



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

(21) **PI 1002245-7 A2**

(22) Data de Depósito: 23/07/2010
(43) Data da Publicação: 05/06/2012
(RPI 2161)



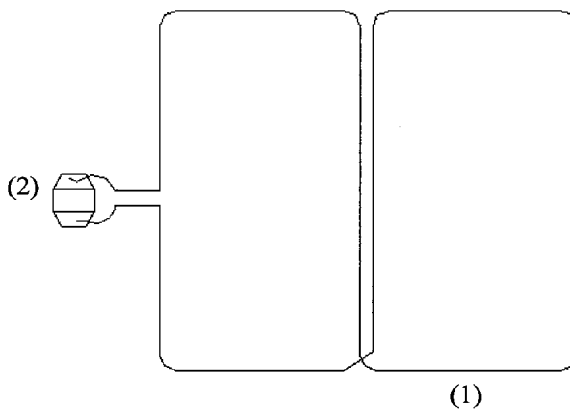
(51) *Int.Cl.:*
H01Q 1/40
H01Q 3/12
G08B 13/14

(54) Título: ANTENA AUTO-PROTEGIDA COM APLICAÇÃO EM (MAS NÃO LIMITADA A) DOCUMENTOS ELETRÔNICOS DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (RFID) INTRINSECAMENTE PROTEGIDOS CONTRA ATIVAÇÃO CLANDESTINA

(73) Titular(es): Jorge de Albuquerque Lambert

(72) Inventor(es): Jorge de Albuquerque Lambert

(57) Resumo: ANTENA AUTO-PROTEGIDA COM APLICAÇÃO EM (MAS NÃO LIMITADA A) DOCUMENTOS ELETRÔNICOS DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (RFID) INTRINSECAMENTE PROTEGIDOS CONTRA ATIVAÇÃO CLANDESTINA A presente invenção é um novo tipo de antena, auto-protegida contra excitação e comunicação não autorizada, sem partes móveis, de baixíssimo custo, completamente embutível em um cartão de polímero típico, para aplicações em (mas não limitada a) cartões inteligentes comerciais e documentos eletrônicos de identificação operáveis sem contato (RFID), capaz de condicionar o funcionamento do dispositivo ao posicionamento da antena em região específica, muito próxima ao terminal leitor autorizado, provendo assim proteção intrínseca à privacidade e à integridade dos dados armazenados na memória. A antena e uma concretização de documento intrinsecamente protegido contra ativação clandestina aqui propostas são compatíveis com os terminais leitores atualmente utilizados, mediante uma adaptação de custo desprezível em relação ao valor dos terminais leitores.



“ANTENA AUTO-PROTEGIDA COM APLICAÇÃO EM (MAS NÃO LIMITADA A) DOCUMENTOS ELETRÔNICOS DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (RFID) INTRINSECAMENTE PROTEGIDOS CONTRA ATIVAÇÃO CLANDESTINA”

5

A presente invenção é um novo tipo de antena, auto-protegida contra excitação e comunicação não autorizada, sem partes móveis, de baixíssimo custo, para aplicações em (mas não limitada a) cartões inteligentes comerciais e documentos eletrônicos de identificação operáveis sem contato (RFID), capaz de condicionar o funcionamento do dispositivo ao posicionamento da antena em região específica, muito próxima ao terminal leitor autorizado, provendo assim proteção intrínseca à privacidade e à integridade dos dados armazenados na memória.

15

As vantagens da utilização dos Cartões de Identificação por Rádio-Frequência são amplamente conhecidas. A principal delas é a diminuição no tempo gasto nas operações. Entretanto, uma vez que a alimentação elétrica e a comunicação com este tipo de dispositivo muitas vezes se dá sem contato, quando os dados armazenados na memória do dispositivo são sensíveis, a principal desvantagem desse tipo de tecnologia é a vulnerabilidade ao acesso aos dados por pessoa mal intencionada (ataques tipo *skimming*). Nesse tipo de ataque, alguém não autorizado utilizará um terminal de leitura clandestino, normalmente dissimulado, para alimentar e estabelecer uma comunicação com o circuito do dispositivo RFID, acessando os dados nele armazenados, atentando contra a privacidade e possivelmente contra a integridade dos mesmos. O comprometimento da privacidade é particularmente grave quando se trata de cartões de identificação, documentos de viagem, ou cartões bancários em que há dados pessoais, biométricos e cadastrais do usuário armazenados no dispositivo. Para evitar os ataques tipo mencionado, diversos dispositivos extrínsecos tem sido desenvolvidos e utilizados com mais ou menos sucesso. Até o presente

momento, os dispositivos que melhor combinam simplicidade e eficiência são aqueles que blindam ou atenuam a passagem do campo eletromagnético, impedindo a alimentação do circuito existente no chip e o estabelecimento de uma comunicação com o terminal não autorizado. Estes dispositivos utilizam-se

5 do conceito de gaiola de Faraday, e caracterizam-se essencialmente pela a interposição de uma superfície eletricamente condutora - folha de alumínio, por exemplo - no caminho que as linhas de fluxo magnético teriam que percorrer para induzir tensão significativa na antena. Para os documentos eletrônicos de viagem - passaportes eletrônicos ou outros documentos que possuam mais de

10 uma página - a utilização de escudos eletromagnéticos tipo gaiola de Faraday não traz maiores inconvenientes, uma vez que a superfície condutiva (ou bobina) pode ser acondicionada em uma página ou contracapa do documento, naturalmente impedindo o acesso aos dados quando o mesmo estiver fechado e permitindo a leitura quando está aberto, no equipamento leitor autorizado.

15 Quando se tratam de cartões RFID inteligentes constituídos de apenas uma folha, normalmente de polímero não dobrável, formato típico dos cartões de crédito, de identidade e bancários, a situação é muito diferente. Não há no estado da técnica nenhuma solução para o problema que torne o dispositivo intrinsecamente protegido. Soluções extrínsecas foram propostas, envolvendo, por exemplo, um

20 circuito de bloqueio externo, a ser justaposto ao cartão RFID e retirado apenas no momento da leitura (patente publicada US2007/0096924).

Outros dispositivos e proteções para cartões inteligentes com RFID, visando ao bloqueio de ondas eletromagnéticas por gaiola de Faraday, estão sendo divulgados e vendidos em diversos sítios na rede mundial de computadores,

25 evidenciando serem estas soluções as de melhor relação benefício/custo disponíveis (exemplo: www.smartcardfocus.com, *RFID blocking*, acessado em 22 de Julho de 2010). De fato, no atual estado da técnica, a solução mais simples e popular encontrada para o problema do acesso não autorizado aos dados sensíveis em cartões inteligentes com RFID é o uso de envelopes de papel

condutivo (escudos eletromagnéticos tipo gaiolas de Faraday) para armazenar os cartões quando os mesmos não estão em uso.

5 A utilização de dispositivos de proteção extrínsecos ao documento propriamente dito traz, pelo menos, quatro desvantagens:

- 1) a proteção pode ser perdida ou negligenciada;
- 2) a proteção pode se desgastar ou danificar, sobretudo em documentos muito manuseados, perdendo a sua eficácia;
- 3) é um custo adicional em relação ao cartão RFID propriamente dito;
- 10 4) é mais um item para ser levado pelo usuário.

As duas primeiras desvantagens citadas são as mais importantes, uma vez que podem comprometer a privacidade e a segurança do usuário.

15 No estado da técnica, todos os dispositivos encontrados apresentam a deficiência de serem externos ao circuito de RFID e a desvantagem de serem operacionalmente inconvenientes e muito mais dispendiosos que a solução viabilizada pela invenção ora apresentada.

20 Qualquer circuito eletrônico tem seu funcionamento condicionado à sua alimentação, que deverá fornecer a potência (tensão e corrente) demandada pelo circuito em funcionamento. O valor de projeto para a potência costuma ser referido como *potência nominal*. Entretanto, a potência efetivamente demandada por um circuito pode ser menor do que a sua potência nominal, sobretudo se o circuito ou as funções que realiza forem configuráveis, como é o caso dos microprocessadores, incluindo os documentos eletrônicos dotados de RFID.

25

Seja o circuito de RFID definido como o conjunto formado pelo circuito integrado (chip) e a sua antena. Note-se que, dependendo da distância de operação, da frequência e da geometria da antena do RFID, seu

funcionamento se assemelha a um acoplador magnético. Basicamente, a fonte de alimentação deve ser capaz de manter a tensão elétrica em seus terminais acima de um valor mínimo que garante o suprimento da corrente elétrica demandada pelo circuito nas condições mais críticas, ou seja, quando o circuito funciona na plenitude das suas possibilidades. Esse valor de tensão, que garante o funcionamento do circuito, fica aqui definido como *tensão de funcionamento* do circuito. Entretanto, sobretudo se o circuito for utilizado em condição sub-crítica (de ambiente ou solicitação), é normal que o seu funcionamento possa ocorrer, ainda que de forma não confiável, mesmo quando alimentado com tensões inferiores à sua tensão de funcionamento. Logo, para garantir que um circuito não funcionará por falta de alimentação, é necessário definir um valor de tensão abaixo da qual não é possível o funcionamento do circuito, mesmo nas condições menos exigentes. Esse valor de tensão fica definido no contexto desse documento como *tensão de não-funcionamento* do circuito.

O conceito de antena auto-protégida aqui proposto se caracteriza pelo fato de que, exceto em condições específicas a serem atendidas no leitor autorizado, pela própria geometria do(s) condutor(es), existe pelo menos uma região do(s) mesmo(s) que contribui negativamente para a magnitude da tensão elétrica resultante em seus terminais. Essa região da antena funcionará como *região protetora*. A geometria da antena auto-protégida é pensada de tal forma que a alimentação do circuito RFID só é possível mediante exposição parcial e adequada da antena a um fluxo magnético variável suficientemente homogêneo ou mediante a exposição da antena a um campo eletromagnético cujas linhas de fluxo magnético atravessem em sentido conveniente a(s) área(s) enlaçada pelas espiras. Pela geometria e dimensões da antena, definidas em projeto específico, qualquer destas duas condições de funcionamento da antena só podem ocorrer nas proximidades (distância dependente do projeto) de um local de leitura específico, onde o dispositivo RFID dificilmente seria colocado sem o conhecimento do proprietário. Esta

condição inviabiliza o acesso ao conteúdo do documento por um terminal leitor clandestino dissimulado.

O terminal de leitura autorizado a ler o dispositivo RFID auto-protegido deverá prover:

- 5 1) uma blindagem eletromagnética parcial da antena, pela interposição de uma superfície condutora (máscara de metal) no caminho das linhas de fluxo que atravessariam a região protetora, anulando a tensão induzida no(s) segmento(s) de antena que contribuiria(m) negativamente para a alimentação do circuito, ou
- 10 2) uma configuração de linhas de fluxo magnético capaz de induzir tensões de mesma polaridade em uma quantidade suficiente de espiras, idealmente em todo o conjunto.

O custo de um cartão RFID auto-protegido pelo invento deverá ser essencialmente o mesmo de um cartão no estado da técnica e custo da
15 adaptação dos terminais leitores para a leitura de tais cartões deve ser desprezível em relação ao preço do terminal de leitura.

A invenção é descrita a seguir com relação ao conceito básico nela envolvido, com referências a concretizações típicas da mesma e também
20 com referência às ilustrações apresentadas, nas quais:

A **figura 1-A** apresenta a vista de uma antena auto-protegida elementar, caracterizada por um condutor elétrico (1) cujo percurso descreve duas espiras reversas situadas, à esquerda e à direita, no plano do papel, e cujos
25 terminais encontram-se ligados a um chip de RFID (2).

A **figura 1-B** apresenta, em perspectiva, a mesma antena auto-protegida elementar ilustrada na figura 1-A.

A **figura 1-C** apresenta, em vista superior, a antena auto-protegida (1) sendo atravessada por um campo magnético uniforme (B), cuja

orientação é no sentido descendente (entrando no papel), ortogonal ao plano das espiras.

A **figura 1-D** apresenta, em perspectiva, a antena auto-protegida (1) sendo atravessada por um campo magnético uniforme (B), cuja
5 orientação é no sentido descendente e ortogonal ao plano das espiras (mesma situação ilustrada na figura 1-C).

A **figura 1-E** apresenta, em vista superior, a antena auto-protegida (1) sendo parcialmente atravessada por um campo magnético uniforme (B), cuja orientação é descendente e ortogonal ao plano das espiras. A exposição
10 parcial da antena ocorre graças a uma máscara em forma de folha metálica (3) que obstrui eletromagneticamente a passagem do fluxo magnético B pelo interior da espira da direita.

A **figura 1-F** apresenta, em perspectiva, a antena auto-protegida (1) sendo parcialmente atravessada por um campo magnético uniforme
15 (B), cuja orientação é descendente e ortogonal ao plano das espiras. A exposição parcial da antena ocorre graças a uma máscara em forma de folha metálica (3) que obstrui eletromagneticamente a passagem do fluxo magnético B pelo interior da espira da direita (mesma situação ilustrada na figura 1-E).

A **figura 1-G** apresenta, em vista superior, a antena auto-protegida (1) sendo atravessada por um campo magnético (B), cuja orientação é
20 ascendente na espira da esquerda (saindo do papel) e descendente na espira da direita, situação em que as tensões induzidas em cada espira se somam construtivamente nos terminais do chip RFID (2).

A **figura 1-H** apresenta, em perspectiva, a antena auto-protegida (1) sendo atravessada por um campo magnético (B), cuja orientação é
25 ascendente na espira da esquerda e descendente na espira da direita, situação em que as tensões induzidas em cada espira se somam construtivamente nos terminais do chip (mesma situação ilustrada na figura 1-G).

A **figura 1-I** apresenta, em vista superior, a antena auto-protegida (1) sendo atravessada por um campo magnético (B), cuja orientação é

descendente na espira da direita (entrando no papel) e ascendente na espira da esquerda. A figura também apresenta uma terceira espira (4), ativa, que estaria instalada em um equipamento leitor (5) autorizado a ativar e ler o chip.

5 A **figura 1-J** apresenta, em perspectiva, a antena auto-protegida (1) sendo atravessada por um campo magnético (B), cuja orientação é descendente na espira da direita e ascendente na espira da esquerda. A figura também apresenta uma terceira espira (4), que estaria instalada em um equipamento leitor (5) autorizado a ativar e ler o chip (mesma situação ilustrada na figura 1-I).

10 A **figura 2-A** apresenta a vista superior de um cartão de polímero (6), dotado de dispositivo de RFID, com antena auto-protegida (7), formada por duas bobinas reversas, uma à esquerda e outra à direita, cada uma com um percurso de duas voltas concêntricas, tudo embutido no cartão (*cartão conceitual* em relação à invenção apresentada neste documento, formado por
15 chip, antena e suporte em polímero).

A **figura 2-B** apresenta a vista frontal do mesmo cartão conceitual ilustrado na figura 2-A, evidenciando o embutimento total do circuito de RFID (chip e antena) no polímero.

A **figura 2-C** apresenta, em perspectiva, o cartão conceito
20 ilustrado nas figuras 2-A e 2-B.

A **figura 2-D** apresenta, em perspectiva, o cartão conceitual completamente submetido a um fluxo magnético ascendente, homogêneo em toda a região do cartão.

A **figura 2-E** apresenta, em perspectiva, o cartão conceitual
25 submetido a um fluxo magnético significativamente diferente nas duas espiras, em razão da presença da máscara de blindagem (8).

A **figura 2-F** apresenta, em vista superior, a mesma situação ilustrada na figura 2-E.

A **figura 2-G** apresenta, em vista superior, o circuito RFID auto-protegido sendo na região de leitura autorizada de um leitor RFID cuja

antena (9) foi projetada especificamente para acoplar magneticamente as duas regiões da antena auto-protegida - situação alternativa à da blindagem (8) apresentada nas figuras 2-E e 2-F.

5 A **figura 2-H** apresenta, em vista frontal, a mesma situação ilustrada na figura 2-G.

A **figura 2-I** apresenta, em perspectiva, a mesma situação ilustrada nas figuras 2-G e 2-H.

10 As figuras de 1-A a 1-J ilustram o conceito fundamental no qual se baseia o invento. A disposição coplanar e o sentido do enrolamento das espiras faz com que, quando submetidas a um fluxo magnético variável de mesma direção e sentido, a tensão induzida em uma das espiras tenha sinal oposto ao da tensão induzida na outra espira, tendendo a reduzir o módulo da tensão resultante nos terminais. Note-se que o cruzamento do condutor no ponto
15 de intersecção das espiras ocorre sem contato elétrico e que o vetor **B**, utilizado nas ilustrações, é a componente da densidade de fluxo magnético na direção ortogonal ao plano das espiras, uma vez que apenas esta componente produz algum efeito de interesse. Dado um fluxo magnético homogêneo (vetor densidade de fluxo magnético **B** suficientemente uniforme na região da antena) e
20 variável no tempo, a magnitude da tensão induzida em cada espira a ele submetida é proporcional à área envolvida pela espira e a polaridade relativa da tensão induzida em cada espira depende do sentido (horário ou anti-horário) do caminho percorrido pelo condutor. Portanto, uma vez que as duas espiras apresentadas nas figuras 1-A a 1-J encontram-se ligadas em série e envolvem as
25 respectivas áreas internas (no plano do papel) em sentidos opostos, se o dispositivo for submetido a um campo magnético variável uniforme, a tensão resultante nos terminais é a diferença (e não a soma) dos módulos das tensões induzidas em cada espira. Ou seja, a tensão induzida nos terminais é proporcional à diferença (e não à soma) destas áreas. Nesta configuração, se as áreas forem aproximadamente iguais, a tensão resultante será aproximadamente

nula. Se um circuito integrado RFID está ligado a esses terminais, ele não será eletricamente alimentado e a comunicação não será possível, garantindo a integridade e a privacidade dos dados armazenados na memória. De fato, a produção de um campo magnético não homogêneo na região do dispositivo RFID só é possível para um leitor muito próximo e convenientemente posicionado em relação ao circuito RFID auto-protegido, sendo a distância limite e a tolerância relativa ao posicionamento dependentes do projeto específico. No caso de documentos de segurança, como passaportes eletrônicos e documentos de identidade, diversos elementos de segurança presentes no suporte precisam ser verificados opticamente pelos terminais de leitura. Logo, a necessidade de colocar o documento na região de leitura já é atualmente uma realidade operacional compatível com a utilização dos novos dispositivos de RFID auto-protegidos aqui apresentados.

Alternativamente à máscara para blindagem eletromagnética de parte da antena, o leitor pode incorporar uma espira ou um conjunto de espiras capaz de acoplar magneticamente a antena auto-protegida sem a necessidade da máscara. Essa situação é ilustrada nas figuras 1-I e 1-J, onde se vê uma espira (4), pertencente a um leitor autorizado (5), pela qual circula uma corrente indutora I_L , oriunda do leitor. Como a espira (4) encontra-se em plano paralelo e suficiente próximo ao plano do dispositivo a ser ativado (1) e a espira da direita de (1) está posicionada sobre a área da espira (4) do leitor, no caminho natural das linhas de fluxo magnético, a corrente I_L induz um campo magnético B descendente na área envolvida pela espira da direita de (1). Uma consequência natural disso é que o fluxo que atravessa o mesmo plano pela região externa da espira (4) é ascendente e parte desse fluxo atravessará também a área enlaçada pela espira esquerda de (1), contribuindo para aumentar a tensão induzida resultante nos terminais do chip (2). Nessa situação, a espira da direita funciona como acoplador, e não como região protetora do circuito RFID, uma vez que todas as espiras contribuirão construtivamente para o módulo da tensão induzida.

As figuras 2-A, 2-B e 2-C ilustram uma possível forma construtiva de um cartão de identificação intrinsecamente protegido pela invenção ora apresentada. Esse cartão conceitual é composto de basicamente três partes construtivas: um *suporte* de polímero (6), em policarbonato, medindo aproximadamente 54 mm x 86 mm x 0,85 mm, um fio de cobre esmaltado (7), de bitola AWG 32, de 81 centímetros de comprimento total, cuja geometria na montagem caracteriza a *antena auto-protegida* (7), e um chip especificado de acordo com a aplicação. A *antena auto-protegida* (7) apresenta, nesse caso, duas bobinas (uma à esquerda e outra à direita), cada uma constituída por duas espiras (voltas) do elemento condutor, ligadas em série, de modo que, percorrendo-se o condutor a partir de um dos terminais em direção ao outro, a área no interior da bobina à esquerda é envolvida em sentido (horário ou anti-horário) oposto ao sentido em que será envolvida a área no interior da bobina à direita. Note-se que, quando n espiras ligadas em série envolvem a mesma área no mesmo sentido, caracterizando uma bobina, a tensão induzida é multiplicada pelo número de espiras n . O espaçamento entre os segmentos paralelos de fio é de 0,3 mm e a periferia da antena dista cerca de 1,5 mm das margens do suporte. Ressalte-se que este é um exemplo de concretização, não restritivo, meramente ilustrativo do conceito da inovação. Os seguintes parâmetros do cartão devem ser dimensionados e ajustados de acordo com o projeto específico para a aplicação desejada: geometria, material e número de camadas do suporte, quantidade e geometria das bobinas, número e sentido de enrolamento das espiras em cada bobina, tipo de condutor (fio de cobre esmaltado, trilhas desenhadas por corrosão ou deposição, etc), espaçamento entre linhas condutoras paralelas, localização e modelo e demais parâmetros do chip. Todos estes parâmetros devem ser especificados e dimensionados de modo a garantir que, quando completamente exposta a um fluxo magnético aproximadamente homogêneo (figura 2-D), o módulo da tensão induzida resultante nos terminais do chip seja sempre menor que a *tensão de não funcionamento*. Esta é uma condição de segurança, uma vez que a configuração de linhas de fluxo magnético ilustrada na figura 2-D é

tipicamente a que seria aplicado ao documento por um leitor não muito próximo ou mal posicionado (caso de um leitor clandestino). Além disso, uma vez blindada por uma lâmina metálica (8) a região protetora da antena (figuras 2-E e 2-F), a exposição do dispositivo a uma intensidade de campo magnético B (dependente do projeto), mesmo que homogêneo, deverá garantir que o módulo da tensão resultante induzida nos terminais do chip seja superior à *tensão de funcionamento* (garantia de eficiência). A máscara apresentada (8) é uma parte integrante de (ou adaptada a) um leitor legítimo, leitor este autorizado a ativar e se comunicar com o documento de segurança eletrônico auto-protegido. A máscara deve ser colocada no leitor de forma conveniente, sob ou sobre a espira que se pretende blindar, de modo a não interferir com o escaner óptico, conforme o caso.

Analogamente ao que se pode ver nas figuras 1-I e 1-J, a indução da tensão de funcionamento neste circuito RFID auto-protegido conceitual, pode ser conseguida sem a blindagem eletromagnética, utilizando-se no leitor autorizado uma espira (ou conjunto de espiras) capaz de acoplar magneticamente o circuito RFID a ser lido. Esta situação é ilustrada nas figuras 2-G, 2-H e 2-I, nas quais, para melhor visualização, foi omitido o suporte de policarbinato. Vê-se nestas figuras a antena auto-protegida (7), com o chip RFID (2), e o par de espiras (9) que seria parte do leitor autorizado. Comparando a espira (4) do leitor (5), ilustrada nas figuras 1-I e 1-J, com o par de espiras reversas (9), ilustrado nas figuras 2-G, 2-H e 2-I, é esperado que este par de espiras produza um fluxo magnético mais concentrado em ambas as regiões da antena auto-protegida, produzindo um acoplamento mais eficiente.

Foi apresentado, portanto, um conjunto - não exaustivo - de três formas alternativas para que um leitor autorizado possa produzir, na região de leitura, um fluxo magnético capaz de ativar o circuito RFID intrinsecamente protegido, a saber:

1) uma máscara (3) que utiliza o conceito da gaiola de Faraday para bloquear convenientemente o fluxo que passaria através da região protetora da antena (figuras 1-E e 1-F);

2) uma espira (4) capaz de acoplar predominantemente um conjunto de espiras de mesma orientação no dispositivo RFID (figs. 1-I e 1-J); e

3) um par de espiras reversas (9) capaz de acoplar de modo mais eficiente mais de uma região do circuito RFID intrinsecamente protegido.

A alternativa 1) é a mais simples e barata de ser implementada, passível de adoção inclusive em leitores de cartões convencionais já em uso, sem necessariamente comprometer as demais funcionalidades do terminal. As restrições e exigências de projeto e oportunidade poderão sugerir a conveniência da adoção das alternativas 2), 3) ou outras mais eficientes e possivelmente mais complexas e onerosas.

A concretização do invento aqui apresentada é realizável com técnicas de produção de conhecimento público, usando os mesmos insumos e processos já utilizados na produção de cartões inteligentes com RFID, sem mudança significativa do custo de produção.

20

25

REIVINDICAÇÕES

1. Uma ANTENA AUTO-PROTEGIDA COM APLICAÇÃO EM (MAS NÃO
RESTRITA A) DOCUMENTOS ELETRÔNICOS DE IDENTIFICAÇÃO POR
5 RADIOFREQUENCIA (RFID) INTRINSECAMENTE PROTEGIDOS
CONTRA EXCITAÇÃO CLANDESTINA, caracterizada por um condutor
elétrico cuja geometria configura pelo menos duas espiras coplanares em série
(peças (1) e (7) nos desenhos), sem partes móveis, embutíveis no suporte do
documento protegido, que envolvem áreas distintas em sentidos de circulação
10 opostos, de modo que, quando o dispositivo é submetido a um fluxo magnético
variável e homogêneo, existe pelo menos uma região da antena que contribui
para diminuir a magnitude da tensão resultante induzida no conjunto,
inviabilizando ou dificultando significativamente a ativação do circuito por
leitores não autorizados.
- 15
2. Um DOCUMENTO ELETRÔNICO IDENTIFICAÇÃO POR
RADIOFREQUÊNCIA (RFID) INTRINSECAMENTE PROTEGIDO
CONTRA ATIVAÇÃO CLANDESTINA caracterizado por utilizar uma antena
cuja geometria configura pelo menos duas espiras coplanares em série (7), sem
20 partes móveis, embutíveis no suporte (6) do documento, que envolvem áreas
distintas em sentidos de circulação opostos, de modo que, quando o documento é
submetido a um fluxo magnético variável e homogêneo, existe pelo menos uma
região da antena que contribui para diminuir a magnitude da tensão resultante
induzida nos terminais do circuito integrado (2), inviabilizando ou dificultando
25 significativamente a ativação do circuito por leitores não autorizados.

DESENHOS

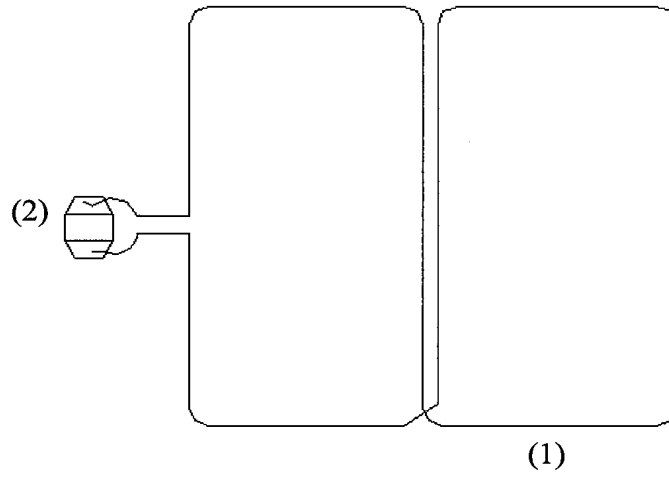


Fig. 1-A

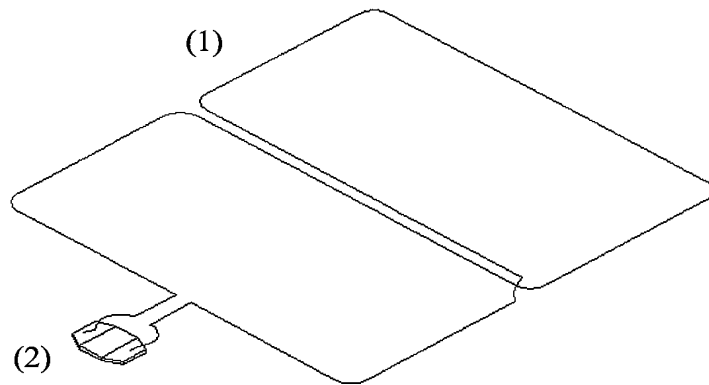


Fig. 1-B

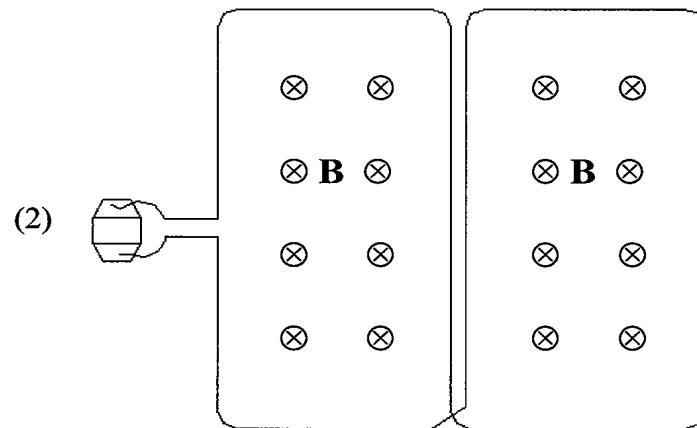


Fig. 1-C

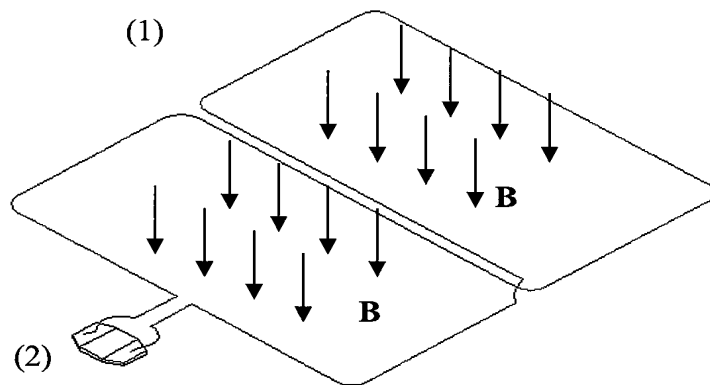


Fig. 1-D

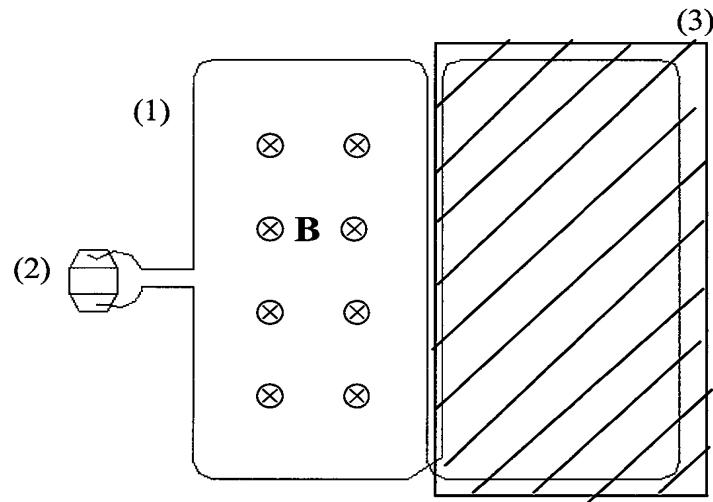


Fig. 1-E

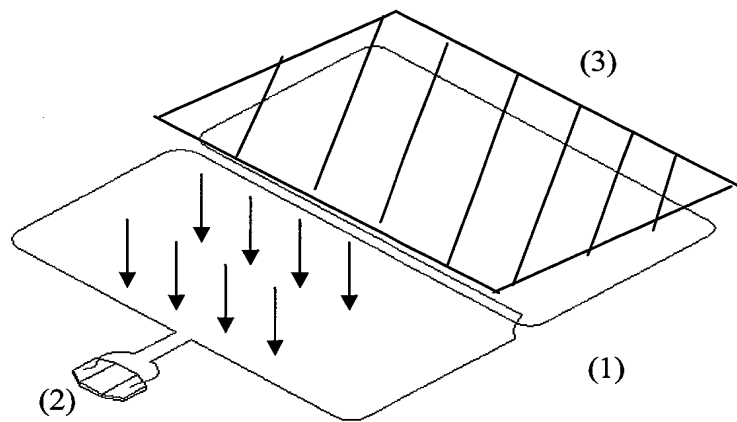


Fig. 1-F

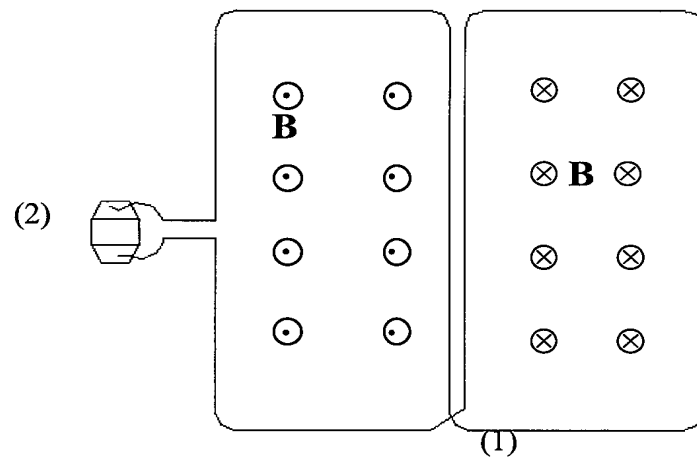


Fig. 1-G

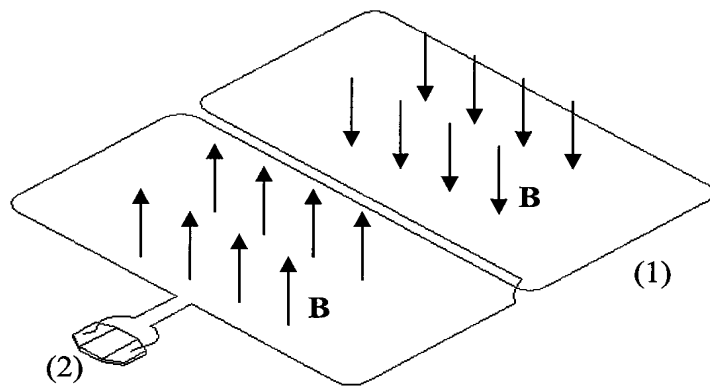


Fig. 1-H

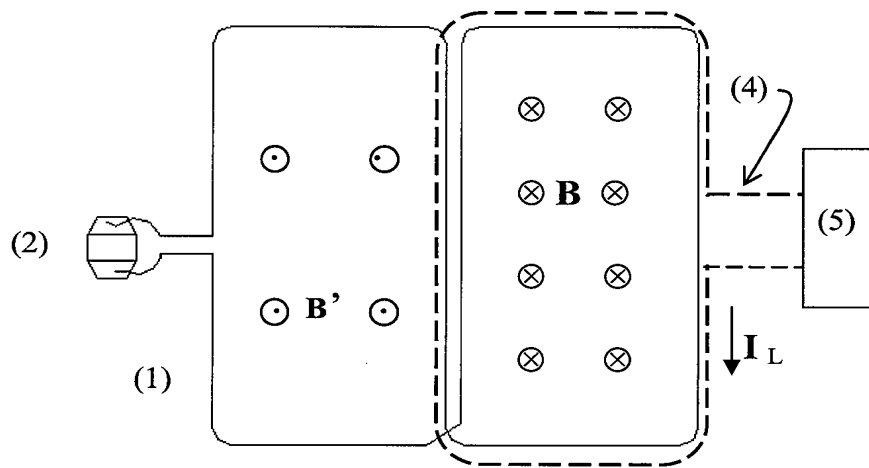


Fig. 1-I

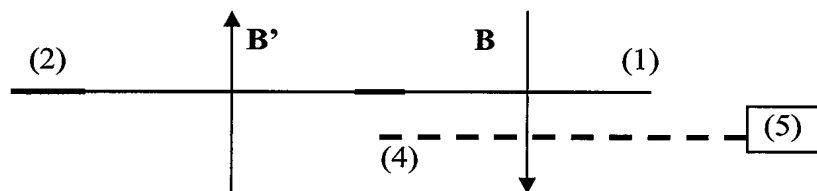


Fig. 1-J

Fig. 2-A

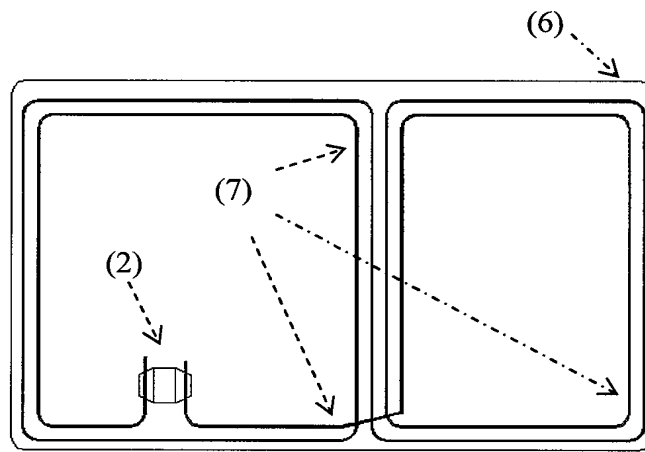


Fig. 2-B

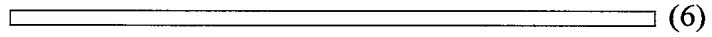


Fig. 2-C

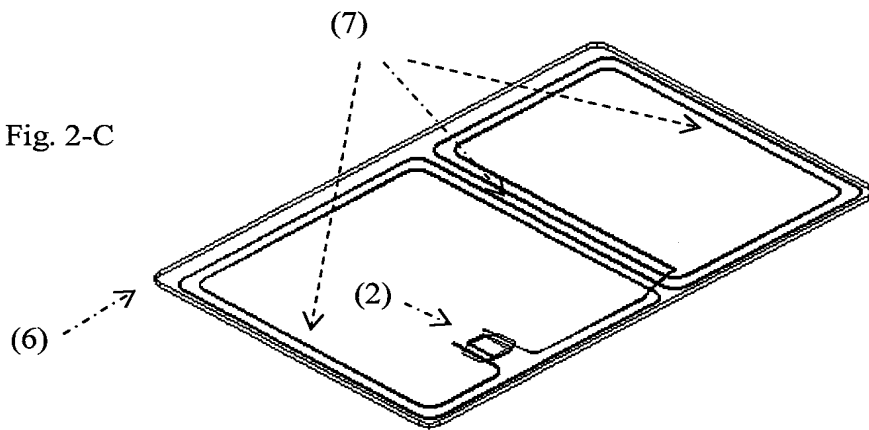


Fig. 2-D

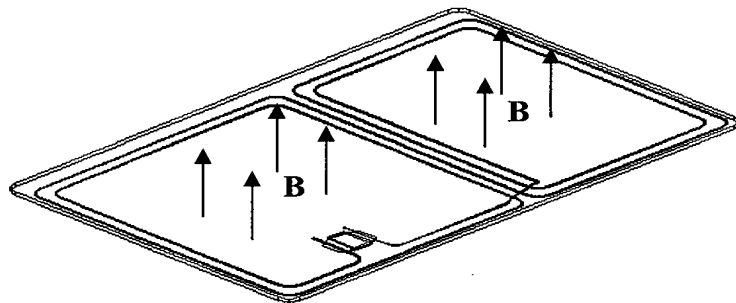


Fig. 2-E

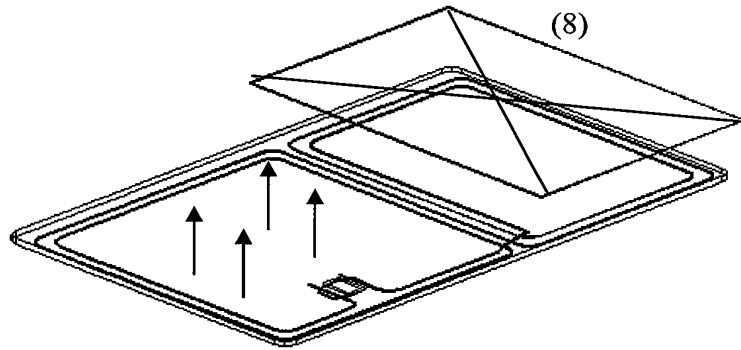


Fig. 2-F

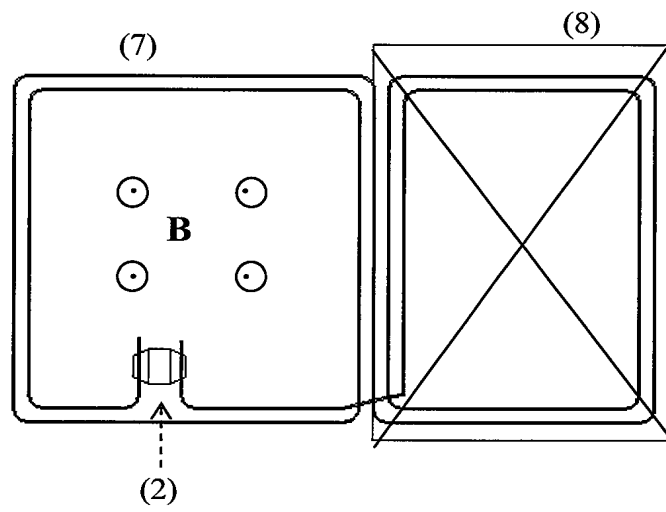


Fig. 2-G

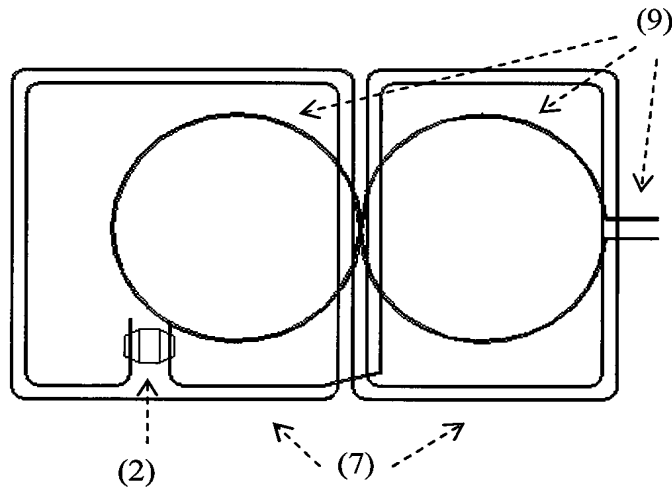


Fig. 2-H

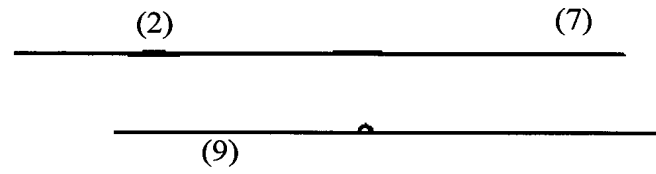
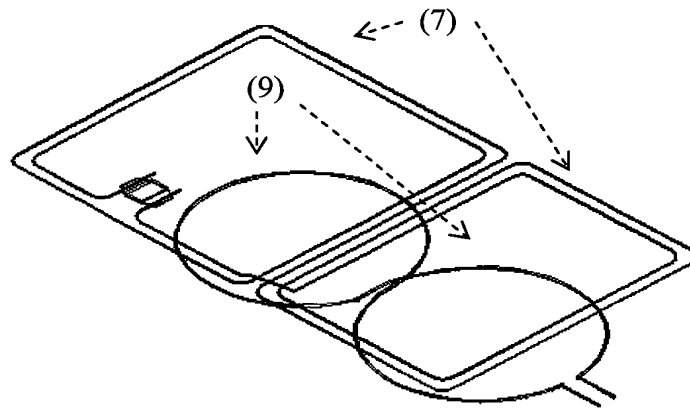


Fig. 2-I



RESUMO

Patente de Invenção “ANTENA AUTO-PROTEGIDA COM
APLICAÇÃO EM (MAS NÃO LIMITADA A) DOCUMENTOS
5 ELETRÔNICOS DE IDENTIFICAÇÃO POR RADIOFREQUÊNCIA (RFID)
INTRINSECAMENTE PROTEGIDOS CONTRA ATIVAÇÃO
CLANDESTINA”

A presente invenção é um novo tipo de antena, auto-protegida
contra excitação e comunicação não autorizada, sem partes móveis, de
10 baixíssimo custo, completamente embutível em um cartão de polímero típico,
para aplicações em (mas não limitada a) cartões inteligentes comerciais e
documentos eletrônicos de identificação operáveis sem contato (RFID), capaz de
condicionar o funcionamento do dispositivo ao posicionamento da antena em
região específica, muito próxima ao terminal leitor autorizado, provendo assim
15 proteção intrínseca à privacidade e à integridade dos dados armazenados na
memória. A antena e uma concretização de documento intrinsecamente protegido
contra ativação clandestina aqui propostas são compatíveis com os terminais
leitores atualmente utilizados, mediante uma adaptação de custo desprezível em
relação ao valor dos terminais leitores.

20

25