L 9/00; G06F 15/16

(30) Prioridade Unionista: 06/06/2002 US 10/164,070, 24/08/2001 US 60/314,926

(73) Titular(es): ZIH CORP.

(72) Inventor(es): CLIVE P. HOHBERGER, BORIS Y. TSIRLINE

Relatório Descritivo da Patente de Invenção para **"APARELHO DE AUTENTICAÇÃO DE ARTIGO, ARTIGO PARA AUTENTICAÇÃO E SISTEMA DE PROCESSAMENTO".**

Esta invenção refere-se em geral a uma técnica de autenticação para um artigo utilizado em um dispositivo hospedeiro. De forma mais específica, uma modalidade particular desta invenção refere-se a um aperfeiçoamento para um cassete ou cartucho de tinta em um aparelho de marcação térmica onde o cassete de tinta ou o cartucho de fita pode ser autenticado como sendo um tipo adequado e proveniente a partir de uma fonte autorizada.

FUNDAMENTO

Outros modos de se abordar foram tentados para autenticar consumíveis em um hospedeiro, mas nenhum destes tem sido satisfatório. Em particular, os modos de se abordar do fundamento discutido abaixo não proporcionam uma repressão antipirataria eficaz. Estes conhecidos modos de se abordar anteriormente não proporcionam autenticação adequada e podem ser de forma freqüente superados por cópia, fraude ou técnicas similares.

Uma técnica anterior para autenticar consumíveis contava com, os formatos em chave do consumível. Tais formatos em chave podem ser projetados de modo que somente um consumível no formato chavetado irá se encaixar dentro de um dado tipo de hospedeiro. Como um exemplo, um aparelho de barbear pode ser adaptado para receber somente as lâminas de barbear possuindo um formato chavetado particular. Como um segundo exemplo, uma impressora a jato de tinta pode ser adaptada para receber somente cartuchos de tinta de recarga possuindo um formato chavetado particular. O uso de tal formato chavetado pode impedir a troca de consumíveis entre tipos diferentes de hospedeiro. Este modo de se abordar é de forma geral ineficaz para a antipirataria, entretanto, porque o formato chavetado do consumível pode ser prontamente observado e facilmente duplicado.

Também insatisfatórios são os algoritmos de autenticação de "desafio e resposta" utilizados em transponders de comunicação para os

sistemas de segurança de automóvel, tal como o Atmel TK556 e equivalentes. Os sistemas de segurança automotivos foram projetados para aplicações de "uma trava, poucas chaves", onde um único número secreto é programado em cada chave e em cada trava. Se um dispositivo hospedeiro, tal como uma impressora ou uma câmara for a "trava", então os tais transponders de comunicação de desafio - resposta requerem que todas as chaves (meio) e travas (impressoras) sejam programados com o mesmo número secreto.

É conhecido proporcionar codificações nos consumíveis, tais como unidades de filme e/ou hospedeiros tal como câmaras, para propósitos de identificação e para transportar a informação sobre a unidade ou câmara de filme. O termo "codificação" muito amplamente descreve uma característica do meio físico utilizada para comunicar uma ou mais partes de informação para uma máquina. "Codificação" inclui texto alfanumérico e outros índicios, símbolos e coisas parecidas. Uma codificação pode ser detectável por vários dispositivos, incluindo mas não limitado às leitoras óticas, magnéticas e/ou de perfuração.

A Patente dos Estados Unidos N.º 6.106.166 revela um dispositivo possuindo um transponder de comunicação e um transponder. Uma memória de leitura/gravação eletricamente ou eletronicamente programável contida no transponder de comunicação está de forma inteiriça ligada à um consumível. O transponder de comunicação está apto a receber um primeiro campo eletromagnético de freqüência RF e a derivar energia e a informação de endereço a partir do mesmo, e então gerar um segundo campo eletromagnético de freqüência RF em resposta. O segundo campo eletromagnético é característico dos dados armazenados na memória. Um transponder está disposto dentro do hospedeiro com uma antena e com componentes de suporte para fazer consulta seqüencial em cada transponder de comunicação. Como instruído por um processador de lógica de controle, o transponder pode ler os dados de fabricação a partir do transponder pode ler os dados de fabricação a partir do transponder de comunicação e gravar os dados de utilização e de processamento junto ao transponder de comunicação

para armazenamento na memória.

Os transponders de comunicação de identificação por radiofreqüência estão amplamente disponíveis em uma variedade de formas. Uma forma, referida como "transponders de comunicação embutidos" são transponders de comunicação que possuem um formato substancialmente plano. A antena para um transponder de comunicação embutido está na forma de um traço condutor depositado em um suporte não-condutor. A antena pode possuir o formato de uma bobina plana e assim por diante. Os condutores para a antena também são depositados, com camadas não-condutoras interpostas como necessário. Os componentes de memória, comunicações RF e quaisquer funções de controle são proporcionados por um chip montado sobre o suporte e de forma operativa conectados através dos condutores com a antena. Os transponderes de comunicação embutidos tem sido utilizados como camadas de etiquetas e rótulos de identificação para proporcionar codificações que são acessíveis em uma distância. Uma câmara possuindo um transponder de comunicação de identificação por radiofreqüência que pode ser acessado para gravação e leitura à distância é revelada na Patente dos Estados Unidos N.º 6.173.119.

Outro tipo conhecido de transponder de identificação é um transponder de comunicação de identificação por radiofreqüência (RFID). Um transponder de comunicação RFID pode tipicamente incluir um identificador único instalado pelo fabricante na memória não-volátil.

Com respeito aos dispositivos hospedeiros, é conhecido proporcionar um artigo consumível, tal como um cartucho de impressão, com um transponder de comunicação. O dispositivo hospedeiro, tal como uma impressora dentro da qual o cartucho é instalado, inclui um transponder para detectar o tipo de meio no cartucho de impressão. Um transponder e um transponder de comunicação deste tipo geral são revelados na Patente dos Estados Unidos N.º 6.099.178 para Spurr et al. A patente de Spurr revela uma impressora adaptada para perceber o tipo de meio instalado e inclui um transponder por radiofreqüência para transmitir um primeiro campo eletromagnético e para perceber um segundo campo eletromagnético. Entretanto,

Spurr não ensina ou sugere um dispositivo para autenticar o meio suportando o transponder de comunicação. A informação codificada no transponder de comunicação no Spurr pode ser facilmente forjada, assim produzindo o sistema ineficaz como uma medida antipirataria.

O Publicação Internacional Número WO 98/52762 revela uma impressora a jato de tinta que utiliza uma etiqueta RFID para identificar o tipo de papel que é carregado em uma impressora a jato de tinta. Este modo de se abordar oferece comunicação sem contato com uma memória de leitura/gravação que é adicionada ao cilindro de jato de tinta. Entretanto, esta publicação não ensina ou sugere um método e aparelho de autenticação de acordo com esta revelação.

Portanto, existe uma necessidade de uma medida antipirataria eficaz utilizando um transponder de comunicação e um transponder para perceber a informação codificada em um artigo consumível para uso em um dispositivo hospedeiro, tal como meio para uso em uma impressora.

BREVE DESCRIÇÃO DOS DESENHOS

É acreditado que a invenção será melhor entendida a partir da descrição seguinte quando feita em conjunto com os desenhos acompanhantes, onde:

A FIGURA 1A é uma vista em perspectiva de cima esquerda de um artigo consumível sendo carregado em um dispositivo hospedeiro de acordo com uma modalidade.

A FIGURA 1B é uma vista em perspectiva de cima frontal de um artigo consumível sendo carregado em um dispositivo hospedeiro de acordo com uma modalidade.

A FIGURA 2A é um fluxograma de programa descrevendo uma modalidade de uma seqüência de operações para preparar um artigo consumível que pode ser autenticado.

A FIGURA 2B é um fluxograma de programa descrevendo uma modalidade de uma seqüência de operações para preparar um artigo consumível que pode ser autenticado.

A FIGURA 3A é uma vista em perspectiva de cima direita de um

artigo consumível a ser autenticado e de um dispositivo hospedeiro de acordo com uma modalidade.

A FIGURA 3B é uma vista em perspectiva de cima direita de um artigo consumível para autenticação e de um dispositivo hospedeiro para autenticar a invenção de acordo com uma modalidade

A FIGURA 4 é um fluxograma de sistema ilustrando uma seqüência de operações e o fluxo de dados em uma modalidade de um método para autenticar um consumível.

A FIGURA 5 é uma vista em perspectiva esquerda de cima em seção parcial de um artigo consumível carregado em um dispositivo hospedeiro ilustrando a colocação dos componentes de autenticação de acordo com uma modalidade.

A FIGURA 6 é uma vista em perspectiva direita de cima em seção parcial de um artigo consumível carregado em um dispositivo hospedeiro ilustrando a colocação dos componentes de autenticação de acordo com uma modalidade.

A FIGURA 7A é uma vista em perspectiva de um cartucho de impressão de artigo consumível com um circuito autenticador montado em um lado de acordo com uma modalidade.

A FIGURA 7B é uma vista ampliada de um componente de autenticação montado em um artigo consumível.

A FIGURA 7C é uma vista ortogonal lateral de um cartucho de impressão de artigo consumível com um circuito autenticador montado em um lado de acordo com uma modalidade.

A FIGURA 7D é uma vista ortogonal de cima de um cartucho de impressão de artigo consumível com um circuito autenticador montado em um lado de acordo com uma modalidade.

A FIGURA 8 é um diagrama de blocos de um artigo consumível, de um dispositivo hospedeiro e de um circuitamento de autenticação de acordo com uma modalidade.

A FIGURA 9 é uma vista em perspectiva ilustrando a colocação de uma placa de circuito em um dispositivo hospedeiro para autenticar um

artigo consumível de acordo com uma modalidade.

A FIGURA 10A é uma vista ortogonal em retaguarda de uma primeira modalidade de uma placa de circuito para montagem em um dispositivo hospedeiro para autenticar um artigo consumível.

A FIGURA 10B é uma vista ortogonal frontal de uma primeira modalidade de uma placa de circuito para montagem em um dispositivo hospedeiro para autenticar um consumível.

A FIGURA 11 é uma vista em perspectiva de uma bobina de um cartucho de impressão de artigo consumível com um circuito autenticador montado em uma flange de acordo com uma modalidade.

A FIGURA 12A é uma vista ortogonal lateral de uma bobina de um cartucho de impressão de artigo consumível com um circuito autenticador montado em um flange de acordo com uma modalidade.

A FIGURA 12B é uma vista ortogonal da primeira extremidade de uma bobina de cartucho de impressão de artigo consumível com um circuito autenticador montado em um flange de acordo com uma modalidade.

A FIGURA 12C é uma vista ortogonal da segunda extremidade de uma bobina de cartucho de impressão de artigo consumível com um circuito autenticador montado em um flange de acordo com uma modalidade.

A FIGURA 12D é uma vista ortogonal lateral em seção de uma bobina de cartucho de impressão de artigo consumível com um circuito autenticador montado em um flange de acordo com uma modalidade.

A FIGURA 13 é um diagrama de blocos de um artigo consumível, um dispositivo hospedeiro e de um circuitamento de autenticação de acordo com uma modalidade utilizando uma conexão de rede.

DESCRIÇÃO DETALHADA

A presente descrição é direcionada em particular aos elementos formando parte, ou cooperando mais diretamente com o aparelho de acordo com a invenção. É para ser compreendido que os elementos não apresentados ou descritos de forma específica podem tomar várias formas conhecidas pelo os com conhecimento na técnica. Nesta descrição, o termo "consumível" refere-se a um componente projetado para ser utilizado e substituí-

do em um dispositivo referido como um hospedeiro. Exemplos de consumíveis e de seus respectivos hospedeiros incluem reservatórios de jato de tinta para uso em impressoras, filme para uso em câmaras, uma fita para uso em uma máquina de escrever e/ou um cartucho de pigmento em pó para uso em uma copiadora.

Referindo-se agora à FIGURA 1A, um dispositivo hospedeiro (100) é configurado para receber um artigo consumível (120). O dispositivo hospedeiro (100) nesta modalidade específica pode ser uma impressora de cartão plástico para imprimir códigos de barra nos cartões plásticos utilizando um processo de transferência térmica. O artigo consumível (120) desta modalidade pode ser um cartucho de fita contendo uma fita (150) tal como, por exemplo, uma fita de resina de transferência térmica ou uma fita de sublimação de pigmento. Um dispositivo hospedeiro impressora de cartão plástico (100) pode incluir outros componentes convencionais (não apresentados) tais como, uma cabeça de impressão, uma estação codificadora magnética, interruptor de energia, painel de controle, alimentador de cartão, depósito alimentador de saída de cartão e outros componentes. Uma cobertura da impressora que pode ser aberta (162) oculta o mecanismo interno do artigo consumível cartucho de fita (120) e ajuda a limitar a entrada de contaminantes, tal como poeira e material em partícula. Um botão de liberação da cobertura (160) é apresentado em um lado do dispositivo hospedeiro impressora de cartão plástico (100) nesta modalidade. Um segundo botão de liberação da cobertura (não apresentado) pode estar localizado no lado oposto. Uma parede interior esquerda (167L) e uma parede interior direita (167R) definem uma fenda (165) no dispositivo hospedeiro impressora de cartão plástico (100) para receber o artigo consumível cartucho de fita (120) nesta modalidade. O artigo consumível cartucho de fita (120) pode ser carregado no dispositivo hospedeiro impressora de cartão plástico por se primeiro pressionar o botão de liberação da cobertura (160) em um lado do dispositivo hospedeiro impressora de cartão plástico (100) para abrir a cobertura da impressora (162) então inserindo o artigo consumível cartucho de fita (120) de forma vertical dentro da fenda (165) e pressionando o artigo

consumível cartucho de fita (120) no lugar. A realimentação tátil ou audível pode indicar que o artigo consumível cartucho de fita (120) foi de forma apropriada assentado.

Ainda referindo-se à modalidade apresentada na FIGURA 1A, o artigo consumível de cartucho de fita (120) pode incluir uma bobina fonte (140) e uma bobina de correção (145). Antes do artigo consumível de cartucho de fita (120) ser utilizado, a fita (150) é disposta em um cilindro enrolado ao redor da bobina fonte (140). À medida que a fita (150) é utilizada e o artigo consumível cartucho de fita (120) é consumido, a fita (150) enrola-se ao redor da bobina de correção (145). A bobina fonte (140) e a bobina de correção (145) são separadas em uma relação fixa na modalidade ilustrada por um membro de grampo de fixação esquerdo (147L) e um membro de grampo de fixação direito (147R). A bobina fonte (140), a bobina de correção (145), o membro de grampo de fixação esquerdo (147L) e o membro de grampo de fixação direito (147R) juntos compreendem quatro lados definindo um espaço em formato retangular através do qual a fita (150) passa. Na modalidade descrita na FIGURA 1A, um transponder de comunicação (130) de identificação por radiofreqüência (RFID) é proporcionado no membro de grampo de fixação esquerdo (147L) do cartucho de fita (120). Apesar de na modalidade ilustrada o transponder de comunicação RFID (130) estar disposto no membro de grampo de fixação esquerdo (147L), na prática o mesmo pode ser também colocado em qualquer localização adequada, tal como no membro de grampo de fixação direito (147R). Sem dúvidas, o transponder de comunicação não precisa estar limitado aos sinais de radiofreqüência, e pode utilizar qualquer forma de radiação eletromagnética adequada, tal como a luz visível, ultravioleta e infravermelha, como é conhecido na técnica.

De acordo com a modalidade ilustrada da FIGURA 1A, o transponder de comunicação RFID (130) pode conter um número de série único programado na fábrica n. Certos transponderes de comunicação RFID disponíveis comercialmente contêm um número de série de identificação do transponder de comunicação único com 32 a 64 bits, n, utilizado no proto-

colo de "anticolisão". Este protocolo permite a separação e a identificação única de vários transponderes de comunicação simultaneamente aparecendo no campo da leitora RFID, o que pode ser causado por múltiplos dispositivos hospedeiros estando localizados relativamente muito próximos.

Um número de autenticação, x, é calculado utilizando uma função de criptografia, F, selecionada por e confidencial para o fabricante do artigo consumível cartucho de fita (120). O número de autenticação é permanentemente armazenado no transponder de comunicação RFID (130). a função de criptografia F é deixada disponível para o dispositivo hospedeiro impressora (100) durante a operação do mesmo. Por exemplo, em uma modalidade apresentada na FIGURA 8, a função de criptografia confidencial F pode ser programada no dispositivo hospedeiro impressora (100) antes ou durante a fabricação. Em outra modalidade, a função de criptografia confidencial F é deixada disponível para o dispositivo hospedeiro impressora (100) através de uma rede. Quando o artigo consumível cartucho de fita (120) é carregado no dispositivo hospedeiro impressora (100), o transponder RFID interno da impressora (não apresentado na FIGURA 1A) lê os valores do número de série, n, e do número de autenticação, x, a partir do transponder de comunicação RFID (130) ligado ou no artigo consumível cartucho de fita (120). Ele então determina se o número de autenticação x associa-se com o número de série n como transformado pela função de criptografia confidencial F. Se os valores combinarem, então o artigo consumível cartucho de fita (120) é julgado como sendo um produto de meio autêntico que pode ser utilizado nesta impressora.

Cada impressora (100) a partir de um dado fabricante pode ser programada com o mesmo algoritmo de criptografia na fábrica. Quando o artigo consumível cartucho de fita (120) é produzido, o mesmo algoritmo de criptografia utilizado para gerar o número de autenticação é proporcionado na impressora. Uma vez que o artigo consumível cartucho de fita (120) esteja instalado, o número de série único do transponder de comunicação, n, é lido. Em uma modalidade preferida, o número de série único transponder de comunicação , n, já está travado na memória do transponder de comunica-

ção RFID (130) pelo fabricante.

O fabricante do artigo consumível de cartucho de fita (120) também conhece o tipo de meio a ser feito, y. Em outra modalidade, os valores tanto de n como também de y são combinados para serem utilizados no algoritmo de criptografia para calcular o código de autenticação x. O fabricante do artigo consumível cartucho de fita (120) então programa e trava os valores x e y na memória do transponder de comunicação (130). O transponder de comunicação (130) é permanentemente montado no artigo de consumível cartucho de fita (120). Um número efetivamente ilimitado de rolos de cassetes de mídia poe er produzido desta maneira, cada um contendo um valor unicamente programado e bloqueado de número de série n, número do tipo de mídia y e número de autenticação x.

Apesar do número de série n, do número de tipo de meio y e do número e autenticação x serem livremente legíveis, a função de criptografia confidencial, F, eles são de preferência selecionados a partir de uma classe conhecida de funções não possuindo inverso óbvio. Por conseqüência, tais funções são difíceis de decodificar, assim proporcionando autenticação segura. Um falsificador de um artigo consumível cartucho de fita (120) teria que reconstruir o algoritmo F disponível para a impressora (100) de modo a fazer que o artigo consumível cartucho de fita falsificado (120) funcione em uma impressora (100) de acordo com a modalidade descrita na FIGURA 1.

Se o valor de x é calculado como alguma função complicada do único e não copiável número de série do transponder de comunicação n, então os valores de n e de x pode ambos serem armazenados no transponder de comunicação RFID (130), onde ambos os números são decriptografados e legíveis por qualquer um. De forma opcional, se um número de tipo de meio y também for utilizado na transformação, ele pode também ser armazenado no transponder de comunicação RFID. Quando o artigo consumível cartucho de fita (120) é instalado na impressora (100), a impressora pode ler tanto o x como n (e, opcionalmente, y) a partir do transponder de comunicação e validar se o valor de leitura de x é correto para o valor de lido de n (e, opcionalmente, de y), assim validando o artigo consumível de

cartucho de fita (120) para a impressora correspondente (100).

A seleção judiciosa de um algoritmo para F a partir do meio de conhecidos algoritmos de criptografia fortes pode deixar a quebra deste sistema de segurança muito difícil e na prática, de forma dispendiosa proibida. O código de autenticação x pode ser calculado utilizando-se os métodos de criptografia por se aplicar algumas funções para criptografar n. A única informação disponível ao falsário é que um dado código de autenticação da fita x é correto para um dado número de série n. De forma mais particular, o falsificador não irá saber ou estar apto a aprender como o valor de x foi obtido para um dado n. Nem pode o falsificador de forma aleatória tentar todos os valores possíveis de n, porque os valores associados de x não serão conhecidos a menos que o falsificador tenha obtido um cilindro de meio válido possuindo tanto este n como o código de autenticação correto x. Assim, o falsificador somente possui amostras limitadas de n e x para testar.

O mesmo é verdadeiro para modalidades nas quais x é calculado em função tanto do número de série n como do número de tipo de meio y. O código de autenticação x pode ser calculado utilizando-se métodos de criptografia por se aplicar alguma função para criptografar n e y. Novamente, a única informação disponível para o falsificador é que um dado código de autenticação da fita x é correto para um dado par, n, y.

Como uma defesa adicional contra o sistema de segurança sendo comprometido, uma pluralidade de funções definindo relações aceitáveis entre os valores de teste podem ser armazenadas no dispositivo hospedeiro. O artigo consumível pode então ser programado com uma pluralidade de códigos de autenticação, cada um dos quais satisfaz uma relação funcional de autenticação particular. Se for aprendido que qualquer função de autenticação foi comprometida, então o meio pode ser validado utilizando-se uma das outras funções de autenticação e os valores de autenticação. A função de autenticação comprometida pode ser desabilitada no dispositivo hospedeiro para impedir autenticação do meio pirata feito utilizando a função de autenticação comprometida. Por exemplo, a função de autenticação comprometida pode ser desabilitada em resposta a uma sinalização estabeleci-

da no meio subsequente ou por atualizações junto ao software ou às rotinas de software armazenadas na memória de leitura do dispositivo hospedeiro.

Como é conhecido na técnica, o dispositivo hospedeiro ou impressora (100) inclui memória adequada, tais como RAM, ROM, EEPROM e outros mais, dispositivos de entrada/saída, computador ou processador central, armazenamento em disco opcional e dispositivos de suporte associados, todos os quais não são apresentados. O computador pode ser, por exemplo, um computador compatível com IBM possuindo, por exemplo, um microprocessador da família Pentium® ou Intel. De forma alternativa, o computador pode ser compatível com APPLE® possuindo um processador da família Motorola. Entretanto, o computador ou processador central pode ser qualquer computador, processador, unidade central de processamento (CPU), microprocessador, RISC (computador de conjunto de instruções reduzidas), computador de grande porte, estação de trabalho, computador de único chip, processador distribuído, servidor, controlador, micro controlador, dispositivo de lógica separado, computador remoto, computador Internet ou computador Rede. A memória e/ou o armazenamento em disco associado com o computador é configurado para armazenar instruções de programa representando os algoritmos e as etapas de processamento descritas aqui dentro. Tais instruções de programa podem ser "transferidas" a partir do armazenamento em disco ou a partir de uma memória não-volátil, tais como ROM, PROM, EPROM e outros mais, ou podem ser transferidas a partir de uma fonte remota via uma rede ou outra ligação de comunicação.

Referindo-se agora à modalidade apresentada na FIGURA 1B, é apresentado o dispositivo hospedeiro impressora de cartão plástico (100) e o artigo consumível cartucho de fita (120). Na FIGURA 1B, o artigo consumível cartucho de fita (120) é apresentado carregado dentro do dispositivo hospedeiro impressora de cartão de plástico (100). O artigo consumível cartucho de fita (120) nesta modalidade particular pode ser inserido entre a parede interna esquerda (167L) e a parede interna direita (167R). O transponder de comunicação RFID é apresentado montado no membro de grampo de fixação esquerdo (147L), mas poderia ser montado em qualquer outro

lugar tal, como no membro de grampo de fixação direito (147R). Como o artigo consumível cartucho de fita (120) carregado, a cobertura (162) pode ser fechada e o dispositivo hospedeiro impressora de cartão plástico (100) operado.

Para a simplicidade da descrição, a execução da invenção descrita a seguir irá empregar somente o número de série n e o número de autenticação x. Entretanto, também está dentro do escopo da invenção utilizar um número de tipo de meio y em conjunto com o número de série n para computar o número de autenticação x. O uso do número de série n pode diferir do uso do número de tipo de meio y pelo fato que o número de série pode ser permanentemente fixado no transponder de comunicação RFID quando o mesmo é fabricado e pode ser único para cada transponder de comunicação. Por outro lado, o número de tipo de meio y pode ser armazenado no transponder de comunicação RFID na fábrica e é o mesmo para cada meio de um dado tipo. Entretanto, o uso do número de série n na autenticação ou nos cálculos de criptografia descritos aqui é o mesmo que o uso do número de tipo de meio y.

A FIGURA 2A é um fluxograma de programa que ilustra uma modalidade de uma seqüência de operações para preparar um artigo consumível que pode ser autenticado para uso em um dispositivo hospedeiro. Primeiro, o fabricante deve escolher uma função de autenticação adequada, escolha esta que é representada pelo processo da função de autenticação de seleção F (202). A função F é de preferência muito difícil de identificar dado somente os valores comparativamente raros de x e n. Após o processo da função de autenticação de seleção F (202), a próxima etapa é um processo de leitura do número de série do transponder de comunicação RFID n (204). O fabricante do artigo consumível que pode ser autenticado tem que ler o número de série n a partir do transponder de comunicação RFID para ser instalado no artigo consumível. O número de série n é instalado na fábrica, e é único para cada transponder de comunicação. A seguir, o fabricante pode executar um processo calcula número de autenticação x = F(n) (208). O domínio da função F não está limitado ao conjunto de valores de n, e em

particular F pode ser uma função multivariável como discutido em maiores detalhes abaixo. Tendo calculado o número de autenticação x com o processo calcula do número de autenticação x = F(n) (208), a seguir o número de autorização x é colocado na área de dados públicos do transponder de comunicação com o número de autenticação de armazenamento x no processo de transponder de comunicação RFID (210).

Uma modalidade alternativa de uma seqüência de operações para preparar um artigo consumível que pode ser autenticado para uso em um dispositivo hospedeiro é ilustrado na FIGURA 2B. Nesta modalidade, o fabricante primeiro seleciona uma função de autenticação com um processo seleciona função de autenticação $F_{M,Q}$ (202'). A função de autenticação $F_{M,Q}$ do processo desta modalidade alternativa é de preferência uma função unidirecional clássica utilizada na criptografia, a qual pode ser baseada na operação de módulo e na aritmética de Galois Field. A aritmética de Galois Field, em particular com a função unidirecional ($[M^G \text{ mod } Q]$), é amplamente utilizada na criptografia de chave pública. Como um exemplo, os métodos de Diffie-Hellman empregam este modo de se abordar. A seleção dos parâmetros M e Q de forma única determina a função $F_{M,Q}(G) = M^G \text{ mod } Q$. Como um exemplo, a notação "módulo" pode ser referida em uma frase da língua Inglesa na seguinte maneira, como é conhecido na técnica:

O valor da função de G é igual ao valor de M elevado à potência do valor do G "módulo" o valor de Q.

Os parâmetros M e Q são dois valores primos, os quais estão relacionados por M sendo o elemento primitivo de um Field Galois primo GF(Q) de ordem Q. Após estabelecer em uma função de criptografia no processo seleciona função de autenticação $F_{M,G}$ (202'), a próxima etapa é a etapa lê número de série do transponder de comunicação RFID n (204). A próxima etapa na modalidade da FIGURA 2B é um processo identificação do tipo de artigo consumível y (206). O número y é um número de peça selecionado pelo fabricante para identificar um tipo particular de meio junto ao qual o fabricante irá afixar este transponder de comunicação RFID particular. A próxima etapa é o processo seleciona função preparatória G(n, y) (208). A

faixa da função G(n, y) torna-se o domínio da função $F_{M,Q}(G)$, de modo que os valores de entrada n, y sejam mapeados pela função composta F ° G para o número de autenticação x. A função G(n, y) é de preferência única e de preferência secreta para a fabricação do artigo consumível que pode ser autenticado. A função preparatória G(n, y) de preferência pode mapear cada par n, y para um resultado único, apesar de tal mapeamento um a um não ser um requerimento da invenção. A função preparatória G(n, y) deve de preferência evitar certos valores degenerativos, patológicos de G. De forma específica, a função deve de preferência evitar resultar em valores nas faixas:

$G \leq 0$,

$G = 1$.

$G = \frac{Q - 1}{2}$, e

$G = (Q-1)$.

Como é conhecido na teoria de número de Galois Field, as funções G que produzem estes valores podem comprometer a segurança da função de criptografia $F_{M,Q}$. Uma função preparatória apropriada G(n, y) tendo sido selecionada, a etapa seguinte na seqüência de operações apresentadas na modalidade particular ilustrada na FIGURA 2B é um processo calcula número de autenticação $x = F_{M,Q}(G(n, y)))$ (208). Após ser calculado, o número de autenticação x é armazenado na área de dados públicos no transponder de comunicação RFID de uma modalidade no número de autenticação de armazenamento x no processo de transponder de comunicação RFID (210). Adicionalmente, o número y identificando um tipo de meio é armazenado no transponder de comunicação em um processo armazena número do tipo de artigo consumível y no transponder de comunicação RFID (212), após o que a seqüência de operações descritas na modalidade da FIGURA 2 para tornar o meio consumível autenticável está completa.

As FIGS. 3A e 3B ilustram outra modalidade descarregando e carregando um artigo consumível (120A, 120B) para fora e para dentro de um dispositivo hospedeiro (100) no qual o artigo consumível (120A, 120B) é

um cartucho de fita e o dispositivo hospedeiro (100) é uma impressora de cartão plástico. Para descarregar um artigo consumível cartucho de fita (120A, 120B) a partir de um dispositivo hospedeiro impressora de cartão plástico (100) após o artigo consumível ter sido utilizado, a tampa (162) é aberta, então o artigo consumível cartucho de fita no dispositivo hospedeiro (120B) é erguido (310), removendo o artigo consumível cartucho de fita (120A). Para carregar o artigo consumível cartucho de fita (120A), o mesmo é inserido verticalmente (320) e pressionado para dentro do local (120B).

A FIGURA 4 é um fluxograma de sistema que geralmente descreve o fluxo de operações e do fluxo de dados de um sistema para uma modalidade específica para verificar a autenticidade de um artigo consumível carregado em um dispositivo hospedeiro. Quando um meio de artigo consumível é instalado em um dispositivo hospedeiro impressora, o dispositivo hospedeiro primeiro percebe o artigo consumível recentemente carregado em um processo detecta artigo consumível (410). O artigo consumível pode ser detectado por um sensor mecânico, por reconhecer a proximidade de um transponder de comunicação RFID, ou por qualquer outro dispositivo de sensor adequado para tal detecção. Após a detecção do novo artigo consumível, o transponder RFID interno da impressora lê a partir do transponder de comunicação no meio instalado os valores do número de série n, do número de autenticação x e do tipo de consumível y.

Isto é apresentado na modalidade ilustrada na FIGURA 4, como três processos sucessivos, um processo lê número série n (415), um processo lê número de tipo de consumível y (420) e um processo lê número de autenticação x (425). A ordem destas operações não é importante e pode ser executada em uma seqüência diferente em outras modalidades sem se afastar do escopo da invenção. Após ler o número do tipo de consumível y, na modalidade ilustrada da FIGURA 4, a validade do consumível para o hospedeiro particular é testada em um processo verifica validade do tipo de consumível (430). Nesta modalidade, os tipos de meio válidos y para o dispositivo hospedeiro particular são conhecidos. Se o consumível for de um tipo inválido para o hospedeiro particular, o hospedeiro irá relatar a condição

de um cartucho incompatível utilizando um processo relata condição (480) e terminar. Se o tipo do meio for incompatível com o hospedeiro particular, é desnecessário verificar a autenticidade do meio.

Referindo-se ainda à modalidade da FIGURA 4, os dados da função de autenticação (490) ficam disponíveis para uso na verificação da autenticidade do meio consumível. O dispositivo hospedeiro pode ser programado antes dele ser vendido com a mesma função de autenticação usada mais tarde para fabricar os artigos consumíveis para uso no dispositivo hospedeiro. A seqüência de etapas definindo a função de autenticação pode ser armazenada no dispositivo hospedeiro como os dados de função de autenticação (490). Se o consumível for de um tipo y válido para o hospedeiro particular, o número de autenticação x é verificado utilizando-se os dados de função de verificação (490) em um processo verifica número de autenticação (440). O processo verifica número de autenticação (440) executa o algoritmo definindo a relação de autenticação utilizando n e y como entrada e compara seu valor calculado internamente de $x = F_{M.Q}(G(n, y))$ com o valor de x lido a partir do transponder de comunicação. Se eles combinarem, então este é um produto de meio autenticado do tipo y que pode ser utilizado nesta impressora. Se um cilindro de meio for detectado com um código de autenticação impróprio x, então todas os indicadores de validez e contadores de meio restantes são reinicializados para zero e travados por um processo reinicia indicadores (475). Esta meio falso é tanto detectado pela impressora quanto deixada inutilizável para qualquer aplicação futura uma vez detectado por configurar sua condição para "totalmente utilizado".

Uma lista de dados de consumíveis utilizados (470) é deixada disponível para o dispositivo hospedeiro nesta modalidade para confirmar se um cartucho consumido anteriormente não está sendo inserido. Após o consumível ser validado, o mesmo é utilizado no hospedeiro em um processo consumível utilizados (460), como por exemplo, por utilizar um cartucho de fita para um produto de impressão. Em uma modalidade, quando for determinado que o artigo consumível foi totalmente gasto pelo processo utiliza consumível (460), um identificador do artigo consumível (tal como o número

de série único n) será armazenado em uma lista de dados de consumíveis utilizados (470) indicando que o artigo consumível particular está totalmente utilizado. Em outra modalidade, a lista de dados de consumíveis utilizados (470) pode incluir uma identificação de todos os artigos consumíveis carregados no dispositivo hospedeiro e da porcentagem de vida útil restante em cada artigo consumível. A lista de dados de consumíveis utilizados (470) pode de forma econômica armazenar informação com respeito a um grande número de consumíveis utilizados anteriormente, tal como, por exemplo, uma lista dos últimos 512 cartuchos de impressão utilizados em uma impressora de cartão plástico. Se um cassete de fita ou um cilindro de fita reaparecer com um valor de contagem de painel restante superior ao do armazenado na memória da impressora de cartão plástico, a impressora de cartão plástico trata o cassete de fita ou cilindro de fita recarregado como se o mesmo tivesse uma autenticação inválida, e não somente pode rejeitar o uso este meio, mas também pode travar seu transponder de comunicação para a condição de "totalmente utilizado".

Referindo-se a seguir à modalidade das FIGS. 5 e 6, é apresentado na FIGURA 5 uma vista em seção parcial em perspectiva de cima esquerda de uma modalidade de um dispositivo hospedeiro contendo um consumível que pode ser autenticado. A FIGURA 6 apresenta uma vista em seção parcial em perspectiva de cima direita de uma modalidade de um dispositivo hospedeiro contendo um consumível que pode ser autenticado. O artigo consumível (120) é apresentado carregado no dispositivo hospedeiro (100). Um transponder de comunicação de identificação por radiofreqüência ("RFID") (130) é apresentado montado no artigo consumível (120). Uma antena (510) no dispositivo hospedeiro (100) permite ao mesmo ler a informação armazenada no transponder de comunicação RFID (130) no artigo consumível (100).

Referindo-se a seguir às FIGS. 7A até 7D, são apresentados várias vistas ilustrando um artigo consumível. Um cartucho de fita está apresentado na vista em perspectiva na FIGURA 7A. O artigo consumível cartucho de fita (700) possui uma bobina fonte (710) em uma extremidade, uma

bobina de correção (720) em outra extremidade, a bobina fonte (710) e a bobina de correção (720) sendo conectadas por um membro de grampo de fixação esquerdo (730L) e por um membro de grampo de fixação direito (730R). Um componente de comunicações (740) é apresentado, o qual pode ser um transponder de comunicação de identificação por radiofreqüência (RFID). Uma fita de impressão (750) passa a partir de uma bobina (710) para a outra bobina (720) entre os membros de grampo de fixação (730L, 730R).

A FIGURA 7B é uma vista ampliada de uma modalidade do rótulo e da montagem de transponder de comunicação RFID do componente de comunicações (740). O transponder de comunicação pode estar localizado na parte de dentro ou na parte de fora do membro de grampo de fixação esquerdo (730L) ou do membro de grampo de fixação direito (730R). Um rótulo pode também ser colocado no membro de grampo de fixação descrevendo o transponder de comunicação RFID.

A FIGURA 7C é uma vista ortogonal lateral de um artigo consumível (700) de acordo com uma modalidade específica. O artigo consumível cartucho de fita (700) possui uma bobina fonte (710) em uma extremidade, uma bobina de correção (720) em outra extremidade, a bobina fonte (710) e a bobina de correção (720) sendo conectadas por um membro de grampo de fixação (730). Montado no membro de grampo de fixação (730) está um componente de comunicações (740), o qual pode ser um transponder de comunicação RFID.

A FIGURA 7D é uma vista ortogonal de cima de um artigo consumível (700) de acordo com uma modalidade específica da invenção. O artigo de consumível cartucho de fita (700) possui uma bobina fonte (710) em uma extremidade, uma bobina de correção (720) em outra extremidade, a bobina fonte (710) e a bobina de correção (720) sendo conectadas por um membro de grampo de fixação esquerdo (730L) e por um membro de grampo de fixação direito (730R). Um componente de comunicações (740), o qual pode ser um transponder de comunicação RFID, está montado no membro de grampo de fixação esquerdo (730L) ou no membro de grampo

de fixação direito (730R).

Referindo-se agora à FIGURA 8, um diagrama esquemático de um sistema de autenticação de artigo consumível para autenticar um artigo consumível em um dispositivo hospedeiro é apresentado. Um artigo consumível (800) pode incluir, por exemplo, um cartucho de fita de impressão possuindo uma bobina fonte (805), uma bobina de correção (810) e um membro de grampo de fixação (815). O artigo consumível (800) pode incluir um componente de comunicações (820, 835) para transmitir informação para um dispositivo hospedeiro (850). O componente de comunicações (820, 835), pode em uma modalidade, ser transponderes de comunicação RFID de baixo custo, possuindo duas propriedades específicas. Em primeiro lugar, o tipo de baixo custo dos transponderes de comunicação RFID de preferência podem incluir um número de série único programado de fábrica n (830), o qual não pode ser alterado por um usuário ou duplicado por se copiar uma área de dados públicos (825) do transponder de comunicação para outro tipo similar de transponder de comunicação. Assim cada transponder de comunicação é de forma única numerado, o que é um requerimento para a maior parte dos tipos de transponderes de comunicação RFID que possuem um protocolo de "anti-colisão" permitindo que múltiplos transponderes de comunicação sejam diferenciados quando todos forem vistos no campo da antena da leitora RFID.

Em segundo lugar, os transponderes de comunicação de baixo custo de preferência possuem a habilidade de gravar (ou de gravar e travar) de uma vez os valores de dados, x e y, em uma área de dados públicos (825) do transponder de comunicação. O valor y nesta modalidade particular é a informação de tipo de meio, desde que nem todos os tipos de meio funcionam em todos os tipos de impressoras. O valor de dado diferente de zero x para este modo ilustrativo será uma função complicada de y e o número de identificação único n deste transponder de comunicação. O valor x neste exemplo descrito será programado na fábrica dentro do transponder de comunicação na hora em que o meio é fabricado, ou pelo menos antes do mesmo deixar a instalação do fabricante.

Tanto o Philips I*Code e equivalentes como qualquer Padrão 15693 da International Standards Organization ("ISO") condescendente com os transponderes de comunicação RFID de 13.56 MHz possuem um número de série de 48-bit programado na fábrica, que não pode ser copiado, com a habilidade de permanentemente armazenar um código de autenticação correspondente (derivado a partir do número de série) no chip. A seção 4.1 do ISO 15693 especifica que cada transponder de comunicação condescendente deve ser identificado por um identificador único (UID) de 64 bits, o qual deve ser estabelecido permanentemente pelo fabricante IC e deve ser estruturado como se segue:

64 57	56 49	48
hexadecimal 'E0'	código IC mfr	número de série do fabricante IC

O byte mais significativo deve ser o hexadecimal 'E0', seguido por um código de fabricante IC com 8 bits, o qual é designado de acordo com o ISO 7816-6/AM1. O número de série com 48-bit deve ser designado pelo fabricante IC identificado. É suposto que vários fabricantes irão produzir transponderes de comunicação ISO 15693 condescendentes com o ISO 15693 com números de série programados de fábrica e com os IDs únicos dos fabricantes registrados sob o ISO 7816. O ID único de 8 bits do fabricante, ou uma lista de IDs de fabricantes qualificados, pode ser incluídos como parte do processo de autenticação.

Referindo-se ainda à modalidade específica da FIGURA 8, um dispositivo hospedeiro (850) inclui um componente de comunicação (855, 860) para ler os valores de n, x e y armazenados no artigo consumível. Um processador (865) pode receber a informação armazenada no artigo consumível e pode utilizar uma função de autenticação (870) F (M, Q, x, y) disponível para o processador para confirmar que uma relação de autenticação existe entre o código de autenticação x e o número de série n e o código de tipo de meio y. O processador (865) de preferência é um micro processador seguro. O programa de autenticação do meio da impressora é escondido de pirataria potencial por ser armazenado no microprocessador seguro. O programa de autenticação não pode ser lido a partir da impressora nem pode o

programa ser observado durante a execução. Isto ajuda a impedir um pirata potencial de determinar ou de reconstruir o algoritmo de autenticação que calcula x para n e y.

O artigo consumível de preferência inclui os indicadores (827) para indicar o número de unidade de meio tal como painéis de fita utilizados no artigo consumível. Cada núcleo ou cassete de cilindro de fita somente pode ser utilizado uma vez. Outros elementos de memória no transponder de comunicação mantém o rastro de utilização do meio e a contagem restante do meio. Os indicadores na memória do transponder de comunicação são reinicializados e travados a media que cada parte da unidade (tipicamente 10 até 15%) deste meio é utilizada. Desde que somente um máximo de 15% de meio adicional pode ser recarregado no núcleo ou cassete, isto torna a reutilização de núcleos ou cassetes parcialmente utilizados economicamente não atrativa. Obviamente, os indicadores podem ser utilizados para indicar qualquer grau de utilização.

Referindo-se ainda à modalidade ilustrada na FIGURA 8, existe disponível para o processador (865) uma lista de consumíveis utilizados (880). Uma lista de "cassetes utilizados" é mantida em cada impressora. Os últimos 512 números de série de cassete n e sua contagem de painel restante podem ser armazenados em cada impressora. Caso um cassete reapareça com um valor de contagem de painel restante mais alto do que armazenado na memória da impressora, a impressora pode tratar o cassete ou cilindro de fita recarregado como se ele tivesse uma autenticação inválida e não somente recusar a utilizar este meio mas também pode travar seu transponder de comunicação na condição "totalmente utilizado", assim impedindo a "recarga" do meio utilizado.

Referindo-se a seguir à FIGURA 9, é apresentada uma modalidade específica de um componente de comunicações montado em um dispositivo hospedeiro para ler um componente de comunicações em um artigo consumível. É apresentada a estrutura do dispositivo hospedeiro (910). A estrutura do dispositivo hospedeiro particular (910) aqui descrita é uma estrutura de impressora de cartão plástico com o alojamento plástico exterior

removível. Uma placa de circuito (920) está montada na estrutura de dispositivo hospedeiro particular (910). A placa de circuito (920) inclui uma antena (930) para ler um transponder de comunicação de identificação por freqüência de rádio (não apresentado). A antena (930) na placa de circuito (920) é um transponder para ler o transponder (não apresentado) em um artigo consumível a ser carregado na estrutura de dispositivo hospedeiro (910). Este transponder é somente uma modalidade de um componente de comunicações de um modo para ler a informação armazenada em um artigo consumível. Outros exemplos de componentes de comunicações incluem contatos elétricos para completar um circuito, sensores de luz infravermelha e outros sensores para comunicação com um LED ou coisa parecida, um interruptor mecânico estabelecido, por exemplo, por um dispositivo eletromecânico, ou qualquer dispositivo adequado para comunicar tal sinal.

Uma modalidade de uma placa de circuito adequada para praticar um modo da invenção é apresentada na FIGURA 10A e na FIGURA 10B. A FIGURA 10A é o anverso da placa de circuito e a FIGURA 10B é o reverso. Um receptáculo (1015) é proporcionado na placa de circuito nesta modalidade particular para incluir um microprocessador. Como descrito com respeito à FIGURA 8, o programa de autenticação do meio da impressora de preferência é oculto de pirataria potencial por ser armazenado em um microprocessador seguro.

Referindo-se a seguir à FIGURA 11, uma modalidade alternativa de um componente de comunicações para montagem em um artigo consumível é apresentada. Uma bobina (1310) é proporcionada para uso em um artigo consumível. Em uma modalidade, o artigo consumível pode ser, por exemplo, um cartucho de fita para uso em um dispositivo hospedeiro. Em outra modalidade, o artigo consumível pode ser, por exemplo, um rolo de filme para uso em uma câmara. A fita ou meio é enrolado ao redor da bobina (1310). Uma flange (1320) está associada com a bobina (1310). A flange (1320) pode estar localizada em uma extremidade da bobina (1310) ou em qualquer localização conveniente associada com a bobina (1310). Na modalidade ilustrada, as tiras condutoras (1330) dispostas na flange em anéis

concêntricos servem como um componente de comunicações para transmitir informação armazenada no artigo consumível para um dispositivo hospedeiro.

Referindo-se a seguir às FIGS. 12A até 12D, são apresentadas várias vistas de uma peça para uso em um artigo consumível. A FIGURA 12A é uma vista ortogonal lateral de uma bobina de enrolar (1405). Um tambor de enrolar (1410) é proporcionado, ao redor do qual o meio pode ser enrolado, tal como fita em um cartucho de impressão para uso em uma impressora ou filme em um rolo de filme para uso em uma câmara. Uma flange (1415) está associada com o tambor de enrolar e pode, por exemplo, estar ligada com uma extremidade do tambor de enrolar. Outras configurações são possíveis e consideradas como sendo equivalentes. Um componente de comunicações pode ser montado na flange para comunicação com um dispositivo hospedeiro tal como uma impressora ou câmara.

A FIGURA 12B é uma vista ortogonal de extremidade a partir da extremidade oposta à flange (1415) no tambor de enrolar (1410). Na modalidade particular apresentada, o tambor de enrolar (1410) é oco, possuindo uma superfície interior (1420) definindo uma cavidade. A FIGURA 12C é uma vista ortogonal de extremidade a partir da extremidade, na qual a flange (1415) é montada. Novamente visível está a superfície interior (1420) definindo a cavidade oca cilíndrica encontrada nesta modalidade particular.

Referindo-se agora à FIGURA 12D, é apresentada uma vista em seção ao longo da linha de corte A-A da vista apresentada na FIGURA 12A. A haste (1405) possui um tambor de enrolar (1410) com uma superfície exterior (1425) ao redor da qual o meio tal como uma fita para uma impressora ou filme para uma câmara pode ser enrolado. Uma superfície interior (1420) nesta modalidade define uma cavidade no interior oco. Uma flange (1415) em uma extremidade pode ser utilizada para montar um componente de comunicações, tal como um transponder RFID. Em uma modalidade alternativa, um primeiro componente de comunicações (1430), tal como um transponder RFID, pode ser montado na superfície interior (1420), o qual comunica-se com o dispositivo hospedeiro por meio de um segundo compo-

nente de comunicação (não apresentado) disposto axialmente dentro da cavidade oca definida pela parede interior da bobina.

Referindo-se agora à FIGURA 13, é revelado um diagrama esquemático de um sistema de autenticação de artigo consumível para autenticar um artigo consumível em um dispositivo hospedeiro. Um artigo consumível (1500) pode incluir, por exemplo, um cartucho de fita de impressão possuindo uma bobina fonte (1505), uma bobina de correção (1510) e um membro de grampo de fixação (1515). O artigo consumível (1500) pode incluir um componente de comunicações (1520, 1535) para transmitir informação para um dispositivo hospedeiro (1550). Em uma modalidade, o componente de comunicações (1520, 1535) pode ser um transponder RFID de baixo custo possuindo duas propriedades específicas. Primeiro, os transponders RFID de baixo custo pode de preferência incluir um número de série único programado de fábrica n (1530), o qual não pode ser alterado por um usuário, ou duplicado por se copiar uma área de dados públicos (1525) do transponder para outro transponder de tipo similar. Assim, cada transponder é numerado de forma única, o que é um requerimento para a maioria dos tipos de transponderes RFID que possuem um protocolo de "anticolisão" permitindo que múltiplos transponderes seja diferenciados quando todos são vistos no campo da antena da leitora RFID.

Em segundo lugar, o tipo de baixo custo dos transponderes RFID de preferência pode ter a habilidade de gravar (ou gravar e travar) de uma vez os valores de dado, *x* e *y*, em uma área de dados públicos (1525) do transponder. O valor *y* nesta modalidade particular é a informação de tipo do meio, desde que nem todos os meios trabalham em todos os tipos de impressora. O valor de dado que não é zero, *x*, para este modo ilustrativo será uma função complicada de *y* e o número de identificação único *n* deste transponder. O valor *x* neste exemplo descrito pode ser programado de fábrica dentro do transponder na hora que o meio é fabricado, ou pelo menos antes que ele deixe o depósito do fabricante.

Também apresentado está um dispositivo hospedeiro (1550), o qual inclui um componente de comunicação (1555, 1560) para ler os valores

de *n*, *x* e *y* armazenados no artigo consumível. Um processador (1565) pode receber a informação armazenada no artigo consumível e pode utilizar uma função de autenticação (1570) *F*(*M*, *Q*, *x*, *y*) disponível para o processador para confirmar se existe uma relação de autenticação entre o código de autenticação *x* e o número de série *n* e o código de tipo do meio *y*. O processador (1565) pode estar remoto do dispositivo hospedeiro e pode comunicar-se com o dispositivo hospedeiro através de um canal de comunicações (1590), tal como uma rede ou um link de telecomunicações.

O artigo consumível de preferência inclui os indicadores (1527) para indicar o número de unidades do meio, tal como painéis de fita, utilizados no artigo consumível. Cada núcleo ou cassete de rolo de fita pode somente ser utilizado uma vez. Outros elementos de memória no transponder mantêm o rastro de utilização do meio e a contagem de meio restante. Os indicadores na memória do transponder podem ser reinicializados e travados à medida que cada parte (tipicamente de 10 até 15%) do meio é utilizada. Pelo fato de somente um máximo de 15% de meio adicionar poder ser recarregado no núcleo ou cassete, isto torna a reutilização dos núcleos ou cassetes parcialmente utilizados economicamente não atrativa.

Referindo-se ainda à FIGURA 13, existe disponível para o processador (1565) uma lista de consumíveis utilizados (1580). Uma lista de "cassetes utilizados" é mantida em cada impressora. Os últimos 512 números de série de cassete n e sua contagem de painel restante são armazenados em cada impressora. Caso um cassete reapareça com um valor de contagem de painel restante mais alto do que armazenado na memória da impressora, a impressora trata o cassete recarregado ou rolo de fita como se ele tivesse uma autenticação inválida e não somente recusa-se a utilizar este meio mas trava seu transponder para a condição de "totalmente utilizado".

A implementação do método e aparelho descritos acima inclui operações repetidas da forma M^N, onde *M* e *N* são ambos números primos. Quando *M* e *N* são ambos números primos, então M^N pode teoricamente centenas de dígitos (ou bits). Para melhor implementar o algoritmo de au-

tenticação descrito acima, foi derivado um método que permite que M^N tanto seja rapidamente avaliado em um pequeno microprocessador como restrinja o número de bits de duas vezes o comprimento de Q.

Como um exemplo, assuma que $M<<Q$ e Q tenha 64 bits, de modo que a multiplicação de 64 bits vezes 64 bits (resultado com 128 bits) é tudo que é requerido. Este exemplo é oferecido a título de ilustração e outras modalidades são possíveis.

Deixe N ser definido com um número binário de 64 bits, o qual é alguma função de *n* e *y*:

$$N(n,y)=c_0 2^0 + c_1 2^1 + ... + c_{63} 2^{63} = \sum_{i=0}^{63} c_i 2^i \qquad \text{Equação 1}$$

Nesta equação cada c_i representa dígitos binários sucessivos. Substituindo-se o dito acima por M^N produz-se:

$$M^N = M^{c_0 2^0 + c_1 2^1 + ... + c_{63} 2^{63}} = M^{\sum_{i=0}^{63} c_i 2^i} \qquad \text{Equação 2}$$

$$M^N = \prod_{i=0}^{63} M^{c_i 2^i}$$

Utilizando esta transformação de M^N, a equação M^N mod Q pode ser avaliada utilizando-se o lema:

$$(axb)\text{mod}c = [(a\text{mod}c)x(b\text{mod}c)]\text{mod}c \qquad \text{Equação 3}$$

Aplicando-se este lema produz-se:

$$M^N \text{mod} Q = \left(\prod_{i=0}^{63} \left(M^{c_i 2^i} \right) \text{mod} Q \right) \text{mod} Q \qquad \text{Equação 4}$$

Deixando

$$Ti = (M^{c_i 2^i}) \text{mod} Q \qquad \text{Equação 5}$$

então

$$M^N \text{mod} Q = \left(\prod_{i=0}^{63} T_i \right) \text{mod} Q \qquad \text{Equação 6}$$

Cada termo T_i pode agora ser estimado utilizando-se o fato de que cada c_i é 0 ou 1.

$$\text{se } c^1 = 0 \text{ então } T_i = M^{c_i 2^i} \text{mod} Q = M^0 \text{mod} Q = 1 \qquad \text{Equação 7}$$

$$\text{se } c^1 = 1 \text{ então } T_i = M^{c_i 2^i} \text{mod} Q = M^{2^i} \text{mod} Q$$

Os até 64 valores de T_i para c_i podem ser anteriormente calculados e armazenados em uma tabela ou podem ser seqüencialmente esti-

mados. Utilizando esta tabela ou estes valores calculados para T_i, o valor de M^N mod Q pode ser estimado progressivamente. Deixe P_i ser o produto parcial em cada estágio, i, a partir de 1 até 63. Calculando-se de uma maneira recursiva em pares:

$$P_1 = (T_0 \times T_1) \text{mod} Q$$

$$P_2 = (P_1 \times T_2) \text{mod} Q$$

. Equação 8

.

.

$$P_i = (P_{i-1} \times T_i) \text{mod} Q$$

até

$$M^N \text{mod} Q = P_{63} = (P_{62} \times T_{63}) \text{mod} Q \quad \text{Equação 9}$$

Utilizando o fato de que quando $c_i = 0$ então $T_i = 1$, corta-se o número da operação de multiplicação de 64x64 bits em 50% em média. De modo a implementar o sistema seguro descrito aqui dentro, entretanto, permanece uma necessidade por uma operação rápida de módulo Q com 64 bits em um número com 128 bits.

Para cada uma das etapas acima, quando $c_i = 1$, uma redução da forma (W mod Q) deve ser executada. Normalmente, isto é feito por uma operação de divisão longa de número inteiro para encontrar o número inteiro restante. No caso aqui, onde o divisor Q é da ordem de 64 bits e o dividendo W é da ordem de 128 bits, um grande número de operações de mudança e de subtração deve ser executado.

Para melhor implementar o sistema de segurança descrito aqui dentro, um método que é aproximadamente 20 vezes mais rápido do que a divisão longa foi desenvolvido. Assuma que Q é escolhido para ser

$$Q = 2^n - k, \text{ onde } K << 2^n \quad \text{Equação 10}$$

Isto inclui os números Primos Mersenner, da forma $2^n - 1$. Mas, se (W div Q) pode ser precisamente estimado (ou seja, o quociente de número inteiro da operação de divisão) então o restante pode ser facilmente encontrado por:

$$Q \text{ mod } Q = W - Q \times (W \text{ div } Q) \quad \text{Equação 11}$$

O quociente de número inteiro da operação de divisão pode ser

estimado como se segue. Primeiro, escreva a equivalência

$$WdivQ = int\left(\frac{W}{2^n - k}\right) \qquad \text{Equação 12}$$

Multiplicando-se tanto o numerador como o denominador do lado direito por 2^{-n} produz-se

$$WdivQ = int\frac{2^{-n}W}{1-2^{-n}k} \qquad \text{Equação 13}$$

Pelo fato de Q tipicamente ser maior (aqui na ordem de n ~ 63 bits), então (2^{-n} k) << 1 e o denominador na Equação 14 pode ser expandido utilizando-se as séries finitas

$$\frac{1}{1-u} = \sum_{i=0}^{\infty} u^i \qquad \text{Equação 14}$$

Substituindo-se a Equação 14 na Equação 13 produz-se:

$$WdivQ = int\left(2^{-n}W\sum_{i=0}^{\infty}(2^{-n}k)^i\right) \qquad \text{Equação 15}$$

Estimando-se os primeiros poucos termos da Equação 15 revela-se que

$$WdivQ \approx int(2^{-n}W + w^{-2n}kW = 2^{-3n}k2W + ...) \qquad \text{Equação 16}$$

Sabendo-se os valores máximos de *n*, *k* e *W*, pode-se estimar os termos da Equação 16 até que o primeiro termo seja encontrado, o qual seja suficientemente pequeno (tal como menos do que ½) de modo que termos adicionais não irão afetar a parte de número inteiro visto que todos os termos subsequentes serão menores. Estes termos que não irão afetar o valor da parte de número inteiro podem então ser de formam segura ignorados na avaliação da Equação 16.

Na prática, *N*, *Q* e *k* podem ser escolhidos de modo que a Equação 16 convirja após somente alguns termos. Este método para calcular *W* modo *Q* prova ser na prática várias vezes mais rápido do que encontrar o mesmo pela divisão longa diretamente.

Como outro exemplo de uma modalidade alternativa, o consumível e o hospedeiro podem ser comunicar por um acoplamento ótico. Outros exemplos incluem contatos elétricos e cabeças de leitura - gravação magnética. Esta invenção não está limitada a qualquer um dos modos de comunicação ilustrativos entre o consumível e o hospedeiro enumerados

nesta descrição e as reivindicações abaixo são pretendidas para cobrir qualquer modo adequado de comunicação.

Ao passo que a invenção foi descrita como sendo de preferência aplicada junto a um sistema de processamento de meio na forma de uma impressora de transferência térmica, a invenção possui aplicabilidade igual junto a impressoras térmicas, tal como descrito nas Patentes dos Estados Unidos 5.266.968 e 5.455.617, aparelhos de fotoprocessamento, tal como descritos na patente dos Estados Unidos 6.106.166, câmaras fotográficas, tal como descrito na patente dos Estados Unidos 6.173.119, câmaras de raio X, tal como descrito na Patente dos Estados Unidos 5.428.659, impressoras a jato de tinta e similares. Ao mesmo tempo que a invenção foi descrita como aplicada junto a um sistema de processamento de meio onde a montagem do meio e o sistema de processamento do meio comunicam-se sem fios, a invenção também é prontamente adaptada para uso em sistemas onde a montagem do meio e o sistema de processamento do meio comunicam-se por uma conexão com fios, como apresentando nas patentes dos Estados Unidos 5.266.968 e 5.455.617.

Modalidades específicas do presente método e aparelho foram descritas para o propósito de ilustrar a maneira na qual a invenção pode ser feita e utilizada. Deve ser entendido que a implementação de outras variações e modificações da invenção e de seus vários aspectos serão aparentes para aqueles versados na técnica e que a invenção não está limitada pelas modalidades específicas descritas. Portanto é contemplado cobrir pela presente invenção qualquer uma e todas as modificações, variações, ou equivalentes que caiam dentro do verdadeiro espírito e escopo dos princípios básicos subjacentes descritos e reivindicados aqui dentro.

REIVINDICAÇÕES

1. Aparelho (100, 850, 910, 1550) configurado para autenticar um artigo (120, 700, 800, 1500) que pode ser instalado ou associado com o aparelho, o aparelho (100, 850, 910, 1550) **caracterizado pelo fato de que** compreende:

uma leitora configurada para ler pelo menos um número de referência único e um número de autenticação armazenados no artigo (120, 700, 800, 1500);

o aparelho (100, 850, 910, 1550) sendo configurado para empregar um algoritmo de criptografia para transformar o pelo menos um número de referência em um número de saída e para comparar o número de saída com o número de autenticação.

2. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** é configurado para autenticar o artigo (120, 700, 800, 1500) se o número de saída corresponder ao número de autenticação.

3. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** o pelo menos um número de referência inclui um número de série de forma única associado com o artigo (120, 700, 800, 1500).

4. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 3, **caracterizado pelo fato de que** o número de série é o número de série de um transponder RFID (130) carregado no artigo (120, 700, 800, 1500).

5. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** pelo menos um número de referência inclui um segundo número de referência.

6. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 5, **caracterizado pelo fato de que** o artigo (120, 700, 800, 1500) compreende uma mídia consumível e onde o segundo número de referência identifica o tipo de mídia.

7. Aparelho (100, 850, 910, 1550), de acordo com a reivindica-

ção 1, **caracterizado pelo fato de que** o aparelho (100, 850, 910, 1550) possui uma memória armazenando um programa de computador incluindo o algoritmo de criptografia.

8. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** o aparelho (100, 850, 910, 1550) compreende uma impressora térmica ou de transferência térmica, onde o artigo (120, 700, 800, 1500) compreende um artigo consumível para a impressora e onde o pelo menos um número de referência e o número de autenticação são armazenados no artigo (120, 700, 800, 1500) em um transponder RFID (130).

9. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 8, **caracterizado pelo fato de que** é configurado para armazenar identificadores dos artigos consumíveis (120, 700, 800, 1500) anteriormente instalados em um aparelho particular e associados com o mesmo os respectivos valores representando a extensão de uso ou a vida útil restante dos artigos consumíveis (120, 700, 800, 1500).

10. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 9, **caracterizado pelo fato de que** é configurado para utilizar os valores para determinar a validade ou a autenticidade dos artigos consumíveis (120, 700, 800, 1500).

11. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** a leitora é um transponder montado no aparelho.

12. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 7, **caracterizado pelo fato de que** o programa de computador que transforma o número de identificação em um número de saída compreende:

um programa de computador preparatório em uma memória do aparelho (100, 850, 910, 1550) configurado para transformar um primeiro número de referência em um número intermediário;

um programa de computador de criptografia em uma memória do aparelho (100, 850, 910, 1550) configurado para criptografar o número intermediário para proporcionar o número de saída; e

onde o número de saída é comparado com o número de autenticação por determinar a autenticidade do artigo (120, 700, 800, 1500) no aparelho (100, 850, 910, 1550).

13. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 12, **caracterizado pelo fato de que** o programa de computador preparatório executa uma transformação um para um de modo que o número intermediário seja igual ao primeiro número de referência.

14. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** a leitora é configurada para ler um número de tipo de mídia armazenado no artigo (120, 700, 800, 1500).

15. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 13, **caracterizado pelo fato de que** o programa preparatório utiliza um número de tipo de mídia como entrada para calcular o número intermediário.

16. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 12, **caracterizado pelo fato de que** o programa de computador de criptografia está contido em uma mídia legível por computador que calcula (a) um segundo número primo elevado à potência do valor intermediário (b) o módulo de um primeiro número primo.

17. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 16, **caracterizado pelo fato de que** o segundo número primo é selecionado de modo que o segundo número primo seja maior do que 0, o segundo número primo não seja igual a 1 e o segundo número primo não seja igual à metade do primeiro número primo menos 1.

18. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 16, **caracterizado pelo fato de que** o programa de computador de criptografia contido em uma mídia legível por computador ainda compreende:

a) um segmento de código de inicialização do programa de computador que:

(i) estabelece um multiplicador igual ao segundo número primo;

(ii) estabelece o produto parcial igual a 1 se o bit menos significativo do número intermediário for igual a 0;

(iii) estabelece o produto parcial igual ao multiplicador módulo do

primeiro número primo se o bit menos significativo do número intermediário for igual a 1;

b) um segmento de código de estimativa de produto parcial do programa de computador que estima o produto parcial repetidamente a partir do bit menos significativo do número intermediário até o bit mais significativo do número intermediário por:

(i) dobrar o multiplicador;

(ii) reinicializar o produto parcial igual ao produto parcial anterior módulo do primeiro número primo se um próximo bit não estimado do número intermediário for igual a 0;

(iii) reinicializar o produto parcial igual (a) ao produto parcial anterior vezes o módulo do multiplicador através do segundo número primo (b) ao módulo do segundo número primo, se o próximo bit não estimado do número intermediário for igual a 1;

c) terminar uma estimativa repetitiva do produto parcial após estimar o produto parcial correspondendo ao bit mais significativo do número intermediário; e

d) emitir o produto parcial final como o número de saída.

19. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 18, **caracterizado pelo fato de que** ainda compreende uma memória para armazenar uma tabela com uma entrada para cada bit do número intermediário, os conteúdos da entrada sendo iguais ao multiplicador correspondendo a este bit, módulo do primeiro número primo.

20. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** produz uma pluralidade de números de saída e onde o artigo (120, 700, 800, 1500) é autenticado se uma da pluralidade de números de saída corresponder ao número de autenticação.

21. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** ainda inclui um contador no artigo (120, 700, 800, 1500), o contador configurado para ser lido pelo aparelho (100, 850, 910, 1550) onde a leitora lê um valor de utilização do artigo (120, 700, 800, 1500) no contador, o valor de utilização do artigo (120, 700, 800,

1500) refletindo uma extensão de utilização ou a vida útil restante do artigo (120, 700, 800, 1500).

22. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 21, **caracterizado pelo fato de que** é configurado para determinar se um artigo (120, 700, 800, 1500) instalado no aparelho (100, 850, 910, 1550) é válido por comparar seu valor de utilização com um valor de utilização predeterminado.

23. Aparelho (100, 850, 910, 1550), de acordo com a reivindicação 1, **caracterizado pelo fato de que** ainda inclui:

uma estrutura de memória contendo números de identificação correspondendo a uma pluralidade de artigos (120, 700, 800, 1500) anteriormente utilizados em um aparelho particular; e

cada um dos números de identificação possuindo associado com o mesmo um último valor de utilização do artigo (120, 700, 800, 1500) lido de cada artigo (120, 700, 800, 1500) utilizado no aparelho (100, 850, 910, 1550), e onde o aparelho (100, 850, 910, 1550) determina se um artigo (120, 700, 800, 1500) instalado no aparelho (100, 850, 910, 1550) é válido se seu valor de utilização de artigo (120, 700, 800, 1500) for menor do que o último valor de utilização de artigo (120, 700, 800, 1500) lido para o número de identificação correspondente na tabela.

24. Artigo (120, 700, 800, 1500) adaptado para ser autenticado por um aparelho hospedeiro (100, 850, 910, 1550), **caracterizado pelo fato de que** o artigo (120, 700, 800, 1500) armazena pelo menos um número de referência e um número de autenticação, o número de autenticação representando uma transformação por criptografia do pelo menos um número de referência.

25. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 24, **caracterizado pelo fato de que** o pelo menos um número de referência inclui um número de série de forma única associado com o artigo (120, 700, 800, 1500).

26. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 25, **caracterizado pelo fato de que** o número de série é o número de série

de um transponder RFID (130) carregado no artigo (120, 700, 800, 1500).

27. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 26, **caracterizado pelo fato de que** o pelo menos um número de referência inclui um segundo número de referência.

28. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 27, **caracterizado pelo fato de que** o artigo (120, 700, 800, 1500) compreende uma mídia consumível e onde o segundo número de referência identifica o tipo de mídia.

29. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 24, **caracterizado pelo fato de que** o aparelho (100, 850, 910, 1550) possui uma memória armazenando um programa de computador incluindo o algoritmo de criptografia.

30. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 24, **caracterizado pelo fato de que** o aparelho (100, 850, 910, 1550) compreende uma impressora térmica ou de transferência térmica, onde o artigo (120, 700, 800, 1500) compreende um artigo consumível (120, 700, 800, 1500) para a impressora, e onde o pelo menos um número de referência e o número de autenticação são armazenados no artigo (120, 700, 800, 1500) em um transponder RFID (130).

31. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 30, **caracterizado pelo fato de que** é configurado para armazenar identificadores dos artigos consumíveis (120, 700, 800, 1500) anteriormente instalados em um aparelho particular e para armazenar em associação com os mesmos os respectivos valores representando a extensão de uso ou a vida útil restante dos artigos consumíveis (120, 700, 800, 1500).

32. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 22, **caracterizado pelo fato de que** o número predeterminado é um número de série único instalado na fábrica.

33. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 24, **caracterizado pelo fato de que** o número de autenticação é calculado por:

proporcionar um primeiro número primo, Q;

proporcionar um segundo número primo, M;

o segundo número primo sendo um elemento primitivo do primo do Galois Field do primeiro número primo; e

calcular o número de saída de acordo com a fórmula:

número de saída = M^N MOD Q, onde N é um primeiro número de referência predeterminado.

34. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 33, **caracterizado pelo fato de que** o segundo número primo é selecionado de modo que o segundo número primo seja maior do que 0, o segundo número primo não seja igual a 1 e o segundo número primo não seja igual à metade do primeiro número primo menos 1.

35. Artigo (120, 700, 800, 1500), de acordo com a reivindicação 33, **caracterizado pelo fato de que** a etapa de determinar o número de saída ainda compreende as etapas de:

a) inicializar um produto parcial por:

estabelecer um multiplicador igual ao segundo número primo;

estabelecer o produto parcial igual a 1 se o bit menos significativo do primeiro número de referência predeterminado for igual a 0;

estabelecer o produto parcial igual ao multiplicador módulo do primeiro número primo se o bit menos significativo do primeiro número de referência predeterminado for igual a 1;

b) estimar o produto parcial repetidamente a partir do bit menos significativo do primeiro número de referência predeterminado até o bit mais significativo do primeiro número de referência predeterminado por:

dobrar o multiplicador;

reinicializar o produto parcial igual ao produto parcial anterior módulo do primeiro número primo se um próximo bit não estimado do primeiro número de referência predeterminado for igual a 0;

reinicializar o produto parcial igual (a) ao produto parcial anterior vezes o módulo do multiplicador através do segundo número primo (b) ao módulo do segundo número primo, se o dito próximo bit não estimado do primeiro número de referência predeterminado for igual a 1; e

c) terminar a estimativa repetitiva do produto parcial após estimar o produto parcial para o bit mais significativo do primeiro número de referência predeterminado.

36. Sistema de processamento de impressora de transferência térmica, térmica ou outra, ou câmera fotográfica ou de raio X, ou de outra mídia adaptado para identificar um conjunto de mídia falsificada, **caracterizado pelo fato de que** inclui um programa configurado para executar um algoritmo de criptografia empregado para validar um conjunto de mídia.

37. Sistema, de acordo com a reivindicação 36, **caracterizado pelo fato de que** o algoritmo é executado em um microprocessador seguro.

38. Sistema, de acordo com a reivindicação 36, **caracterizado pelo fato de que** o sistema inclui um processador de mídia (865, 1565) e onde o programa reside no processador de mídia (865, 1565).

39. Sistema, de acordo com a reivindicação 36, **caracterizado pelo fato de que** o sistema inclui um processador de mídia (865, 1565) e uma estação de processamento remota, e onde o programa reside na estação de processamento remota.

40. Sistema, de acordo com a reivindicação 36, **caracterizado pelo fato de que** o algoritmo de criptografia opera sobre os dados armazenados no conjunto de mídia.

41. Sistema, de acordo com a reivindicação 40, **caracterizado pelo fato de que** os dados incluem dados de referência e dados criptografados derivados a partir dos dados de referência.

42. Sistema, de acordo com a reivindicação 41, **caracterizado pelo fato de que** os dados criptografados são desenvolvidos empregando-se o algoritmo de criptografia.

43. Sistema, de acordo com a reivindicação 36, **caracterizado pelo fato de que** o algoritmo de criptografia compreende uma função unidirecional.

44. Sistema, de acordo com a reivindicação 43, **caracterizado pelo fato de que** a função unidirecional utiliza a aritmética de módulo em um Galois Field.

FIG. 1A

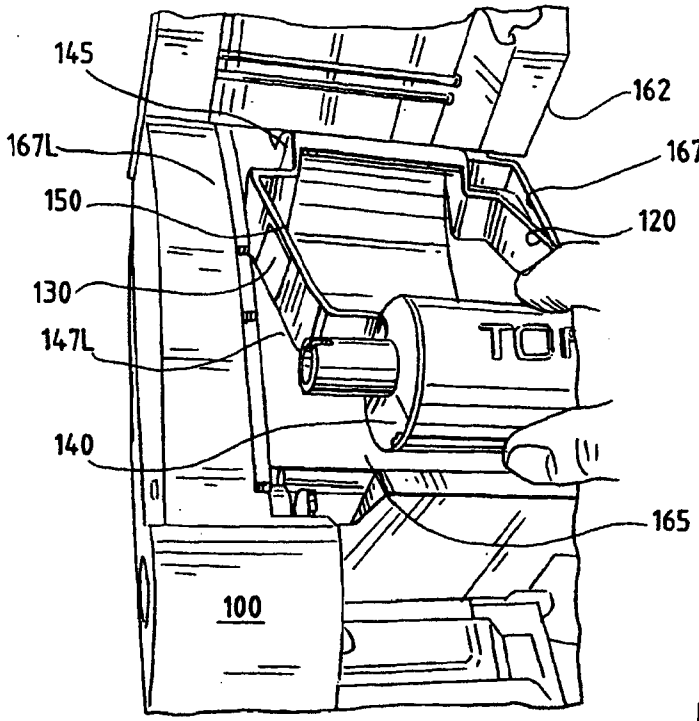

145
162
167L
167R
150
120
130
TOP
147L
140
165
100

FIG. 1B

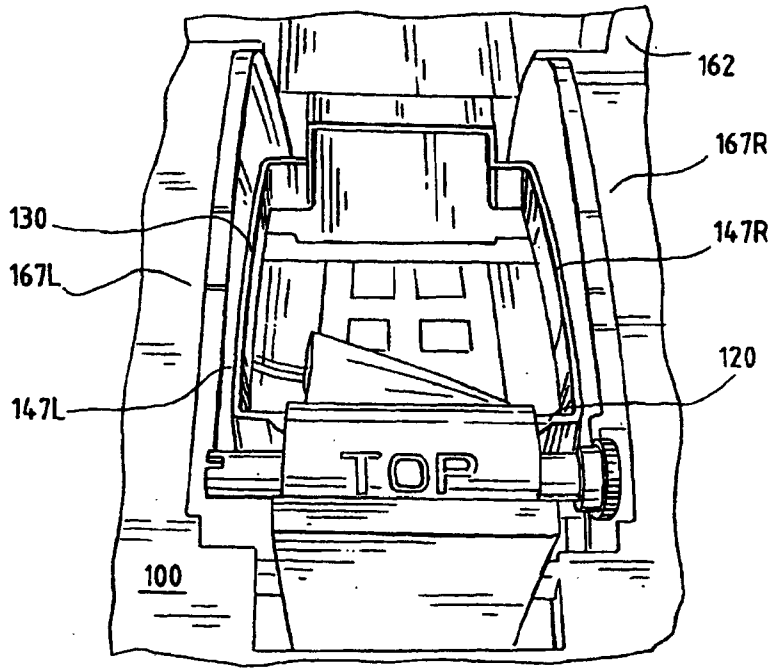

162
167R
130
147R
167L
120
147L
TOP
100

FIG. 2A

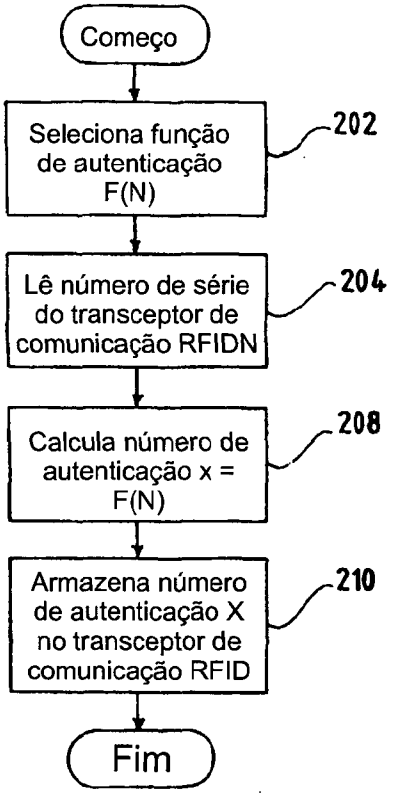

Começo
Seleciona função de autenticação F(N)
202
Lê número de série do transceptor de comunicação RFIDN
204
Calcula número de autenticação x = F(N)
208
Armazena número de autenticação X no transceptor de comunicação RFID
210
Fim

FIG. 2B

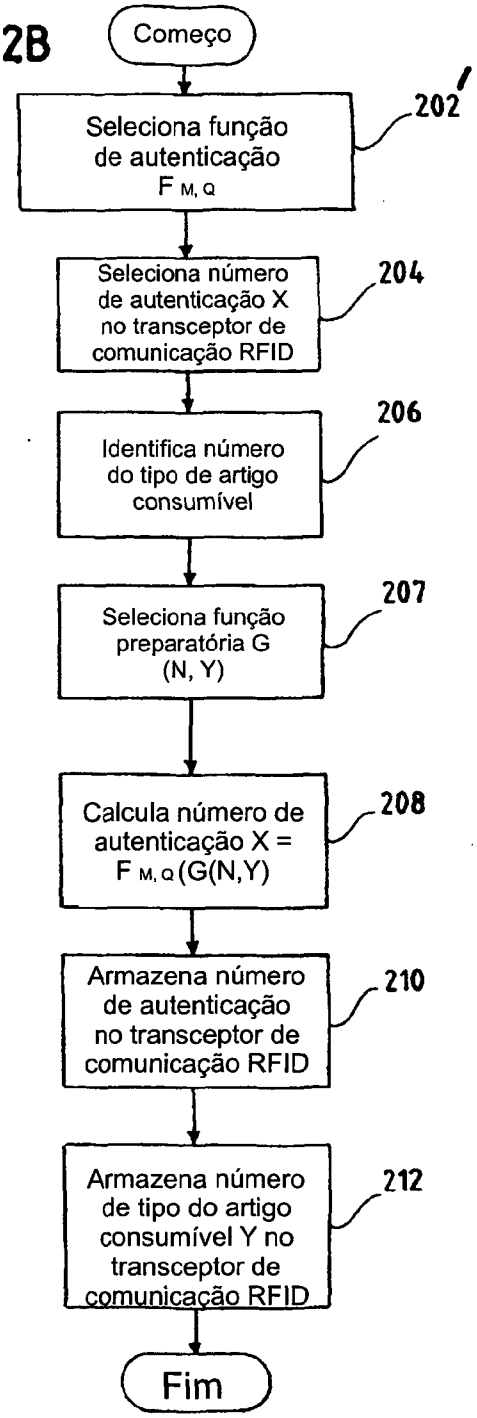

Começo
Seleciona função de autenticação F M, Q
202'
Seleciona número de autenticação X no transceptor de comunicação RFID
204
Identifica número do tipo de artigo consumível
206
Seleciona função preparatória G (N, Y)
207
Calcula número de autenticação X = F M, Q (G(N,Y)
208
Armazena número de autenticação no transceptor de comunicação RFID
210
Armazena número de tipo do artigo consumível Y no transceptor de comunicação RFID
212
Fim

FIG. 3A

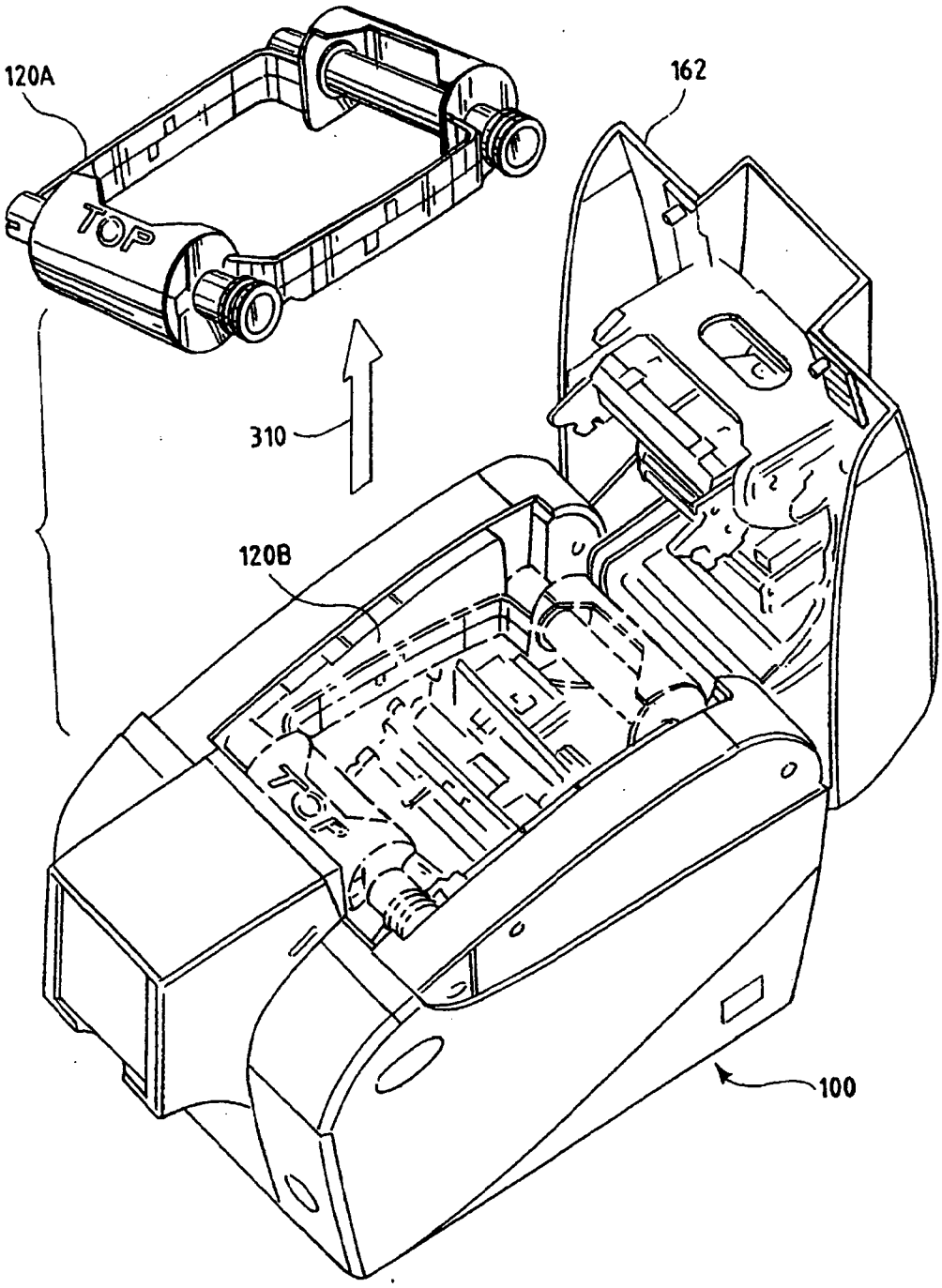


FIG. 3B

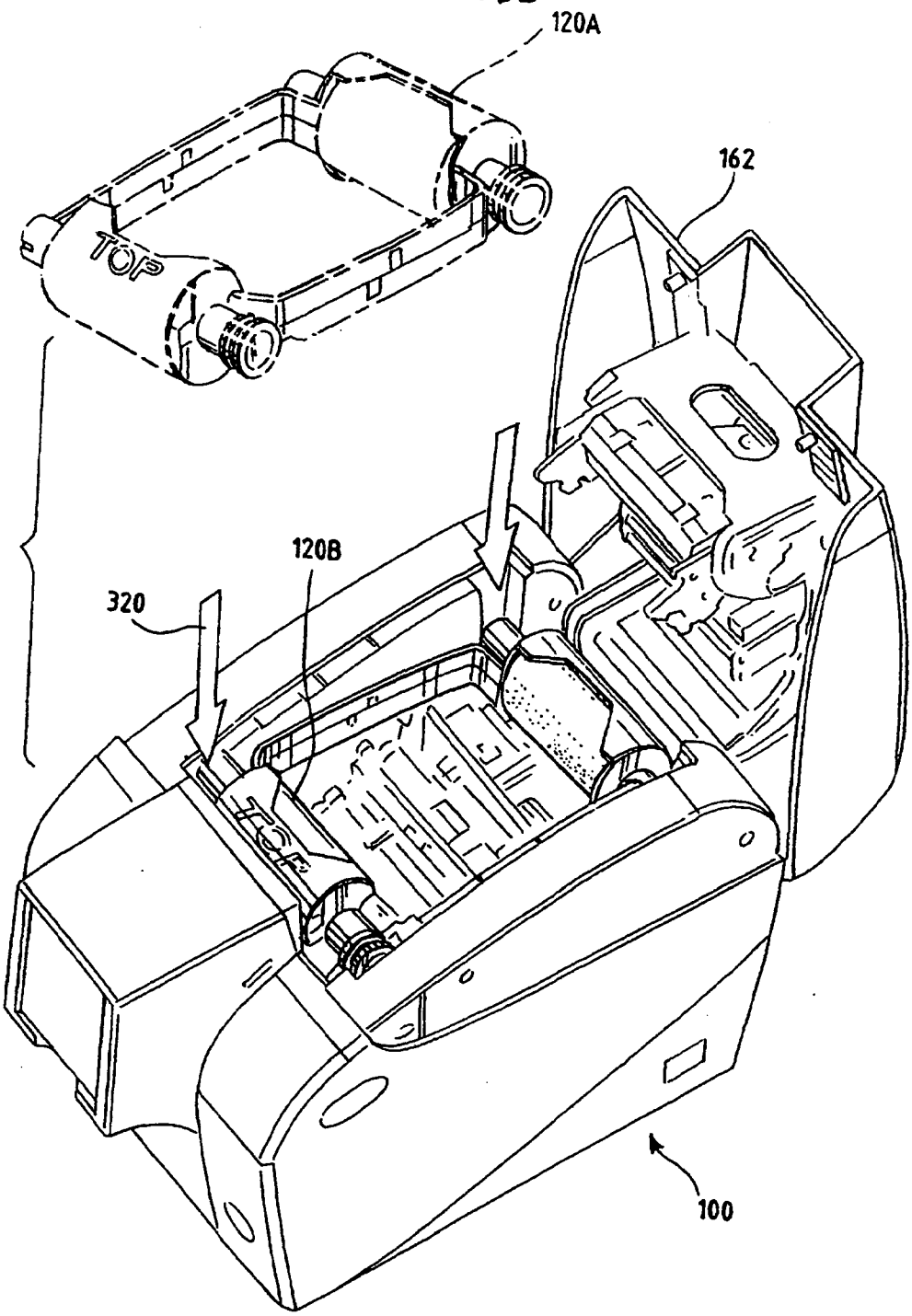


FIG. 4

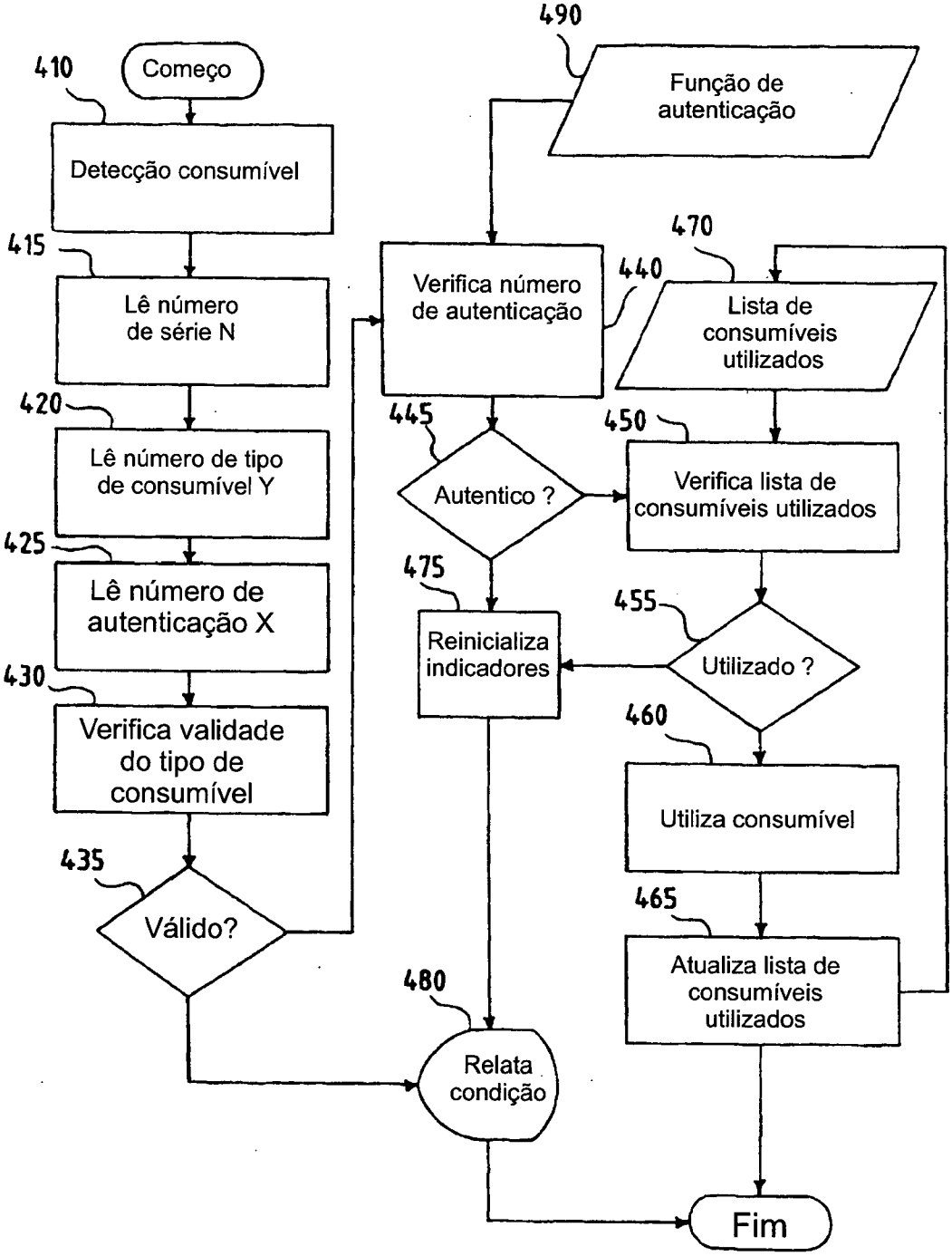

490
Função de autenticação
410
Começo
Detecção consumível
415
Lê número de série N
420
Lê número de tipo de consumível Y
425
Lê número de autenticação X
430
Verifica validade do tipo de consumível
435
Válido?
Verifica número de autenticação
440
470
Lista de consumíveis utilizados
445
Autentico ?
450
Verifica lista de consumíveis utilizados
475
Reinicializa indicadores
455
Utilizado ?
460
Utiliza consumível
465
Atualiza lista de consumíveis utilizados
480
Relata condição
Fim

FIG. 5

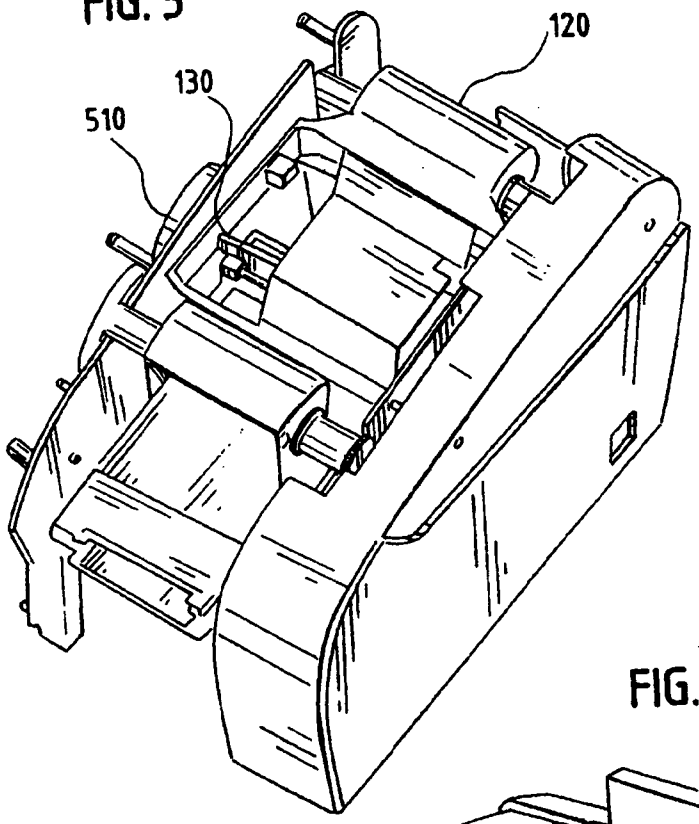


FIG. 6

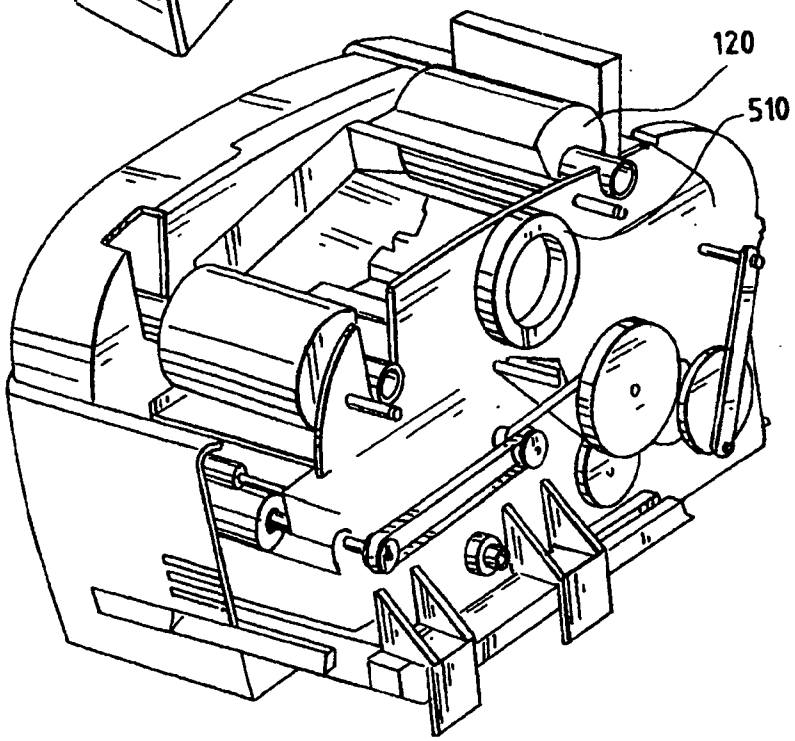


FIG. 7A

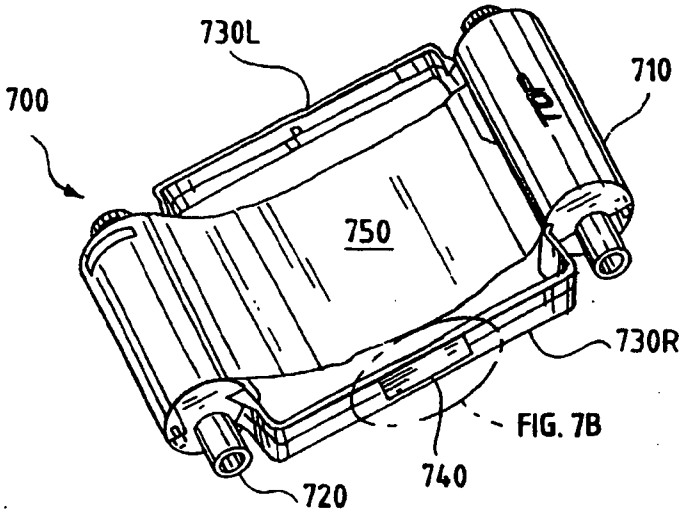


FIG. 7B

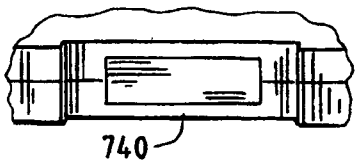


FIG. 7C

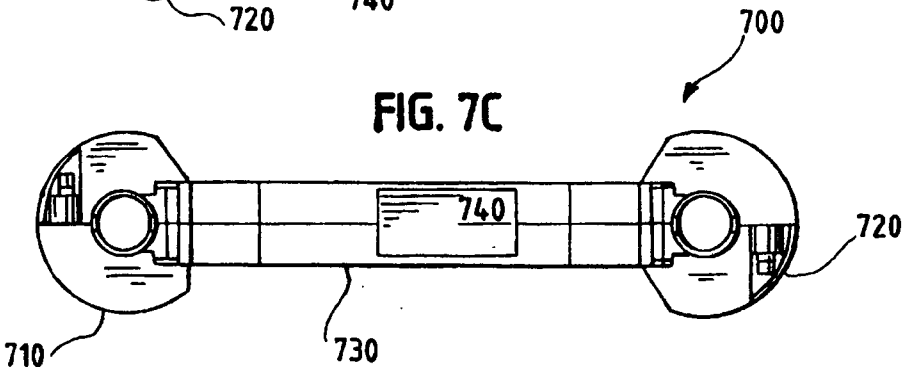


FIG. 7D

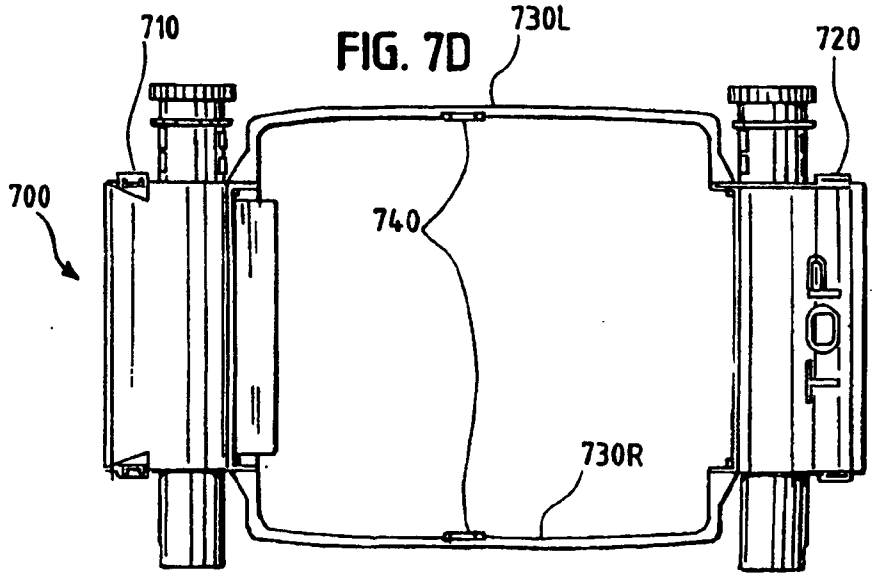


FIG. 8

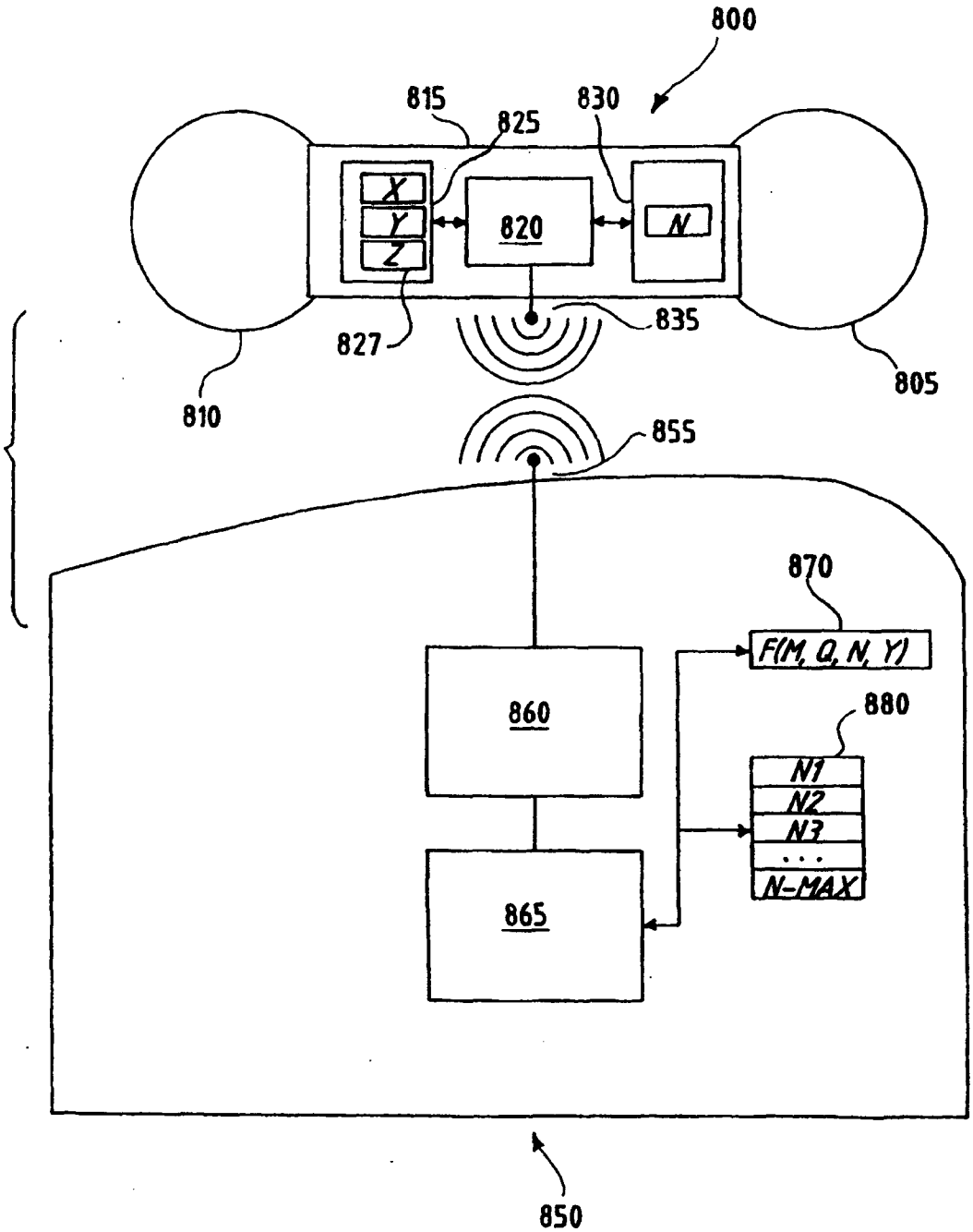

800
815
825
830
X
Y
Z
820
N
827
835
805
810
855
870
F(M, Q, N, Y)
860
880
N1
N2
N3
...
N-MAX
865
850

FIG. 9

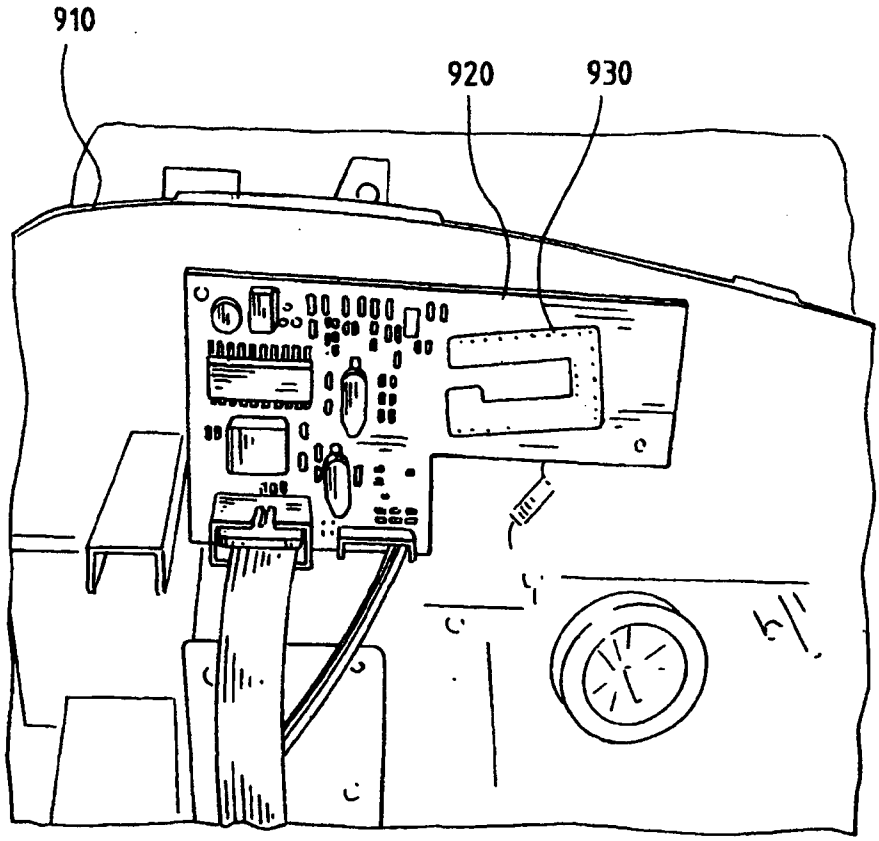


FIG. 10A

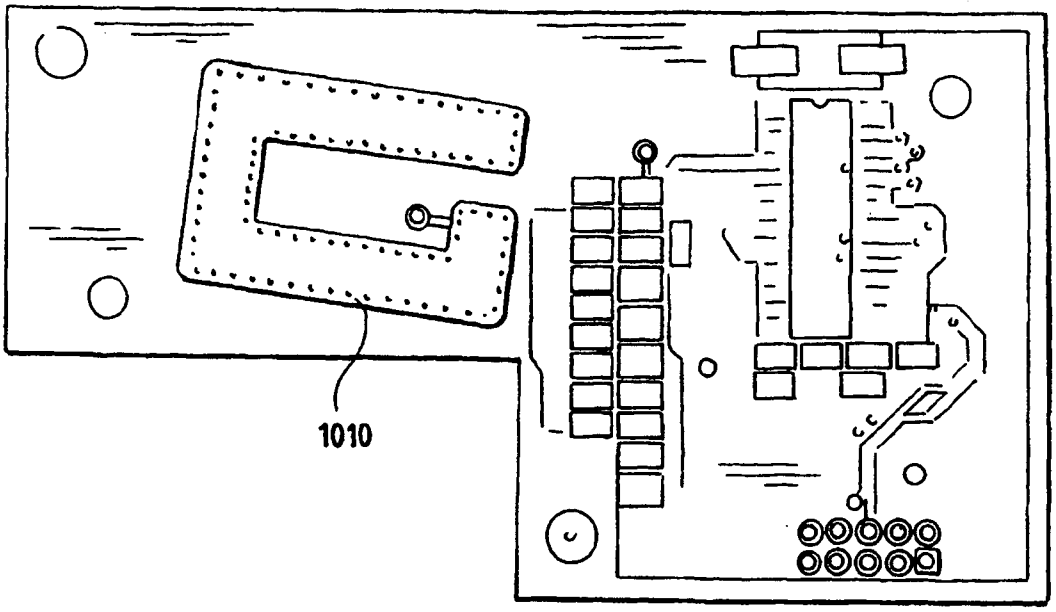


FIG. 10B

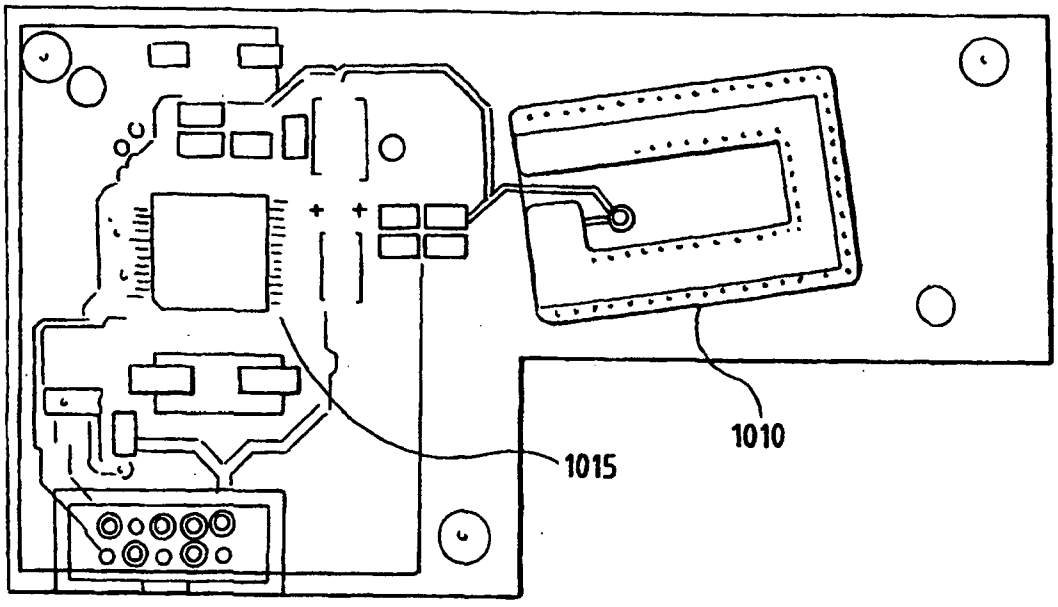


FIG. 11

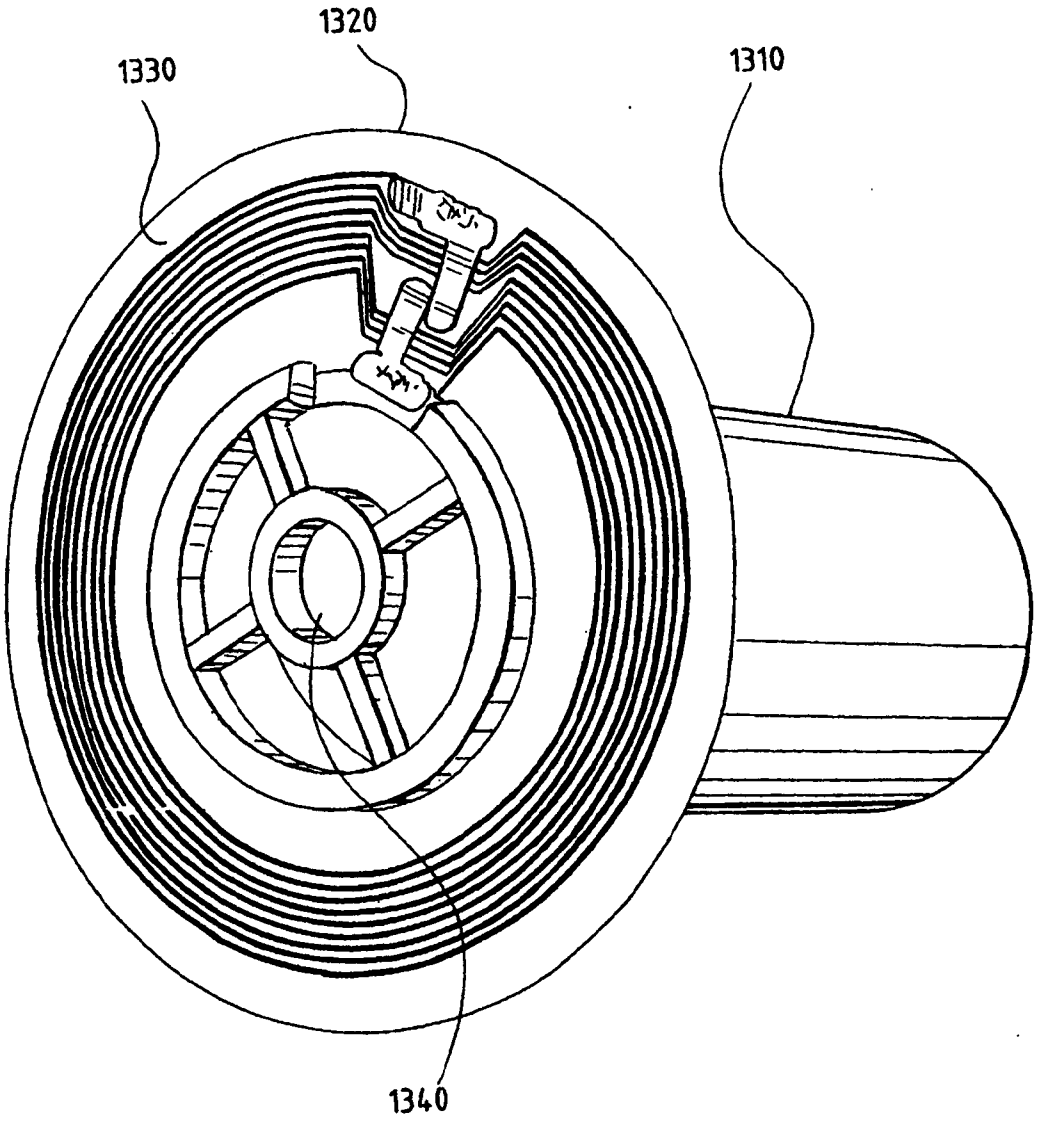


FIG. 12A

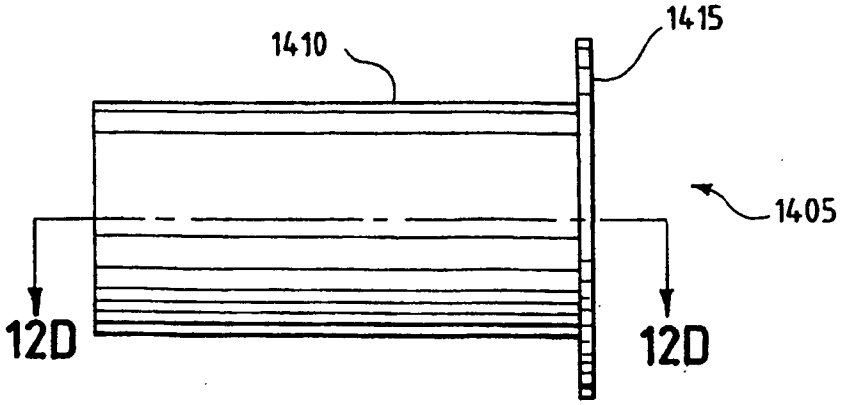


FIG. 12B

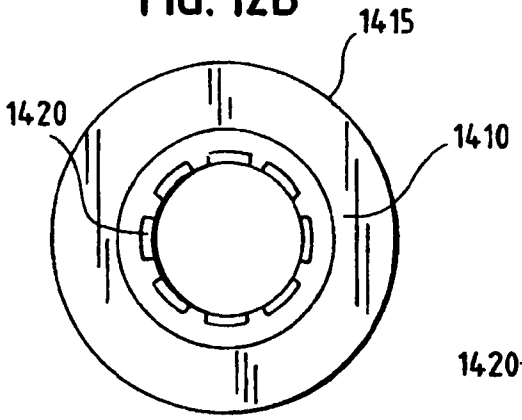


FIG. 12C

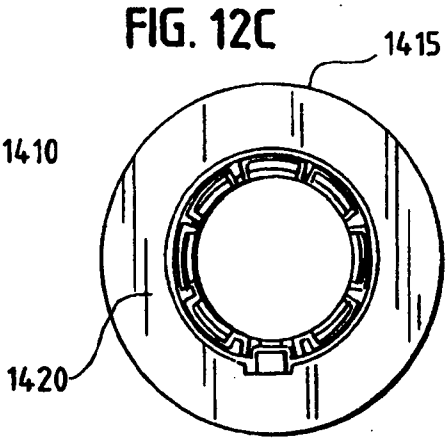


FIG. 12D

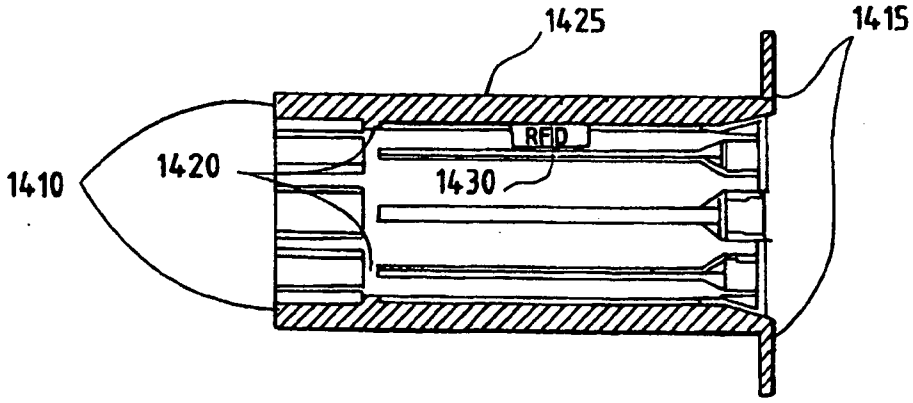
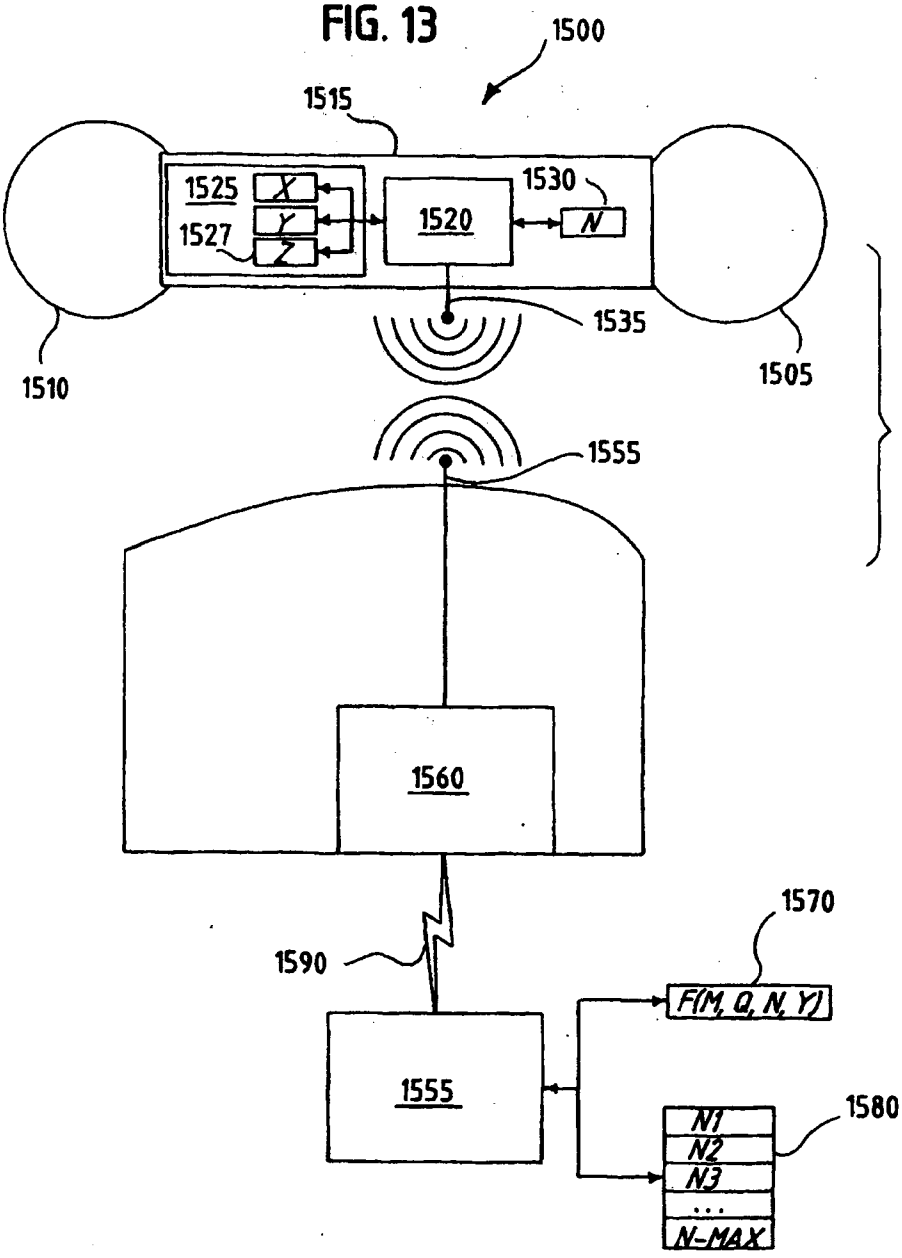


FIG. 13


1500
1515
1525
X
Y
Z
1527
1520
1530
N
1535
1510
1505
1555
1560
1570
1590
F(M, Q, N, Y)
1555
1580
N1
N2
N3
...
N-MAX

RESUMO

Patente de Invenção: **"APARELHO DE AUTENTICAÇÃO DE ARTIGO, ARTIGO PARA AUTENTICAÇÃO E SISTEMA DE PROCESSAMENTO".**

A presente invenção refere-se a um aparelho configurado para autenticar um artigo que pode ser instalado ou estar associado com o aparelho, o aparelho compreendendo uma leitora configurada para ler pelo menos um número de referência único e um número de autenticação armazenados no artigo, o aparelho sendo configurado para empregar um algoritmo de criptografia para transformar o pelo menos um número de referência em um número de saída e comparar o número de saída com o número de autenticação.