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

(21) **PI0611402-4 A2**

BRPI0611402A2

(22) Data de Depósito: 19/05/2006
(43) Data da Publicação: 08/09/2010
(RPI 2070)

(51) Int.Cl.:
G06F 7/72

(54) Título: **DETERMINAÇÃO DE UM INVERSO MODULAR**

(30) Prioridade Unionista: 25/05/2005 DE 10 2005 024 609.5

(73) Titular(es): SIEMENS VDO AUTOMOTIVE AG

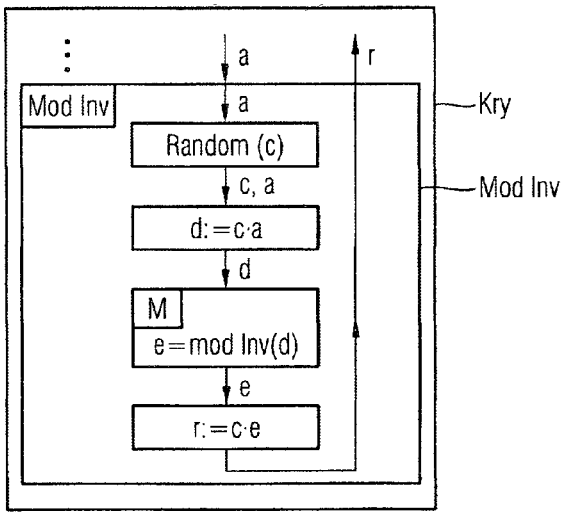
(72) Inventor(es): BERND MEYER

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

(86) Pedido Internacional: PCT EP2006062443 de 19/05/2006

(87) Publicação Internacional: WO 2006/125754de 30/11/2006

(57) Resumo: DETERMINAÇÃO DE UM INVERSO MODULAR. A presente invenção refere-se a métodos de decodificação de dados resistente ao ataque por canal secundário, segundo o qual um valor de retorno (r) é determinado como o inverso modular de um valor de entrada (a), por meio de um módulo (M). O objetivo da invenção é conseguir uma resistência ao ataque por canal secundário com as mínimas restrições na implementação ou determinação do inverso modular com a mínima complexidade técnica. Tal objetivo é atingido, segundo o qual, em uma primeira subetapa, um primeiro produto (d) do valor de entrada (a) e um número aleatório é gerado (c), em uma segunda subetapa, o inverso modular (e) do primeiro produto (d) é determinado por meio do módulo (M), em uma terceira subetapa, um segundo produto (b) do número aleatório (c) é determinado por meio do inverso modular (e) e em uma quarta subetapa, o valor de retorno (r) é igualado ao segundo produto(b).



Relatório Descritivo da Patente de Invenção para **"DETERMINAÇÃO DE UM INVERSO MODULAR".**

A presente invenção refere-se a um método para computação resistente ao ataque por canal secundário de um valor de retorno como um inverso modular de um valor de entrada usando um módulo.

Ataques por canal secundário são uma classe de métodos para criptanálise. Em contraste com os ataques prévios sobre aplicações criptográficas, um atacante nesse caso não tenta romper o algoritmo matemático abstrato básico, mas ao invés disso, ataca uma implementação específica de um método criptográfico. Para essa finalidade, o atacante usa variáveis medidas físicas facilmente acessíveis para a implementação real, tais como tempo de execução da computação, consumo de força e radiação eletromagnética do processador durante a computação ou o comportamento da implementação quando os erros são induzidos. Os valores medidos físicos de uma única computação podem ser analisados diretamente, por exemplo, usando a análise de força simples [SPA] ou um atacante grava os valores medidos de uma pluralidade de computações (por exemplo, usando um osciloscópio de armazenamento) e a seguir avalia os valores medidos estatisticamente, por exemplo, usando análise de força diferencial [DPA]. Os ataques por canal secundário são freqüentemente muito mais eficientes do que as técnicas de criptanálise convencionais e podem até mesmo romper métodos que são considerados como sendo seguros do ponto de vista dos algoritmos se a implementação desses algoritmos não é protegida contra os ataques por canal secundário. Medidas defensivas para impedir os ataques por canal secundário são particularmente importantes para cartões inteligentes e aplicações embutidas.

Os ataques por canal secundário já são tratados nas seguintes publicações: Kocher: Timing attacks on implementations of Diffie-Hellman, RSA, DSS and other systems, Crypto 1996, LNCS 1109, páginas 104-113, Springer; Kocher, Jaffe, Jun: Differential power analysis, Crypto 1999, LNCS 1666, páginas 388-397, Springer; Messerger, Dabbish, Sloan: Power analysis attacks of modular exponentiation in smartcards, CHES 1999, LNCS

1717, páginas 144-157, Springer.

Nesse contexto, Boneh, Demillo, Lipton: On the importance of checking cryptographic protocols for faults, Eurocrypt 1997, LNCS 1233, páginas 37-51, Springer, já refere-se à utilização da informação proveniente do consumo de força e proveniente da radiação eletromagnética do processador durante a computação ou o comportamento da implementação quando erros são induzidos.

Métodos matemáticos para a inversão são também encontrados em Menezes, van Oorschot, Vanstone: Handbook of applied cryptography, CRC-Press 1996.

Técnicas de mascarar para cripto métodos, particularmente para DES e AES, são também conhecidas de Goubin, Patarin: DES and differential power analysis, CHES 1999, LNCS 1717, páginas 158-172, Springer; Akkar, Giraud: An implementation of DES and AES, secure against some attacks, CHES 2001, LNCS 2162, páginas 309-318, Springer; Messerges: Securing the AES finalists against power analysis attacks, FSE 2000, LNCS 1978, páginas 150-164, Springer; Coron, Goubin: On boolean and arithmetic masking against differential power analysis, CHES 2000, LNCS 1965, páginas 213-237, Springer; Trichina, de Seta, Germani: Simplified adaptive multiplicative masking for AES and its securized implementation, CHES 2002, LNCS 2523, páginas 187-197, Springer; Golic, Tymen: Multiplicative masking and power analysis of AES, CHES 2002, LNCS 2523, páginas 198-212, Springer.

A geração das assinaturas digitais com base no padrão de assinatura digital é também um assunto de discussão em FIPS 186: Digital signature standard, Federal Information Processing Standards Publication 186, NIST 1997.

É um objetivo da invenção proteger a inversão modular de SPA e DPA, in particular. Muitos métodos criptográficos (particularmente método de chave pública) usam aritmética em corpos finitos. Uma etapa de computação importante usada nesse contexto é a computação das inversões modulares nos corpos finitos.

Métodos para a inversão modular geralmente envolvem algorit-

mos para calcular os maiores divisores comuns (algoritmo Euclidiano estendido ou suas variações, tal como o algoritmo de Stein da operação binária) ou usam o pequeno teorema de Fermat e, portanto, atribuem a inversão à exponenciação modular. Os algoritmos com base no cálculo de um maior divisor comum têm uma seqüência de operação altamente dependente dos dados: o número de operações de divisão pode ser usado para deduzir o número a ser invertido, por exemplo. No caso do algoritmo de Stein da operação binária, um é adicionado em um valor provisório para o cálculo do módulo do corpo se esse valor provisório é desigual. Se um atacante pode observar se essa adição é executada na iª etapa do algoritmo, ele pode descobrir o número a ser invertido bit por bit. Esses algoritmos, portanto, permitem que um atacante deduza facilmente o número que é para ser invertido a partir do tempo de execução, consumo de força ou radiação eletromagnética. Embora algoritmos baseados no pequeno teorema de Fermat tenham uma seqüência de operação constante, eles são muito mais lentos e, portanto, mais ineficientes.

As técnicas geralmente usadas para impedir os ataques por canal secundário tentam piorar a razão de sinal para ruído entre a informação a ser protegida e todos os outros sinais mensuráveis e, portanto, tornar a observação da informação secreta mais difícil ou usar técnicas de randomização a fim de remover a correlação entre a informação a ser protegida e os valores medidos. Métodos para tornar a observação da informação secreta mais difícil incluem, por meio de exemplo, evitar as ramificações dependentes de dados que são dependentes da informação que merece proteção, o uso de etapas de programa com um perfil corrente que tem pouca flutuação ou o uso de partes de programa cujo tempo de execução não é mais dependente dos dados de computação, execução de partes de programa aleatórias e/ou redundantes, etc. Essas medidas defensivas geralmente protegem contra ataques de SPA, mas têm a desvantagem que a implementação é submetida a restrições desvantajosas.

As técnicas de randomização para remover a correlação entre a informação que é para ser protegida e os valores medidos são usadas para

proteger contra os métodos de análise estatística de DPA. Tais medidas geralmente envolvem mascarar a informação secreta com valores aleatórios. Para cada novo cálculo, novos números aleatórios independentes são então escolhidos para as máscaras. Um atacante então mede um cálculo que ele vê como aleatório toda vez, porque ele não sabe a máscara e não pode estabelecer quaisquer correlações simples entre os valores físicos medidos e os dados de entrada ou saída.

Contra o antecedente dos problemas e as desvantagens da técnica anterior, a invenção é baseada no objetivo de prover um método para o cálculo do inverso modular que seja resistente aos ataques por canal secundário e ao mesmo tempo reprima as restrições para a implementação e a complexidade adicional com a finalidade de proteger contra ataques por canal secundário.

Para essa finalidade, a invenção propõe um método de acordo com a reivindicação 1. Além disso, um tacógrafo de acordo com a reivindicação 3 e um cartão de dados de acordo com a reivindicação 4 são propostos que são respectivamente em uma forma tal que eles operam usando o método da reivindicação 1. As subreivindicações respectivas com referência de volta contêm desenvolvimentos vantajosos.

A técnica inventiva permite quaisquer implementações de métodos para o cálculo de inversões modulares (incluindo os algoritmos muito eficientes com base no cálculo de um maior divisor comum) a serem protegidas contra SPA e DPA por uma transformação simples.

O uso de uma técnica de mascarar homomórfica aritmética com base na invenção tem, entre outras, a vantagem que a ação de mascarar pode ser executada no começo da computação e o resultado poderia ser desmascarado no fim e, ao mesmo tempo, a implementação para a inversão modular é protegida contra ataques de SPA e DPA.

Uma aplicação vantajosa da invenção para um método de criptografia ou decriptografia, particularmente em um tacógrafo inventivo ou um meio de armazenamento de dados móvel inventivo é a inversão necessária quando gerando as assinaturas digitais com base no padrão de assinatura

digital DSA, por exemplo:

Deixe p ser um número primário, q | p-1 ser um número primário, 0 < g < p ser um gerador para o subgrupo cíclico da ordem q em (Z/pZ)*, 0 < a < q ser uma chave secreta, A = g^a mod p ser a chave pública associada e 0 <= m < p ser a mensagem a ser assinada. Para calcular a assinatura (r, s) para a mensagem m e a chave pública A, as seguintes etapas de computação são executadas pela unidade de computação em linha com a DSA:

1) seleção de um número aleatório 0 < k < q que precisa ser mantido secreto

2) cálculo de r = (a^k mod p) mod q

3) cálculo da inversão modular h = 1/k mod q usando um módulo M

4) cálculo de s = h*(m+a*r) mod q

O cálculo da inversão modular na etapa 3) pode ser particularmente protegido de maneira vantajosa contra SPA de acordo com a invenção, de modo que o número aleatório secreto k, que é conhecido como a chave efêmera, não se torna conhecido para o atacante. Se um atacante descobre a chave efêmera k, ele poderia calcular a chave secreta a da pessoa criando essa assinatura.

O módulo inventivo M, que tem uma implementação para calcular os inversos modulares em um corpo finito K, pode determinar o inverso modular no modo resistente ao canal secundário a partir de um elemento a pertencente ao corpo finito K, por exemplo. Nesse contexto, o método inventivo funciona usando as seguintes etapas, por exemplo:

1) a unidade de computação seleciona um elemento aleatório c de K

2) a unidade de computação determina d = a*c

3) o módulo M determina o inverso e = M(d)

4) a unidade de computação determina b = e*c

5) a unidade de computação estabelece o valor de retorno r :=b

Na etapa 3), um atacante observa apenas a inversão de um elemento de corpo aleatório d que é escolhido com uma distribuição uniforme e que é independente da entrada real a para o cálculo. Desde que ele não conhece o elemento aleatoriamente selecionado c, nem os ataques de SPA

nem de DAP o mune com qualquer informação das etapas de computação executadas por M.

Uma outra vantagem do método é que uma implementação desprotegida precisa ser estendida, em linha com a invenção, somente pelas etapas 1), 2), 4) e 5) a fim de obter resistência contra SPA e DPA. Em particular, os métodos eficientes para calcular os inversos modulares podem ser usados na base do algoritmo Euclidiano sem mudanças. Nesse caso, a complexidade de computação adicional é muito menor do que no caso de métodos para inversão que envolvem o pequeno teorema de Fermat.

Um desenvolvimento conveniente do método inventivo proporciona os resultados provisórios c, d e e a serem apagados depois das respectivas etapas de computação.

O texto abaixo explica a invenção em mais detalhes usando uma modalidade exemplar específica com relação aos desenhos, a invenção não sendo limitada às ilustrações nesse exemplo. Nos desenhos:

a figura 1 mostra uma ilustração em perspectiva esquemática de um tacógrafo inventivo com um cartão de dados inventivo,

a figura 2 mostra uma ilustração esquemática da seqüência de operação com base no método inventivo.

A figura 1 mostra um tacógrafo inventivo DTCO e um cartão de dados inventivo DC. O cartão de dados DC pode ser inserido no DTCO através de uma das duas fendas de recepção 2, de modo que durante a transmissão dos dados entre os dois elementos, o cartão de dados DC é mantido no tacógrafo DTCO de modo que ele fica inacessível do exterior. Na sua parte frontal 3, próximo das duas fendas de recepção 2, o tacógrafo DTCO tem uma unidade de exibição 1 e elementos de controle do operador 4. Seguinte à inserção em uma fenda de recepção 2, o cartão de dados DC é conectado em um processador central CPU por meio de linhas de dados 5, o dito processador central tendo acesso a uma memória interna MEM. O cartão de dados, da mesma forma, tem uma memória interna (não mostrada em detalhes) e um processador central.

A transmissão de dados entre o tacógrafo DTCO e o cartão de

dados DC é executada com criptografia por meio de uma chave de sessão, com os processadores centrais CPU no tacógrafo DTCO e no cartão de dados DC determinando um inverso modular de um valor de entrada A, entre outras coisas, durante a criptografia e a decriptografia. Para esta finalidade, os processadores CPU fazem uso do módulo KRY mostrado na figura 2.

O módulo KRY é parte de uma seqüência para a criptografia. O valor de entrada a é transferido para o módulo KRY e é enviado para o módulo Mod Inv dentro deste módulo. O módulo Mod Inv, em primeiro lugar, determina um número aleatório C e multiplica esse número pelo valor de entrada a para obter um produto d. O módulo M é usado para determinar o inverso modular e do produto d e a seguir para multiplicá-lo pelo número aleatório c. Um valor de retorno r é igualado com esse produto e é retornado para o módulo KRY como o resultado.

REIVINDICAÇÕES

1. Método para criptografia e/ou decriptografia de dados resistente ao ataque por canal secundário usando uma unidade de computação, onde a etapa de criptografia e/ou decriptografia envolve determinar um valor de retorno (r) como o inverso modular de um valor de entrada (a) usando um módulo (M), caracterizado em que

- uma primeira subetapa envolve produzir um primeiro produto (d) a partir do valor de entrada (a) e um número aleatório (c),

- uma segunda subetapa envolve o módulo (M) determinar o inverso modular (e) do primeiro produto (d),

- uma terceira subetapa envolve determinar um segundo produto (b) a partir do número aleatório (c) e do inverso modular (e),

- uma quarta subetapa envolve igualar o valor de retorno (r) com o segundo produto (b).

2. Método de acordo com a reivindicação 1 ou 2, caracterizado em que o número aleatório (c), o primeiro produto (d), o segundo produto (b) e o inverso modular (e) são apagados seguinte a determinação do valor de retorno (r).

3. Tacógrafo tendo uma unidade de computação, onde a unidade de computação criptografa e/ou decriptografa os dados e fica em uma forma tal que a etapa de criptografia e/ou decriptografia envolve determinar um valor de retorno (r) como o inverso modular de um valor de entrada (a) usando um módulo (M) da unidade de computação, caracterizado em que a unidade de computação

- usa uma primeira subetapa para produzir um primeiro produto (d) a partir do valor de entrada (a) e de um número aleatório (c),

- usa uma segunda subetapa para o módulo (M) determinar o inverso modular (e) do primeiro produto (d),

- usa uma terceira subetapa para a unidade de computação determinar um segundo produto (b) a partir do número aleatório (c) e do inverso modular (e),

- usa uma quarta subetapa para a unidade de computação igualar o valor de retorno (r) com o segundo produto (b).

4. Meio de armazenamento de dados móvel, particularmente um meio de armazenamento de dados na forma de um cartão de dados, tendo uma unidade de computação, onde a unidade de computação criptografa e/ou decriptografa os dados e é em uma forma tal que a etapa de criptografia e/ou decriptografia é usada para determinar um valor de retorno (r) como o inverso modular de um valor de entrada (a) usando um módulo (M) da unidade de computação, caracterizado em que a unidade de computação

- usa uma primeira subetapa para produzir um primeiro produto (d) a partir do valor de entrada (a) e de um número aleatório (c),

- usa uma segunda subetapa para o módulo (M) determinar o inverso modular (e) do primeiro produto (d),

- usa uma terceira subetapa para a unidade de computação determinar um segundo produto (b) a partir do número aleatório (c) e do inverso modular (e),

- usa uma quarta subetapa para a unidade de computação igualar o valor de retorno (r) com o segundo produto (b).

FIG 1

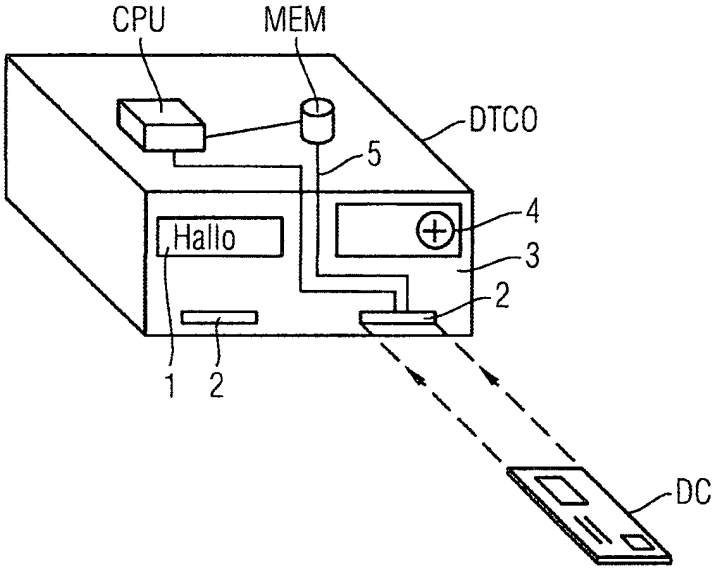
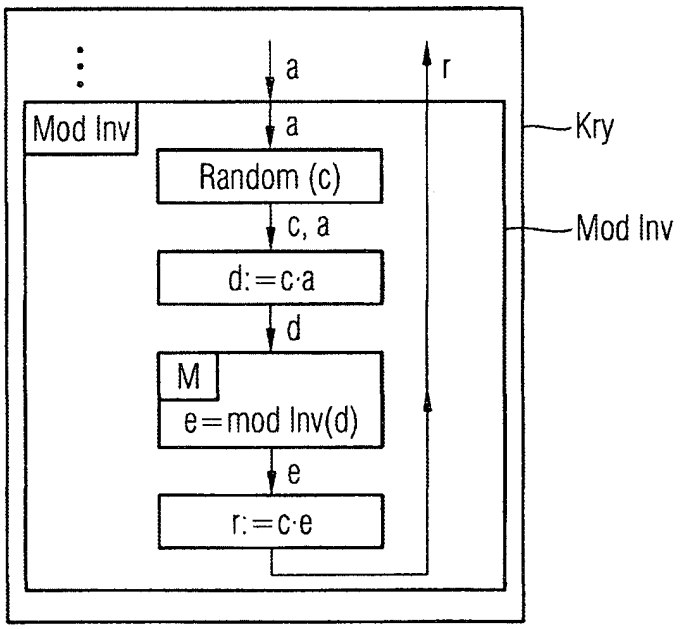

CPU
MEM
DTCO
5
4
Hallo
3
2
1
2
DC

FIG 2


a
r
Mod Inv
a
Random (c)
c, a
d:=c·a
d
M
e=mod Inv(d)
e
r:=c·e
Kry
Mod Inv

PI0611402-4

RESUMO

Patente de Invenção: **"DETERMINAÇÃO DE UM INVERSO MODULAR".**

A presente invenção refere-se a métodos de decodificação de dados resistente ao ataque por canal secundário, segundo o qual um valor de retorno (r) é determinado como o inverso modular de um valor de entrada (a), por meio de um módulo (M). O objetivo da invenção é conseguir uma resistência ao ataque por canal secundário com as mínimas restrições na implementação ou determinação do inverso modular com a mínima complexidade técnica. Tal objetivo é atingido, segundo o qual, em uma primeira subetapa, um primeiro produto (d) do valor de entrada (a) e um número aleatório é gerado (c), em uma segunda subetapa, o inverso modular (e) do primeiro produto (d) é determinado por meio do módulo (M), em uma terceira subetapa, um segundo produto (b) do número aleatório (c) é determinado por meio do inverso modular (e) e em uma quarta subetapa, o valor de retorno (r) é igualado ao segundo produto(b).

Novo quadro reivindicatório (total de 5 reivindicações), incorporando as emendas às reivindicações conforme Relatório de Exame Preliminar.

REIVINDICAÇÕES

1. Método para criptografia e/ou decriptografia de dados resistente ao ataque por canal secundário usando uma unidade de computação, onde a etapa de criptografia e/ou decriptografia envolve determinar um valor de retorno (r) como o inverso modular de um valor de entrada (a) usando um módulo (M), caracterizado em que

- uma primeira subetapa envolve selecionar um número aleatório (c),

- uma segunda subetapa envolver produzir um primeiro produto (d) a partir do valor de entrada (a) e do número aleatório (c),

- uma terceira subetapa envolve o módulo (M) determinar o inverso modular (e) do primeiro produto (d), implementando um algoritmo para calcular o inverso modular (e) sem proteção contra um ataque por canal secundário,

- uma quarta subetapa envolve determinar um segundo produto (b) a partir do número aleatório (c) e do inverso modular (e),

- uma quinta subetapa envolve igualar o valor de retorno (r) com o segundo produto (b).

2. Método como reivindicado na reivindicação 1, caracterizado em que o número aleatório (c), o primeiro produto (d), o segundo produto (b) e o inverso modular (e) são apagados seguinte a determinação do valor de retorno (r).

3. Método como reivindicado na reivindicação 1 ou 2, caracterizado em que a implementação desprotegida é baseada no algoritmo Euclidiano.

4. Tacógrafo (DTCO) tendo uma unidade de computação, onde a unidade de computação criptografa e/ou decriptografa os dados e fica em uma forma tal que a etapa de criptografia e/ou decriptografia envolve determinar.

um valor de retorno (r) como o inverso modular de um valor de entrada (a) usando um módulo (M) da unidade de computação, caracterizado em que a unidade de computação é configurada para

- usar uma primeira subetapa para selecionar um número aleatório (c),

- usar uma segunda subetapa para produzir um primeiro produto

(d) a partir do valor de entrada (a) e do número aleatório (c),

- usar uma terceira subetapa para usar o módulo (M) para determinar o inverso modular (e) do primeiro produto (d), implementando um algoritmo para calcular o inverso modular (e) sem proteção contra um ataque por canal secundário,

- usar uma quarta subetapa para determinar um segundo produto (b) a partir do número aleatório (c) e do inverso modular (e),

- usar uma quinta subetapa para igualar o valor de retorno (r) com o segundo produto (b).

5. Meio de armazenamento de dados móvel, particularmente um meio de armazenamento de dados na forma de um cartão de dados, tendo uma unidade de computação, onde a unidade de computação criptografa e/ou decriptografa os dados e é em uma forma tal que a etapa de criptografia e/ou decriptografia é usada para determinar um valor de retorno (r) como o inverso modular de um valor de entrada (a) usando um módulo (M) da unidade de computação, caracterizado em que a unidade de computação é configurada para

- usar uma primeira subetapa para selecionar um número aleatório (c),

- usar uma segunda subetapa para produzir um primeiro produto (d) a partir do valor de entrada (a) e do número aleatório (c),

- usar uma terceira subetapa para usar o módulo (M) para determinar o inverso modular (e) do primeiro produto (d), implementando um algoritmo para calcular o inverso modular (e) sem proteção contra um ataque por canal secundário,

- usar uma quarta subetapa para determinar um segundo produto (b) a partir do número aleatório (c) e do inverso modular (e),

- usar uma quinta subetapa para igualar o valor de retorno (r) com o segundo produto (b).

definindo a passagem de encaixe (156, 222, 332) se estendendo através do alojamento de encaixe;

o corpo de encaixe (318, 318', 522) recebido dentro da passagem de encaixe (156, 222, 332) do alojamento de encaixe de modo que o flange (148, 322, 322', 524, 608) engata de forma adjacente ao alojamento de encaixe e o primeiro membro de vedação é posicionado de forma compressiva entre o corpo de encaixe (318, 318', 522) e a primeira parede interna (154, 330) do alojamento de encaixe.

3. Montagem de mola pneumática, de acordo com a reivindicação 2, **caracterizada pelo fato de que** os primeiro e segundo membros de retenção incluem uma projeção (354, 636) que se estende para fora disposta ao longo da segunda extremidade dos mesmos, as projeções engatando a segunda parede de extremidade do alojamento de encaixe para reter o encaixe de conector (312, 406, 504, 600) no mesmo.

4. Montagem de mola pneumática, de acordo com a reivindicação 1, **caracterizada pelo fato de que** o corpo de encaixe (318, 318', 522) se estende longitudinalmente entre as primeira e segunda extremidades opostas, o corpo de encaixe (318, 318', 522) incluindo uma primeira porção do corpo que se estende longitudinalmente na direção da primeira extremidade tendo uma primeira dimensão de seção transversal e uma segunda porção que se estende longitudinalmente na direção da segunda extremidade tendo uma segunda dimensão de seção transversal que é menor do que a primeira dimensão de seção transversal.

5. Montagem de mola pneumática, de acordo com a reivindicação 4, **caracterizada pelo fato de que** o primeiro membro inclui uma parede de passagem (512) pelo menos parcialmente definindo a passagem de encaixe (156, 222, 332), a parede de passagem (512) incluindo uma primeira porção de parede complementar a primeira dimensão de seção transversal e adaptada para receber a primeira porção do corpo que se estende longitudinalmente do corpo de encaixe (318, 318', 522), e a parede de passagem (512) incluindo uma segunda porção de parede complementar a segunda dimensão de seção transversal e adaptada para receber a segunda porção

do corpo que se estende longitudinalmente do corpo de encaixe (318, 318', 522).

6. Montagem de mola pneumática (100, 300, 400, 500) **caracterizada pelo fato de que** compreende:

um primeiro membro de extremidade (102, 302) incluindo um primeiro lado, um segundo lado oposto e uma abertura (122, 310, 410) se estende através do mesmo;

um segundo membro de extremidade (104, 304) disposto em relação espaçada ao primeiro membro de extremidade (102, 302) e em relação de frente ao primeiro lado do mesmo de modo que um eixo que se estende longitudinalmente é formado entre eles;

uma parede flexível (106, 306) presa entre os primeiro e segundo membros de extremidade e pelo menos parcialmente definindo uma câmara de mola entre o primeiro lado do primeiro membro de extremidade (102, 302) e o segundo membro de extremidade (104, 304); e

um encaixe de conector (312, 406, 504, 600) pelo menos parcialmente recebido dentro da abertura (122, 310, 410) e em comunicação fluida com a câmara de mola, o encaixe de conector (312, 406, 504, 600) incluindo:

um corpo de encaixe (318, 318', 522) que se estende longitudinalmente entre as primeira e segunda extremidades opostas;

primeiro e segundo membros de retenção que se estendem longitudinalmente ao longo do corpo de encaixe (318, 318', 522) em relação espaçada radialmente para fora de modo que uma brecha (632) é formada entre o corpo de encaixe (318, 318', 522) e os primeiro e segundo membros de retenção, os primeiro e segundo membros de retenção incluindo uma extremidade fixa (350, 536, 630) e uma extremidade livre (352, 538, 634) oposta, a extremidade fixa (350, 536, 630) conectada operativamente ao corpo de encaixe (318, 318', 522) através da primeira extremidade do mesmo, e a extremidade livre (352, 538, 634) sendo capaz de deflexão resiliente na direção do corpo de encaixe (318, 318', 522) e incluindo uma projeção que se estende para fora radialmente adaptada para inter-engatar o primeiro mem-

bro de extremidade (102, 302); e

um flange (148, 322, 322', 524, 608) que se estende para fora radialmente formado em pelo menos um dentre os corpo de encaixe (318, 318', 522), primeiro membro de retenção e segundo membro de retenção, o flange (148, 322, 322', 524, 608) sendo disposto uma posição longitudinal intermediária entre a extremidade fixa (350, 536, 630) e a extremidade livre (352, 538, 634) dos primeiro e segundo membros de retenção de modo que uma porção de retenção (638) que se estende longitudinalmente do encaixe de conector (312, 406, 504, 600) é formada entre o flange (148, 322, 322', 524, 608) e a projeção e de modo que uma porção externa do encaixe de conector (312, 406, 504, 600) é formada longitudinalmente para fora do flange (148, 322, 322', 524, 608) na direção da primeira extremidade do corpo de encaixe (318, 318', 522); e,

um membro de vedação disposto vedativemente entre o encaixe de conector (312, 406, 504, 600) e o primeiro membro de extremidade (102, 302);

o encaixe de conector (312, 406, 504, 600) inter-engatando o primeiro membro de extremidade (102, 302) de modo que a porção de retenção (638) está pelo menos parcialmente disposta entre os primeiro e segundo lados do primeiro membro de extremidade (102, 302) e a porção externa é disposta para fora do primeiro membro de extremidade (102, 302) de forma oposta à câmara de mola de modo que uma força radial para dentro pode ser aplicada aos primeiro e segundo membros e retenção ao longo da porção externa para deslocar radialmente para dentro as extremidades livres para remover de forma seletiva o encaixe de conector (312, 406, 504, 600) do primeiro membro de extremidade (102, 302).

7. Montagem de mola pneumática, de acordo com a reivindicação 6, **caracterizada pelo fato de que** a extremidade livre (352, 538, 634) dos primeiro e segundo membros de retenção é espaçada longitudinalmente para dentro da segunda extremidade do corpo de encaixe (318, 318', 522) de modo que uma primeira porção do corpo de encaixe (318, 318', 522) ao longo da segunda extremidade do mesmo se estende longitudinalmente para

fora além da extremidade livre (352, 538, 634) em uma direção geralmente oposta do flange (148, 322, 322', 524, 608), o membro de vedação é posicionado ao longo da primeira porção do corpo de encaixe (318, 318', 522).

8. Montagem de mola pneumática, de acordo com a reivindicação 7, **caracterizada pelo fato de que** um entre o primeiro membro de extremidade (102, 302) e a primeira porção do corpo de encaixe (318, 318', 522) inclui uma ranhura adaptada para receber o membro de vedação.

9. Montagem de mola pneumática, de acordo com a reivindicação 7, **caracterizada pelo fato de que** o corpo de encaixe (318, 318', 522) inclui uma primeira porção se estendendo longitudinalmente na direção da primeira extremidade com uma primeira dimensão de seção transversal e inclui uma segunda porção se estendendo longitudinalmente na direção da segunda extremidade com uma segunda dimensão de seção transversal que é menor do que a primeira dimensão de seção transversal.

10. Montagem de mola pneumática, de acordo com a reivindicação 9, **caracterizada pelo fato de que** o primeiro membro de extremidade (102, 302) inclui uma parede de abertura (120, 408) pelo menos parcialmente definindo a abertura (122, 310, 410) se estendendo através do primeiro membro de extremidade (102, 302), a parede de abertura (120, 408) incluindo uma primeira porção de parede e uma segunda porção de parede dispostas longitudinalmente para dentro a partir da primeira porção de parede na direção do primeiro lado do primeiro membro de extremidade (102, 302), a primeira porção de parede pelo menos parcialmente definindo uma primeira seção da abertura que tem uma primeira dimensão de seção transversal complementar a primeira dimensão de seção transversal do corpo de encaixe (318, 318', 522), a segunda porção de parede pelo menos parcialmente definindo uma segunda seção da abertura que tem uma segunda dimensão de seção transversal complementar a segunda dimensão de seção transversal do corpo de encaixe (318, 318', 522).

11. Montagem de mola pneumática, de acordo com a reivindicação 6, **caracterizada pelo fato de que** o primeiro membro de extremidade (102, 302) inclui um alojamento de encaixe suportado no mesmo e o aloja-

mento de encaixe inclui um primeiro lado, o segundo lado oposto e pelo menos uma porção da abertura se estende através do primeiro membro de extremidade (102, 302), o encaixe de conector (312, 406, 504, 600) interengatando o alojamento de encaixe do primeiro membro de extremidade (102, 302).

12. Montagem de mola pneumática, de acordo com a reivindicação 11, **caracterizada pelo fato de que** o alojamento de encaixe é pelo menos parcialmente seguro no primeiro lado do primeiro membro de extremidade (102, 302) de modo que o alojamento de encaixe é pelo menos parcialmente disposto dentro da câmara de mola.

13. Montagem de mola pneumática, de acordo com a reivindicação 6, **caracterizada pelo fato de que** o membro de vedação é um primeiro membro de vedação, o corpo de encaixe (318, 318', 522) inclui uma parede interna (154, 330) pelo menos parcialmente definindo uma passagem de encaixe (156, 222, 332) formada através do corpo de encaixe (318, 318', 522), e o encaixe de conector (312, 406, 504, 600) inclui ainda:

um colar de retenção recebido na passagem de encaixe (156, 222, 332) e adaptado para engatar uma superfície externa associada da linha de fluido associada;

uma luva de suporte interna (166, 334) recebida na passagem de encaixe (156, 222, 332) adjacente ao colar de retenção e adaptada para engatar uma superfície interna associada com a linha de fluido; e

um segundo membro de vedação disposto dentro da passagem de encaixe (156, 222, 332) e adaptado para engatar de forma compressiva o corpo de encaixe (318, 318', 522) e a superfície externa associada da linha de fluido associada.

14. Montagem de mola pneumática, de acordo com a reivindicação 6, **caracterizada pelo fato de que** pelo menos a porção de retenção (638) se estendendo longitudinalmente do encaixe de conector (312, 406, 504, 600) tem uma forma aproximadamente circular de seção transversal com pelo menos uma porção do corpo de encaixe (318, 318', 522), o primeiro membro de retenção e o segundo membro de retenção definindo a forma

aproximadamente circular de seção transversal, o corpo de encaixe (318, 318', 522) incluindo primeiro e segundo planos se estendendo longitudinalmente ao longo dos mesmos adjacente aos primeiro e segundo membros de retenção de modo que os primeiro e segundo planos pelo menos parcialmente definem as brechas ente o corpo de encaixe (318, 318', 522) e os primeiro e segundo membros de retenção.

15. Montagem de mola pneumática (100, 300, 400, 500) **caracterizada pelo fato de que** compreende:

um primeiro membro de extremidade (102, 302) que inclui um primeiro lado, um segundo lado oposto e uma abertura (122, 310, 410) que se estende através do mesmo;

um segundo membro de extremidade (104, 304) disposto em relação espaçada ao primeiro membro de extremidade (102, 302) e em relação de frente ao primeiro lado do mesmo de modo que um eixo que se estende longitudinalmente é formado entre eles;

uma parede flexível (106, 306) presa entre os primeiro e segundo membros de extremidade e pelo menos parcialmente definindo uma câmara de mola entre o primeiro lado do primeiro membro de extremidade (102, 302) e o segundo membro de extremidade (104, 304); e

um encaixe de conector (312, 406, 504, 600) pelo menos parcialmente recebido dentro da abertura (122, 310, 410) e em comunicação fluida com a câmara de mola, o encaixe de conector (312, 406, 504, 600) incluindo:

um corpo de encaixe (318, 318', 522) que se estende longitudinalmente entre as primeira e segunda extremidades opostas;

primeiro e segundo membros de retenção que se estendem longitudinalmente a partir do corpo de encaixe (318, 318', 522), os primeiro e segundo membros de retenção incluindo uma extremidade fixa (350, 536, 630) e uma extremidade livre (352, 538, 634) oposta, a extremidade fixa (350, 536, 630) conectada de forma operativa ao corpo de encaixe (318, 318', 522), a extremidade livre (352, 538, 634) sendo capaz de deflexão resiliente e incluindo uma projeção que se estende longitudinalmente para fora

adaptada para inter-engatar o primeiro membro de extremidade (102, 302), a extremidade livre (352, 538, 634) espaçada longitudinalmente para dentro da segunda do corpo de encaixe (318, 318', 522) de modo que uma porção do corpo de encaixe (318, 318', 522) ao longo da segunda extremidade do mesmo se estende longitudinalmente para fora mais distante da extremidade livre (352, 538, 634); e

um flange (148, 322, 322', 524, 608) que se estende para fora radialmente formado no corpo de encaixe (318, 318', 522) e disposto em uma relação espaçada longitudinalmente da extremidade livre (352, 538, 634) e do segundo membro de retenção de modo que uma porção de retenção (638) se estendendo longitudinalmente do encaixe de conector (312, 406, 504, 600) é formada entre o flange (148, 322, 322', 524, 608) e a projeção; e

um membro de vedação disposto vedativemente entre o encaixe de conector (312, 406, 504, 600) e o primeiro membro de extremidade (102, 302), o conector de vedação posicionado em relação longitudinalmente espaçada à extremidade livre (352, 538, 634) dos primeiro e segundo membros de retenção em uma direção geralmente oposta ao flange (148, 322, 322', 524, 608).

16. Montagem de mola pneumática, de acordo com a reivindicação 15, **caracterizada pelo fato de que** o primeiro membro de extremidade (102, 302) inclui uma parede de abertura (120, 408) pelo menos parcialmente definindo a abertura (122, 310, 410) estendendo através do primeiro membro de extremidade (102, 302), a parede de abertura (120, 408) incluindo uma primeira porção de parede, e uma segunda porção de parede disposta longitudinalmente para dentro da primeira porção da parede na direção do primeiro lado do primeiro membro de extremidade (102, 302), a primeira porção da parede adaptada para receber e inter-engatar o encaixe de conector (312, 406, 504, 600) no primeiro membro de extremidade (102, 302), e a segunda porção da parede adaptada para receber e engatar de forma vedativa a segunda extremidade do encaixe de conector (312, 406, 504, 600) .

17. Montagem de mola pneumática, de acordo com a reivindicação 16, **caracterizada pelo fato de que** a primeira porção da parede pelo menos parcialmente define uma primeira seção da abertura que tem uma primeira dimensão de seção transversal e a segunda porção de parede pelo menos parcialmente define uma segunda seção da abertura que tem uma segunda dimensão de seção transversal com a primeira dimensão de seção transversal sendo maior do que a segunda dimensão de seção transversal.

18. Montagem de mola pneumática, de acordo com a reivindicação 17, **caracterizada pelo fato de que** a primeira extremidade do corpo de encaixe (318, 318', 522) tem uma primeira dimensão de seção transversal que é complementar a primeira dimensão de seção transversal da primeira seção da abertura, e a segunda abertura do corpo de encaixe (318, 318', 522) tem uma segunda dimensão de seção transversal que é menor do que a primeira dimensão de seção transversal do corpo de encaixe (318, 318', 522) e é complementar a segunda dimensão da seção transversal da segunda seção da abertura.

19. Montagem de mola pneumática, de acordo com a reivindicação 16, **caracterizada pelo fato de que** a parede de abertura (120, 408) inclui uma ranhura que se estende radialmente para fora formada dentro do primeiro membro de extremidade (102, 302) entre as primeira e segunda porções de parede, a ranhura definindo uma parede de ressalto se estendendo aproximadamente de forma lateral para fora a partir de ao longo da primeira porção de parede.

20. Montagem de mola pneumática, de acordo com a reivindicação 19, **caracterizada pelo fato de que** o encaixe de conector (312, 406, 504, 600) é recebido na abertura (122, 310, 410) de modo que o flange (148, 322, 322', 524, 608) é disposto de forma adjacente ao segundo lado do primeiro membro de extremidade (102, 302) e a projeção nos primeiro e segundo membros de retenção operativamente inter-engatar a parede de ressalto para deste modo reter o encaixe de conector (312, 406, 504, 600) no primeiro membro de extremidade (102, 302).

21. Montagem de mola pneumática, de acordo com a reivindica-

ção 15, **caracterizada pelo fato de que** a segunda extremidade do corpo de encaixe (318, 318', 522) inclui uma ranhura se estendendo radialmente para fora e o membro de vedação é pelo menos parcialmente recebido dentro da ranhura.

22. Montagem de mola pneumática, de acordo com a reivindicação 15, **caracterizada pelo fato de que** o membro de vedação é um primeiro membro de vedação, o corpo de encaixe (318, 318', 522) inclui uma parede interna (154, 330) pelo menos parcialmente definindo uma passagem de encaixe (156, 222, 332) formada através do corpo de encaixe (318, 318', 522), o encaixe de conector (312, 406, 504, 600) inclui ainda:

um colar de retenção recebido na passagem de encaixe (156, 222, 332) e adaptado para engatar uma superfície externa associada da linha de fluido associada;

uma luva de suporte interna (166, 334) recebida na passagem de encaixe (156, 222, 332) adjacente ao colar de retenção e adaptada para engatar uma superfície interna associada com a linha de fluido; e

um segundo membro de vedação disposto dentro da passagem de encaixe (156, 222, 332) e adaptado para engatar de forma compressiva o corpo de encaixe (318, 318', 522) e a superfície externa associada da linha de fluido associada.

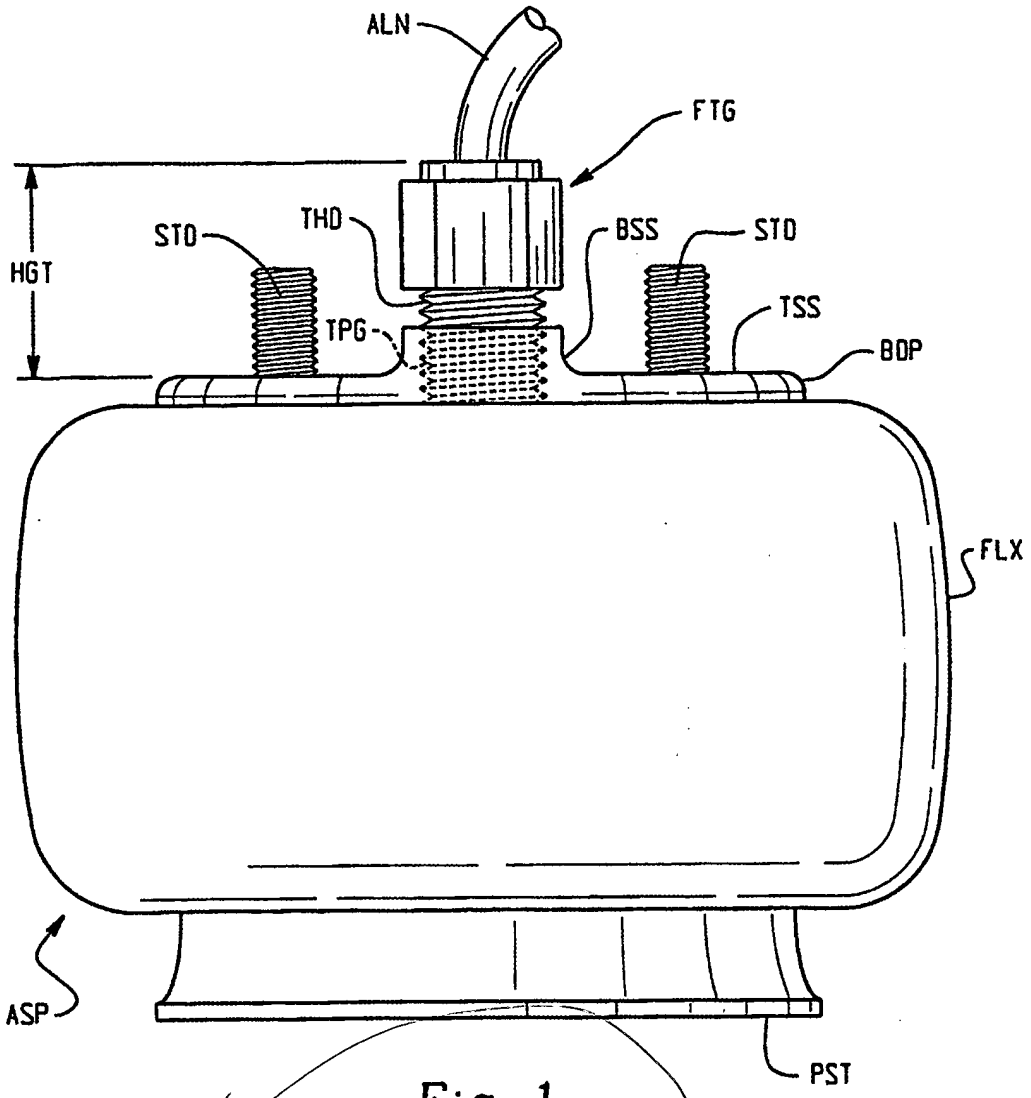


Fig. 1

Técnica Anterior

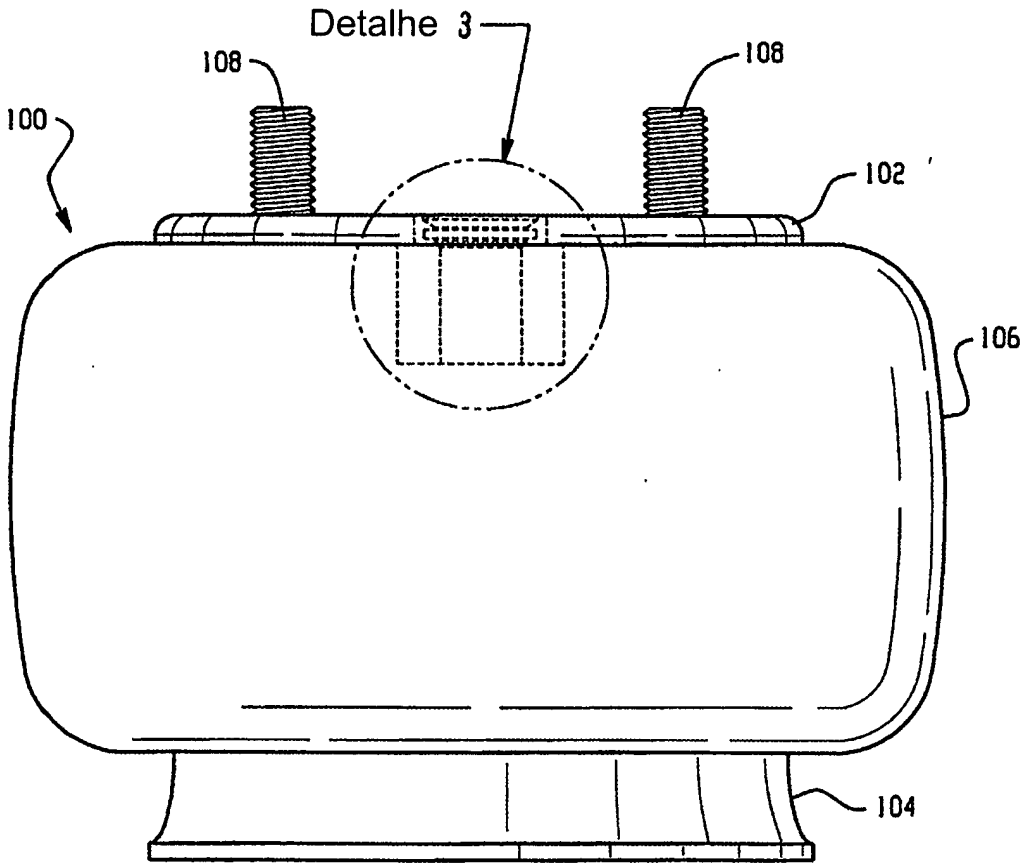


Fig. 2

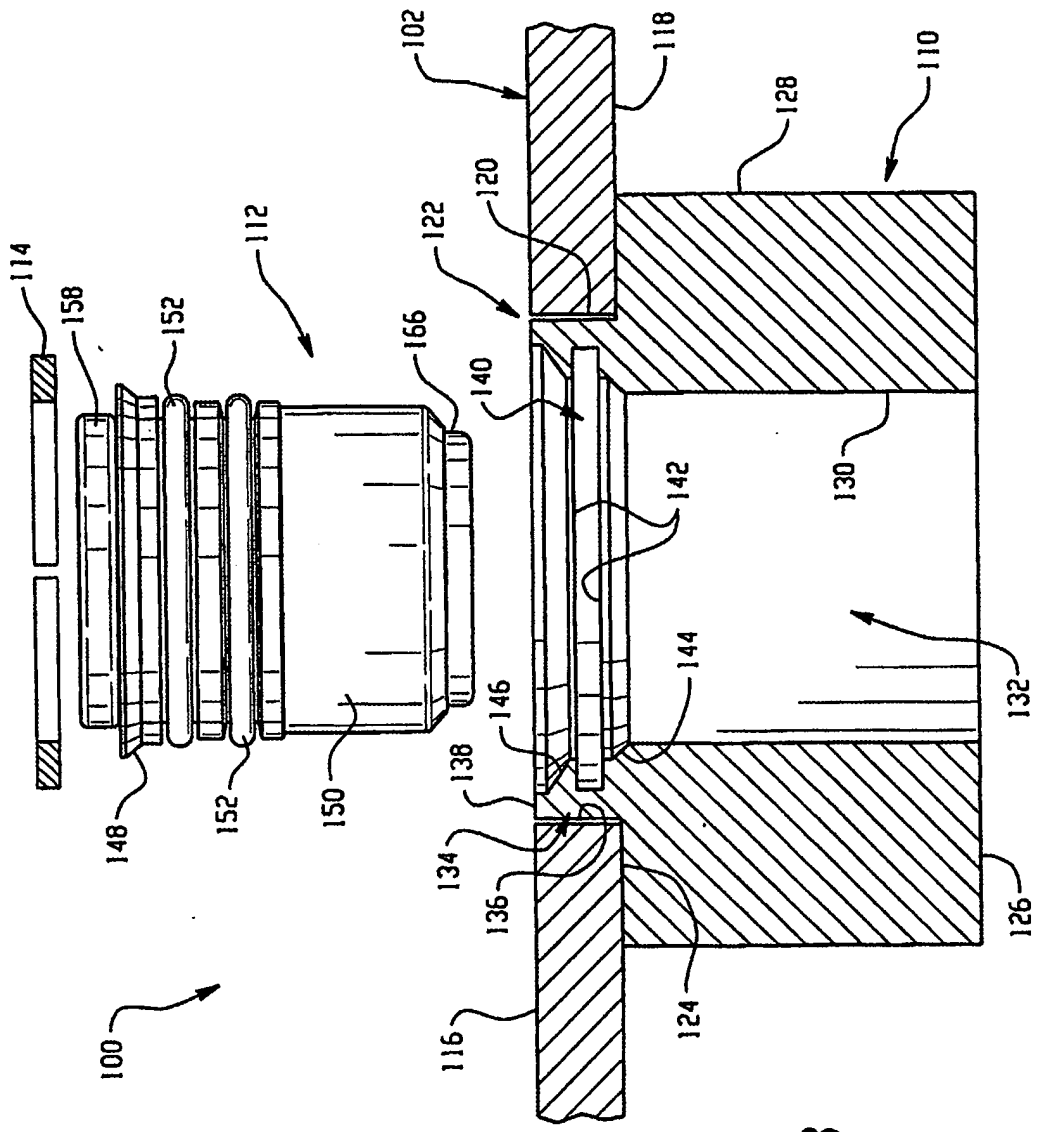

102
118
110
128
120
122
112
114
158
152
166
140
142
130
144
132
146
138
134
136
148
152
150
116
124
126
100

Fig. 3

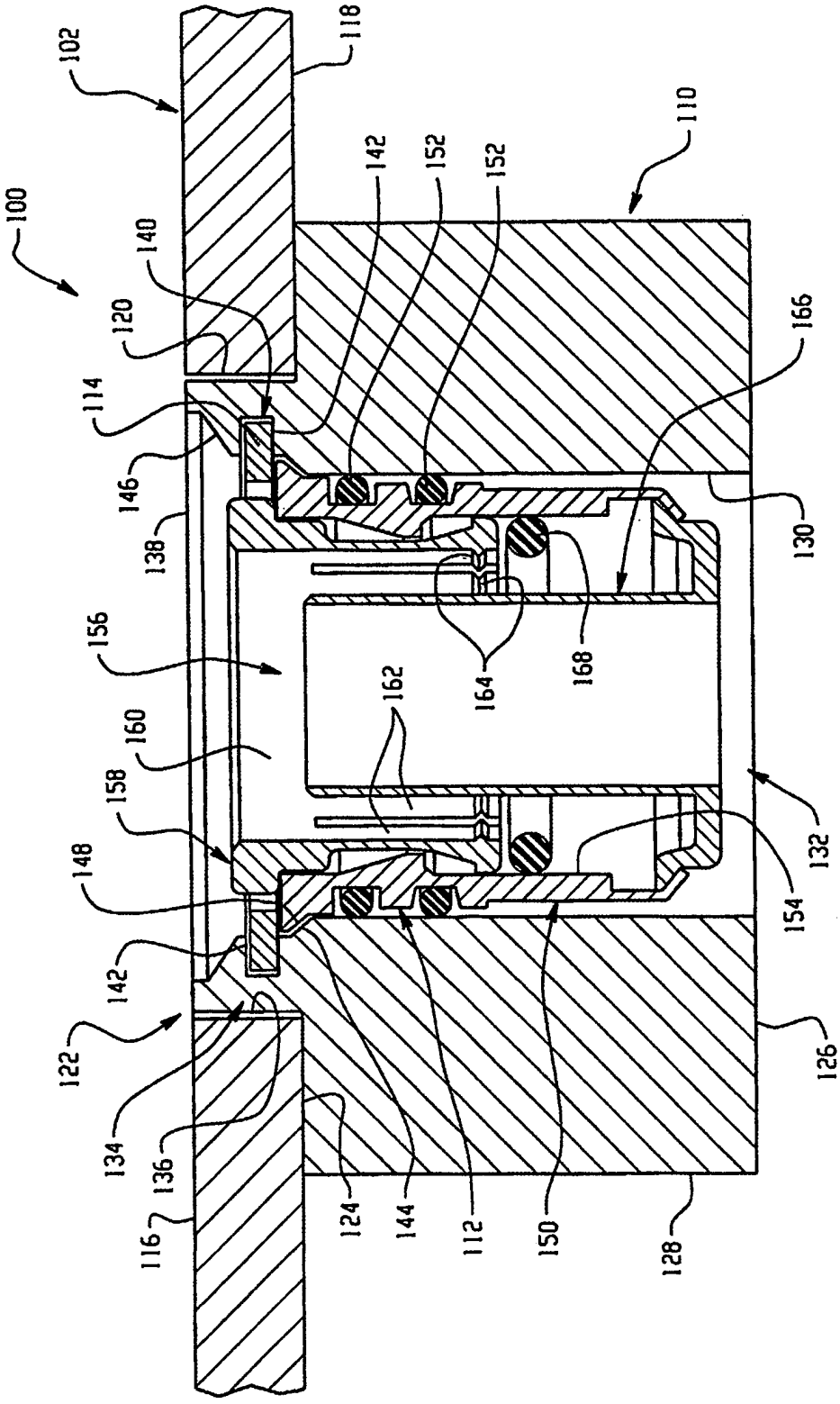

100
102
110
112
114
116
118
120
122
124
126
128
130
132
134
136
138
140
142
142
144
146
148
150
152
152
154
156
158
160
162
164
166
168

Fig. 4

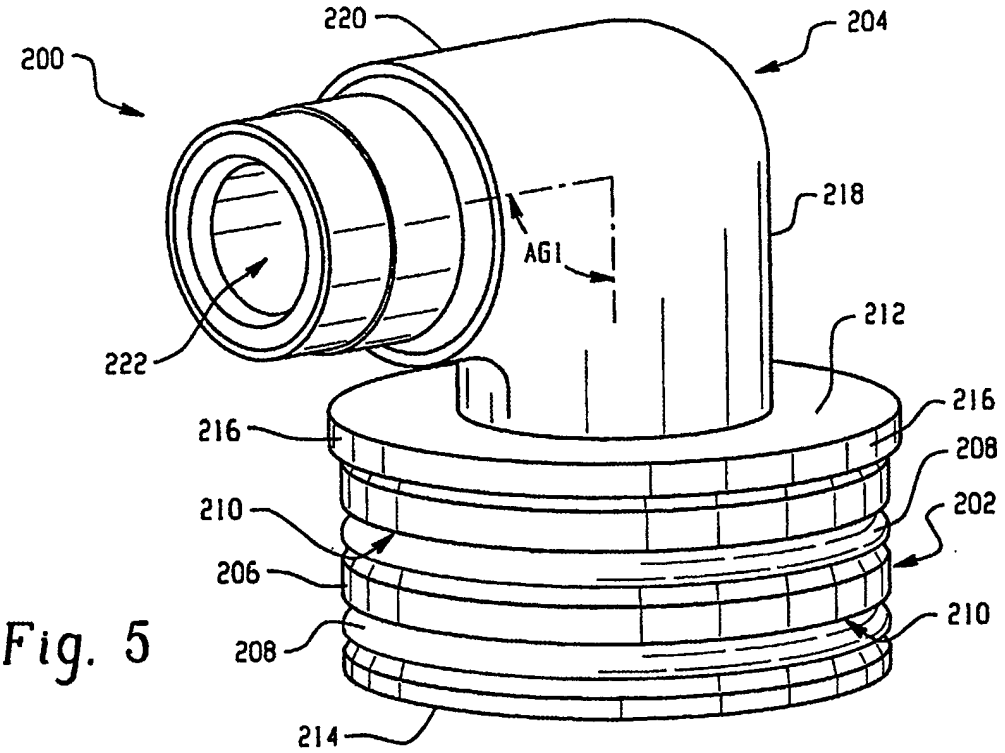

220
204
200
218
AG1
212
222
216
216
208
210
202
206
210
208
214

Fig. 5

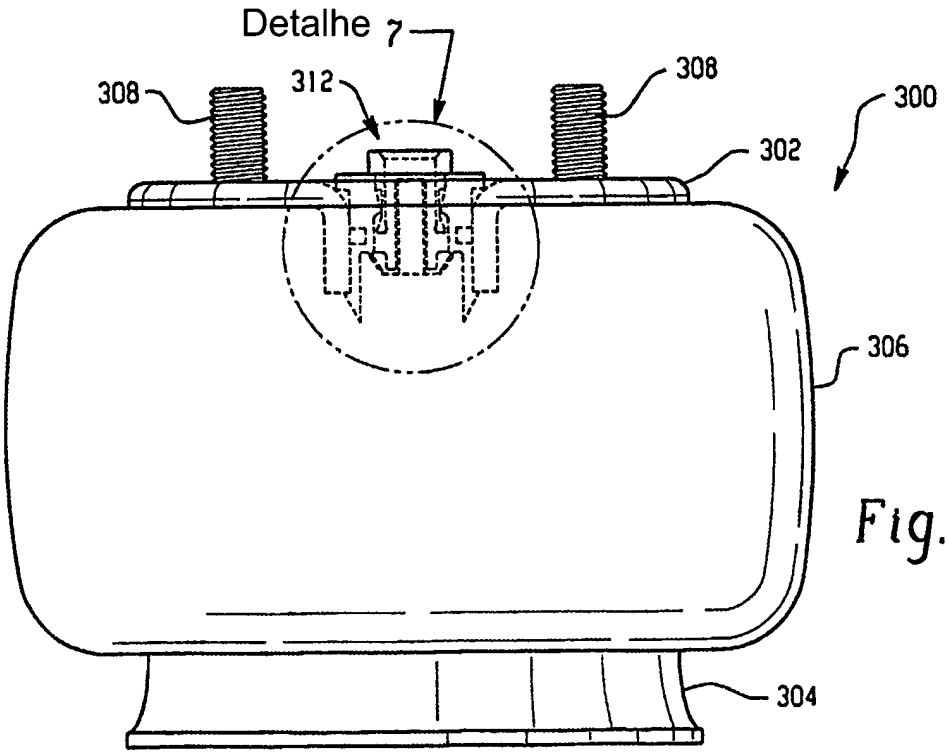

Detalhe 7
308
312
308
300
302
306
304

Fig. 6

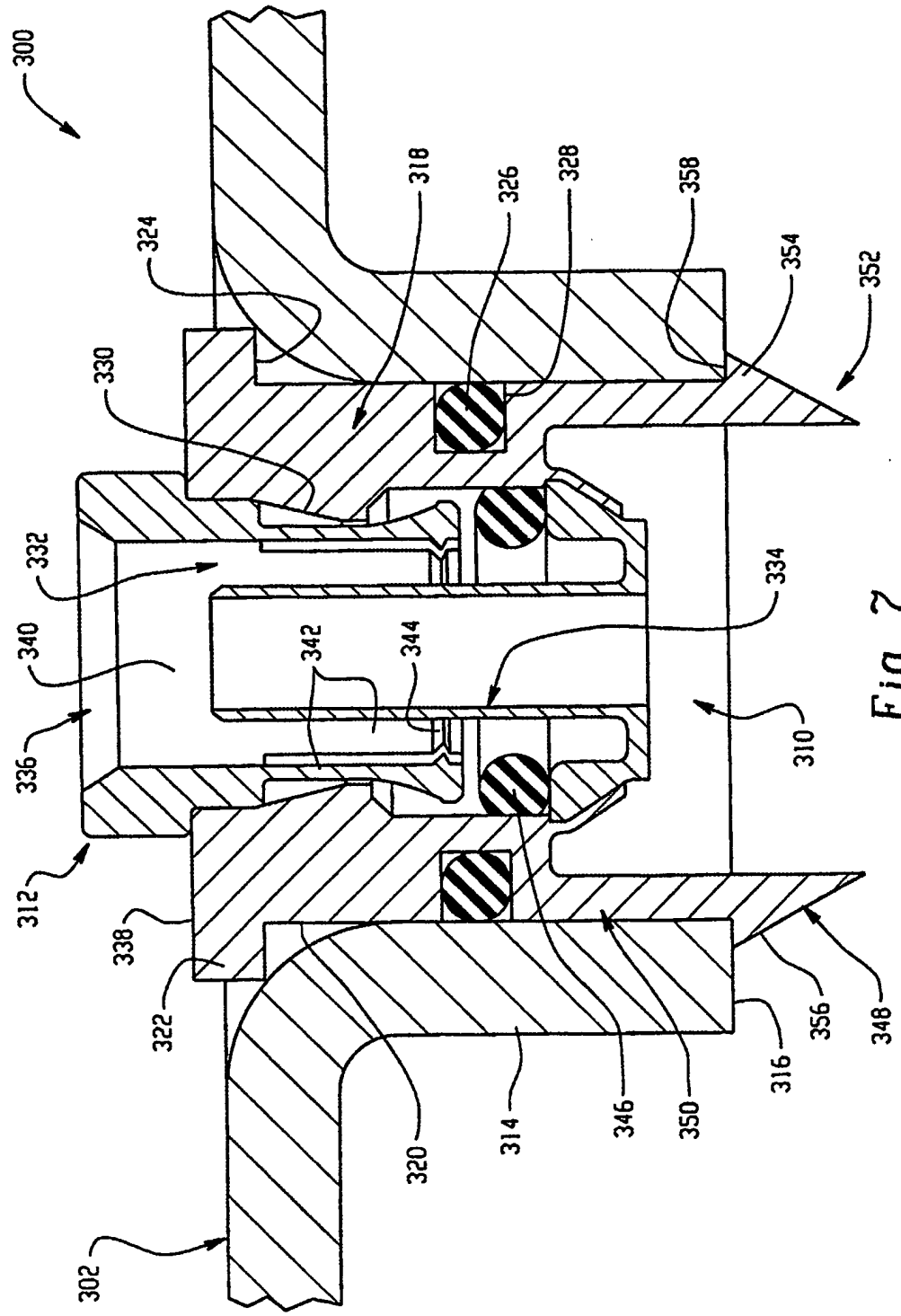

300
318
326
328
358
354
352
324
330
332
334
340
342
344
336
310
312
338
322
316
356
348
320
314
346
350
302

Fig. 7

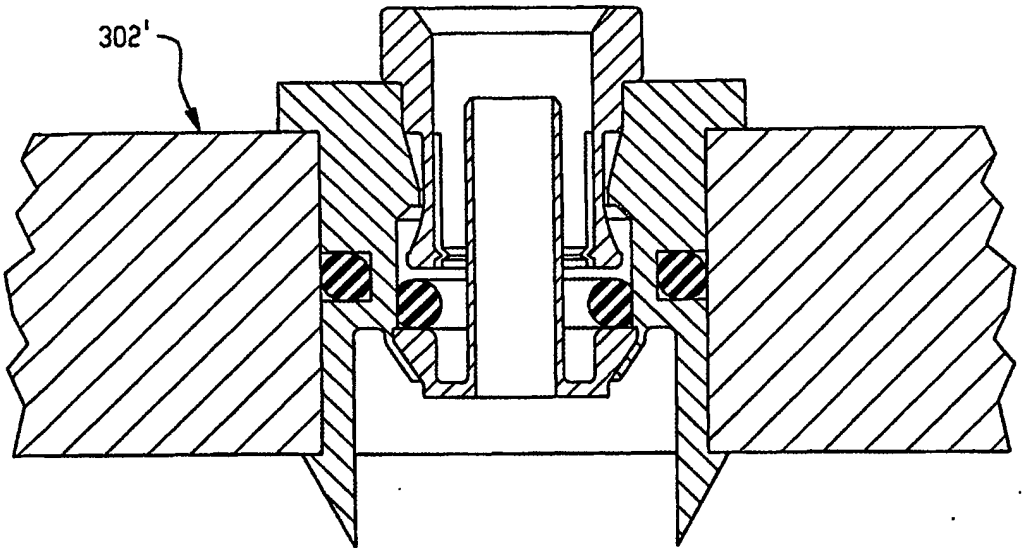


Fig. 8

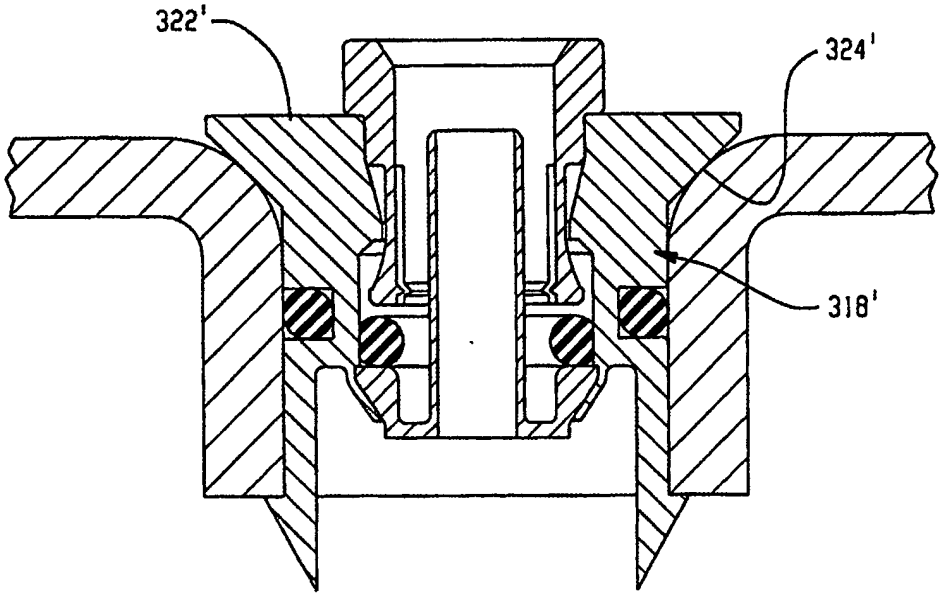


Fig. 9

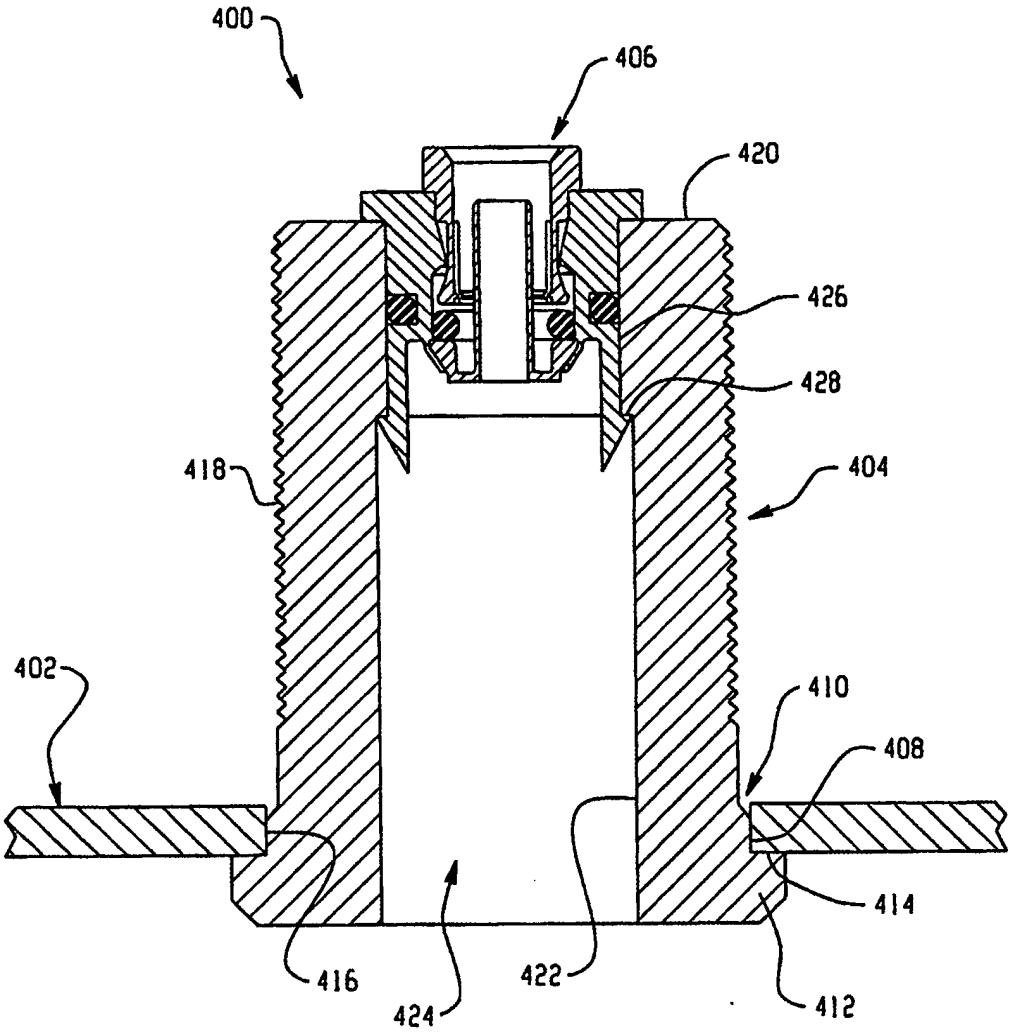


Fig. 10

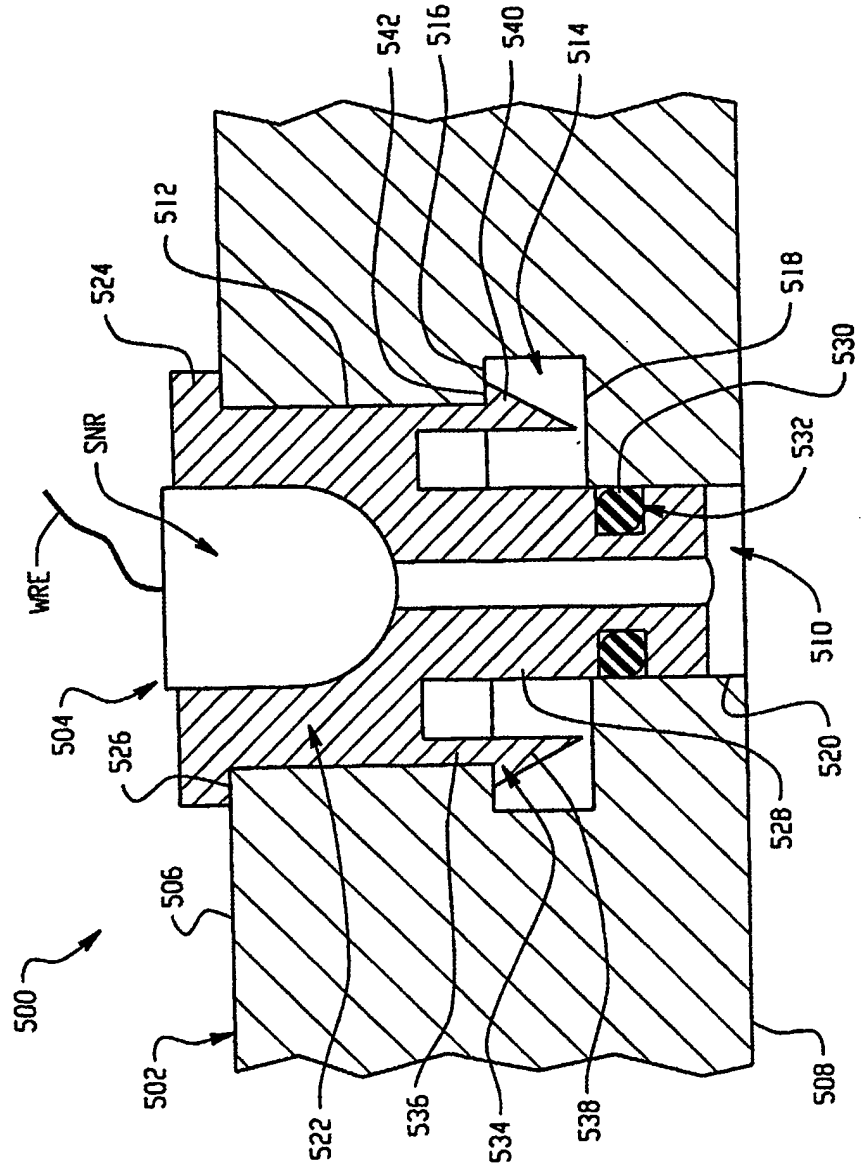

542
516
540
514
512
524
518
530
SNR
532
WRE
510
504
526
520
528
506
500
502
522
536
534
538
508

Fig. 11

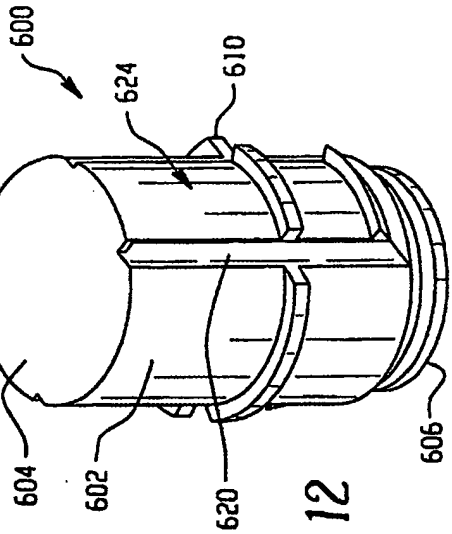


Fig. 12

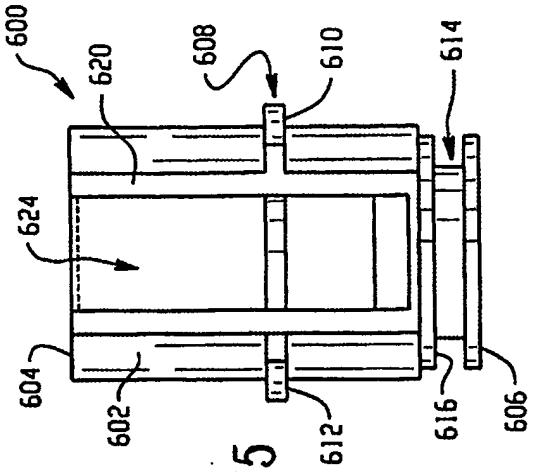


Fig. 15

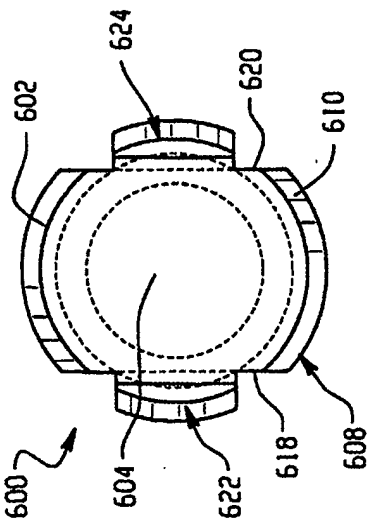


Fig. 13

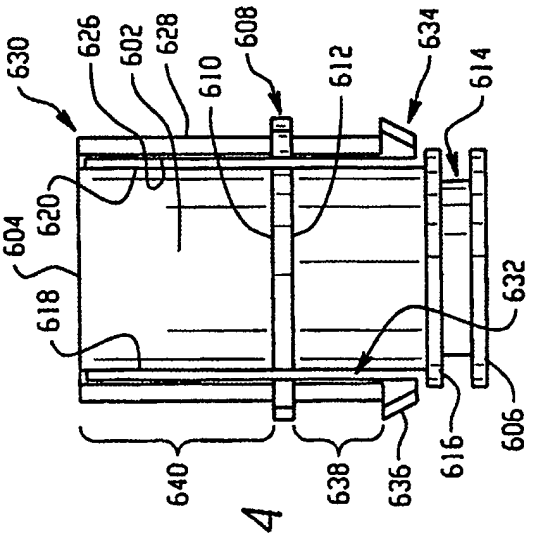


Fig. 14