

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

(21) **PI 1013129-9 A2**

(22) Data de Depósito: 26/08/2010
(43) Data da Publicação: 09/10/2012
(RPI 2179)



(51) *Int.Cl.:*

G06F 21/00
G06F 3/041
H04L 9/32
G06Q 40/00

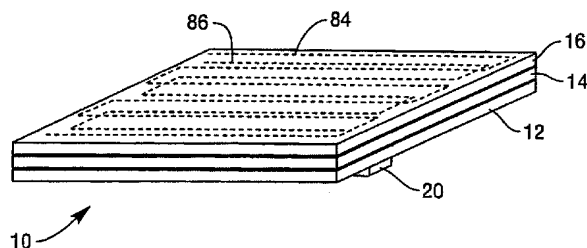
(54) **Título:** CONJUNTO DE PLACA DE CIRCUITO INTEGRADO SEGURO

(30) **Prioridade Unionista:** 31/08/2009 US 12/551,097

(73) **Titular(es):** NCR Corporation

(72) **Inventor(es):** Charles Harrow, Grant A. Mcnicoll, Ian J. Walker

(57) **Resumo:** CONJUNTO DE PLACA DE CIRCUITO INTEGRADO SEGURO. Um conjunto de placa de circuito integrado seguro é proporcionado. O conjunto de placa de circuito integrado seguro compreende: uma placa de controle incluindo um processador criptográfico; uma parte espaçadora montada na placa de controle; e uma tampa montada na parte espaçadora. A placa de controle, a parte espaçadora e a tampa proporcionam coletivamente uma câmara fechada segura, na qual o processador criptográfico é montado. A parte espaçadora proporciona proteção contra ataques laterais ao processador criptográfico.



"CONJUNTO DE PLACA DE CIRCUITO INTEGRADO SEGURO"

CAMPO DA INVENÇÃO

A presente invenção se refere a um conjunto de placa de circuito integrado seguro. Em particular, ainda que não exclusivamente, a invenção se refere a um conjunto de placa de circuito integrado seguro para montagem de um processador criptográfico.

ANTECEDENTES DA INVENÇÃO

Os processadores criptográficos são usados em dispositivos seguros, tais como teclados de criptografia e visores sensíveis ao toque de criptografia, para garantir que os dados introduzidos pelo dispositivo seguro sejam transmitidos apenas em forma criptografada, quando deixam o dispositivo seguro.

Há vários requisitos que precisam ser satisfeitos para que um dispositivo seguro obedeça aos padrões de segurança internacionais. Um desses padrões é o estabelecido pelo Conselho de Padrões de Segurança PCI.

Um ataque potencial em um dispositivo seguro é um ataque lateral, que envolve uma tentativa de sondar um processador criptográfico da parte lateral do dispositivo seguro, em vez de da parte de topo ou de fundo do dispositivo seguro. Os dispositivos seguros da técnica anterior têm tentado atenuar esses ataques circundando o processador criptográfico com uma malha condutora, e embutindo a malha condutora em epóxi. No entanto, essa abordagem não foi inteiramente bem-sucedida, não sendo confiável, intensa em tempo e relativamente cara.

RESUMO DA INVENÇÃO

Consequentemente, a invenção proporciona geralmente métodos, sistemas e aparelho para proteger um dispositivo seguro, particularmente de ataques laterais.

Além do RESUMO DA INVENÇÃO proporcionado acima e do objeto descrito abaixo na DESCRIÇÃO DETALHADA, os parágrafos apresentados a seguir dessa seção são intencionados para proporcionar ainda mais base para uma linguagem reivindicativa alternativa, para possível uso na condução deste pedido de patente, se necessário. Se este pedido de patente for concedido, alguns aspectos da invenção podem se referir às reivindicações incorporadas durante a condução deste pedido de patente, outros aspectos podem se relacionar às reivindicações eliminadas durante a condução, outros aspectos podem se relacionar a objeto nunca reivindicado. Além do mais, os vários aspectos detalhados a seguir são independentes entre si, exceto quando indicado de outro modo. Qualquer reivindicação correspondente a um aspecto não deve ser considerada como incorporando qualquer elemento ou aspecto dos outros aspectos, a menos que indicado explicitamente nessa reivindicação.

De acordo com um primeiro aspecto, proporciona-se um conjunto de placa de circuito integrado seguro, que compreende uma placa de circuito integrado incluindo um processador criptográfico; uma parte espaçadora montada na placa de controle; e uma tampa

montada na parte espaçadora, de modo que a placa de controle, a parte espaçadora e a tampa proporcionem coletivamente uma câmara fechada segura, na qual o processador criptográfico é montado.

5 A parte espaçadora pode compreender uma placa de circuito integrado separada, ou camadas adicionais na placa de controle.

10 A parte espaçadora pode incluir camadas alternadas ligadas, para formar uma rota condutora, de modo que qualquer brecha de qualquer parte dessa rota é detectada pelo processador criptográfico. Por exemplo, as camadas um, três e cinco podem ser acopladas conjuntamente a uma voltagem positiva (tal como 3,3 V), e as camadas dois, quatro e seis podem ser acopladas conjuntamente ao potencial terra elétrico (0 V). As rotas condutoras podem ser localizadas em torno de um perímetro da parte espaçadora, ou em torno de toda a parte espaçadora, em que a parte espaçadora é na forma de um quadro em associação com um perímetro da placa de controle.

15 A rota definida pelas camadas adjacentes pode ser deslocada para limitar a possibilidade de mesmo um controle de penetração estreito desconsiderar as camadas adjacentes.

20 A parte espaçadora pode definir uma pluralidade de aberturas. Uma abertura pode proporcionar suporte para uma conexão elastomérica, tal como uma conexão elastomérica Zebra (marca registrada), disponível da Fujipoly America Corporation, 900 Milik Street, P.O. Box 119, Carteret, NJ 07008, EUA. Uma conexão elastomérica opera por contato de blocos de condução, opostos, espaçados entre si (tipicamente na forma de duas tiras lineares de blocos) e sendo mantidos em compressão pelos blocos condutores opostos, para manter uma conexão estreita entre cada lado da conexão elastomérica e os blocos condutores.

25 Uma outra abertura pode circundar o processador criptográfico. Uma outra abertura pode circundar o controlador de painel sensível ao toque. Ainda uma outra abertura pode ser alinhada com uma parte rebaixada, para definir uma rota de níveis dirigidos para um conector flexível, para indicar a remoção do conjunto de placa de circuito integrado seguro (ou de um dispositivo seguro incluindo a placa de circuito integrado segura) de uma instalação, tal como de um terminal de autoatendimento.

30 Um lado da parte espaçadora da placa de controle e um lado da placa de controle da parte espaçadora podem ambos incluir dois ou mais blocos, os blocos no lado da parte espaçadora estando em associação com os blocos no lado da placa de controle da parte espaçadora, de modo que os blocos correspondentes fiquem em contato quando a parte espaçadora é montada na placa de controle. Um ou mais desses blocos podem se projetar de uma superfície, na qual são dispostos, para proporcionar um melhor contato com um bloco correspondente.

35 Um bloco pode transportar uma voltagem positiva (o bloco positivo), o outro bloco pode transportar potencial terra (ou massa) elétrico (o bloco massa). Pode haver uma plura-

lidade de blocos positivos e uma pluralidade de blocos terra. Os blocos em qualquer uma (ou em ambas) da placa de controle e da parte espaçadora podem ser configurados como círculos concêntricos isolados. Um círculo interno pode ser usado para transportar a voltagem necessária (terra ou positiva), e um círculo externo concêntrico pode ser proporcionado com a outra voltagem (isto é, positiva ou terra), de modo que se um terceiro tentar colocar uma folha ou sonda condutora entre a parte espaçadora e a placa de controle, então a folha ou sonda condutora vão criar um curto-circuito entre os círculos interno e externo, que vai ser detectado pelo processador criptográfico. Uma vez que apenas o círculo interno transporta a voltagem necessária, o bloco correspondente apenas precisa ficar associado com esse círculo interno, e isolado eletricamente do círculo externo.

O bloco positivo pode ser acoplado ao primeiro grupo de camadas alternadas ligadas, para formar uma primeira rota condutora, e o bloco terra pode ser acoplado ao segundo grupo de camadas alternadas ligadas, para formar uma segunda rota condutora.

Um lado da tampa da parte espaçadora e um lado da parte espaçadora da tampa podem ambos incluir dois ou mais blocos, os blocos no lado da tampa da parte espaçadora sendo associados com os blocos no lado da parte espaçadora, de modo que os blocos correspondentes fiquem em contato quando a parte espaçadora é montada na tampa. Um bloco pode transportar uma voltagem positiva (o bloco positivo), o outro bloco pode transportar potencial terra (ou massa) elétrico (o bloco terra). Pode haver uma pluralidade de blocos positivos e uma pluralidade de blocos terra. Os blocos em qualquer um (ou ambos) do lado da tampa da parte espaçadora ou do lado da parte espaçadora da tampa podem ser configurados como círculos concêntricos isolados. Um círculo interno pode ser usado para transportar a voltagem necessária (terra ou positiva), e um círculo externo concêntrico pode ser dotado com a outra voltagem (isto é, positiva ou terra), de modo que se um terceiro tentar colocar uma folha condutora entre a parte espaçadora e a placa de controle, então a folha condutora vai criar um curto-circuito entre os círculos interno e externo, que vai ser detectado pelo processador criptográfico, ou a folha vai separar os blocos no lado da tampa da parte espaçadora dos blocos na parte espaçadora, o que vai ser detectado pelo processador criptográfico.

Um ou mais blocos terra e/ou blocos positivos no lado da tampa da parte espaçadora podem compreender dois semicírculos isolados conectados eletricamente por um bloco terra ou positivo (respectivamente) no lado da parte espaçadora da tampa. Isso garante que se a tampa for levantada da parte espaçadora, então os dois semicírculos vão ficar separados, o que vai ser detectado pelo processador criptográfico.

A placa de controle pode incluir uma pluralidade de componentes circundando o processador criptográfico e/ou o controlador de painel sensível ao toque. A pluralidade de componentes pode incluir resistores, ferritas de baixo valor (por exemplo, zero ohm) ou as-

semelhados. Qualquer ataque lateral pode danificar esses componentes, rompendo a continuidade elétrica do circuito, o que vai ser detectado pelo processador criptográfico.

A parte espaçadora pode compreender uma pluralidade de camadas ligadas permanentemente à placa de controle, isto é, a placa de controle e a parte espaçadora podem compreender uma unidade integral, que é não é projetada para desmontagem. Alternativamente, a parte espaçadora pode compreender uma placa separada, que entra em contato com a placa de controle e é retida no lugar por parafusos, pinos ou assemelhados.

Como uma outra opção, podem ser proporcionadas partes espaçadores adicionais, de modo que cada parte espaçadora seja uma placa separada. Uma primeira parte espaçadora pode incluir uma primeira tira de bloco de conexão, em associação com uma tira de bloco de conexão em um lado da parte espaçadora da tampa, mas separada dela por uma segunda parte espaçadora, a segunda parte espaçadora definindo uma abertura para acomodar um conector elastomérico, para proporcionar continuidade elétrica entre as duas tiras de blocos de conexão.

A segunda parte espaçadora pode incluir uma segunda tira de bloco de conexão, em associação com uma tira de bloco de conexão em um lado da parte espaçadora da placa de controle (a tira do bloco da placa de controle), mas separada dela pela primeira parte espaçadora, a primeira parte espaçadora definindo uma abertura para acomodar um conector elastomérico, para proporcionar continuidade elétrica entre a segunda tira e a tira do bloco de controle. As aberturas definidas pelas primeira e segunda partes espaçadoras podem ser deslocadas entre si.

De acordo com um segundo aspecto, proporciona-se um dispositivo seguro, incluindo a placa de circuito integrado segura do primeiro aspecto da invenção.

O dispositivo seguro pode incluir ainda uma tira de remoção, acoplada à placa de circuito integrado segura, em uma extremidade, e tendo uma chave, em uma extremidade oposta, para fixação em um dispositivo hospedeiro, de modo que a chave seja fechada (ou aberta) quando a tira de remoção é fixada.

O dispositivo seguro pode ser operável para detectar uma variação de estado da chave, detectando, desse modo, a remoção do dispositivo seguro do dispositivo hospedeiro.

O dispositivo hospedeiro pode ser um terminal de autoatendimento.

O dispositivo seguro pode compreender uma placa de circuito integrado segura montada em um alojamento.

De acordo com um terceiro aspecto, proporciona-se um terminal de autoatendimento incluindo o dispositivo seguro do segundo aspecto.

O terminal de autoatendimento pode ser uma máquina de caixa de banco automática (ATM), um quiosque de informações, um centro de serviços financeiros, um quiosque para pagamento de contas, um quiosque de loteria, uma máquina de serviços postais, um

terminal de chegada e/ou saída, tais como aqueles usados em setores de venda a varejo, hotéis, aluguel de automóveis, jogos eletrônicos, assistência médica e linhas aéreas, e semelhantes.

Esses e outros aspectos vão ficar evidentes da descrição específica apresentada a seguir, apresentada por meio de exemplo, com referência aos desenhos em anexo.

BREVE DESCRIÇÃO DOS DESENHOS

A Figura 1 é um diagrama ilustrado simplificado de um conjunto de placa de circuito integrado seguro, compreendendo três placas diferentes, de acordo com uma concretização da presente invenção.

A Figura 2 é uma vista detalhada do conjunto de placa de circuito integrado seguro da Figura 1, ilustrando as três diferentes placas.

A Figura 3 é um diagrama esquemático das conexões elétricas entre as três diferentes placas da Figura 1.

As Figuras 4A a 4C são diagramas ilustrados mostrando três tipos de blocos, usados nas três diferentes placas da Figura 1.

A Figura 5 é um diagrama esquemático do conjunto de placa de circuito integrado seguro da Figura 1, montado em um alojamento para criar uma placa de circuito integrado segura montado.

A Figura 6 é um diagrama esquemático de um dispositivo seguro incorporando a placa de circuito integrado segura montada da Figura 5.

A Figura 7 é uma vista detalhada de um conjunto de placa de circuito integrado seguro, de acordo com uma segunda concretização da presente invenção.

A Figura 8 é uma vista detalhada de um conjunto de placa de circuito integrado seguro, de acordo com uma terceira concretização da presente invenção.

DESCRIÇÃO DETALHADA

Vai-se fazer primeiro referência à Figura 1, que é um diagrama ilustrado de um conjunto de placa de circuito integrado seguro 10, de acordo com uma concretização da presente invenção, e também à Figura 2, que é uma vista detalhada do conjunto de placa de circuito integrado seguro 10.

O conjunto de placa de circuito integrado seguro 10 compreende uma camada de placa de controle 12, uma parte espaçadora 14 e uma tampa segura 16. A placa de controle 12, a parte espaçadora 14 e a tampa segura 16 são todas na forma de uma placa de circuito integrado impresso (pcb) multicamada. Nessa concretização, a placa de controle 12 compreende uma pcb FR4 de 2 mm de espessura de oito camadas, a parte espaçadora 14 compreende uma pcb FR4 de 2 mm de espessura de oito camadas e a tampa segura 16 compreende uma pcb FR4 de 1,6 mm de quatro camadas. Um conector USB 20 é montado em um lado inferior da placa de controle 12, para conectar o conjunto de placa de circuito

integrado seguro 10 a um controlador (não mostrado). Um conector de painel de toque (não mostrado) é também montado no lado inferior da placa de controle 12, para conectar o conjunto de placa de circuito integrado seguro 10 a um painel de toque (não mostrado).

CAMADA DE PLACA DE CONTROLE 12

5 As finalidades básicas da placa de controle 12 são apresentadas a seguir. Primeiramente, para suportar os componentes (em cada uma das duas superfícies externas da placa de controle 12), em particular, os componentes seguros (tais como um processador criptográfico 30 e um controlador de painel sensível ao toque 32) são suportados em uma superfície voltada para dentro 40 (também referida como um lado da parte espaçadora), e
10 os componentes não seguros (tais como uma ou mais baterias, componentes de suprimento de energia, o conector USB 20 e assemelhados) são suportados em uma superfície voltada para fora 42. Em segundo lugar, para impedir quaisquer ataques nos componentes seguros pela superfície voltada para fora 42, como vai ser descrito em mais detalhes abaixo.

A placa de controle 12 também inclui os componentes redundantes 44 na forma de
15 componentes resistores e de ferrita de baixa resistência. Os componentes redundantes 44 são dispostos na superfície voltada para dentro da placa de controle 40, para circundar o processador criptográfico 30 e o controlador de painel sensível ao toque 32. No caso em que quaisquer desses componentes são danificados, por exemplo, por uma sonda penetrando neles, em uma tentativa de atingir o processador criptográfico 30, então o processa-
20 dor criptográfico 30 detecta isso e pode eliminar quaisquer informações seguras armazenadas dentro do processador criptográfico 30, ou em qualquer outro lugar na placa de circuito integrado seguro 12.

A placa de controle 12 também inclui uma tira linear 45 de blocos condutores localizados aproximadamente na parte central dela, e os quatro blocos condutores 46 a 49 dis-
25 postos adjacentes aos quatro cantos da placa de controle 12. Os quatro blocos condutores 46 a 49 compreendem todos um par de círculos concêntricos isolados, como ilustrado na Figura 4A. Um círculo em cada par de círculos é mantido a uma voltagem positiva (3,3 V) e o outro círculo é mantido em potencial terra elétrico. Apenas o círculo interno é usado para transferir energia (3,3 v) ou potencial terra, o círculo externo é mantido na voltagem oposta,
30 de modo que qualquer tentativa de sondar o círculo interno vai colocar em curto-circuito os círculos externo e interno, que vão ser detectados pelo processador criptográfico 20. Nessa concretização, os círculos internos dos blocos condutores 46 e 48 são mantidos em potencial terra elétrico, enquanto que os círculos internos dos blocos condutores 47 e 49 são mantidos na voltagem positiva (3,3 V).

35 A superfície voltada para fora 42 também inclui uma chave de remoção (não mostrada), para indicar quando a placa de circuito integrado 12 é removida de um visor sensível ao toque (não mostrado).

Embora não mostrada, a placa de controle 12 também contém duas trilhas condutoras, cada trilha ligando camadas alternadas da placa de controle 12. Uma trilha condutora (a 3,3 V) atravessa as camadas pares, voltando atrás nela mesma na medida em que se estende por cada camada, a outra trilha condutora (no potencial terra elétrico) atravessa as camadas ímpares, voltando atrás nela mesma na medida em que se estende por cada camada. Essas trilhas condutoras são usadas para impedir quaisquer ataques pela superfície voltada para fora 42 para a superfície voltada para dentro 40.

CAMADA DE PARTE ESPAÇADORA 14

As finalidades básicas da parte espaçadora 14 são: (i) proporcionar proteção contra quaisquer ataques laterais contra o processador criptográfico 30, o controlador de painel sensível ao toque 32 e outros componentes seguros; e (ii) proporcionar um vão suficiente entre a placa de controle 12 e a tampa segura 16, para considerar a altura dos componentes seguros (tais como o processador criptográfico 30 e o controlador de painel sensível ao toque 32). Para atingir essas finalidades, a parte espaçadora 14 compreende uma pcb de oito camadas, nessa concretização.

A parte espaçadora 14 inclui uma camada voltada para a tampa 50 (a primeira camada) tendo seis blocos condutores 52 a 57, e duas trilhas condutoras perimetrais 58 e 59.

Quatro dos blocos condutores 52, 53, 56 e 57 compreendem todos um par de círculos concêntricos do tipo ilustrado na Figura 4A, que é o mesmo tipo daqueles blocos condutores 46 a 49. No entanto, dois dos blocos condutores 54 e 55 compreendem ambos um círculo externo, circundando um par de partes arqueadas (quase semicírculos), em que cada uma das partes arqueada é isolada da outra parte arqueada e do círculo externo, como ilustrado na Figura 4B.

A trilha condutora perimetral 58 é mantida a uma voltagem positiva (3,3 V nessa concretização) e cobre aproximadamente os dez milímetros externos da camada, não incluindo os blocos condutores 52 a 55, que são isolados da trilha condutora 58. A trilha condutora perimetral 58 se enrola em torno do perímetro, no plano da primeira camada 50, com um passo estreito entre as partes adjacentes da única trilha condutora 58, depois continua na terceira camada (não mostrada), depois na quinta camada (não mostrada) e na sétima camada (não mostrada) na parte espaçadora 14. Desse modo, a trilha condutora perimetral 58 serpenteia em torno das quatro camadas alternadas, e depois se acopla em um círculo interno do bloco condutor 56. Como vai ser explicado abaixo, quando montada, essa conecta a trilha condutora 58 ao processador criptográfico 30, que pode detectar se alguma parte da trilha condutora 58 está rompida, por exemplo, como parte de um ataque lateral.

De modo similar, a trilha condutora perimetral 59 é mantida no potencial terra elétrico e se enrola em torno do perímetro no plano da segunda camada, com um passo estreito entre as partes adjacentes da única trilha condutora 58, depois continua na quarta camada

(não mostrada), depois na sexta camada (não mostrada), e na oitava camada (não mostrada) da parte espaçadora 14. Desse modo, a trilha condutora perimetral terra 59 serpenteia em torno das quatro camadas alternadas, e depois se acopla a um círculo interno do bloco condutor 57. Como vai ser explicado abaixo, quando montada, essa conecta a trilha condutora 59 ao processador criptográfico 30, que pode detectar se alguma parte da trilha condutora 59 está rompida, por exemplo, como parte de ataque lateral. O processador criptográfico 30 pode também detectar se o conjunto de placa de circuito integrado seguro 10 está desmontado, porque isso cria uma condição de circuito aberto entre os blocos condutores, que estão em contato quando o conjunto de placa de circuito integrado seguro 10 está montado adequadamente.

A trilha condutora perimetral terra 59 é deslocada lateralmente da trilha condutora perimetral positiva 58, para reduzir a possibilidade de uma sonda ser inserida entre as partes trilhas adjacentes. O passo entre as partes adjacentes é tipicamente selecionado como o passo mais estreito que a tecnologia de manufatura de pcb vai permitir convenientemente.

A parte espaçadora 14 também define quatro aberturas e dois recessos. A primeira abertura 60 proporciona espaço para o processador criptográfico 30 e os componentes associados, a segunda abertura 62 proporciona espaço para o controlador de painel sensível ao toque 32 e os componentes associados, a terceira abertura 64 proporciona espaço para, e suporta no lugar, um conector elastomérico (não mostrado), que contata a tira linear 45, e a quarta abertura 66 é localizada entre um primeiro recesso 68 (na primeira camada 50) e um segundo recesso 69 (localizado na sexta camada 70 e indicado por linhas tracejadas). A quarta abertura 66 proporciona um canal de nível dividido, pelo qual um cabo flexível de remoção pode ser encaminhado. Ter um canal de nível dividido significa que é difícil inserir um condutor de fora do conjunto de placa de circuito integrado seguro 10, para sondar os blocos (não mostrados), ou promover um curto-circuito em um conector, ao qual o cabo flexível de remoção está acoplado.

Cada um dos quatro blocos condutores 52 a 55 tem um bloco condutor correspondente, 52a a 55a, respectivamente, disposto na oitava camada 70 (o lado voltado para a placa de controle). Esses blocos condutores 52a a 55a são do tipo ilustrado na Figura 4C, e compreendem apenas um círculo interno. Os círculos internos dos blocos condutores 52a a 55a são conectados eletricamente às partes internas (ou os círculos para conduzir os blocos 52 e 53, ou uma das partes arqueadas dos blocos condutores 54 e 55) dos blocos condutores correspondentes 52 a 55. Isso permite que a energia (3,3 v) ou o potencial terra seja dirigido pela parte espaçadora 14 do conjunto de placa de circuito integrado seguro 10.

TAMPA SEGURA 16

As finalidades básicas da tampa segura 16 são: (i) cobrir os componentes seguros; e (ii) proteger contra quaisquer ataques nos componentes seguros pela tampa segura 16.

Para atingir isso, nessa concretização, a tampa segura 16 compreende uma pcb de quatro camadas, tendo uma superfície externa 80 (a primeira camada) e uma superfície interna 82 (a quarta camada). Duas trilhas condutoras 84, e 86 (mostradas na Figura 1) são dirigidas entre essas (primeira e quarta) camadas.

5 A primeira trilha condutora 84 é mantida a uma voltagem positiva (3,3 V nessa concretização) e se enrola por uma segunda camada da tampa segura 16, localizada abaixo da superfície externa 80. A segunda trilha condutora 86 é mantida no potencial terra (terra elétrico) e se enrola em uma terceira camada da tampa segura 16, localizada entre a segunda camada e uma quarta camada (a superfície interna 82). As primeira e segunda trilhas condutoras 84 e 86 são lateralmente deslocadas para tornar mais difícil inserir uma sonda da
10 superfície externa 80 na superfície interna 82, sem tocar uma das duas trilhas condutoras 84, e 86.

A superfície interna 82 inclui uma tira linear localizada no centro 88 de blocos condutores, que se alinha com a terceira abertura 64 na parte espaçadora, e a tira linear 45 na
15 placa de controle 12, de modo que quando as placas são montadas, um conector elastomérico entra em contato com as tiras lineares 45, 88 e é mantido em posição pela terceira abertura 64. Nessa concretização, o conector elastomérico é uma tira Zebra (marca registrada), disponível da Fujipoly America Corporation, 900 Milik Street, P.O. Box 119, Carteret, NJ 07008, EUA.

20 As duas trilhas condutoras 84 e 86 são conectadas às diferentes partes da tira linear 88.

A superfície interna 82 também inclui seis blocos condutores 92 a 97, dispostos em associação com os blocos condutores correspondentes 52 a 57 na camada voltada para a tampa 50. Os seis blocos condutores 92 a 97 são do tipo ilustrado na Figura 4C e compreendem apenas um círculo interno.
25

Quando três diferentes placas 12, 14, 16 são montadas, os blocos condutores 46 a 49, 52 a 57, 52a a 55a, e 92 a 97, e as tiras lineares 45 e 88 formam chaves fechadas, como ilustrado na Figura 3. Qualquer tentativa de desmantelar essas placas, ou inserir uma sonda entre as placas para atingir as câmaras seguras, definidas pelas aberturas 60 e 62, vai ser detectada pelo processador criptográfico 30. Isso ocorre porque uma das trilhas condutoras 58, 59, 84 e 86 vai ficar em curto-circuito ou circuito aberto com a sonda, ou os blocos condutores, que estão em contato, vão ser separados (criando, desse modo, um circuito aberto), ou um curto-circuito.
30

Vai-se fazer agora também referência à Figura 5, que é um diagrama esquemático de um conjunto de placa de circuito integrado seguro 100, compreendendo a placa de circuito integrado segura 10 montada em um alojamento 102. O alojamento 102 facilita a montagem da placa de circuito integrado segura 10, proporcionando dentes ocos rosqueados (não
35

mostrados), em associação com as aberturas circulares (não mostradas) definidas por cada uma das três diferentes placas. Os parafusos 104 podem ser inseridos pelas aberturas circulares (não mostradas) e impulsionados nos dentes rosqueados (não mostrados). Esses parafusos 104 mantêm os blocos condutores correspondentes (por exemplo, os blocos condutores 52 e 92) em contato preciso. Se os parafusos 104 forem removidos, ou mesmo afrouxados, então os blocos condutores vão ser separados, provocando uma condição de circuito aberto.

O alojamento 102 compreende uma folha metálica dobrada com aberturas perfuradas. O alojamento 102 tem uma base 110, cobrindo a superfície voltada para fora 42 e definindo uma abertura (não mostrada), em associação com a chave de remoção (não mostrada) na superfície voltada para fora 42. Três lados 112, 114 e 116 são dobrados a partir da base 110, para proteger os lados do conjunto de placa de circuito integrado seguro 10. Um desses lados 116 define uma abertura de conector USB 118, em associação com o conector USB 20. Um quarto lado 120 é deixado aberto, para proporcionar acesso ao conector do painel de toque (não mostrado) e ao canal de nível dividido 66.

Vai-se fazer também agora referência à Figura 6, que é um diagrama esquemático de um dispositivo seguro 130 (na forma de uma ATM) incorporando a placa de circuito integrado segura 100 acoplada a um conjunto de visor sensível ao toque 140 pela sua superfície voltada para fora 42. O conjunto de visor sensível ao toque 140 compreende um visor 142 e um painel sensível ao toque transparente 144, em associação com e cobrindo o visor 142.

A placa de circuito integrado segura montada 100 é acoplada, elétrica e fisicamente, a um controlador 150 na ATM 130 pelo conector USB 20. A placa de circuito integrado segura montada 100 é também fixada fisicamente na ATM 130 por um cabo flexível de remoção 154, que é retido dentro de um grampo 156. O cabo flexível de remoção 154 inclui uma chave 160, que promove um circuito aberto quando liberado do grampo 156. Quando a chave 160 promove um circuito aberto, então esse é detectado pelo processador criptográfico 30. A placa de circuito integrado segura montada 100 é também conectada eletricamente ao painel sensível ao toque 144 por um cabo flexível de tela de toque 160.

Vai-se considerar então que a placa de circuito integrado segura montada 100 proporciona proteção contra ataques da sua superfície inferior (a superfície voltada para fora 42), da sua superfície superior 80 e dos seus lados.

SEGUNDA CONCRETIZAÇÃO

Outra concretização da presente invenção vai ser descrita a seguir com referência à Figura 7, que é uma vista detalhada de um conjunto de placa de circuito integrado seguro 200, de acordo com uma segunda concretização da presente invenção.

O conjunto de placa de circuito integrado seguro 200 compreende quatro placas

separadas, isto é: uma camada de placa de controle 212, uma primeira parte espaçadora 214, uma segunda parte espaçadora 215 e uma tampa segura 216. A placa de controle 212, as partes espaçadoras 214 e 215 e a tampa segura 216 são todas na forma de uma placa de circuito integrado impresso (pcb) multicamada. Cada uma das quatro placas define seis

5 aberturas 218, pelas quais parafusos (não mostrados) podem ser inseridos para montar as quatro placas em um alojamento (não mostrado), de uma maneira similar à primeira concretização.

De um modo similar à primeira concretização, a placa de controle 212 é dotada com um conector USB 220, um processador criptográfico 230, um controlador de painel sensível

10 ao toque 232 e vários outros componentes necessários ou desejáveis para implementar uma função de criptografia.

Cada uma das quatro placas 212, 214, 215 e 216 inclui trilhas condutoras e assemelhados para dirigir energia, potencial terra e sinais pelas placas. As quatro placas são conectadas por três conectores elastoméricos (não mostrados) na forma de tiras Zebra

15 (marca registrada).

O primeiro conector elastomérico (não mostrado) acopla uma tira linear 234 em uma superfície interna 240 da placa de controle 212 a uma tira linear 235 em uma superfície inferior 241 da segunda parte espaçadora 215.

O segundo conector elastomérico (não mostrado) acopla uma tira linear 236 em

20 uma superfície interna 240 da placa de controle 212 a uma tira linear 237 em uma superfície inferior 282 da tampa segura 216.

O terceiro conector elastomérico (não mostrado) acopla uma tira linear 238 em uma superfície superior 251 da primeira parte espaçadora 214 a uma tira linear 239 em uma superfície inferior 282 da tampa segura 216.

25 Esses três conectores elastoméricos acoplam mutuamente as quatro placas 212, 214, 215 e 216. Os conectores elastoméricos proporcionam uma conexão de contato, que se baseia no conector elastomérico sendo comprimido. Isso significa que se os parafusos (não mostrados) pelas aberturas 218 forem afrouxados, então os conectores elastoméricos não vão ficar mais em contato com as quatro placas, o que vai ser detectado pelo processador criptográfico 230, permitindo, desse modo, que o processador criptográfico 230 elimine

30 quaisquer informações seguras ou sensíveis, tais como as chaves de criptografia, armazenadas nele.

TERCEIRA CONCRETIZAÇÃO

Outra concretização da presente invenção vai ser descrita a seguir com referência à

35 Figura 8, que é uma vista detalhada de um conjunto de placa de circuito integrado seguro 300, de acordo com uma terceira concretização da presente invenção.

O conjunto de placa de circuito integrado seguro 300 compreende uma camada de

placa de controle 312 e uma tampa segura 316.

Em um modo similar às primeira e segunda concretizações, a placa de controle 312 é dotada com um conector USB 320, um processador criptográfico 330, um controlador de painel sensível ao toque 332 e vários outros componentes necessários ou desejáveis para
5 implementar uma função de criptografia.

Diferentemente das primeira e segunda concretizações, a placa de controle 312 define um grande recesso 333, que coopera com a tampa segura 316 para criar uma câmara segura, na qual o processador criptográfico 330 e o controlador de painel sensível ao toque 332 são alojados. O recesso 333 é definido por uma pluralidade de camadas inferiores 336
10 de placa de circuito integrado FR4, nessa concretização duas camadas (aproximadamente de uma espessura total de 1,6 mm), nas quais uma pluralidade de camadas mais altas 338, nessa concretização, seis camadas (aproximadamente de uma espessura total de 2,0 mm), é disposta na forma de um quadro em torno do perímetro das camadas inferiores 336. Desse modo, a altura total da placa de controle 312 é de aproximadamente 3,6 mm.

Uma tira linear 345 é localizada próxima ao centro da placa de controle 312, em associação com uma tira linear 346 montada em um lado inferior 382 da tampa segura 316, de modo que um conector elastomérico (não mostrado) pode acoplar a placa de controle 312 na tampa segura 316, quando a placa de controle 312 e a tampa segura 316 são retidas conjuntamente.

De uma maneira similar às primeira e segunda concretizações, as camadas inferior e superior 336 e 338 e a tampa segura 316 incluem as trilhas condutoras, que são conectadas ao processador criptográfico 300 e dirigidas pelo conector elastomérico (não mostrado). As trilhas condutoras podem ser dirigidas de uma camada para a seguinte por vias ocultas.

Vai-se então considerar que cada uma dessas três concretizações proporciona pelo menos uma câmara segura, na qual podem ser localizados os componentes seguros. Qualquer desmontagem das placas de circuito integrado vai provocar um ou mais circuitos abertos, que vão ser detectados por um componente seguro (o processador criptográfico), propiciando, desse modo, que o componente seguro elimine quaisquer informações sensíveis ou tome alguma ação protetora adequada.

Várias modificações podem ser feitas na concretização descrita acima dentro do âmbito da invenção, por exemplo, em outras concretizações, as voltagens, ou polaridades, usadas podem diferir daquelas descritas acima.

Em outras concretizações, as pcbs usada para a placa de controle, a parte ou partes espaçadoras, e a tampa segura podem compreender diferentes camadas daquelas descritas nas concretizações mencionadas acima. Por exemplo, nas concretizações similares à primeira concretização, a parte espaçadora 14 pode compreender mais ou menos de oito camadas. O número de camadas selecionadas pode depender dos requisitos de uma apli-
35

cação específica.

O conjunto de placa de circuito integrado seguro pode ser montado em um diferente alojamento daquele descrito acima.

5 Uma placa de circuito integrado segura montada pode ser incluída em um diferente terminal daquele descrito, ou a um diferente terminal de autoatendimento daquele descrito.

Em outras concretizações, os valores ou polaridades das voltagens usadas podem ser diferentes daqueles descritos acima. Por exemplo, em vez de uma voltagem positiva e um potencial terra, um potencial terra e uma voltagem negativa podem ser usados, ou uma voltagem negativa e uma positiva podem ser usadas.

10 Em outras concretizações, as trilhas condutoras podem incluir voltagem positiva e trilhas de potencial terra entretecidas na mesma camada.

As etapas dos métodos descritos no presente relatório descritivo podem ser conduzidas em qualquer ordem adequada, ou simultaneamente, quando adequado. Os métodos descritos no presente relatório descritivo podem ser conduzidos por software em forma legível por máquina em um meio de armazenamento tangível, ou como um sinal em propagação.

Os termos "compreendendo", "incluindo", "incorporando" e "tendo" são usados no presente relatório descritivo para relacionar uma lista sem fim de um ou mais elementos ou etapas, não uma lista fechada. Quando esses termos são usados, esses elementos ou etapas relacionados na lista não são exclusivos de outros elementos ou etapas, que podem ser adicionados à lista.

REIVINDICAÇÕES

1. Conjunto de placa de circuito integrado seguro, **CARACTERIZADO** pelo fato de que compreende:

- uma placa de controle incluindo um processador criptográfico;
- 5 uma parte espaçadora montada na placa de controle; e
- uma tampa montada na parte espaçadora, de modo que a placa de controle, a parte espaçadora e a tampa proporcionam coletivamente uma câmara fechada segura, na qual o processador criptográfico é montado.

2. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a parte espaçadora compreende uma placa de circuito integrado separada.

3. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a parte espaçadora compreende camadas adicionais na placa de controle.

15 4. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a parte espaçadora inclui camadas alternadas ligadas para formar uma rota condutora, de modo que qualquer brecha dessa rota é detectada pelo processador criptográfico.

20 5. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a parte espaçadora define uma pluralidade de aberturas, incluindo uma primeira abertura para proporcionar suporte para uma conector elastomérico, e uma segunda abertura para circundar o processador criptográfico.

25 6. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 5, **CARACTERIZADO** pelo fato de que a parte espaçadora define uma terceira abertura, para circundar um controlador de painel sensível ao toque, e uma quarta abertura alinhada com uma parte rebaixada, para definir uma rota de nível dividido para um conector flexível, para indicar a remoção do conjunto de placa de circuito integrado seguro.

30 7. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que um lado da parte espaçadora da placa de controle e um lado da placa de controle da parte espaçadora incluem ambos dois ou mais blocos, os blocos no lado da parte espaçadora da placa de controle ficando em associação com os blocos no lado da placa de controle da parte espaçadora, de modo que os blocos correspondentes ficam em contato quando a parte espaçadora é montada na placa de controle.

35 8. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a placa de controle inclui uma pluralidade de componentes circundando o processador criptográfico, a pluralidade de componentes incluindo resistores de baixo valor, de modo que qualquer ataque lateral, que danifica esses compo-

nentes, vai ser detectado pelo processador criptográfico.

9. Conjunto de placa de circuito integrado seguro, de acordo com a reivindicação 1, **CARACTERIZADO** pelo fato de que a parte espaçadora compreende uma pluralidade de camadas ligadas permanentemente à placa de controle.

5 10. Dispositivo seguro, **CARACTERIZADO** pelo fato de que inclui a placa de circuito integrado segura de acordo com a reivindicação 1.

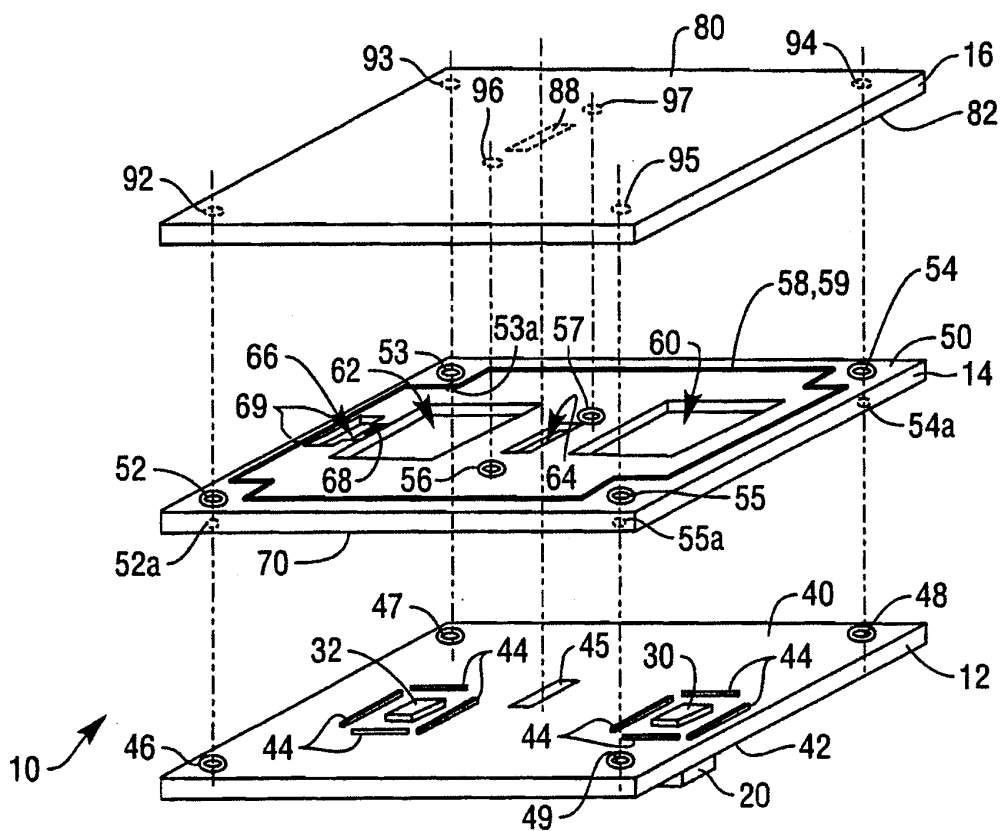
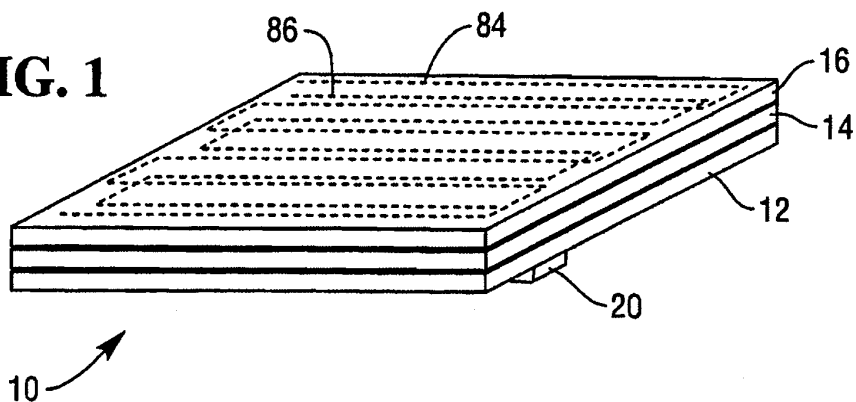
10 11. Dispositivo seguro, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o dispositivo seguro compreende ainda uma tira de remoção, acoplada à placa de circuito integrado segura, em uma extremidade, e tendo uma chave, em uma extremidade oposta, para fixação em um dispositivo hospedeiro, de modo que a chave mude de estado quando a tira de remoção é solta.

12. Dispositivo seguro, de acordo com a reivindicação 10, **CARACTERIZADO** pelo fato de que o dispositivo seguro compreende uma placa de circuito integrado segura montada em um alojamento.

15 13. Terminal de autoatendimento, **CARACTERIZADO** pelo fato de que inclui o dispositivo seguro de acordo com a reivindicação 10.

14. Terminal de autoatendimento, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o terminal de autoatendimento compreende ainda um dispensador de caixa.

20 15. Terminal de autoatendimento, de acordo com a reivindicação 13, **CARACTERIZADO** pelo fato de que o terminal de autoatendimento compreende ainda um painel sensível ao toque cobrindo um visor, para permitir que usuários introduzam um número de identificação pelo painel sensível ao toque.

FIG. 1**FIG. 2**

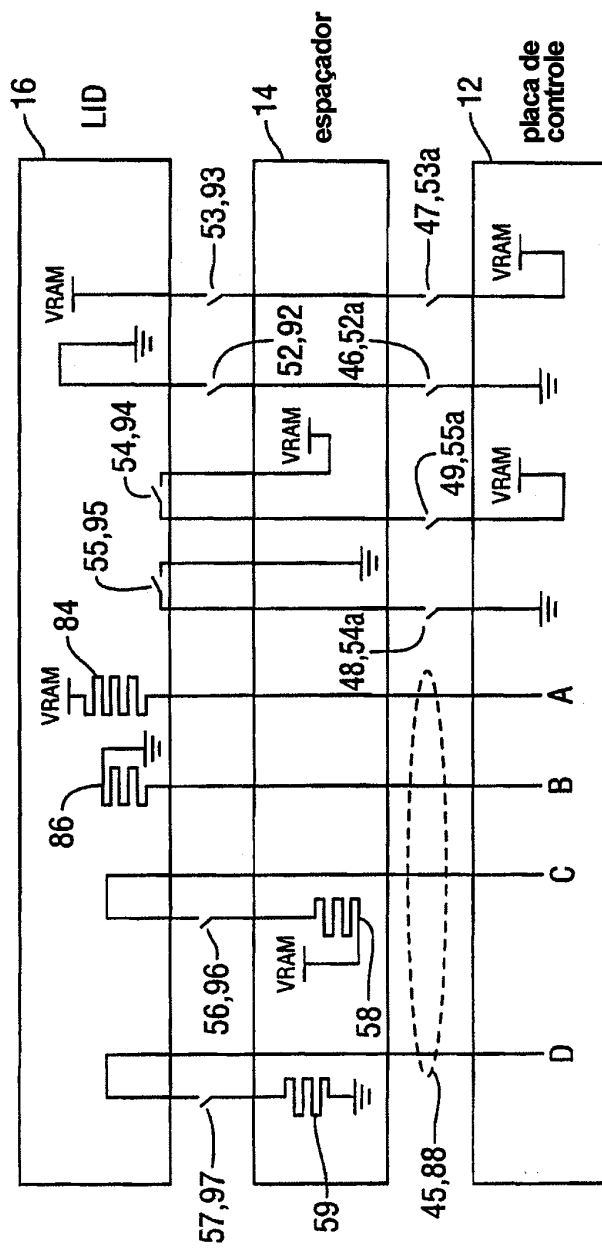


FIG. 3

FIG. 4A

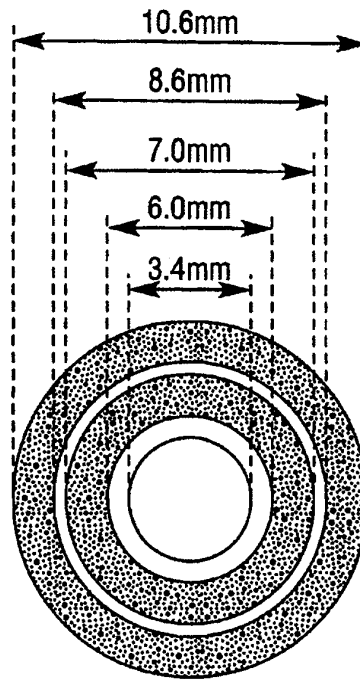


FIG. 4B



FIG. 4C

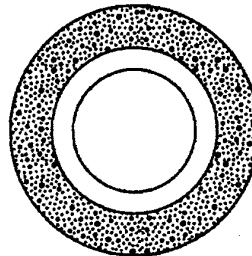
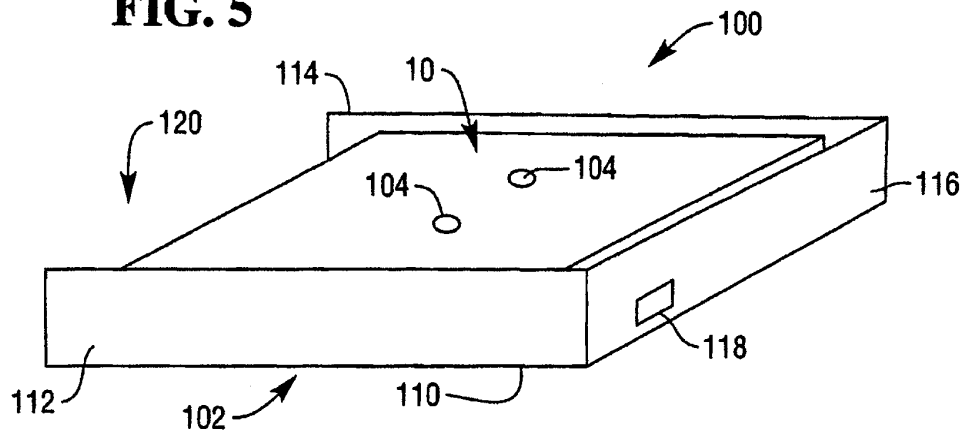
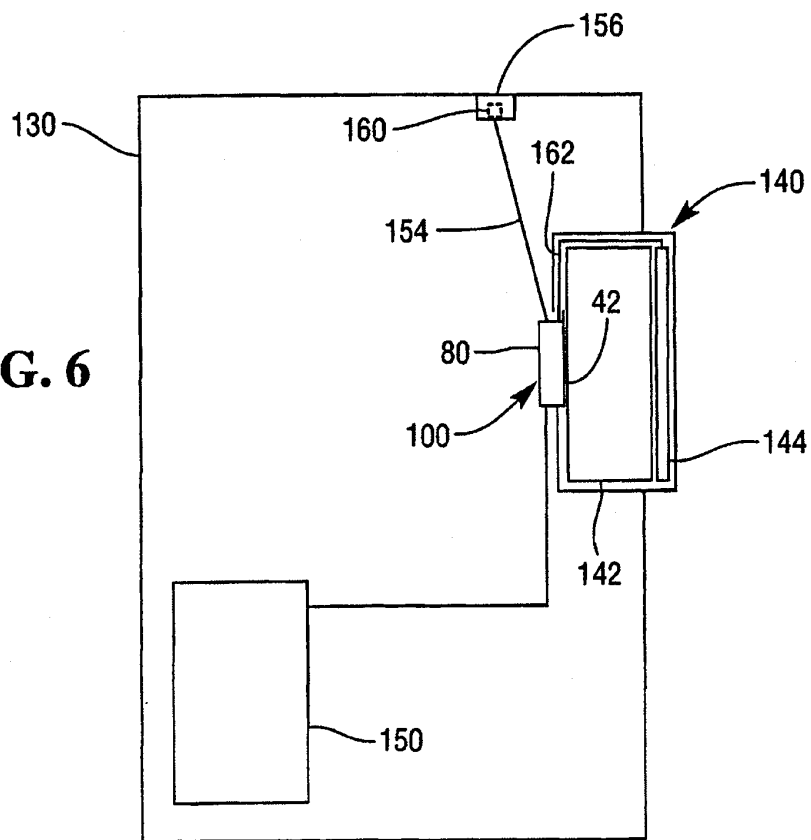


FIG. 5**FIG. 6**

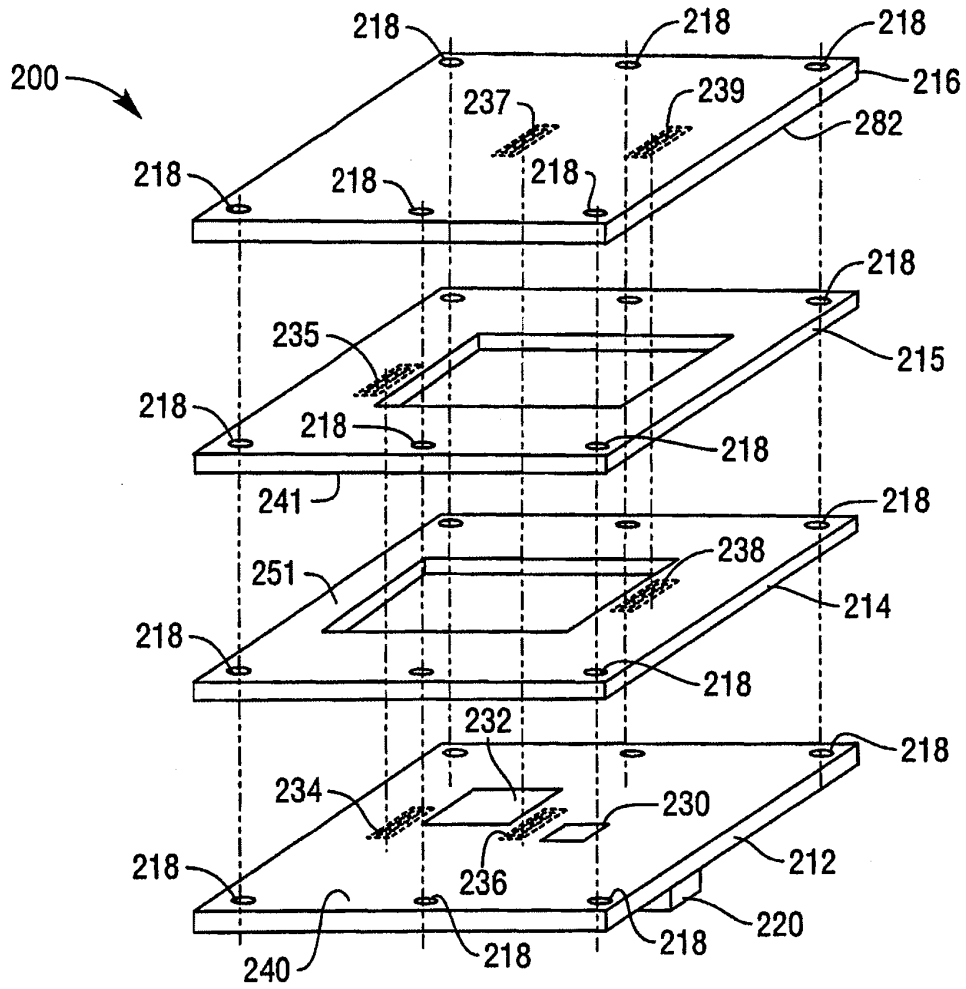
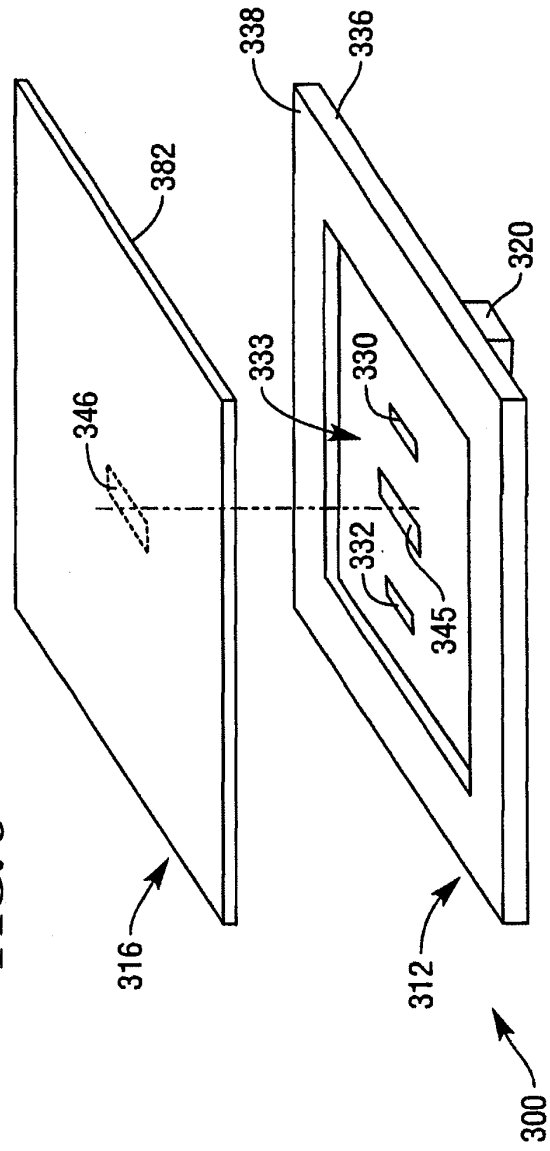


FIG. 7

FIG. 8



RESUMO

“CONJUNTO DE PLACA DE CIRCUITO INTEGRADO SEGURO”

Um conjunto de placa de circuito integrado seguro é proporcionado. O conjunto de placa de circuito integrado seguro compreende: uma placa de controle incluindo um processador criptográfico; uma parte espaçadora montada na placa de controle; e uma tampa montada na parte espaçadora. A placa de controle, a parte espaçadora e a tampa proporcionam coletivamente uma câmara fechada segura, na qual o processador criptográfico é montado. A parte espaçadora proporciona proteção contra ataques laterais ao processador criptográfico.