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

(21) **PI0607201-1 A2**

* B R P I 0 6 0 7 2 0 1 A 2 *

(22) Data de Depósito: 13/02/2006
(43) Data da Publicação: 02/03/2010
(RPI 2043)

(51) Int.Cl.:
H04L 9/26 (2010.01)

(54) Título: **PROCESSO DE GERAÇÃO DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, GERADOR DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, DISPOSITIVO DE CODIFICAÇÃO/ DECODIFICAÇÃO, E, SISTEMA TORNADO SEGURO**

(30) Prioridade Unionista: 14/02/2005 FR 0501481

(73) Titular(es): France Telecom

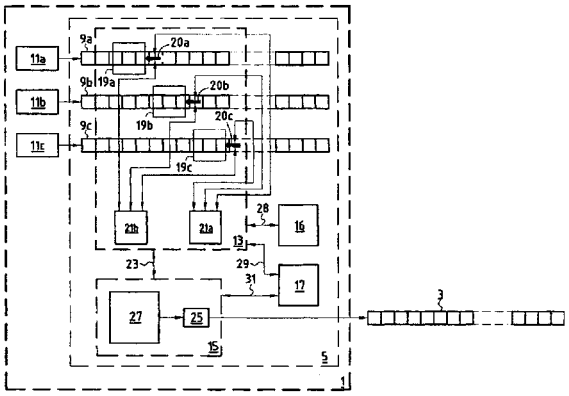
(72) Inventor(es): ALINE GOUGET, HERVÉ SIBERT

(74) Procurador(es): Momsen, Leonardos & CIA.

(86) Pedido Internacional: PCT FR2006050124 de 13/02/2006

(87) Publicação Internacional: WO 2006/085038de 17/08/2006

(57) Resumo: PROCESSO DE GERAÇÃO DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, GERADOR DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATORIA, DISPOSITIVO DE CODIFICAÇÃO/DECODIFICAÇÃO, E, SISTEMA TORNADO SEGURO. A invenção se refere a um processo e a um gerador de uma sequência de dados pseudo-aleatória (3), que compreende um meio de combinação (5) para combinar dados que pertencem a uma pluralidade de seqüências de dados iniciais (9a, 9b, 9c) de acordo com um processo de busca de pelo menos um motivo de busca.



"PROCESSO DE GERAÇÃO DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, GERADOR DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, DISPOSITIVO DE CODIFICAÇÃO/ DECODIFICAÇÃO, E, SISTEMA TORNADO SEGURO"

Domínio técnico da invenção

A invenção é relativa ao domínio da codificação/decodificação e se refere a um sistema e a um processo de geração de uma seqüência de dados pseudo-aleatória.

A invenção encontra uma aplicação muito vantajosa pelo fato de que ela permite criar sucessões de bits destinadas à codificação simétrica, para a qual a codificação e decodificação utilizam uma mesma chave secreta. Por um lado, a invenção se inscreve no âmbito de um processo de codificação em fluxo que consiste em adicionar bit a bit uma mensagem com uma seqüência de dados pseudo-aleatória de mesmo comprimento. Por outro lado, ela se inscreve no âmbito de um processo no qual a operação de codificação e a operação de decodificação são idênticas. Será notado que a codificação simétrica é empregada correntemente em todos os tipos de comunicações, tais como as comunicações móveis (GSM, UMTS...), a Internet (SSL...), os cartões com chip (cartões de banco), etc.

Plano de fundo da invenção

O método mais difundido de codificação em fluxo consiste em gerar uma sucessão codificante de maneira independente da mensagem a codificar recorrendo, com um objetivo de economia material, a registros de decalagem de retroação linear.

O inconveniente maior dos registros de decalagem de retroação linear é a linearidade dos mesmos. De fato, o conhecimento de um número de bits de saída do registro igual ao comprimento do registro assim como do polinômio de retroação associado ao registro permite conhecer os bits de saída assim como todos os estados ulteriores do registro.

De maneira que, a fim de "quebrar" a linearidade dos registros de decalagem de retroação linear, é de costume combinar a saída de vários registros, assim, eventualmente, como seu estado interno, com o auxílio por exemplo de uma função binária não linear.

A figura 6 mostra um tal gerador 100 chamado "*shrinking generator*" descrito não pedido de patente europeu EP 0 619 659 que compreende um primeiro registro de decalagem de retroação linear 111a, um segundo registro de decalagem de retroação linear 111b, e um meio 112 para selecionar a saída do gerador 100.

Assim, a cada decalagem, os dois registros 111a e 111b são deslocados simultaneamente, e a saída do dispositivo 100 é igual à saída do segundo registro 111b se a saída do primeiro registro 111a é "1", senão nenhum bit saiu.

O *shrinking generator* permite combinar não somente as saídas de dois registros de decalagem de retroação linear mas também, mais geralmente, qualquer par de sucessões de bits. O *shrinking generator* faz parte de uma classe de processos de codificação em fluxo, nos quais um registro de decalagem de retroação linear controla um outro. A idéia é fazer o número de decalagens variar, por um lado, entre os diferentes registros empregados e, por outro lado, entre dois bits consecutivos, a fim de quebrar a linearidade dos registros.

Uma variante do *shrinking generator*, chamada "*self-shrinking generator*", repousa no mesmo princípio, mas a partir, desta vez de um só registro. Os bits de saída do registro 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.

Os inconvenientes do emprego de registros de decalagem de retroação linear sozinhos são numerosos. O principal é a fraqueza devida à linearidade do dispositivo. Quando registros 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.

Por outro lado, métodos estatísticos colocaram em evidência certas fraquezas do "*shrinking generator*" e outros processo de codificação de controle de relógio. Em especial, no *shrinking generator*, o número de decalagens efetuadas pelos dois registros entre dois bits de saída varia, mas tem o mesmo valor para os dois registros.

Objeto e sumário da invenção

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

Um outro objetivo é realizar um gerador muito eficaz e pouco custoso.

Esses objetivos são atingidos graças a um processo de geração de uma seqüência de dados pseudo-aleatória constituída por uma sucessão de motivos de saídas, esses motivos de saídas são obtidos com o auxílio das etapas seguintes:

- escolher pelo menos um motivo de busca;

- buscar o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial entre uma pluralidade de seqüências de dados iniciais;

- determinar um motivo de saída de acordo com uma aplicação que depende da dita busca e do conteúdo de pelo menos duas seqüências de dados iniciais entre a dita pluralidade de seqüências de dados iniciais;

- re-atribuir a escolha e a busca de pelo menos um motivo de busca no seio da dita pluralidade de seqüências de dados iniciais.

Assim, o processo de acordo com a invenção é baseado na detecção de motivos que permitem combinar ou "misturar" uma pluralidade

de seqüências de dados iniciais para obter uma seqüência de dados pseudo-aleatória. Ao mesmo tempo em que é simples de realizar, esse processo compreende uma complexidade intrínseca para poder produzir uma seqüência de dados pseudo-aleatória de boa qualidade. De fato, as diferentes operações do processo são distribuídas na pluralidade de seqüências de dados iniciais de modo que a repartição dessas operações seja extremamente difícil de encontrar melhorando então a qualidade da seqüência de dados pseudo-aleatória.

Esse processo permite assim melhorar a complexidade da relação entre as seqüências de dados iniciais e a seqüência de dados pseudo-aleatória de modo que seja difícil preverá seqüência de dados pseudo-aleatória.

Vantajosamente, a dita re-atribuição é realizada em função da dita busca e/ou do conteúdo de pelo menos uma seqüência de dados inicial da dita pluralidade de seqüências de dados iniciais.

Assim, a distribuição das operações nas seqüências de dados iniciais pode variar no decorrer do desenrolar do processo, melhorando ainda mais a qualidade da seqüência de dados pseudo-aleatória.

De acordo com um aspecto da invenção, as ditas etapas são efetuadas por uma sucessão de regras que compreende:

- um primeiro conjunto de regras que permite definir pelo menos um modo de deslocamento para deslocar pelo menos uma janela em cada seqüência de dados inicial da dita pluralidade de seqüências de dados iniciais, cada janela sendo associada a uma seqüência de dados inicial formando assim uma pluralidade de janelas,

- um segundo conjunto de regras que gere a escolha do dito pelo menos um motivo de busca e/ou uma atualização do dito motivo de saída, e/ou da re-atribuição das operações com o auxílio de uma pluralidade de ponteiros que manipulam a dita pluralidade de janelas, e

- um terceiro conjunto de regras que determinam os modos de execuções dos deslocamentos da dita pluralidade de janelas.

Assim, a interação entre as diferentes etapas ou operações pode ser gerida e executada de uma maneira simples e eficaz.

De acordo com um aspecto especial da invenção, a dita pluralidade de seqüências de dados iniciais compreende pelo menos duas seqüências de dados iniciais, e as janelas são de tamanho 1 permitindo ler as ditas pelo menos duas seqüências de dados iniciais de maneira contínua bit a bit para determinar um motivo de saída de 1 bit.

Assim, a busca do ou dos motivos pode ser acelerada ao mesmo tempo em que se economiza o tempo de cálculo.

De acordo com um outro aspecto da invenção, cada bit da dita seqüência de dados pseudo-aleatória pode ser combinado com um bit correspondente de uma seqüência de dados de uma mensagem a codificar por uma adição módulo 2 para formar uma seqüência de dado codificada.

Assim, a seqüência de dado codificada produzida compreende uma complexidade interna que torna difícil sua decodificação. Por outro lado, o mecanismo de decodificação sendo idêntico ao mecanismo de codificação, ele apresenta portanto as mesmas vantagens.

A invenção visa também um gerador de uma seqüência de dados pseudo-aleatória que compreende um meio de combinação para combinar dados que pertencem a uma pluralidade de seqüências de dados iniciais de acordo com um processo de busca de pelo menos um motivo de busca.

Assim, o gerador combina a pluralidade de seqüências de dados iniciais que torna a relação entre a saída do gerador e os estados internos sucessivos do gerador extremamente complexa de modo que seja difícil prever com uma possibilidade diferente de cerca de ½ a próxima saída do gerador.

Além disso, esse gerador é fácil de implementar ao mesmo tempo em que é eficaz e pouco custoso.

Vantajosamente, o meio de combinação do gerador compreende:

- uma pluralidade de ponteiros em correspondência com uma pluralidade de janelas que são destinadas a se deslocar na pluralidade de seqüências de dados iniciais;

- um meio de escolha que age na pluralidade de ponteiros que manipulam a pluralidade de janelas para escolher o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial;

- um meio de detecção que age na pluralidade de ponteiros para buscar o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial;

- um meio de produção para determinar um motivo de saída de acordo com uma aplicação que depende da dita busca e do conteúdo de pelo menos duas seqüências de dados iniciais entre a dita pluralidade de seqüências de dados iniciais;

- um meio de atribuição para re-atribuir as correspondências entre as pluralidades de ponteiros e de janelas para re-atribuir as operações de escolha e de busca de pelo menos um motivo de busca à dita pluralidade de seqüências de dados iniciais; e

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

Assim, esses diferentes meios do gerador permitem distribuir operações na pluralidade de seqüências de dados iniciais, eventualmente de maneira intercambiável, de modo que a dificuldade de previsão da seqüência de dados pseudo-aleatória na saída do gerador seja reforçada.

A invenção visa também um dispositivo de codificação/decodificação que compreende uma porta lógica "ou-exclusivo" e

um gerador de acordo com as características acima.

Esse dispositivo permite combinar cada bit da seqüência de dados pseudo-aleatória com um bit correspondente de uma seqüência de dados de uma mensagem a codificar por uma adição módulo 2 para formar uma seqüência de dado codificada que apresenta uma grande complexidade linear.

A invenção visa também um sistema tornado seguro que compreende pelo menos duas entidades conectadas via uma rede, cada uma das ditas pelo menos duas entidades compreende um dispositivo de codificação/decodificação de acordo com as características acima.

Assim, o sistema tornado seguro compreende uma estrutura simples de realizar ao mesmo tempo em que tem um mecanismo intrinsecamente complexo.

Breve descrição dos desenhos

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:

- a figura 1 ilustra um exemplo muito esquemático de um gerador de uma seqüência de dados pseudo-aleatória, de acordo com a invenção;

- a figura 2 mostra um sistema tornado seguro que compreende geradores da figura 1;

- as figuras 3 a 5 mostram modos de realização especiais de um procedimento de busca para a geração da seqüência de dados pseudo-aleatória, de acordo com a invenção; e

- a figura 6 é uma vista muito esquemática de um gerador de acordo com a arte anterior.

Descrição detalhada de modos de realização

De acordo com a invenção, a figura 1 ilustra um exemplo

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

O gerador 1 compreende um meio de combinação 5 para combinar dados que pertencem a uma pluralidade de seqüências de dados iniciais 9a, 9b e 9c de acordo com um procedimento de busca de pelo menos um motivo de busca. O procedimento de busca faz intervir operações que podem ser atribuídas de maneira variável na pluralidade de seqüências de dados iniciais.

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

Cada seqüência de dados inicial é um fluxo de um número inteiro de bits (por exemplo N bits) de período não igual a "1". Cada seqüência é gerada por um meio inicial que pode compreender um registro de decalagem de retroação linear de período máximo. Assim, o gerador 1 pode compreender uma pluralidade de registros de decalagem 11a, 11b, e 11c que geram a pluralidade de seqüências de dados iniciais 9a, 9b e 9c.

Um registro de decalagem de retroação linear é uma tabela de bits de comprimento finito (o registro) munida de uma combinação linear, representada por um polinômio chamado de polinômio de retroação das casas da tabela. A cada decalagem, o bit de índice mais elevado saiu, todos os outros bits são deslocados de um índice, e o bit de índice menor toma o valor da combinação linear antes da decalagem.

Vantajosamente, o polinômio de retroação pode por exemplo ser um polinômio primitivo que corresponde a um registro de decalagem de retroação linear que produz uma sucessão de período máximo, ou então um polinômio da forma $Q = (x^2 + 1)P$, com P um polinômio primitivo.

Em uma tal sucessão de período máximo T, é sabido que todas

as palavras ou motivos de comprimento L (onde $T = 2^L-1$) aparecem pelo menos uma vez.

O meio de combinação 5 do gerador 1 compreende um meio de busca 13 de um ou vários motivos de busca, um meio de determinação 15, um meio de atribuição 16 e um meio de repetição 17.

O meio de busca 13 é destinado a buscar um ou vários motivos de busca e compreende uma pluralidade de janelas 19a, 19b e 19c, uma pluralidade de ponteiros 20a, 20b e 20c, um meio de escolha 21a, e um meio de detecção 21b.

As janelas 19a, 19b, 19c têm tamanhos não nulos e são destinadas a se deslocar na pluralidade de seqüências de dados iniciais 9a, 9b, 9c. Cada janela é associada a uma e uma única seqüência de dado inicial 9a, 9b, 9c e pode ser colocada em uma posição inicial determinada em uma seqüência de dados inicial e possui um tamanho determinado de bits. Por exemplo, uma janela de tamanho t colocada em uma seqüência de dados inicial de tamanho N (t sendo um número inteiro inferior a N e inferior ou igual a L) é uma máscara que pode se deslocar nessa seqüência deixando aparecer a cada deslocamento exatamente t bits da seqüência de dado inicial. Assim, a cada deslocamento, os bits que se encontram nas janelas 19a, 19b, 19c podem ser utilizados para determinar a saída do gerador 1.

Por outro lado, as janelas 19a, 19b, 19c podem ser manipuladas pelos ponteiros 20a, 20b, 20c que estão em correspondência com essas janelas 19a, 19b, 19c. Será notado que essa correspondência entre as janelas 19a, 19b, 19c e os ponteiros 20a, 20b, 20c pode variar ao longo de toda a geração da seqüência de dados pseudo-aleatória 3.

De fato, o meio de escolha 21a age sobre a pluralidade de ponteiros 20a, 20b, 20c que manipulam a pluralidade de janelas 19a, 19b, 19c para escolher o ou os motivos de busca em pelo menos uma seqüência de dados inicial.

Do mesmo modo, o meio de detecção 21b pode também agir sobre os ponteiros 20a, 20b, 20c para controlar o deslocamento das janelas 19a, 19b, 19c nas seqüências de dados iniciais 9a, 9b, 9c a fim de buscar o ou os motivos de busca em pelo menos uma seqüência de dados inicial. Assim, os motivos a buscar podem eles próprios depender do conteúdo das janelas.

A título de exemplo, o meio de detecção 21b pode detectar um motivo de busca de t bits escolhido pelo meio de escolha 21a em uma seqüência de dados inicial de N bits, onde t é um número inteiro inferior ou igual a L. Assim, ele está certo de encontrar o motivo de busca em uma seqüência de dados inicial de período igual a 2^L-1.

Será notado que a escolha e a detecção do ou dos motivos de busca podem ser realizadas em seqüências de dados iniciais diferentes ou nas mesmas seqüências de dados iniciais.

Por outro lado, o meio de determinação 145 está em interação com o meio de busca 13 via uma ligação 23 e compreende um motivo de saída 25 e um meio de produção 27.

O meio de produção 27 é destinado a determinar um motivo de saída 25 (por exemplo de t bits) de acordo com uma aplicação que depende da busca e do conteúdo de pelo menos duas seqüências de dados inicial da dita pluralidade de seqüências de dados iniciais 9a, 9b, 9c.

Será notado que o meio de determinação 15 pode também compreender um meio de controle para definir ou atualizar um conjunto de motivos de busca. Esse conjunto de motivos de busca pode, por exemplo, ser vazio, ou depender do conteúdo das janelas ou ainda depender do histórico da busca de motivos.

Por outro lado, o meio de atribuição 16 está em interação com o meio de busca 13 via uma ligação 28. Esse meio de atribuição 16 é destinado a re-atribuir as correspondências entre as pluralidades de ponteiros 20a, 20b, 20c e janelas 19a, 19b, 19c e a re-atribuir as operações de escolha e

de busca do ou dos motivos de busca à pluralidade de seqüências de dados iniciais 9a, 9b, 9c.

Vantajosamente, a re-atribuição é realizada em função da busca, quer dizer em função do desenrolar das operações realizadas pelos meios de busca 13 e de determinação 15 e/ou do conteúdo de pelo menos uma seqüência de dados inicial da pluralidade de seqüências de dados iniciais 9a, 9b, 9c.

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

Assim, o meio de repetição 17 pode trocar sinais com os meios de busca 13 e de terminação 15 para recomeçar as operações de busca de motivo de busca e de determinação do motivo de saída, por exemplo depois de ter recebido do meio de determinação 15 o sinal de que um motivo de saída 15 acaba de ser determinado, isso enquanto uma condição de paralisação previamente determinada não for preenchida. O meio de repetição 17 pode por outro lado testar a condição de paralisação graças às trocas de sinais com os meios de busca 13 e de determinação 15. Isso permite gerar uma sucessão de motivos de saída 25 que formam por concatenação a seqüência de dados pseudo-aleatória 3.

Será notado que os meios de atribuição 16 e de repetição 17 podem também ser integrados ao meio de busca 13 ou ao meio de determinação 15.

Assim, os diferentes meios de gerador 1 permitem separar as operações de escolher um motivo de busca, de buscar um motivo de busca e de produzir um motivo de saída. Por outro lado, esses meios permitem distribuir as etapas ou operações em vários fluxos ou seqüências de dados iniciais e modificar o mecanismo de atribuição depois de cada execução ou produção de um motivo de saída.

A figura 2 mostra um sistema tornado seguro 30 que

compreende pelo menos duas entidades conectadas entre si via uma rede de comunicação 35 de tipo Internet, GSM, UMTS, etc.

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

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

Cada um dos primeiro e segundo dispositivo de codificação/decodificação 39a, 39b compreende um gerador 1 de uma seqüência de dados pseudo-aleatória 3 tal como descrito precedentemente e uma porta lógica "ou-exclusivo" 43.

Cada dispositivo de codificação/decodificação 39a, 39b é destinado a fazer uma codificação ou uma decodificação em fluxo que consiste em codificar ou decodificar uma mensagem bit após bit.

De acordo com esse exemplo, o primeiro dispositivo de codificação/decodificação 39a faz uma operação de codificação. Assim, a seqüência de dados pseudo-aleatória 3 chamada de sucessão codificante, é combinada pela porta ou-exclusivo 43 com cada bit de posição correspondente de uma mensagem não codificada 45 enviada pelo primeiro terminal 37a para obter um texto codificado 47 que é em seguida enviado pelo primeiro modem 41a para a segunda entidade 33b. Assim, a operação de codificação consiste em adicionar bit a bit uma sucessão codificante 3 ao texto não codificado da mensagem 45 para obter o texto codificado.

O segundo dispositivo de codificação/decodificação 39b faz uma operação de decodificação que consiste em adicionar bit a bit essa

mesma sucessão codificante 3 ao texto codificado 47 enviado pela primeira entidade 33a para reformar a mensagem para o texto não codificado 45. Assim, as operações de codificação e de decodificação são idênticas.

De uma maneira geral, o processo de acordo com a invenção consiste em gerar a seqüência de dados pseudo-aleatória 3 combinando para isso dados que pertencem às seqüências de dados iniciais 9a, 9b, 9c de acordo com um procedimento de busca de pelo menos um motivo de busca.

Assim, é possível dispor de n seqüências de dados iniciais 9a, 9b, 9c ou fluxo de bits. Em cada seqüência de dados, se desloca pelo menos uma janela de tamanho não nulo e então é possível dispor de *k* janelas (k sendo superior ou igual a n).

No início do processo, cada janela se encontra em uma posição inicial na seqüência de dados à qual ela é associada (por exemplo, cada uma das janelas pode ser posicionada no início da seqüência de dados à qual ela é associada). As k janelas podem ser manipuladas por k ponteiros 20a, 20b, 20c.

Será anotado em tudo o que se segue, o valor de um motivo de busca por E, o valor do motivo de saída 25 por s, e os números dos ponteiros 20a, 20b, 20c nas janelas k por pf_1, pf_2,... pf_k.

Por outro lado, o processo de acordo com a invenção compreende uma sucessão de etapas. Uma primeira etapa consiste em escolher o ou os motivos de busca.

Será notado que o ou os motivos de busca podem ser predeterminados, ou de preferência escolhidos em pelo menos uma seqüência de dados inicial 9a, 9b, 9c.

Uma segunda etapa consiste em buscar o ou os motivos de busca em pelo menos uma seqüência de dados inicial 9a, 9b, 9c.

Uma terceira etapa consiste em determinar um motivo s de saída 25 de acordo com uma aplicação que depende da busca e do conteúdo

de pelo menos uma seqüência de dados inicial da pluralidade de seqüências de dados iniciais 9a, 9b, 9c. Assim, o motivo *s* de saída pode por exemplo, ser vazio, ou depender do conteúdo das janelas, ou ainda depender da execução das etapas precedentes do processo. De fato, a determinação do motivo *s* de saída 25 pode depender dos motivos de busca e da histórico da busca, em especial do número de etapas ou de iterações efetuadas antes de encontrar o motivo E de busca em questão na ou nas seqüências de dados iniciais 9a, 9b, 9c.

Uma quarta etapa consiste em re-atribuir as operações de escolha e de detecção de pelo menos um motivo E de busca no seios da pluralidade de seqüências de dados iniciais 9a, 9b, 9c. A re-atribuição pode ser realizada em função da busca e/ou do conteúdo de pelo menos uma seqüência de dados inicial da pluralidade de seqüências de dados iniciais 9a, 9b, 9c.

Essas etapas ou operações precedentes são repetidas de maneira sucessiva para formar a seqüência de dados pseudo-aleatória 3 a partir de uma sucessão de motivos s de saída 25.

Por outro lado, essas operações são efetuadas por uma sucessão de regras.

Essa sucessão de regras compreende um primeiro conjunto de regras R1 implementadas pelo meio de combinação 5 do gerador 1, que permite definir pelo menos um modo de deslocamento para deslocar pelo menos uma janela 19a, 19b, 19c em cada seqüência de dados inicial da pluralidade de seqüências de dados iniciais 9a, 9b, 9c para escolher e/ou detectar o ou os motivos E de busca.

O primeiro conjunto de regras R1 pode definir o sentido de deslocamento, a amplitude de deslocamento, ou a forma de deslocamento das janelas 19a, 19b, 19c,, por exemplo um deslocamento cíclico em uma parte das seqüências de dados iniciais 9a, 9b, 9c.

A título de exemplo, o primeiro conjunto de regras R1 pode compreender uma regra $r_{1,1}$ definida da seguinte maneira:

$r_{1,1}$ = "deslocar de um bit para a direita".

Por outro lado, a sucessão de operações compreende um segundo conjunto de regras R2 implementado pelo meio de combinação 5 do gerador 1, que gere a escolha do ou dos motivos E de busca e/ou uma atualização do motivo s de saída, e/ou a re-atribuição das operações aos meios dos ponteiros 20a, 20b, 20c que manipulam as janelas 19a, 19b, 19c.

Finalmente, a sucessão de operações compreende um terceiro conjunto de regras R3 implementado pelo meio de combinação 5 do gerador 1 que determina os modos de execução dos deslocamento da pluralidade de janelas 19a, 19b, 19c, por exemplo as condições de paralisação do deslocamento da ou das janelas nas diferentes seqüências de dados iniciais 9a, 9b, 9c.

Pelo menos uma das regras de atualização do segundo conjunto de regras R2 depende da execução de pelo menos uma das regras do terceiro conjunto de regras R3 e de pelo menos uma das regras do primeiro conjunto de regras R1 da forma seguinte: "enquanto o conteúdo da janela indicada por pf_i não for um motivo do conjunto de motivos, deslocar as janelas indicadas por pf_{j1}, pf_{j2},..., pf_{jn} de acordo com a regras r_{k1}, r_{k2},..., r_{ki},..., r_{km}", onde os r_{ki} são regras do primeiro conjunto de regras R1.

Será notado que, a sucessão de etapas ou de operações pode ser repetida até que uma condição previamente determinada seja preenchida. Por exemplo, a sucessão de operações é repetida até que a aplicação de uma das regras faça sair uma janela de uma seqüência de dados inicial, se essa última acabou. Também é possível repetir a sucessão de operações até que uma condição definida pelo usuário seja preenchida.

Por outro lado, pode também ser considerado modificar a sucessão de operações depois de cada execução.

Assim, a determinação dos elementos da seqüência de dados pseudo-aleatória de acordo com a invenção pode depender da distribuição das operações nas seqüências de dados iniciais, da variação dessa distribuição, do ou dos motivos buscados, e do histórico ou da maneira pela qual a busca foi realizada.

As figuras 3 a 5 mostram modos de realização especiais do processo de acordo com a invenção.

De acordo com esses exemplos, a sucessão de operações permanece invariável depois de cada execução, a pluralidade de seqüências de dados iniciais 9a, 9b, 9c compreende pelo menos duas seqüências de dados iniciais que podem ser as saídas de pelo menos dois registros 11a, 11b, 11c de decalagem de retroação linear (LFSR) de período máximo. Por outro lado, a ou as janelas 19a, 19b, 19c são de "tamanho um" (quer dizer que cada janela compreende 1 bit), o conjunto de motivos de busca contém pelo menos um motivo de busca E, e os motivos de busca e de saída 25 são também de tamanho um (quer dizer que cada motivo compreende 1 bit).

Além disso, a amplitude de deslocamento das janelas 19a, 19b, 19c é igual a uma unidade, quer dizer que cada janela se desloca de um bit a cada iteração, por exemplo, do bit corrente para o bit seguinte (quer dizer da esquerda para a direita).

Assim, cada seqüência de dados inicial 9a, 9b, 9c pode ser lida de uma maneira contínua, quer dizer bit a bit, o que faz modos de realização muito simples a implementar.

No início, os motivos de busca e de saída 25 são inicializados atribuindo-se para isso um bit vazio a cada um deles, quer dizer $E \leftarrow \phi$ e $s \leftarrow \phi$, ϕ sendo o conjunto vazio.

De acordo com o primeiro modo de realização, duas janelas 19a e 19b se deslocam em suas seqüências de dados iniciais 9a e 9b. A janela 19a se desloca na seqüência de dados inicial 9a, e a janela 19b se desloca na

seqüência de dados inicial 9b. Cada janela é inicializada no primeiro bit da seqüência de dados associada. Dispõe-se de dois ponteiros 20a, 20b (numerados pf_1 e pf_2) nas janelas 19a e 19b. Nesse primeiro modo de realização, os ponteiros 20a, 20b nas janelas 19a e 19b não são modificados no decorrer da execução, quer dizer que o ponteiro pf_1 indica sempre a janela 19a e o ponteiro pf_2 indica sempre a janela 19b. Do mesmo modo, define-se um valor binário constante anotado b que permanece fixo no decorrer da execução, quer dizer a cada aplicação da sucessão de operações do processo desse primeiro modo de realização.

A sucessão de operações do primeiro modo de realização pode ser definida da seguinte maneira:

- colocar como única regra de deslocamento de R1, a regra $r_{1,1}$ = "deslocar de um bit apara a direita",

- colocar como regras de atualização do segundo conjunto de regras R2, as seguintes regras:

$r_{2,1}$ = "colocar o bit da janela indicada por pf_1 em E";

$r_{2,2}$ = "se o conteúdo da janela indicada por pf_2 é um motivo de RE, então atualizada $s \leftarrow b$";

$r_{2,3}$ = "se o conteúdo da janela indicada por pf_2 não é um motivo de E, então atualizar $s \leftarrow b \oplus 1$".

- colocar como terceiro conjunto de regras R3, as seguintes regras:

$r_{3,1}$ = "enquanto o conteúdo da janela indicada por pf_2 não for um motivo de E, deslocar a janela indicada por pf_2 de acordo com a regra $r_{1,1}$";

$r_{3,2}$ = "deslocar as janelas indicadas por pf_1 e pf_2 de acordo com a regra $r_{1,1}$";

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

- tirar o motivo s de saída.

De fato, o organograma da figura 3 mostra o desenrolar da sucessão de operações acima.

Na etapa E11, o meio de escolha 21a age sobre o ponteiro 20a para escolher o motivo de busca E. Dito de outra forma, essa etapa consiste em colocar o bit da janela 19 a indicada por pf_1 no motivo de busca E.

Em seguida, o meio de detecção 21b age sobre o ponteiro 20b (numerado pf_2) para buscar o motivo de busca E na seqüência de dados inicial 9b. Assim, a etapa E12 é um teste que compara o conteúdo da janela 19b indicada por pf_2 com aquele do motivo de busca E.

Na etapa E13, o meio de produção 27 atualiza o motivo s de saída 25 de acordo com uma primeira lei ($s \leftarrow b$).

Assim, o conteúdo da janela 19b indicada por pf_2 é igual àquele do motivo de busca E, então o motivo de saída 25 toma o valor determinado b.

Na etapa E14, o meio de produção 27 atualiza o motivo de saída 25 de acordo com uma segunda lei ($s \leftarrow b \oplus 1$). Assim, se o conteúdo da janela 19b indicada por pf_2 não é um motivo do conjunto E, então o motivo s toma o valor complementar do bit b, quer dizer fazer uma adição módulo dois entre o valor determinado b e o valor "1" e atribuir o resultado dessa adição ao motivo de saída 25,

De acordo com esse modo de realização, o meio de atribuição 16 atribui sempre a mesma correspondência entre os ponteiros 20a, 20b e as janelas 19a, 19b.

Assim, as etapas E15 e E16 formam um laço que consiste em deslocar (etapa E15) a janela 19b indicada por pf_2 bit por bit na direção dos bits seguintes enquanto o conteúdo da janela 19b não for igual (teste E16) ao bit do motivo de busca E.

A etapa E17 consiste em deslocar as janelas 19a e 19b indicadas pelos ponteiros pf_1 e pf_2 de um bit, do bit corrente para o bit

seguinte.

Finalmente, na etapa E18, o meio de repetição 17 faz o motivo de saída s sair do gerador 1, a fim de gerar a seqüência de dados pseudo-aleatória 3 permitindo assim a repetição das etapas precedentes.

Esquematicamente, a sucessão de operações pode ser resumida assim: lê-se o conteúdo na janela 19a indicada por pf_1, e depois enquanto o bit contido na janela indicada por pf_2 não coincidir com o bit contido na janela indicada por pf_1, desloca-se a janela indicada por pf_2 de uma posição para a direita. Se a janela indicada por pf_2 não foi deslocada, então tira-se b, senão tira-se $b \oplus 1$. Desloca-se em seguida as duas janelas de um bit para a direita antes de recomeçar.

Naturalmente, o organograma pode compreender um teste de paralisação (não representado na figura por preocupação com a simplificação) para determinar se uma condição previamente definida está preenchida.

A título de exemplo, essas etapas podem ser repetidas para formar a seqüência de dados pseudo-aleatória até que a janela 19b indicada pelo ponteiro pf_2 saia da seqüência de dados inicial 9.

A figura 4 é um organograma que mostra o desenrolar da sucessão de operações de um segundo modo de realização.

Esse segundo modo de realização compreende três seqüências de dados iniciais 9a, 9b e 9c e três janelas 19a, 19b e 19c de comprimento "1". A janela 19a se desloca na seqüência 9a, a janela 19b se desloca na seqüência 9b e a janela 19c se desloca na seqüência 9c. Cada uma dessas três janelas está inicialmente posicionada no primeiro bit da seqüência de dados associada.

São definidos três ponteiros 20a, 20b, 20c numerados pf_1, pf_2 e pf_3 nas janelas 19a, 19b e 19c. A inicialização pf_1 indica a janela 19a, pf_2 indica a janela 19b e pf_3 indica a janela 19c. É definido um quarto ponteiro numerado pf_{temp} que será utilizado para estocar temporariamente o valor de

pf_1 por ocasião das modificações dos valores de pf_1, pf_2 e pf_3. O conjunto E dos motivos de busca é inicializado no conjunto vazio antes de cada execução da sucessão de operações ou mecanismo do processo.

A sucessão de operações ou mecanismo do segundo modo de realização pode ser definida da seguinte maneira:

- coloca-se como única regra de deslocamento de R_1 a regra $r_{1,1}$ = "de um bit para a direita",

- coloca-se como regras de atualização de R_2 as regras:

$r_{2,1}$ = "colocar o bit da janela indicada por pf_1 em E",

$r_{2,2}$ = "colocar o bit da janela indicada por pf_3 em s",

$r_{2,3}$ = "modificar os valores dos ponteiros efetuando-se para isso a permutação circular seguinte: pf_{temp} indica a janela indicada por pf_1, e depois; pf_1 indica a janela indicada por pf_2, e depois; pf_2 indica a janela indicada por pf_3, e depois; pf_3 indica a janela apontada por pf_{temp}",

- coloca-se como regras de execução de R_3 as regras:

$r_{3,1}$ = "enquanto o conteúdo da janela indicada por pf_2 não for um motivo do conjunto E, aplicar a regra $r_{1,1}$ às janelas indicadas por pf_2 e pf_3",

$r_{3,2}$ = "aplicar a regra $r_{1,1}$ às janelas indicadas por pf_1, pf_2 e pf_3",

- aplica-se na ordem as regras $r_{2,1}$, $r_{3,1}$, $r_{2,2}$, $r_{2,3}$ e $r_{3,2}$.

- tira-se o motivo *s* de saída.

Assim, na etapa E21 do organograma da figura 4, o meio de escolha 21a age sobre o ponteiro 20a para escolher o motivo de busca E. Isso consiste em colocar o bit da janela 19a indicada por pf_1 no motivo de busca E.

Em seguida, o meio de detecção 21b age sobre o ponteiro numerado pf_2 para buscar o motivo de busca E.

As etapas E22 e E23 formam então um laço que consiste em verificar que enquanto o conteúdo da janela indicada por pf_2 não for um

motivo de E (teste E22), as janelas indicadas por pf_2 e pf_3 são deslocadas (etapa E23) bit por bit para a direita.

Na etapa E24, o meio de produção 27 dá ao motivo s, o valor do bit da janela indicadas por pf_3.

Na etapa E25, o meio de atribuição 16 re-atribui os valores de pf_1, pf_2 e pf_3 da seguinte maneira: pf_1 toma o valor de pf_2, pf_2 toma o valor de pf_3 e pf_3 toma o valor precedente de pf_1.

Na etapa E26, o meio de detecção 21b age sobre os ponteiros para deslocar as janela sindicadas por pf_1, pf_2 e pf_3 bit por bit para a direita.

Finalmente, na etapa E27, o meio de repetição 17 faz o motivo de saída s sair do gerador 1, a fim de gerar a seqüência de dados pseudo-aleatória 3 permitindo assim a repetição das etapas precedentes.

Esquematicamente, a sucessão de operações pode ser resumida assim: lê-se o bit E corrente da janela indicada por pf_1, e depois enquanto o bit da janela indicada por pf_2 não coincidir com o bit E, as janelas indicadas por pf_2 e pf_3 são deslocadas de uma posição para a direita; o motivo s de saída toma o valor do bit contido na janela indicada por pf_3; opera-se uma permutação nos três ponteiros pf_1, pf_2 e pf_3; e depois desloca-se as três de uma posição antes de recomeçar.

A figura 5 é um organograma que mostra o desenrolar da sucessão de operações de um terceiro modo de realização.

Esse terceiro modo de realização compreende duas seqüências de dados iniciais 9a, 9b e duas janelas 19a e 19b. A janela 19a se desloca na seqüência 9a e a janela 19b se desloca na seqüência 9b. Cada janela é inicialmente fixada no primeiro bit da seqüência associada. São definidos dois ponteiros 20a e 20b numerados pf_1 e pf_2 nas janelas 19a, 19b. Na inicialização pf_1 indica a janela 19a e pf_2 indica a janela 19b.

A sucessão de operações ou mecanismo do terceiro modo de realização pode ser definido da seguinte maneira:

- coloca-se como única regra de deslocamento de R_1 a regra $r_{1,1}$ = "de um bit para a direita",

- coloca-se como regras de atualização de R_2 as regras:

$r_{2,1}$ = "colocar o bit da janela indicada por pf_1 em E",

$r_{2,2}$ = "atribuir a s o valor do bit da janela indicada por pf_1",

$r_{2,3}$ = "trocar os valores dos ponteiros pf_1 e pf_2",

- coloca-se como regras de execução de R_3 as regras:

$r_{3,1}$ = "deslocar a janela indicada por pf_1 de acordo com $r_{1,1}$",

$r_{3,2}$ = "enquanto o conteúdo da janela indicada por pf_1 não for um motivo do conjunto E, deslocar a janela indicada por pf_1 de acordo com $r_{1,1}$",

$r_{3,3}$ = "se s não for um motivo de E, então aplicar a regra $r_{2,3}$",

- aplica-se na ordem as regras $r_{2,1}$, $r_{3,1}$, $r_{2,2}$, $r_{3,2}$, $r_{3,1}$ e $r_{3,3}$.

- tira-se o motivo *s* de saída.

Assim, na etapa E31 do organograma da figura 4, o meio de escolha 21a age sobre o ponteiro 20a para escolher o motivo de busca E. Isso consiste em colocar o bit da janela indicada por pf_1 no conjunto E.

Na etapa E32, o meio de detecção 21b desloca a janela indicada por pf_1 de um bit para a direita.

Na etapa E33, o meio de produção 27 permite que o motivo s tome o valor do bit contido na janela indicada por pf_1.

Em seguida, o meio de detecção 21b age sobre o ponteiro numerado pf_1 para buscar o motivo de busca E.

Assim, as etapas E34 e E35 indicam que enquanto o conteúdo da janela indicada por pf_1 não for um motivo E (teste E34), a janela indicaDA POR PF_1 É DESLOCAda (etapa E35) bit por bit para a direita.

Na etapa E36, a janela indicada por pf_1 é deslocada de um bit para a direita.

As etapas E37 e E38 indicam que se o motivo não é um

motivo do conjunto E, então os valores dos ponteiros pf_1 e pf_2 são torçados pelo meio de atribuição 16 (etapa E38).

Finalmente, o meio de repetição 17 permite, na etapa E39, fazer o motivo de saída s sair do gerador 1.

Esquematicamente, a sucessão de operações pode ser resumida assim; o motivo E é inicializado com o conteúdo da janela indicada por pf_1, e depois a janela indicada por pf_1 é deslocada de uma posição para a direita e o motivo s toma o valor do bit da janela indicada por pf_1; enquanto o conteúdo da janela indicada por pf_1 não for um motivo E, a janela indicadas por pf_1 é deslocada de uma posição para a direita; a janela indicada por pf_1 é então deslocada de uma posição para a direita: se o motivo s não for um motivo de E, então os valores dos ponteiros pf_1 e pf_2 são trocados, e o motivo s é tirado.

Assim, o processo de acordo com a invenção consiste, a partir de várias seqüências de bits iniciais, em construir uma nova seqüência de bits proveniente de deslocamentos de janelas de acordo com regras nas seqüências iniciais. Vantajosamente, a seleção de motivos é distribuída em várias seqüências iniciais que podem ser intercambiadas no decorrer do desenrolar do processo permitindo assim produzir uma seqüência de bit pseudo-aleatória de boa qualidade.

Os modos de realização propostos são rápidos e sua implementação material é menos custosa do que aquela dos sistemas de codificação que fazem intervir funções binárias. Eles são adaptados para a codificação de comunicações de alta vazão (Internet, GSM, UMTS, WiFi).

De fato, cada bit da seqüência de dados pseudo-aleatória 3 pode ser combinado com um bit correspondente de uma seqüência de dados de uma mensagem 45 a codificar por uma adição módulo 2 para formar uma seqüência de dado codificada 47 (ver a figura 2).

REIVINDICAÇÕES

1. Processo de geração de uma seqüência de dados pseudo-aleatória (3) constituída por uma sucessão de motivos de saídas (25), caracterizado pelo fato de que esses motivos de saídas (25) são obtidos com o auxílio das etapas seguintes:

- escolher pelo menos um motivo de busca;

- buscar o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial entre uma pluralidade de seqüências de dados iniciais (9a, 9b, 9c);

- determinar um motivo de saída (25) de acordo com uma aplicação que depende da dita busca e do conteúdo de pelo menos duas seqüências de dados iniciais entre a dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c); e

- re-atribuir a escolha e a busca de pelo menos um motivo de busca no seio da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c).

2. Processo de acordo com a reivindicação 1, caracterizado pelo fato de que a dita re-atribuição é realizada em função da dita busca e/ou do conteúdo de pelo menos uma seqüência de dados inicial da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c).

3. Processo de acordo com uma qualquer das reivindicações 1 e 2, caracterizado pelo fato de que as ditas etapas são efetuadas por uma sucessão de regras que compreende:

- um primeiro conjunto de regras que permite definir pelo menos um modo de deslocamento para deslocar pelo menos uma janela (19a, 19b, 19c) em cada seqüência de dados inicial da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c), cada janela sendo associada a uma seqüência de dados inicial formando assim uma pluralidade de janelas (9a, 9b, 9c);

- um segundo conjunto de regras que gere a escolha do dito

pelo menos um motivo de busca e/ou uma atualização do dito motivo de saída (25), e/ou da re-atribuição das operações com o auxílio de uma pluralidade de ponteiros que manipulam a dita pluralidade de janelas (19a, 19b, 19c), e

- um terceiro conjunto de regras que determinam os modos de execuções dos deslocamentos da dita pluralidade de janelas.

4. Processo de acordo com a reivindicação 3, caracterizado pelo fato de que a dita pluralidade de seqüências de dados iniciais compreende pelo menos duas seqüências de dados iniciais, e pelo fato de que as janelas (19a, 19b, 19c) são de tamanho 1 permitindo ler as ditas pelo menos duas seqüências de dados iniciais de maneira contínua bit a bit para determinar um motivo de saída (25) de 1 bit.

5. Processo de acordo com uma qualquer das reivindicações 1 a 4, caracterizado pelo fato de que cada bit da dita seqüência de dados pseudo-aleatória (3) é combinado com um bit correspondente de uma seqüência de dados de uma mensagem a codificar por uma adição módulo 2 para formar uma seqüência de dado codificada.

6. Gerador de uma seqüência de dados pseudo-aleatória (3), caracterizado pelo fato de que ele compreende um meio de combinação (5) para combinar dados que pertencem a uma pluralidade de seqüências de dados iniciais (9a, 9b, 9c) de acordo com um processo de busca de pelo menos um motivo de busca.

7. Gerador de acordo com a reivindicação 6, caracterizado pelo fato de que o meio de combinação (5) compreende:

- uma pluralidade de ponteiros (20a, 20b, 20c) em correspondência com uma pluralidade de janelas (19a, 19b, 19c) que são destinadas a se deslocar na pluralidade de seqüências de dados iniciais (9a, 9b, 9c);

- um meio de escolha (21a) que age na pluralidade de ponteiros (20a, 20b, 20c) que manipulam a pluralidade de janelas (19a, 19b,

19c) para escolher o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial;

- um meio de detecção (21b) que age na pluralidade de ponteiros (20a, 20b, 20c) para buscar o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial;

- um meio de produção (27) para determinar um motivo de saída (25) de acordo com uma aplicação que depende da dita busca e do conteúdo de pelo menos duas seqüências de dados iniciais entre a dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c);

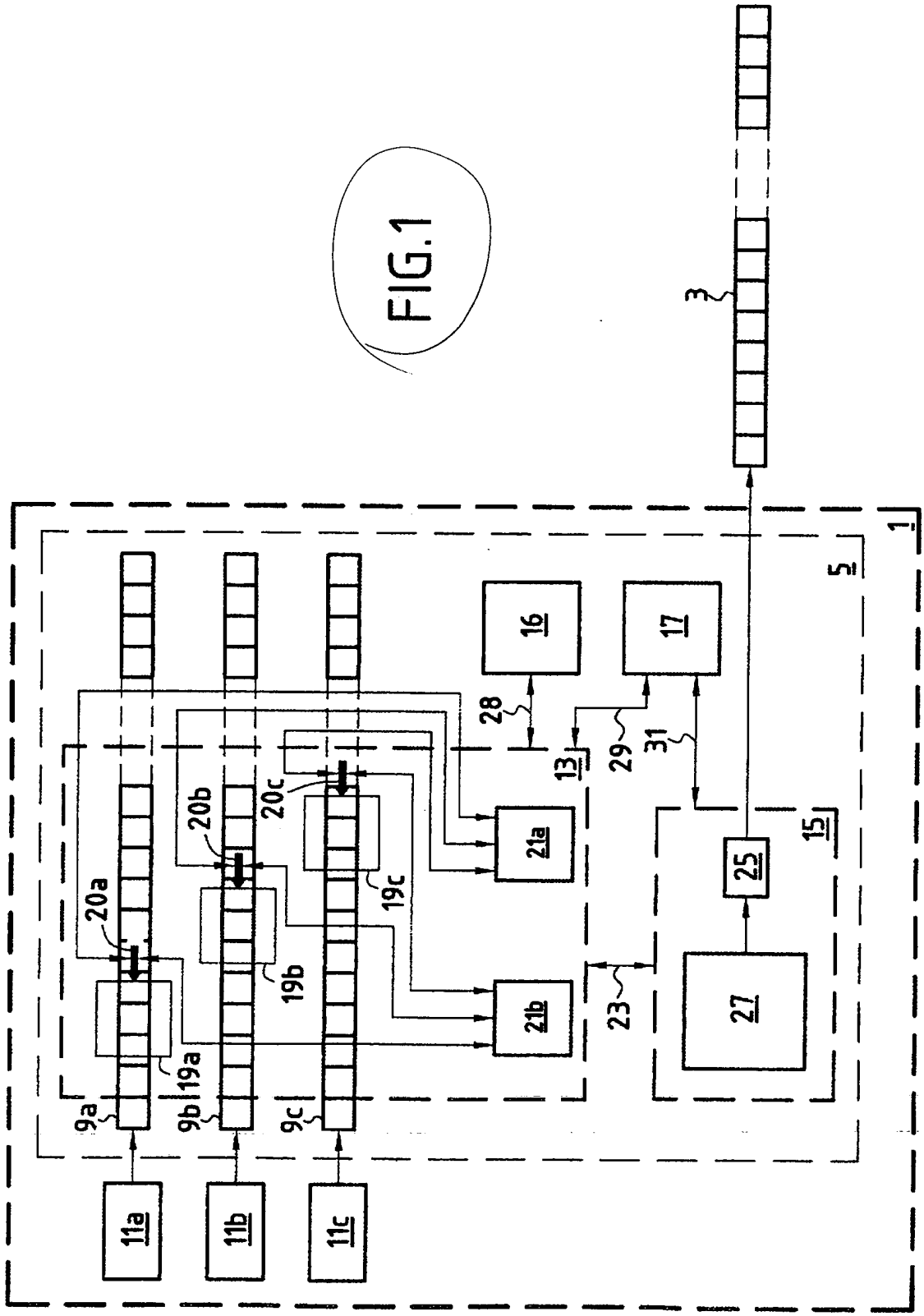
- um meio de atribuição (16) para re-atribuir as correspondências entre as pluralidades de ponteiros (20a, 20b, 20c) e de janelas (19a, 19b, 19c) para re-atribuir as operações de escolha e de busca de pelo menos um motivo de busca ano seio da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c); e

- um meio de repetição (17) para gerar a seqüência de dados pseudo-aleatória (3) a partir de uma sucessão de motivos de saída (25).

8. Dispositivo de codificação/decodificação (39a, 39b) que compreende uma porta lógica ou-exclusivo (43), caracterizado pelo fato de que ele compreende por outro lado um gerador (1) de acordo com uma qualquer das reivindicações 6 e 7.

9. Sistema tornado seguro (30) que compreende pelo menos duas entidades (33a, 33b) conectadas via uma rede (35), caracterizado pelo fato de que cada uma das ditas pelo menos duas entidades compreende um dispositivo de codificação/decodificação (39a, 39b) de acordo com a reivindicação 8.

FIG.1


1
5
3
11a
11b
11c
9a
9b
9c
19a
19b
19c
20a
20b
20c
21a
21b
13
15
16
17
23
25
27
28
29
31

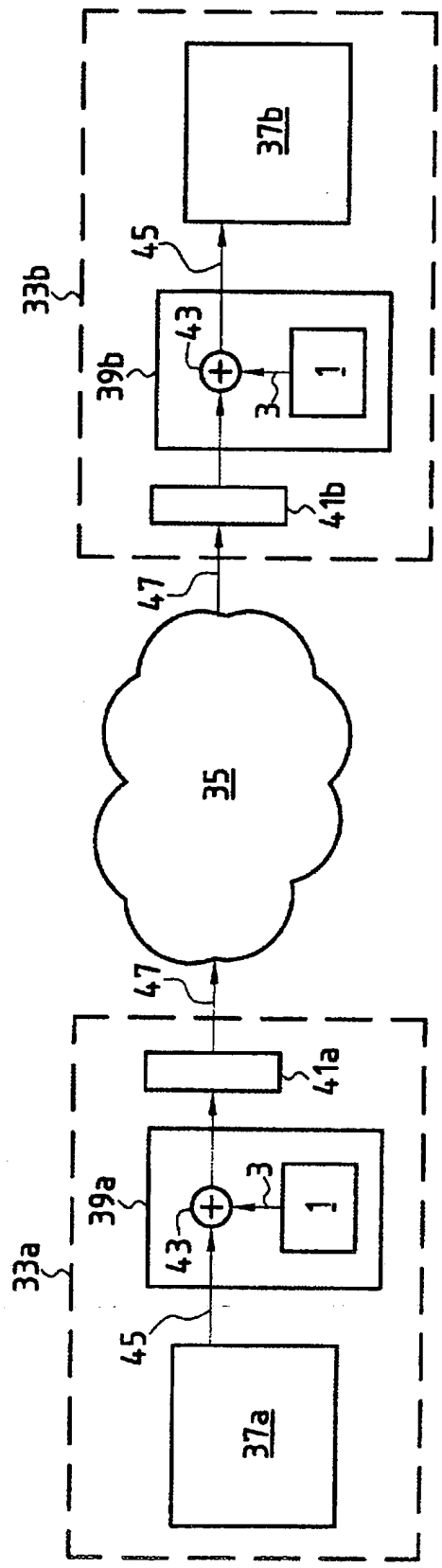


FIG.2

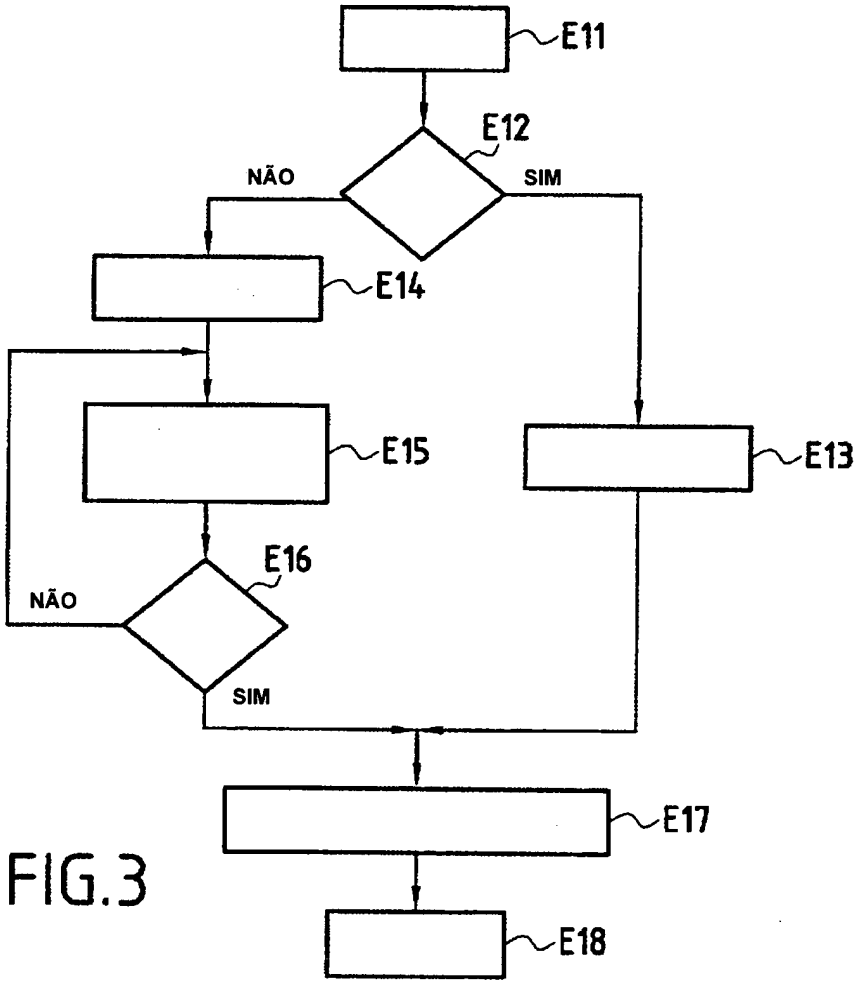

E11
E12
NÃO
SIM
E14
E15
E13
E16
NÃO
SIM
E17
E18

FIG.3

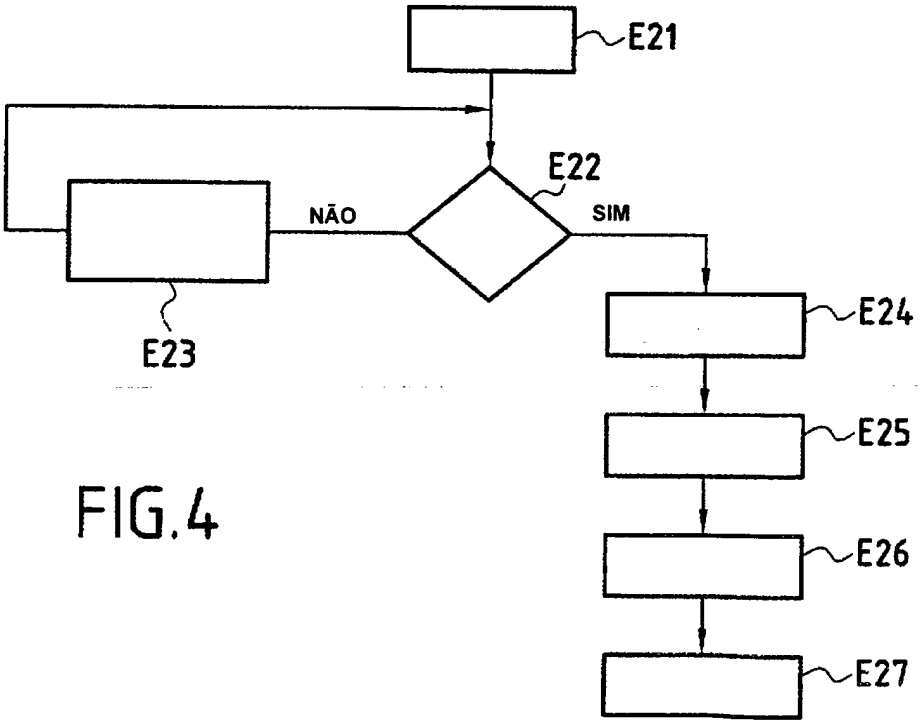

E21
E22
NÃO
SIM
E23
E24
E25
E26
E27

FIG.4

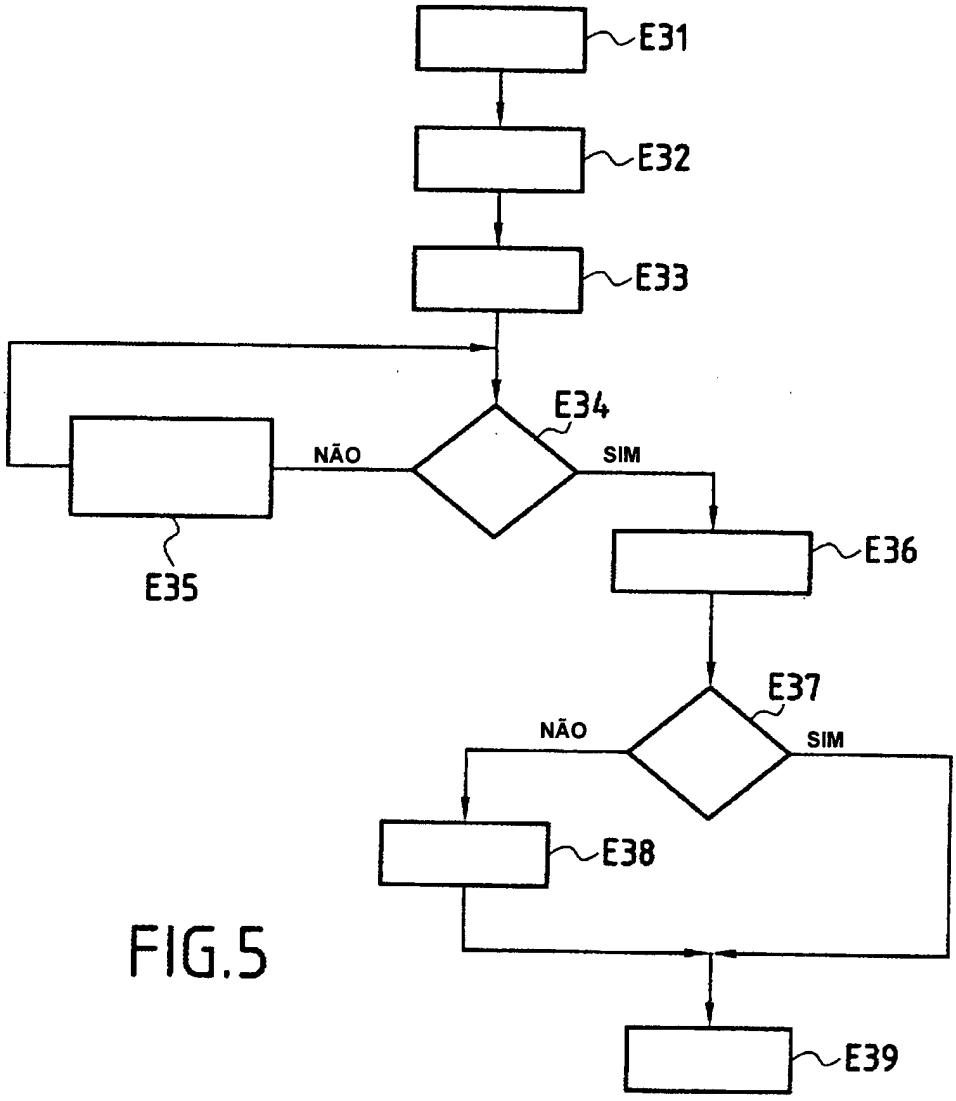


FIG.5

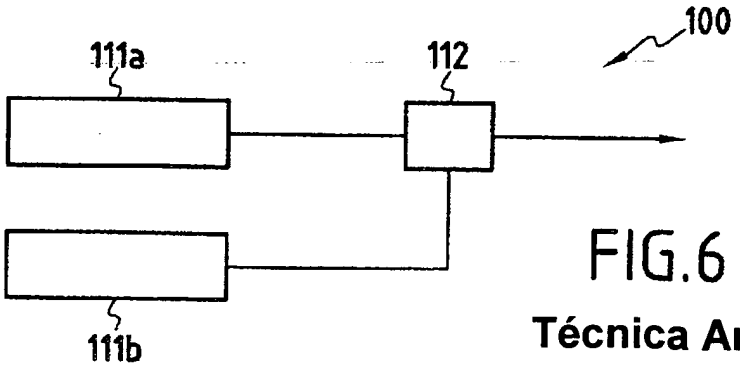


FIG.6

Técnica Anterior

RESUMO

"PROCESSO DE GERAÇÃO DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, GERADOR DE UMA SEQÜÊNCIA DE DADOS PSEUDO-ALEATÓRIA, DISPOSITIVO DE CODIFICAÇÃO/ DECODIFICAÇÃO, E, SISTEMA TORNADO SEGURO"

A invenção se refere a um processo e a um gerador de uma seqüência de dados pseudo-aleatória (3), que compreende um meio de combinação (5) para combinar dados que pertencem a uma pluralidade de seqüências de dados iniciais (9a, 9b, 9c) de acordo com um processo de busca de pelo menos um motivo de busca.

A requerente apresenta novas vias das reivindicações para colocar o pedido em conformidade com o respectivo pedido internacional.

REIVINDICAÇÕES

1. Processo de geração de uma seqüência de dados pseudo-aleatória (3) constituída por uma sucessão de motivos de saídas (25), caracterizado pelo fato de que esses motivos de saídas (25) são obtidos com o auxílio das etapas seguintes:

- escolher pelo menos um motivo de busca;

- buscar o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial entre uma pluralidade de seqüências de dados iniciais (9a, 9b, 9c);

- determinar um motivo de saída (25) de acordo com uma aplicação que depende da dita busca e do conteúdo de pelo menos duas seqüências de dados iniciais entre a dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c); e

- re-atribuir a escolha e a busca de pelo menos um motivo de busca no seio da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c).

2. Processo de acordo com a reivindicação 1, caracterizado pelo fato de que a dita re-atribuição é realizada em função da dita busca e/ou do conteúdo de pelo menos uma seqüência de dados inicial da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c).

3. Processo de acordo com uma qualquer das reivindicações 1 e 2, caracterizado pelo fato de que as ditas etapas são efetuadas por uma sucessão de regras que compreende:

- um primeiro conjunto de regras que permite definir pelo menos um modo de deslocamento para deslocar pelo menos uma janela (19a, 19b, 19c) em cada seqüência de dados inicial da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c), cada janela sendo associada a uma seqüência de dados inicial formando assim uma pluralidade de janelas (9a, 9b, 9c);

- um segundo conjunto de regras que gere a escolha do dito

pelo menos um motivo de busca e/ou uma atualização do dito motivo de saída (25), e/ou da re-atribuição das operações com o auxílio de uma pluralidade de ponteiros que manipulam a dita pluralidade de janelas (19a, 19b, 19c), e

- um terceiro conjunto de regras que determinam os modos de execuções dos deslocamentos da dita pluralidade de janelas.

4. Processo de acordo com a reivindicação 3, caracterizado pelo fato de que a dita pluralidade de seqüências de dados iniciais compreende pelo menos duas seqüências de dados iniciais, e pelo fato de que as janelas (19a, 19b, 19c) são de tamanho 1 permitindo ler as ditas pelo menos duas seqüências de dados iniciais de maneira contínua bit a bit para determinar um motivo de saída (25) de 1 bit.

5. Processo de acordo com uma qualquer das reivindicações 1 a 4, caracterizado pelo fato de que cada bit da dita seqüência de dados pseudo-aleatória (3) é combinado com um bit correspondente de uma seqüência de dados de uma mensagem a codificar por uma adição módulo 2 para formar uma seqüência de dado codificada.

6. Gerador de uma seqüência de dados pseudo-aleatória (3), caracterizado pelo fato de que ele compreende um meio de combinação (5) para combinar dados que pertencem a uma pluralidade de seqüências de dados iniciais (9a, 9b, 9c) de acordo com um processo de busca de pelo menos um motivo de busca, o meio de combinação (5) compreendendo:

- uma pluralidade de ponteiros (20a, 20b, 20c) em correspondência com uma pluralidade de janelas (19a, 19b, 19c) que são destinadas a se deslocar na pluralidade de seqüências de dados iniciais (9a, 9b, 9c);

- um meio de escolha (21a) que age na pluralidade de ponteiros (20a, 20b, 20c) que manipulam a pluralidade de janelas (19a, 19b, 19c) para escolher o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial;

- um meio de detecção (21b) que age na pluralidade de ponteiros (20a, 20b, 20c) para buscar o dito pelo menos um motivo de busca em pelo menos uma seqüência de dados inicial;

- um meio de produção (27) para determinar um motivo de saída (25) de acordo com uma aplicação que depende da dita busca e do conteúdo de pelo menos duas seqüências de dados iniciais entre a dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c);

- um meio de atribuição (16) para re-atribuir as correspondências entre as pluralidades de ponteiros (20a, 20b, 20c) e de janelas (19a, 19b, 19c) para re-atribuir as operações de escolha e de busca de pelo menos um motivo de busca ano seio da dita pluralidade de seqüências de dados iniciais (9a, 9b, 9c); e

- um meio de repetição (17) para gerar a seqüência de dados pseudo-aleatória (3) a partir de uma sucessão de motivos de saída (25).

7. Dispositivo de codificação/decodificação (39a, 39b) que compreende uma porta lógica ou-exclusivo (43), caracterizado pelo fato de que ele compreende por outro lado um gerador (1) de acordo com a reivindicação 6.

8. Sistema tornado seguro (30) que compreende pelo menos duas entidades (33a, 33b) conectadas via uma rede (35), caracterizado pelo fato de que cada uma das ditas pelo menos duas entidades compreende um dispositivo de codificação/decodificação (39a, 39b) de acordo com a reivindicação 8.