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

(11) PI 0418985-0 B1

(22) Data do Depósito: 02/08/2004

(45) Data de Concessão: 30/05/2017

(54) Título: PROCESSO DE GERAÇÃO DE UMA SEQUÊNCIA DE DADOS PSEUDO-ALEATÓRIA, DISPOSITIVO DE CODIFICAÇÃO E SISTEMA TORNADO SEGURO

(51) Int.Cl.: G06F 7/58

(52) CPC: G06F 7/58

(73) Titular(es): FRANCE TELECOM. UNIVERSITE DE CAEN BASSE NORMANDIE

(72) Inventor(es): HERVÉ SIBERT; ALINE GOUGET

"PROCESSO DE GERAÇÃO DE UMA SEQUÊNCIA DE DADOS PSEUDO-ALEATÓRIA, DISPOSITIVO DE CODIFICAÇÃO E SISTEMA TORNADO SEGURO"

Campo técnico da invenção

[0001] A invenção se refere ao campo da codificação/decodificação e se refere a um sistema e a um processo de geração de uma sequência de dados pseudo-aleatória.

[0002] A invenção encontra uma aplicação muito vantajosa pelo fato de que ela permite criar séries de bits destinadas à cifragem simétrica, para o qual a cifragem e decifragem utilizam uma mesma chave secreta. Ela se inscreve no processo clássico dito de cifragem que flutua para o qual a operação de cifragem e a operação de decifragem são idênticas. A cifragem simétrica é empregada atualmente em todos os tipos de comunicações, tais como as comunicações móveis (GSM, UMTS...), a Internet (SSL...), os cartões com chip (cartões de banco), etc.

Fundamentos da invenção

[0003] O método mais difundido de cifragem que flutua consiste em gerar uma série cifradora de maneira independente da mensagem a cifrar recorrendo-se para isso, com um objetivo de economia material, a registradores de deslocamento com retroalimentação linear.

[0004] O inconveniente maior dos registradores de deslocamento com retroalimentação linear é sua linearidade. De fato, o conhecimento de um número de bits de saída do registrador igual ao comprimento do registrador assim como do polinômio de retroação associado ao registrador permite conhecer os bits de saída assim como todos os estados ulteriores do registrador.

[0005] Também, a fim de "quebrar" a linearidade dos registradores de deslocamento com retroalimentação linear, é comum combinar a saída de vários registradores, assim, eventualmente, como seu estado interno, com o auxílio de uma função binária não linear, por exemplo.

[0006] A figura 7 mostra um tal gerador 100 chamado "shrinking generator" descrito no pedido de patente europeia EP 0 619 659 que compreende um primeiro registrador de deslocamento com retroalimentação linear 111a, um segundo

registrador de deslocamento com retroalimentação linear 111b, e um meio 112 para selecionar a saída do gerador 100.

[0007] Assim, a cada deslocamento, os dois registradores 111a e 111b são deslocados simultaneamente, e a saída do dispositivos 100 é igual à saída do segundo registrador 111b se a saída do primeiro registrador 111a é "1", senão nenhum bit saiu.

[0008] O shrinking generator permite combinar não somente as saídas dos dois registradores de deslocamento com retroalimentação linear mas também, mais geralmente, qualquer par de séries de bits. O shrinking generator faz parte de uma classe de processos de cifragem que flutua, nos quais um registrador de deslocamento com retroalimentação linear controla um outro. A ideia é fazer variar o número de deslocamentos, por um lado, entre os diferentes registradores empregados e, por outro lado, entre dois bits consecutivos, a fim de quebrar a linearidade dos registradores.

[0009] Uma variante do shrinking generator, chamada "self-shrinking generator", repouso no mesmo princípio, mas a partir, dessa vez de um só registrador. Os bits de saída do registrador são lidos dois a dois, e o primeiro bit controla a saída do segundo de modo que a saída do sistema é o segundo bit se o primeiro é "1", e nenhum bit saiu senão.

[0010] Os inconvenientes do emprego de registradores de deslocamento com retroalimentação linear sozinhos são numerosos. O principal é a fraqueza devida à linearidade do dispositivo. Quando registradores são combinados por uma função binária, aí também inconvenientes aparecem. Ao nível material, eles provêm da complexidade da implementação da função. Além disso, essa função é fixada, e é possível atacá-la.

[0011] Por outro lado, métodos estatísticos colocaram em evidência certas fraquezas do "shrinking generator" e de outros processos de cifragem de controle de relógio. Em especial, no shrinking generator, o número de deslocamentos efetuadas pelos dois registradores entre dois bits de saída varia, mas tem o mesmo valor para os dois registradores.

[0012] Finalmente, um último inconveniente do shrinking generator é sua baixa relação do número de bits extraídos sobre o número de bits calculados que é igual em média a 1/4. Essa relação é a mesma para o self-shrinking generator, que possui a maior parte das vulnerabilidades do shrinking generator.

Objeto e Sumário da invenção

[0013] A invenção tem como objetivo corrigir esses inconvenientes, e simplificar a geração de uma sequência de dados pseudo-aleatória de boa qualidade.

[0014] Um outro objetivo é propor um processo e um gerador que permitem que se tenha uma relação entre o número de bits extraídos e o número de bits calculados superior a 1/4.

[0015] Mais um outro objetivo é realizar um gerador muito eficaz e pouco custoso.

[0016] Esses objetivos são atingidos graças a um processo de geração de uma sequência de dados pseudo-aleatória, no qual a dita sequência de dados pseudo-aleatória é gerada a partir de um processo de busca de pelo menos um padrão de busca em uma sequência de dados inicial de N bits.

[0017] Assim, o processo de acordo com a invenção se refere a um processo não linear de geração de dados pseudo-aleatórios e baseado na detecção de padrões que permitem combinar de maneira não linear um ou vários fluxos de bits para obter um novo fluxo de bits.

[0018] Esse processo, ao mesmo tempo em que é simples de realizar compreende uma complexidade intrínseca para poder produzir uma sequência de dados pseudo-aleatórios de boa qualidade.

[0019] O processo de busca compreende as seguintes etapas:

- detectar pelo menos um padrão de busca de r bits definido entre um conjunto de padrões de busca na dita sequência de dados inicial;

- determinar um padrão de saída de k bits de acordo com uma operação que depende do desenrolar da etapa precedente; e

- repetir as etapas precedentes de maneira sucessiva para formar a sequência de dados pseudo-aleatória a partir de uma sucessão de padrões de

saída.

[0020] As etapas de detecção do dito pelo menos um padrão de busca e de determinação do dito padrão de saída são efetuadas por uma série de operações que compreende um primeiro conjunto de regras que permite definir pelo menos um modo de deslocamento para deslocar pelo menos uma janela na dita sequência de dados inicial para detectar o dito pelo menos um padrão de busca, cada janela tendo uma posição inicial determinada na dita sequência de dados inicial e um tamanho determinado de bits.

[0021] A série de operações compreende por outro lado um segundo conjunto de regras que determinam as condições de interrupção do deslocamento da dita pelo menos uma janela na dita frequência de dados inicial.

[0022] Pelo menos uma regra do dito segundo conjunto de regras gere uma atualização do dito conjunto de padrões de busca e/ou do dito padrão de saída, em função do deslocamento e/ou do conteúdo da dita pelo menos uma janela.

[0023] A série de operações pode ser repetida até que uma condição previamente determinada seja preenchida.

[0024] Vantajosamente, a série de operações é modificada depois de cada execução.

[0025] De acordo com uma particularidade da invenção, a série de operações permanece invariável depois de cada execução e ela permite com o auxílio de pelo menos uma janela de 1 bit percorrer a dita sequência de dados inicial de maneira contínua bit a bit para detectar um padrão de busca de 1 bit e para determinar um padrão de saída de 1 bit.

[0026] De acordo com um primeiro modo de realização da invenção, a série de operações compreende as seguintes etapas:

- colocar o bit de uma janela no padrão de busca;
- deslocar a janela de um bit do bit atual para o bit seguinte;
- atualizar o padrão de saída de acordo com uma primeira lei, se o conteúdo da janela é igual àquele do padrão de busca;
- atualizar o padrão de saída de acordo com uma segunda lei, se o

conteúdo da janela não é igual ao bit do padrão de busca;

- deslocar a janela bit por bit na direção dos bits seguintes enquanto o conteúdo da janela não for igual ao bit do padrão de busca;

- deslocar a janela de um bit, do bit atual para o bit seguinte; e

- fazer sair o padrão de saída.

[0027] De acordo com o primeiro modo de realização a primeira lei atribui um valor determinado b ao padrão de saída, e a segunda lei faz uma adição módulo dois entre o dito valor determinado b e o valor 1 e atribui o resultado da dita adição ao padrão de saída.

[0028] De acordo com um segundo modo de realização da invenção, a primeira lei faz uma adição módulo dois entre um valor determinado b e o valor E do dito padrão de busca e atribui o resultado da dita adição ao padrão de saída, e a segunda lei faz uma adição módulo dois entre o dito valor determinado b, o valor E do padrão de busca, e o valor 1 e atribui o resultado da dita adição ao padrão de saída.

[0029] De acordo com um terceiro modo de realização da invenção, a série de operações compreende as seguintes etapas:

- colocar o bit de uma primeira janela no padrão de busca;

- deslocar a primeira janela de um bit do bit atual para o bit seguinte;

- atualizar o padrão de saída atribuindo-lhe o resultado de uma adição módulo dois entre um primeiro valor determinado e o valor do padrão de busca, se o conteúdo da primeira janela é igual ao valor do padrão de busca;

- atualizar o padrão de saída atribuindo-lhe o resultado de uma adição módulo dois entre o dito primeiro valor determinado, o valor do padrão de busca, e o valor 1, se o conteúdo da primeira janela não é igual ao valor E do padrão de busca;

- deslocar a primeira janela bit por bit na direção dos bits seguintes enquanto o conteúdo dessa primeira janela não for igual ao bit do padrão de busca;

- deslocar a primeira janela de um bit, do bit atual para o bit seguinte;

- substituir o valor do padrão de busca pelo bit de uma segunda janela;

- deslocar a segunda janela de um bit, do bit atual para o bit seguinte;

- atualizar o padrão de saída atribuindo-lhe o resultado de uma adição módulo dois entre um segundo valor determinado, o valor atual do padrão de saída, e o valor do padrão de busca, se o conteúdo da segunda janela é igual ao valor do padrão de busca;

- atualizar o padrão de saída atribuindo-lhe o resultado de uma adição módulo dois entre o valor atual do padrão de saída, o dito segundo valor determinado, o valor do padrão de busca, e o valor 1, se o conteúdo da segunda janela não é igual ao valor do padrão de busca;

- deslocar a segunda janela bit por bit na direção dos bits seguintes enquanto o conteúdo dessa segunda janela não for igual ao valor do padrão de busca;

- deslocar a segunda janela de um bit do bit atual para o bit seguinte; e

- extrair o padrão de saída.

[0030] De acordo com uma aplicação do processo da presente invenção, cada bit da dita sequência de dados pseudo-aleatória é combinado com um bit correspondente de uma sequência de dados de uma mensagem a cifrar por uma adição módulo 2 para formar uma sequência de dados cifrada.

[0031] A invenção também visa um gerador de uma sequência de dados pseudo-aleatória, que compreende um meio de busca para buscar pelo menos um padrão de busca em uma sequência de dados inicial de N bits.

[0032] O meio de busca do gerador compreende:

- um meio de detecção para detectar pelo menos um padrão de busca de r bits definido entre um conjunto de padrões de busca na dita sequência de dados inicial;

- um meio de determinação para determinar um padrão de saída de k bits de acordo com uma operação que depende do desenrolar da detecção do dito pelo menos um padrão de busca; e

- um meio de repetição para gerar a sequência de dados pseudo-aleatória a partir de uma sucessão de padrões de saída.

[0033] O meio de detecção compreende pelo menos uma janela destinada a se

deslocar na dita sequência de dados inicial e um primeiro meio de controle para controlar o deslocamento da dita pelo menos uma janela na dita sequência de dados inicial.

[0034] O meio de determinação compreende um segundo meio de controle para atualizar o dito conjunto de padrões de busca e/ou o dito padrão de saída.

[0035] O gerador compreende por outro lado um meio inicial para gerar a sequência de dados inicial de N bits.

[0036] O meio inicial pode compreender um registrador de deslocamento com retroalimentação linear.

[0037] A invenção visa também um dispositivo de codificação que compreende uma porta lógica ou-exclusivo e um gerador de acordo com as características acima.

[0038] A invenção visa também um sistema tornado seguro que compreende pelo menos duas entidades das quais cada uma delas compreende um dispositivo de codificação.

Breve descrição dos desenhos

[0039] Outras particularidades e vantagens da invenção se destacarão com a leitura da descrição feita, abaixo, a título indicativo mas não limitativo, em referência aos desenhos anexos, nos quais:

[0040] - A figura 1 ilustra um exemplo bastante esquemático de um gerador de uma sequência de dados pseudo-aleatória, de acordo com a invenção;

[0041] - A figura 2 mostra um sistema tornado seguro que compreende geradores da figura 1;

[0042] - A figura 3 ilustra um exemplo de um processo de busca para a geração da sequência de dados pseudo-aleatória, de acordo com a invenção;

[0043] - As figuras 4 a 6 mostram modos de realização especiais do processo de acordo com a invenção; e

[0044] - A figura 7 é uma vista bastante esquemática de um gerador de acordo com a arte anterior.

Descrição detalhada de modos de realização

[0045] De acordo com a invenção, a figura 1 ilustra ume exemplo bastante

esquemático de um gerador 1 de uma sequência de dados pseudo-aleatória 3.

[0046] O gerador 1 compreende um meio de busca 5 para buscar pelo menos um padrão de busca 7 em uma sequência de dados inicial 9 de N bits. Esse ou esses dispositivos de busca figuram entre um conjunto de padrões de busca.

[0047] É chamado, em tudo o que se segue, de um "padrão" qualquer palavra composta unicamente por 0 e por 1. Por exemplo 0, 11, 000, 1010, 00111 são padrões de comprimentos respectivos 1, 2, 3, 4, e 5. Por outro lado, um padrão "vazio" é uma palavra vazia.

[0048] A sequência de dados inicial de N bits (N sendo um número inteiro) é gerada por um meio inicial 11 que pode compreender um registrador de deslocamento com retroalimentação linear de período máximo.

[0049] Um registrador de deslocamento com retroalimentação linear é uma tabela de bits de comprimento finito (o registrador) munida de uma combinação linear, representada por um polinômio chamado de polinômio de retroação das casas da tabela. A cada deslocamento, o bit de índice mais elevado é extraído, todos os outros bits são deslocados de um índice, e o bit de índice menor toma o valor da combinação linear antes da deslocamento.

[0050] Vantajosamente, o polinômio de retroação pode por exemplo ser um polinômio primitivo que corresponde a um registrador de deslocamento linear de período máximo, ou então um polinômio da forma $Q = (x^2 + 1)P$, com P um polinômio primitivo.

[0051] O meio de busca 5 do gerador 1 compreende um meio de detecção 13, um meio de determinação 15, e um meio de repetição 17.

[0052] O meio de detecção 13 é destinado a detectar pelo menos um padrão de busca 7 de r bits na sequência de dados inicial, onde r é um número inteiro inferior a N. O meio de determinação 15 define o conjunto de padrões de busca ao qual pertence o padrão de busca 7 detectado pelo meio de detecção 13.

[0053] O meio de detecção compreende pelo menos uma janela 19 destinada a se deslocar na sequência de dados inicial 9 e um primeiro meio de controle 21 para controlar o deslocamento da ou das janelas 19 na sequência de dados inicial 9.

[0054] Cada janela 19 é colocada em uma posição inicial determinada na sequência de dados inicial 9 e possui um tamanho determinado de bits. Por exemplo, uma janela 19 de tamanho t (t sendo um número inteiro inferior a N) colocada na sequência de dados inicial 9 é uma máscara que pode se deslocar nessa sequência 9 deixando aparecer a cada deslocamento exatamente t bits da sequência 9.

[0055] O meio de determinação 15 está em interação com o meio de detecção 13 via uma ligação 23. Esse meio de determinação 15 é destinado a determinar um padrão de saída 25 de k bits (k sendo um número inteiro inferior a N), de acordo com uma operação que depende do desenrolar da busca do ou dos padrões de busca 7.

[0056] De fato, o meio de determinação 15 compreende um segundo meio de controle 27 para definir ou atualizar o conjunto de padrões de busca e/ou o padrão de saída 25.

[0057] Por outro lado, o meio de repetição 17 é ligado aos meios de detecção 13 e de determinação 15 via ligações 29 e 31 respectivamente.

[0058] Assim, o meio de repetição 17 pode traçar sinais com os meios de detecção 13 e de determinação 15 para recomeçar as operações de detecção e de determinação, por exemplo depois de ter recebido do meio de determinação 15 o sinal que um padrão de saída 25 acaba de sair, isso enquanto uma condição de interrupção previamente determinada não for preenchida. O meio de repetição 17 pode por outro lado testar a condição de interrupção graças às trocas de sinais com os meios de detecção 13 e de determinação 15. Isso permite gerar uma sucessão de padrões de saída 25 que formam por concatenação a sequência de dados pseudo-aleatória 3.

[0059] Será notado que o meio de repetição 17 pode também ser integrado ao primeiro ou segundo meio de controle 21 ou 27 dos meios de detecção 13 e de determinação 15.

[0060] A figura 2 mostra um sistema tornado seguro 31 que compreende pelo menos duas entidades conectadas entre si via uma rede de comunicação 35 de tipo Internet, GSM, UMTS, etc.

[0061] O exemplo dessa figura mostra uma primeira entidade 33a conectada via a rede de comunicação 35 a uma segunda entidade 33b.

[0062] A primeira entidade 33a (respectivamente a segunda entidade 33b) compreende um primeiro terminal 37a (respectivamente um segundo terminal 37b), um primeiro dispositivo de codificação 39a (respectivamente um segundo dispositivo de codificação 39b) e um primeiro modem 41a (respectivamente um segundo modem 41b), os modems 41a e 41b podendo ser qualquer dispositivo que permite formar uma interface com a rede de comunicação 35.

[0063] Cada um dos primeiro e segundo dispositivos de codificação 39a, 39b compreende um gerador 1 de uma sequência de dados pseudo-aleatória 3 tal como descrito precedentemente e uma porta lógica "ou-exclusivo" 43.

[0064] Cada dispositivo de codificação 39a, 39b é destinado a fazer um cifragem ou um decifragem que flutua que consiste em cifrar ou decifrar uma mensagem bit após bit.

[0065] De acordo com esse exemplo, o primeiro dispositivo de codificação 39a faz uma operação de cifragem. Assim, a sequência de dados pseudo-aleatória 3 chamada de série cifradora, é combinada pela porta ou-exclusivo 43 com cada bit de posição correspondente de uma mensagem em branco 45 enviada pelo primeiro terminal 37 a para obter um texto cifrado 47 que é em seguida enviado pelo primeiro modem 41a para a segunda entidade 33b. Assim, a operação de cifragem consiste em adicionar bit a bit uma série cifradora 3 ao texto claro da mensagem 45 para obter o texto cifrado 47.

[0066] O segundo dispositivo de codificação 39b faz uma operação de decifragem que consiste em adicionar bit a bit essa mesma série cifradora 3 ao texto cifrado 47 enviado pela primeira entidade 33 a para reformar a mensagem ao texto claro 45.

[0067] Assim, as operações de cifragem e de decifragem são idênticas.

[0068] As figuras 3 a 6 ilustram o processo de geração de dados pseudo-aleatória de acordo com a invenção.

[0069] Esse processo consiste em gerar a sequência de dados pseudo-aleatória

3 a partir de um processo de busca de pelo menos um padrão de busca na sequência de dados inicial 9.

[0070] Assim, a determinação dos elementos da sequência de dados pseudo-aleatória de acordo com a invenção pode depender do padrão buscado e do histórico ou da maneira pela qual a busca foi realizada.

[0071] A figura 3 ilustra um exemplo de um processo de busca para a geração da sequência de dados pseudo-aleatória 3 de acordo com a invenção.

[0072] A etapa E1, se refere à detecção de pelo menos um padrão de busca 7 de r bits definido entre um conjunto de padrões de busca na sequência de dados inicial 9.

[0073] A etapa E2, se refere à determinação de um padrão de saída 25 de k bits, de acordo com uma operação que depende do desenrolar da etapa precedente E1.

[0074] De fato, a determinação do padrão de saída 25 pode depender do padrão de busca 7 e do histórico da busca, em especial do número de etapas ou de iterações efetuadas antes de encontrar o padrão de busca 7 em questão na sequência de dados inicial 9.

[0075] Essas etapas de detecção E1 do padrão de busca 7 e de determinação E2 do padrão de saída 25 são efetuadas por uma série de operações.

[0076] Essa série de operações compreende um primeiro conjunto de regras implementadas pelo primeiro meio de controle 21 do gerador 1, que permite definir pelo menos um modo de deslocamento para deslocar pelo menos uma janela 19 na sequência de dados inicial 9 para detectar o ou os padrões de busca 7.

[0077] De uma maneira geral, uma ou várias janelas 19 de tamanhos não nulos, se deslocam na sequência de dados inicial 9. No início do processo de busca, cada janela 19 se encontra em uma posição inicial na sequência inicial 9 (por exemplo, elas podem estar todas no início da sequência inicial 9). O ou os bits que se encontram na ou nas janelas 19 vão ser utilizados para determinar o padrão de saída 25.

[0078] O primeiro conjunto de regras pode definir o sentido de deslocamento, a amplitude do deslocamento, ou a forma de deslocamento das janelas 19, por

exemplo um deslocamento cíclico em uma parte da sequência de dados inicial 9.

[0079] A título de exemplo, o primeiro conjunto de regras pode compreender uma regra r_1 definida da seguinte maneira:

r_1 = "deslocar de um bit para a direita".

[0080] Por outro lado, a série de operações compreende um segundo conjunto de regras implementadas pelo segundo meio de controle 27 do gerador 1, que determinam as condições de interrupção do deslocamento da ou das janelas 19 na sequência de dados inicial 9.

[0081] O segundo conjunto de regras pode compreender uma pluralidade de regras que deve, ser aplicadas de acordo com uma ordem determinada, antes que o gerador 1 forneça o padrão de saída 24. Assim, o fornecimento pelo gerador 1 de uma sucessão de padrões de saída 25 permite formar a sequência de dados pseudo-aleatória 3.

[0082] A título de exemplo, o segundo conjunto de regras pode compreender uma regra r_2 definida da seguinte maneira:

[0083] R_2 = "enquanto o conteúdo de uma janela 19 não for um padrão do conjunto de padrões de busca 7, deslocar a janela 19 de acordo com a regra r_1", onde r_1 é uma regra do primeiro conjunto de regras.

[0084] Por outro lado, uma outra regra que pertence a esse segundo conjunto de regras, pode gerir uma atualização do conjunto de padrões de busca 7 e/ou do padrão de saída 25 de acordo com uma lei binária dada e em função do deslocamento e/ou do conteúdo da janela 19.

[0085] Assim, o ou os padrões de busca 7 podem ser vazios, quer dizer sem nenhum padrão, ou depender do conteúdo das janelas 19, ou ainda depender das execuções precedentes da série de operações que compreende os primeiro e segundo conjunto de regras.

[0086] Do mesmo modo, o padrão de saída 25 pode ser vazio, quer dizer sem nenhum padrão, ou depender do conteúdo das janelas 19, ou ainda depender das execuções precedentes da série de operações que compreende os primeiro e segundo conjunto de regras.

[0087] Por outro lado, a etapa E3 do processo de busca consiste em repetir as duas etapas precedentes E1 e E2 de maneira sucessiva para formar por concatenação a sequência de dados pseudo-aleatória 3 a partir de uma sucessão de padrões de saída 25.

[0088] Será notado que, a série de operações pode ser repetida até que uma condição previamente determinada seja preenchida. Essa condição pode ser o conteúdo de uma janela 19 da sequência de dados inicial 9, se essa última acabou. Também é possível repetir a série de operações até que uma condição definida pelo utilizador seja preenchida.

[0089] Por outro lado, a fim de melhorar ainda mais a qualidade da sequência de dados pseudo-aleatória 3, é possível modificar a série de operações depois de cada execução.

[0090] Assim, esse processo consiste em percorrer um fluxo inicial de bits (sequência de dados inicial 9) com o auxílio de uma ou várias janelas 19, de modo que cada bit de saída da sequência de dados pseudo-aleatória 3 dependa de pelo menos uma busca de um ou vários padrões 7 nesse fluxo inicial 9. Além disso, os padrões 7 a buscar podem eles próprios depender do conteúdo e/ou do deslocamento das janelas 19.

[0091] As figuras 4 a 6 mostram modos de realização especiais do processo de acordo com a invenção.

[0092] De acordo com esses exemplos, a série de operações permanece invariável depois de cada execução, a ou as janelas 19 são de “tamanho um” (quer dizer que cada janela compreende 1 bit), o conjunto de padrões de busca contém no máximo um padrão de busca 7, e os padrões de busca 7 e de saída 25 também são de tamanho um.

[0093] Por outro lado, a amplitude de deslocamento das janelas 19 é igual a uma unidade, quer dizer que cada janela 19 se desloca de um bit a cada iteração, por exemplo, do bit atual para o bit seguinte (quer dizer da esquerda para a direita).

[0094] Assim, cada sequência de dados inicial 9 pode ser lida de uma maneira contínua, quer dizer bit a bit, o que faz modos de realização muito simples a

implementar.

[0095] Será anotado em tudo o que se segue, o valor do padrão de busca 7 por E, o valor do padrão de saída 25 por s, e o valor das janelas 19 por f, f_1 e f_2.

[0096] No início, os padrões de busca 7 e de saída 25 são inicializados atribuindo-se um bit vazio a cada um deles, quer dizer $E \leftarrow \phi$ e $s \leftarrow \phi$, ϕ sendo o conjunto vazio. Do mesmo modo, são definidos valores binários ou constantes anotados b, b_1 e b_2 que permanecem fixos a cada aplicação da série de operações desses modos de realização.

[0097] De acordo com o primeiro modo de realização, uma só janela 19 se desloca na sequência de dados inicial 9. Ela pode ser inicialmente fixada no primeiro bit da sequência de dados inicial 9.

[0098] A série de operações do primeiro modo de realização pode ser definida da seguinte maneira:

- colocar como única regra do primeiro conjunto de regras, a regra $r_{1,1}$ = "deslocar de um bit para a direita",

- colocar como regras do segundo conjunto de regras as regras seguintes:

$r_{2,1}$ = "colocar o bit f da janela no padrão de busca ($E \leftarrow f$)",

$r_{2,2}$ = "deslocar a janela uma vez de acordo com $r_{1,1}$",

$r_{2,3}$ = "se o conteúdo da janela é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow b$",

$r_{2,4}$ = "se o conteúdo da janela não é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow b \oplus 1$",

$r_{2,5}$ = "enquanto o conteúdo f da janela não for um padrão de busca, deslocar a janela de acordo com a regra $r_{1,1}$",

$r_{2,6}$ = "deslocar a janela uma vez de acordo com a regra $r_{1,1}$".

- aplicar na ordem as regras $r_{2,1}$, $r_{2,2}$, $r_{2,3}$, $r_{2,4}$, $r_{2,5}$ e $r_{2,6}$, e

- extrair o padrão s de saída.

[0099] De fato, o organograma da figura 4 mostra o desenrolar da série de operações acima.

[00100] A etapa E11 consiste em colocar o bit da janela 19 no padrão de busca 7.

[00101] A etapa E12 consiste em deslocar a janela 19 de um bit, do bit atual para o bit seguinte.

[00102] A etapa E13 é um teste que compara o conteúdo da janela 19 com o conteúdo do padrão de busca 7.

[00103] A etapa E14 consiste em atualizar o padrão de saída 25 de acordo com uma primeira lei, se o conteúdo da janela 19 é igual àquele do padrão de busca 7. De acordo com esse exemplo, a primeira lei corresponde à atribuição do valor determinado b ao padrão de saída 25 ($s \leftarrow b$).

[00104] A etapa E15 consiste em atualizar o padrão de saída 25 de acordo com uma segunda lei, se o conteúdo da janela 19 não é igual ao bit do padrão de busca 7. De acordo com esse exemplo, a segunda lei corresponde a fazer uma adição módulo dois entre o valor determinado b e o valor "1" e atribui o resultado dessa adição ao padrão de saída 25 ($s \leftarrow b \oplus 1$).

[00105] As etapas E16 e E17 formam um laço que consiste em deslocar a janela 19 bit por bit na direção dos bits seguintes enquanto o conteúdo da janela 19 não for igual ao bit do padrão de busca 7.

[00106] A etapa E18 consiste em deslocar a janela 19 de um bit, do bit atual ao bit seguinte.

[00107] Finalmente, a etapa E19 consiste em fazer sair do gerador 1 o padrão de saída.

[00108] Esquematicamente, a série de operações pode ser resumida assim: lê-se o bit E atual na sequência de dados inicial 9, e depois há um deslocamento para a direita na sequência 9 até encontrar o bit E. Se só houve um deslocamento de um índice para encontrar E, então extrai-se b, senão extrai-se $b \oplus 1$. Há em seguida um deslocamento de um bit para a direita antes de recomeçar.

[00109] Naturalmente, o organograma pode compreender um teste de interrupção (não representado na figura por preocupação de simplificação) para determinar se uma condição previamente definida é preenchida.

[00110] A título de exemplo, essas etapas podem ser repetidas para formar a

sequência de dados pseudo-aleatória até que a janela 19 saia da sequência de dados inicial 9.

[00111] A figura 5 é um organograma que mostra o desenrolar da série de operações de um segundo modo de realização.

[00112] O organograma dessa figura se distingue daquele da figura 4 unicamente pelas etapas E24 e E25.

[00113] De fato, na etapa E24, a primeira lei corresponde a fazer uma adição módulo dois entre o valor determinado b e o valor E do padrão de busca 7 e atribuir o resultado dessa adição ao padrão de saída 25 ($s \leftarrow b \oplus E$).

[00114] Em contrapartida, na etapa E25, a segunda lei corresponde a fazer uma adição módulo dois entre o valor determinado b, o valor E do padrão de busca 7, e o valor "1" e atribuir o resultado dessa adição ao padrão de saída 25 ($s \leftarrow b \oplus E \oplus 1$).

[00115] Assim, a série de operações do segundo modo de realização pode ser definida da seguinte maneira:

- colocar como única regra do primeiro conjunto de regras, a regra $r_{1,1}$ = "deslocar de um bit para a direita",
- colocar como regras do segundo conjunto de regras as regras seguintes:

$r_{2,1}$ = "colocar o bit f da janela no padrão de busca ($E \leftarrow f$)",

$r_{2,2}$ = "deslocar a janela uma vez de acordo com $r_{1,1}$",

$r_{2,3}$ = "se o conteúdo da janela, é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow b \oplus E$",

$r_{2,4}$ = "se o conteúdo da janela não é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow b \oplus E \oplus 1$",

$r_{2,5}$ = "enquanto o conteúdo f da janela não for um padrão de busca, deslocar a janela de acordo com a regra $r_{1,1}$",

$r_{2,6}$ = "deslocar a janela uma vez de acordo com a regra $r_{1,1}$".

- aplicar na ordem as regras $r_{2,1}$, $r_{2,2}$, $r_{2,3}$, $r_{2,4}$, $r_{2,5}$ e $r_{2,6}$, e
- extrair o padrão de saída s.

[00116] Esquematicamente, a série de operações do segundo modo de realização

pode ser resumida assim: lê-se o bit E atual na sequência de dados inicial 9, e depois há um deslocamento para a direita na sequência 9 até encontrar o bit E. Se só houve um deslocamento de um índice para encontrar E, então extrai-se b $\oplus$ E, senão extrai-se b $\oplus$ E $\oplus$ 1. Há em seguida um deslocamento de um bit para a direita antes de recomeçar.

[00117] A figura 6 é um organograma que mostra o desenrolar da série de operações de um terceiro modo de realização.

[00118] De acordo com esse terceiro modo, duas janelas 19 se deslocam na sequência de dados inicial. Uma primeira janela é inicialmente fixada no primeiro bit da sequência de dados inicial 9 e uma segunda janela inicialmente fixada no segundo bit dessa sequência. Nesse caso, duas constantes são definidas, um primeiro bit anotado b_1 e um segundo bit anotado b_2. A título de exemplo, as constantes b_1 e b_2 têm o mesmo valor 0.

[00119] A etapa E31 consiste em colocar o bit de uma primeira janela no padrão de busca 7.

[00120] A etapa E32 consiste em deslocar a primeira janela de um bit do bit atual para o bit seguinte.

[00121] A etapa E33 é um teste que compara o conteúdo da primeira janela com o conteúdo do padrão de busca 7.

[00122] A etapa E34 consiste em atualizar o padrão de saída 25 atribuindo a ele o resultado de uma adição módulo dois entre um primeiro valor determinado b_1, e o valor E do padrão de busca, se o conteúdo da primeira janela não é igual ao valor E do padrão de busca 7 ($s \leftarrow b_1 \oplus E$).

[00123] A etapa E35 consiste em atualizar o padrão de saída 25 atribuindo a ele o resultado de uma adição módulo dois entre o primeiro valor determinado b_1, o valor E do padrão de busca 7, e o valor “1”, se o conteúdo da primeira janela não é igual ao valor E do padrão de busca ($s \leftarrow b_1 \oplus E \oplus 1$).

[00124] As etapas E36 e E37 formam um laço que consiste em deslocar a primeira janela bit por bit na direção dos bits seguintes enquanto o conteúdo da primeira janela não for igual ao bit do padrão de busca 7.

[00125] A etapa E38 consiste em deslocar a primeira janela de um bit, do bit atual para o bit seguinte.

[00126] A etapa E39 consiste em colocar o bit da segunda janela no padrão de busca 7.

[00127] A etapa E40 consiste em deslocar a segunda janela de um bit, do bit atual para o bit seguinte.

[00128] A etapa E41 é um teste que compara o conteúdo da segunda janela com o conteúdo do padrão de busca 7.

[00129] A etapa E42 consiste em atualizar o padrão de saída 25 atribuindo a ele o resultado de uma adição módulo dois entre um segundo valor determinado b_2, o valor atual s do padrão de saída 25, e o valor E do padrão de busca 7, se o conteúdo da segunda janela é igual ao valor do padrão de busca 7 ($s \leftarrow s \oplus b_2 \oplus E$).

[00130] A etapa E43 consiste em atualizar o padrão de saída 25 atribuindo a ele o resultado de uma adição módulo dois entre o valor atual s do padrão de saída 25, o dito segundo valor determinado b_2, o valor E do padrão de busca 7, e o valor "1", se o conteúdo f_2 da segunda janela não é igual ao valor do padrão de busca ($s \leftarrow s \oplus b_2 \oplus E \oplus 1$).

[00131] As etapas E44 e E45 formam um laço que consiste em deslocar a primeira janela bit por bit na direção dos bits seguintes enquanto o conteúdo da segunda janela não for igual ao bit do padrão de busca 7.

[00132] A etapa E46 consiste em deslocar a segunda janela de um bit, do bit atual para o bit seguinte.

[00133] Finalmente, a etapa E47 consiste em fazer sair do gerador 1 o padrão de saída 25.

[00134] Assim, a série de operações do terceiro modo de realização pode ser definida da seguinte maneira:

- colocar como única regra do primeiro conjunto de regras, a regra $r_{1,1}$ = "deslocar de um bit para a direita",
- colocar como regras do segundo conjunto de regras as regras seguintes:

$r_{2,1}$ = "colocar o bit f da primeira janela no padrão de busca ($E \leftarrow f_1$)",

$r_{2,2}$ = "deslocar a primeira janela uma vez de acordo com $r_{1,1}$",

$r_{2,3}$ = "se o conteúdo f_1 da primeira janela, é igual ao bit E do padrão de busca, então atualizar $s \leftarrow b_1 \oplus E$",

$r_{2,4}$ = "se o conteúdo da primeira janela não é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow b_1 \oplus E \oplus 1$",

$r_{2,5}$ = "enquanto o conteúdo da primeira janela não for igual ao bit E do padrão de busca, deslocar a primeira janela de acordo com a regra $r_{1,1}$",

$r_{2,6}$ = "deslocar a primeira janela uma vez de acordo com $r_{1,1}$".

$r_{2,7}$ = "substituir o valor do padrão de busca pelo bit f_2 da segunda janela",

$r_{2,8}$ = "deslocar a segunda janela uma vez de acordo com $r_{1,1}$",

$r_{2,9}$ = "se o conteúdo f_2 da segunda janela é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow s \oplus b_2 \oplus E$",

$r_{2,10}$ = "se o conteúdo f_2 da segunda janela não é igual ao bit E do padrão de busca, então atualizar o padrão de saída $s \leftarrow s \oplus b_2 \oplus E \oplus 1$",

$r_{2,11}$ = "enquanto o conteúdo f_2 da segunda janela não for igual ao bit E do padrão de busca, deslocar a segunda janela de acordo com $r_{1,1,}$",

$r_{2,12}$ = "deslocar a segunda janela uma vez de acordo com $r_{1,1}$",

- aplicar na ordem as regras $r_{2,1}$ a $r_{2,12}$, e
- extrair o padrão s de saída.

[00135] Esquematicamente, o terceiro modo de realização é o mesmo que adicionar bit a bit as saídas obtidas executando-se em paralelo por um lado o segundo modo de realização com a primeira janela inicialmente posicionada no primeiro bit da sequência de dados inicial 9, e por outro lado o segundo modo de realização com a segunda janela inicialmente posicionada no segundo bit da sequência de dados inicial 9.

[00136] Esses modos de realização são fáceis de realizar. Além disso sua relação entre o número de bits extraídos e o número de bits calculados é em média 1/3 quando, por exemplo, o meio inicial 11 que dá a sequência de dados inicial 9 é um registrador de deslocamento com retroalimentação linear.

[00137] Assim, o processo de acordo com a invenção permite criar uma sequência

de bits pseudo-aleatória de boa qualidade que pode ser utilizada para a cifragem simétrica do tipo cifragem que flutua.

[00138] De fato, cada bit da sequência de dados pseudo-aleatória 3 pode ser combinado com um bit correspondente de uma sequência de dados de uma mensagem 45 a cifrar por uma adição módulo 2 para formar uma sequência de dado cifrada 47 (ver a figura 2).

REIVINDICAÇÕES

1. Processo de geração de uma sequência de dados pseudo-aleatória (3), executada por um gerador de sequência de dados pseudo-aleatória (1), a dita sequência de dados pseudo-aleatória (3) sendo usada como um fluxo chave em um método de cifragem de fluxo e sendo criada a partir de um procedimento de busca de pelo menos um padrão de busca (7) para um bit em uma sequência de dados inicial (9) de N bits movendo uma janela (19) com um tamanho de um bit através da dita sequência de dados inicial (9), a dita janela sendo colocada em uma posição determinada inicial e a dita sequência de dados inicial sendo criada por um meio compreendendo um registrador de deslocamento de retroalimentação linear, caracterizado pelo fato de que o dito procedimento de busca compreende as seguintes etapas:

- colocar (E11) o bit da janela em um padrão de busca;

- detectar (E12, E13) o dito padrão de busca (7) na dita sequência de dados inicial (9) movendo a dita janela (19) através da dita sequência de dados inicial (9);

- determinar (E14-E17) um padrão de saída (25) de um bit de acordo com uma operação que depende da execução da etapa precedente, o dito padrão de saída sendo determinado:

• de acordo com uma primeira lei (E14), se a janela é deslocada somente uma vez antes de detectar o padrão de busca na sequência de dados inicial, a dita primeira lei atribuindo um valor chamado o valor de saída ao padrão de saída; e

• de acordo com uma segunda lei (E15) do contrário, a dita segunda lei atribuindo ao padrão de saída o resultado da adição módulo dois entre o valor chamado o valor de saída e o valor 1;

- deslocar (E18) a janela por um bit, do bit atual para o bit seguinte; e

- repetir as etapas precedentes de maneira sucessiva para formar a sequência de dados pseudo-aleatória (3) concatenando os padrões de saída (25).

2. Processo de acordo com a reivindicação 1, caracterizado pelo fato de que o valor chamado o valor de saída é igual a:

- um valor determinado; ou

- o resultado da adição módulo dois entre um valor determinado e o padrão de

busca.

3. Processo de acordo com a reivindicação 1 ou 2, caracterizado pelo fato de que as etapas de detectar (E1) o dito padrão de busca (7) e de determinar (E2) o dito padrão de saída (25) são realizadas por uma série de operações compreendendo um primeiro conjunto de regras que possibilita definir pelo menos um modo de deslocamento para deslocar a janela (19) através da dita sequência de dados inicial (9) para detectar o dito pelo menos um padrão de busca (7).

4. Processo de acordo com a reivindicação 3, caracterizado pelo fato de que a série de operações compreende também um segundo conjunto de regras que determinam as condições de interrupção do deslocamento da dita janela (19) através da dita sequência de dados inicial (9).

5. Processo de acordo com a reivindicação 4, caracterizado pelo fato de que pelo menos uma das regras do dito segundo conjunto de regras gerencia uma atualização do padrão de busca e/ou do dito padrão de saída, de acordo com o deslocamento e/ou o conteúdo da dita janela.

6. Processo de acordo com a reivindicação 3 ou 4, caracterizado pelo fato de que a série de operações é repetida até que uma condição previamente determinada seja preenchida.

7. Processo de acordo com a reivindicação 3 ou 4, caracterizado pelo fato de que a série de operações é modificada depois de cada execução.

8. Processo de acordo com a reivindicação 3 ou 4, caracterizado pelo fato de que a série de operações permanece invariável depois de cada execução.

9. Processo de acordo com qualquer uma das reivindicações 1 a 8, caracterizado pelo fato de que cada bit da dita sequência de dados pseudo-aleatória é combinado com um bit correspondente a uma sequência de dados de uma mensagem a ser criptografada por uma adição módulo dois para formar uma sequência de dados criptografada.

10. Dispositivo de codificação (39) compreendendo um gerador de uma sequência de dados pseudo-aleatória (3), o dito dispositivo de decodificação sendo adequado para produzir uma cifragem de fluxo utilizando a sequência de dados pseudo-

aleatória gerada como um fluxo chave, o dito gerador compreendendo um meio inicial (11) para criar uma sequência de dados inicial de N bits compreendendo um registrador de deslocamento de retroalimentação linear, e um meio de busca (5) para buscar por pelo menos um padrão de busca (7) de um bit na sequência de dados inicial (9) de N bits, movendo uma janela com um tamanho de um bit de um meio de detecção do meio de busca através da dita sequência de dados inicial, a dita janela sendo colocada em uma posição inicial determinada, o dito meio de busca (5) também compreendendo um meio de determinação (15) e um meio de repetição (17), caracterizado pelo fato de que:

- o meio de detecção (15) é capaz de colocar o bit da janela em um padrão de busca;

- o meio de detecção (13) é capaz de detectar o padrão de busca (7) na dita sequência de dados inicial (9) movendo a dita janela através da dita sequência de dados inicial;

- o meio de determinação (15) é capaz de determinar um padrão de saída (25) de um bit de acordo com uma operação que depende da execução da detecção do dito pelo menos um padrão de busca (7), o dito padrão de saída sendo determinado:

• de acordo com uma primeira lei, se a janela é deslocada somente uma vez antes de detectar o dito pelo menos um padrão de busca na sequência de dados inicial, a dita primeira lei atribuindo um valor chamado o valor de saída ao padrão de saída; e

• de acordo com uma segunda lei (E15) do contrário, a dita segunda lei atribuindo ao padrão de saída o resultado da adição módulo dois entre o valor chamado o valor de saída e o valor 1;

- o meio de detecção é capaz de deslocar a janela por um bit, do bit atual para o bit seguinte; e

- o meio de repetição (17) é capaz de gerar a sequência de dados pseudo-aleatória (3) concatenando os padrões de saída (25).

11. Dispositivo de codificação de acordo com a reivindicação 10, caracterizado pelo fato de que o valor chamado o valor de saída é igual a:

- um valor determinado; ou

- o resultado da adição módulo dois entre um valor determinado e o padrão de busca.

12. Dispositivo de codificação de acordo com a reivindicação 10 ou 11, caracterizado pelo fato de que o meio de detecção (13) compreende um primeiro meio de controle (21) para controlar o deslocamento da dita janela através da dita sequência de dados inicial.

13. Dispositivo de codificação de acordo com a reivindicação 12, caracterizado pelo fato de que o meio de determinação (15) compreende um segundo meio de controle (27) para atualizar o dito padrão de busca e/ou o dito padrão de saída.

14. Dispositivo de codificação de acordo com qualquer uma das reivindicações 10 a 13, caracterizado pelo fato de também compreender uma porta lógica OU exclusivo.

15. Sistema seguro compreendendo pelo menos duas entidades (33a, 33b) caracterizado pelo fato de que cada uma das ditas pelo menos duas entidades (33a, 33b) compreende um dispositivo de codificação (39a, 39b) do tipo definido na reivindicação 14.

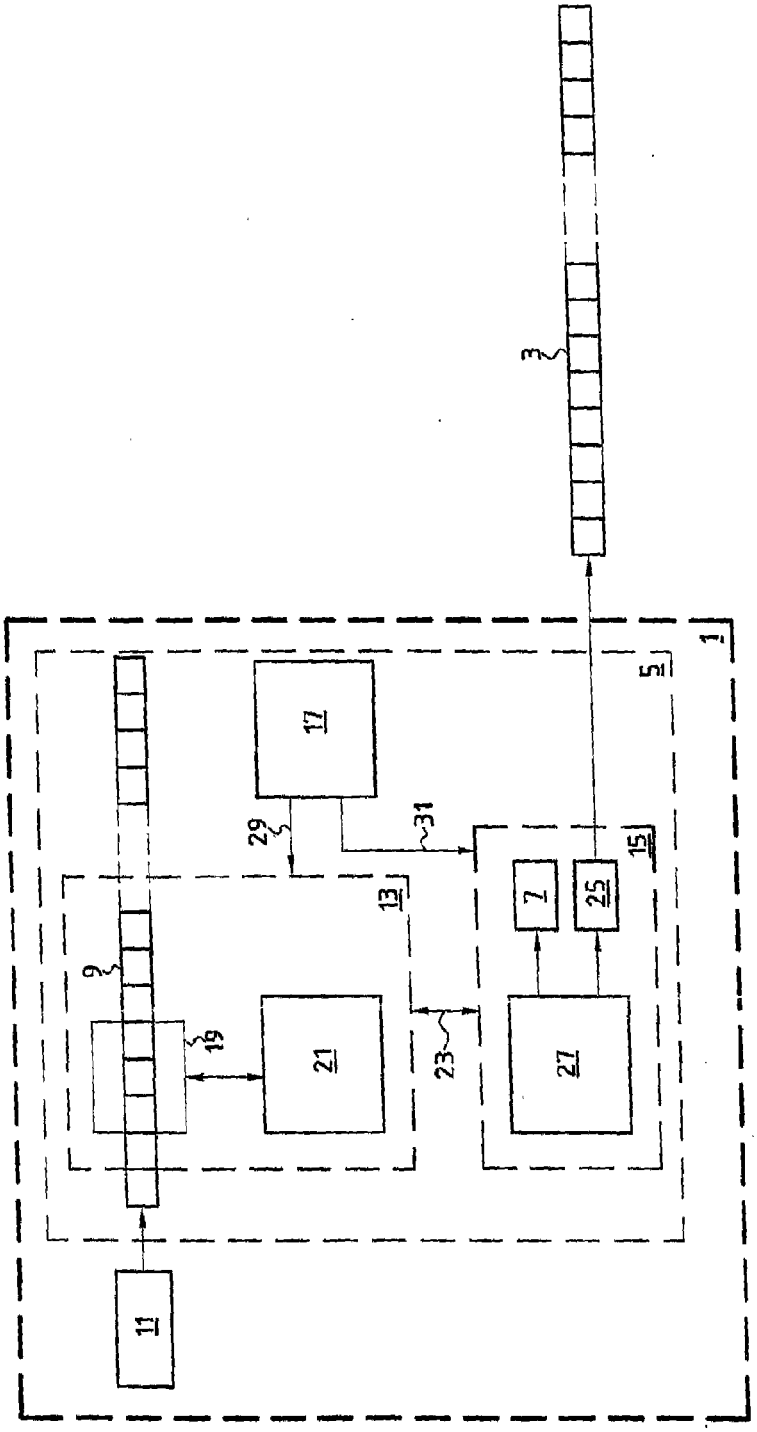

FIG.1

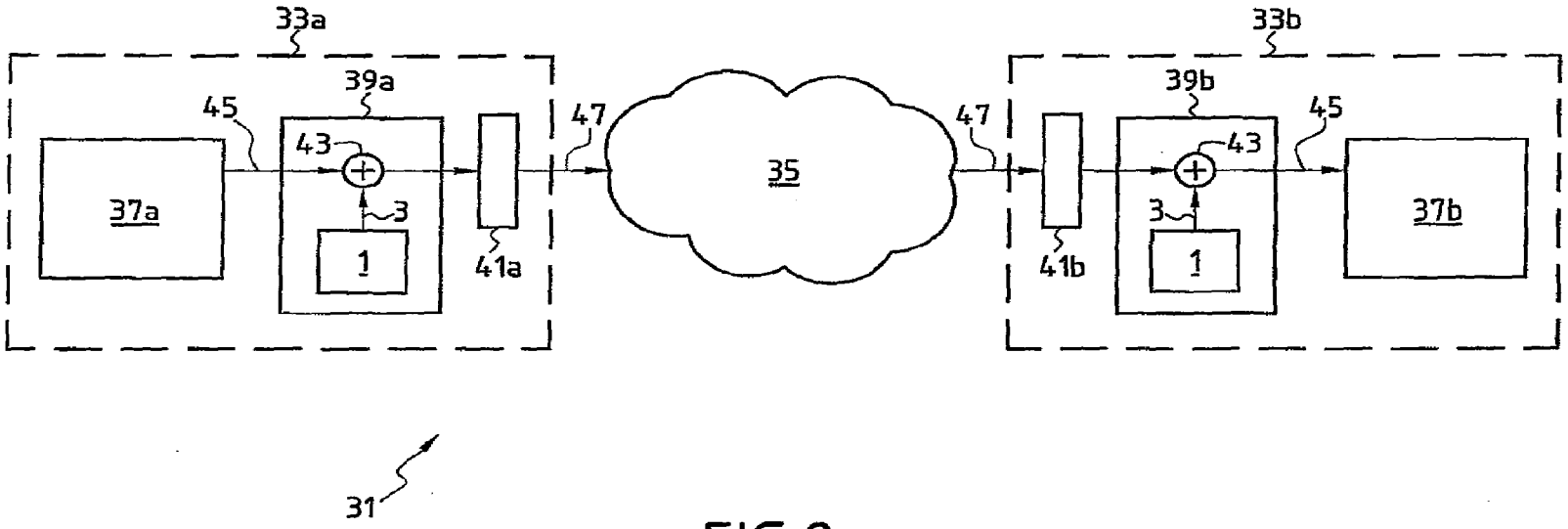

FIG.2

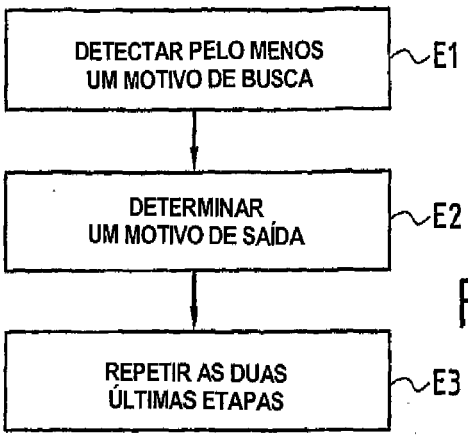
DETECTAR PELO MENOS UM MOTIVO DE BUSCA
E1
DETERMINAR UM MOTIVO DE SAÍDA
E2
REPETIR AS DUAS ÚLTIMAS ETAPAS
E3

FIG.3

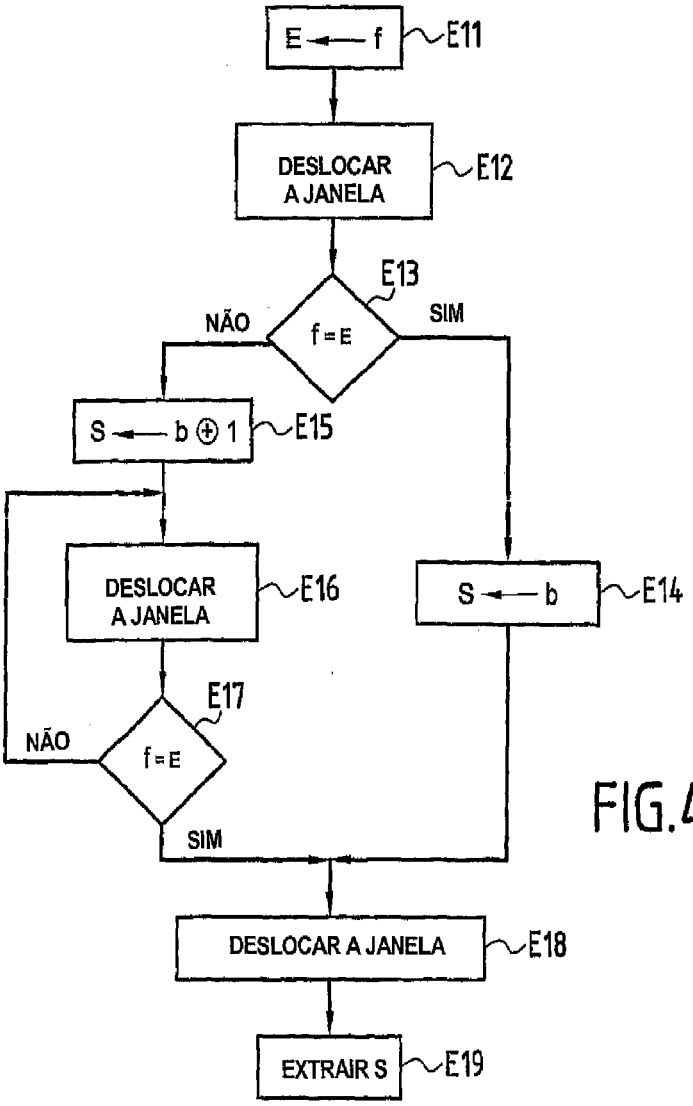
E ← f
E11
DESLOCAR A JANELA
E12
E13
f = E
NÃO
SIM
S ← b ⊕ 1
E15
DESLOCAR A JANELA
E16
S ← b
E14
E17
f = E
NÃO
SIM
DESLOCAR A JANELA
E18
EXTRAIR S
E19

FIG.4

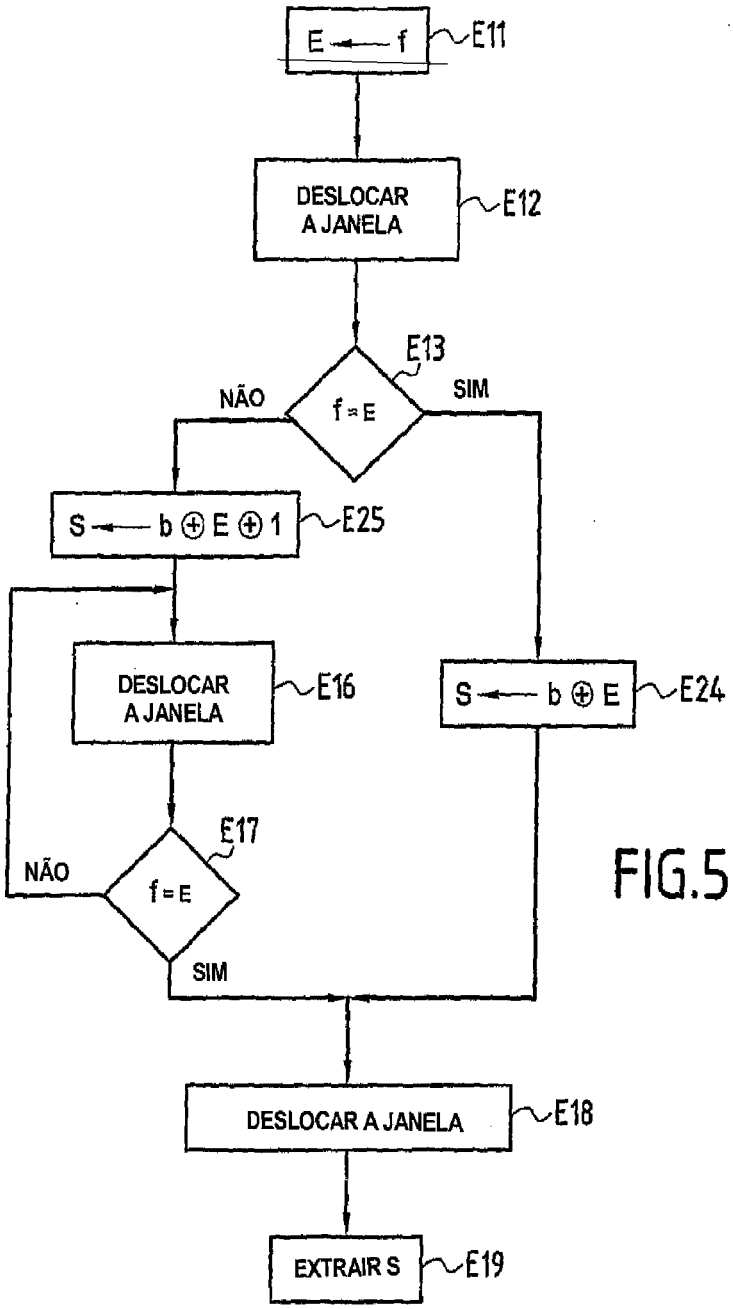

FIG.5

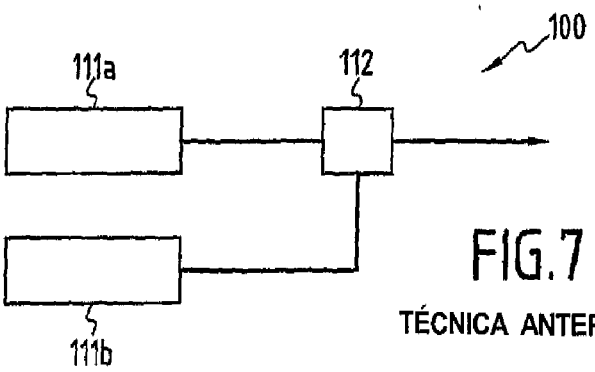

FIG.7

TÉCNICA ANTERIOR

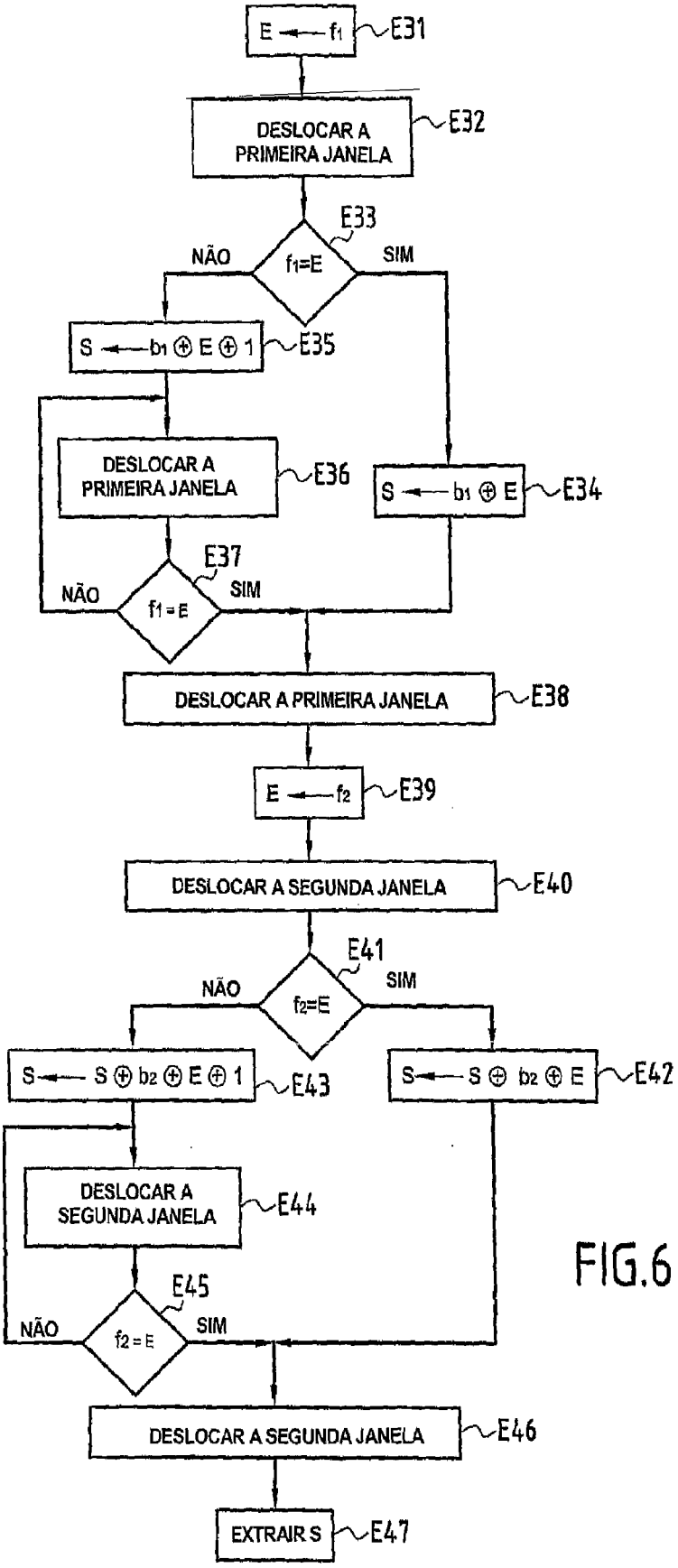
E ← f1
E31
DESLOCAR A PRIMEIRA JANELA
E32
E33
NÃO
f1=E
SIM
S ← b1 ⊕ E ⊕ 1
E35
DESLOCAR A PRIMEIRA JANELA
E36
S ← b1 ⊕ E
E34
E37
NÃO
f1 = E
SIM
DESLOCAR A PRIMEIRA JANELA
E38
E ← f2
E39
DESLOCAR A SEGUNDA JANELA
E40
E41
NÃO
f2=E
SIM
S ← S ⊕ b2 ⊕ E ⊕ 1
E43
S ← S ⊕ b2 ⊕ E
E42
DESLOCAR A SEGUNDA JANELA
E44
E45
NÃO
f2 = E
SIM
DESLOCAR A SEGUNDA JANELA
E46
EXTRAIR S
E47

FIG.6