(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 566 922**

(51) Int. CI.:

H04L 9/26 (2006.01)
G06F 7/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.09.2007 E 07804224 (9)**

(97) Fecha y número de publicación de la concesión europea: **06.01.2016 EP 2060057**

(54) Título: **Generación de número aleatorio**

(30) Prioridad:

13.09.2006 GB 0618019
13.09.2006 EP 06270084

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
18.04.2016

(73) Titular/es:

AIRBUS DEFENCE AND SPACE LIMITED (100.0%)
Gunnels Wood Road
Stevenage, Hertfordshire SG1 2AS, GB

(72) Inventor/es:

OMAR, EMAM;
BENNIE, PETER y
GLANFIELD, JAMES STUART

(74) Agente/Representante:

GONZÁLEZ PALMERO, Fe

DESCRIPCIÓN

Generación de número aleatorio

Esta invención se refiere a la generación de número aleatorio y, en particular, a la generación de números aleatorios para su uso en criptografía para comunicaciones seguras con un vehículo espacial o vehículo situado o que se desplaza por la frontera del espacio. El término “espacio” se usa a continuación en el presente documento para significar el espacio o una región relativamente cerca de la Tierra u otro planeta pero que está sustancialmente fuera de la ionosfera de ese planeta y el término “vehículo espacial” significa un vehículo situado o que se desplaza por el espacio tal como se ha definido por tanto.

Se usan comunicaciones seguras, ya sea entre dos o más vehículos espaciales o entre un vehículo espacial tal como un satélite y la Tierra y otro planeta, por motivos de secreto comercial. La clave para un método de comunicación criptográfica es la generación de número aleatorio. Los números aleatorios también pueden ser útiles en otros campos, por ejemplo juegos de azar, protección frente a virus, etc. pero el uso pretendido en esta invención es la comunicación criptográfica.

Se conoce para determinadas aplicaciones de comunicación criptográfica entre Tierra-espacio usar el denominado cifrado de claves simétricas de comunicaciones entre, digamos, un satélite y una estación terrestre. En este método se almacena la misma clave numérica tanto en la estación terrestre como en el satélite. La clave la desconocen terceros y es posible una conexión relativamente segura usando este método.

A medida que aumenta progresivamente el número de bits en la clave numérica, es probable que disminuya la eficiencia de una disposición de clave simétrica en comparación con un esquema de acuerdo de clave asimétrica. Un esquema de acuerdo de clave asimétrica es cuando las estaciones en comunicación generan un número aleatorio que va a usarse para generar una clave. Entonces tiene lugar una serie de intercambios de comunicación entre las estaciones usando un algoritmo conocido. Aunque estas comunicaciones entre las estaciones pueden interceptarse por cualquier tercera parte interesada, la tercera parte no conoce ninguno de los números aleatorios asimétricos seleccionados. Cada estación sólo conoce su propio número aleatorio. El proceso matemático usado entre las estaciones permite que se establezca una única clave segura que no puede calcularse por un observador. Este proceso depende por tanto de la generación por cada parte en comunicación de un número aleatorio seguro.

Para usar un esquema de acuerdo de clave entre un vehículo espacial y una estación terrestre, sería necesario que se generase un número aleatorio en el vehículo espacial. Por ejemplo, si se generase un número pseudoaleatorio mediante un registro de desplazamiento con retroalimentación lineal (LFSR), sin importar cuántos bits contuviese el registro de desplazamiento, el número no se consideraría suficientemente seguro porque tiene una posición inicial conocidas y sigue un patrón conocido.

Es un objeto de la invención proporcionar un medio de establecimiento de un número aleatorio, es decir, un número cuyo patrón no puede determinarse, medio que puede usarse en un vehículo espacial.

También es un objeto de la invención proporcionar un medio de obtención de una clave criptográfica segura mientras se está en un vehículo espacial.

Según un aspecto de la presente invención, se proporciona un método de generación de un número aleatorio en un vehículo espacial que incluye las etapas de proporcionar un dispositivo que tiene una salida que puede emitir una serie de bits en el que la serie de bits de salida es susceptible al cambio tras el impacto sobre el dispositivo de partículas de radiación que se producen libremente en espacio, exponer el dispositivo a dicha radiación durante un periodo suficiente para cambiar al menos uno de los bits, y leer de la salida la serie de bits tal como cambia mediante dicha radiación, mediante lo cual se produce el número aleatorio.

El método proporciona por tanto un medio de generación de un número aleatorio verdadero, en el espacio, usando el fenómeno que se produce de manera natural de radiación espacial aleatoria tal como rayos cósmicos. Se sabe desde hace mucho tiempo que los “iones pesados” provocan inversiones de bits en un dispositivo electrónico tal como una memoria de acceso aleatorio (“RAM”) cuando pasan a su través. Tales eventos se han denominado “redisposiciones de eventos simples” o “SEU” (*single event upsets*). Para que se produzcan tales SEU, se cree actualmente que el vehículo espacial ha de estar a una distancia de aproximadamente 700 km por encima de la Tierra para que esté fuera de manera suficiente de la influencia de la Tierra como para permitir que la radiación sea eficaz, al menos con los dispositivos conocidos actualmente.

La invención trata de aprovechar este fenómeno de manera que proporcione un procedimiento a bordo relativamente económico y sencillo de implementar que sea fiable y eficaz. La RAM y cualquier otro aparato necesario pueden implementarse, preferiblemente en software solo, en una matriz de puertas programables por campo (“FPGA”) o un circuito integrado para aplicaciones específicas (“ASIC”, *application-specific integrated circuit*) de modo que se mantengan al mínimo el coste, volumen y peso. Se cree que otras soluciones para el problema de generación de un número aleatorio en un vehículo espacial implicarían el uso de más hardware. Esto añadiría peso y aumentaría el

consumo de energía y requeriría la cualificación del hardware y por tanto sería más caro.

Por tanto, el dispositivo puede ser una RAM y la etapa de leer del dispositivo puede comprender interrogar a la RAM.

El método puede incluir la etapa de proporcionar un generador de número pseudoaleatorio para propagar una secuencia de bits, legible como salida, y conectar el dispositivo a una entrada del generador de número pseudoaleatorio, mediante lo cual cada cambio en la salida del dispositivo se propagará mediante el generador de número pseudoaleatorio. El generador de número pseudoaleatorio puede ser convenientemente un LFSR y la etapa de propagación del cambio en el estado, o la salida, del dispositivo puede incluir retroalimentar la salida del LFSR al dispositivo.

La etapa de propagación del cambio en la salida del dispositivo puede incluir las etapas de:

a) leer, de una primera dirección de RAM, los bits almacenados en la misma;

b) usar los bits almacenados como valores semilla del LFSR;

c) temporizar el LFSR;

d) leer de una segunda dirección de RAM los bits almacenados en la misma;

e) leer los bits emitidos desde el LFSR tras la temporización de los mismos;

f) combinar los bits almacenados de la segunda dirección de RAM con los bits emitidos desde el LFSR e introducir el resultado en la primera dirección de RAM;

g) leer de la segunda dirección de RAM los bits almacenados en la misma e introducir los bits almacenados en la entrada del LFSR;

h) temporizar el LFSR;

repetir las etapas c) a h) para direcciones de RAM sucesivas hasta que se alcanza una dirección de RAM final, tras lo cual leer la primera dirección de RAM como la siguiente dirección de RAM sucesiva y, cuando se requiera, interrumpir las etapas c) a h) para temporizar sucesivamente el LFSR un número requerido de veces para leer una serie de bits de longitud requerida de la salida del LFSR.

Este procedimiento tiene el efecto de propagar tanto como sea posible los cambios en la salida de la RAM debidos a las inversiones de bits que se han producido como resultado de SEU. La salida del LFSR es por tanto muy diferente de la salida de la RAM. Una alta velocidad de reloj, combinada con un gran número de bits en la RAM y en el LFSR tiene el efecto de poner a disposición números aleatorios extremadamente largos que son, por tanto, adecuados para usarse en el establecimiento de una clave criptográfica, por ejemplo en un esquema de acuerdo de clave asimétrica, o de intercambio de clave.

El método puede incluir ajustar la tasa de temporización del LFSR y un periodo de tiempo durante el que se hace funcionar el método antes de que se lea un número aleatorio, mediante lo cual se asegura un grado de cambio deseado de un valor semilla existente en el LFSR al comienzo del método.

El dispositivo puede seleccionarse del grupo: electrónico y óptico y también del grupo: analógico y digital. Por tanto, puede aplicarse igualmente bien el principio de la invención, efectos de evento simple (“SEE”, *single event effects*) que provocan cambios en un dispositivo, a dispositivos electrónicos u ópticos y a dispositivos analógicos o digitales. Si se eligiese un dispositivo analógico, es posible que los cambios debidos a SEE se produjeran mucho más frecuentemente que con un dispositivo digital ya que el SEE no tiene que tener una fuerza suficiente como para provocar una inversión de bit, sólo un pequeño cambio en el estado, quizá instantáneo. Entonces podría detectarse un pequeño cambio debido a un SEE, amplificarse y sintonizarse en una señal digital. No existe ningún motivo por el que no deba usarse cualquier dispositivo analógico común con sensibilidad apropiada, por ejemplo, resistencia, condensador, diodo, inductor.

Por supuesto, el uso de una RAM en el método y aparato preferidos almacenará el cambio de estado provocado por el SEU, de modo que la interrogación en un momento posterior recogerá un cambio inducido por SEU. Una RAM, para su uso en el espacio, tiene la ventaja de que está libremente disponible, es relativamente económica, ligera (especialmente cuando se implementa en un microchip) y es probable que esté disponible en una forma cualificada para el espacio.

La RAM y el LFSR pueden incorporarse ventajosamente en un único microchip. Alternativamente, digamos si se requiere una memoria más grande para aprovechar las inversiones de bits a una tasa mayor, la RAM puede formarse por separado, digamos en otro microchip.

Ventajosamente el LFSR se proporciona con suficiente almacenamiento de bits de manera que el número total de bits que puede generarse mediante el LFSR antes de repetirse es de longitud bastante mayor que cualquier número individual que se requiriese que se leyera del LFSR. Con los fines de generar un número aleatorio para su uso en la obtención de una clave criptográfica, se seleccionó una RAM K6R4008CID (marca comercial reg.) de Samsung de 4 millones de bits. Con una predicción de que se producen SEU una vez cada 15.000 días para cada bit, cuando se está en órbita geoestacionaria, la tasa global de inversión de bits sería de una cada 5,4 minutos. Por tanto, en un periodo de una hora, se esperarían 11,1 inversiones de bits. Con una tasa de temporización de 1 MHz, cada dirección de bit se leería 6866 veces en una hora. Esto proporcionaría como aleatorio un número tal como sería probable que fuese necesario.

Según un segundo aspecto de la invención, se proporciona un método de obtención, mientras se está en un vehículo espacial, de una clave criptográfica segura que incluye las etapas de proporcionar, en el vehículo espacial, un dispositivo que puede producir información aleatoria cuando se somete a fenómenos espaciales aleatorios, obtener dicha información aleatoria y producir un número aleatorio a partir de la misma, y ejecutar un algoritmo mediante lo cual se establece la clave segura.

Se prevén otros tipos de fenómenos espaciales aleatorios que sería posible usar en la invención.

Según el tercer aspecto de la invención, se proporciona un aparato de comunicación con vehículos espaciales que incorpora un dispositivo para generar números aleatorios, teniendo el dispositivo una salida que puede emitir una serie de bits en el que la serie de bits de salida es susceptible al cambio tras el impacto sobre el dispositivo de paquetes de radiación que se producen libremente en espacio para permitir que el dispositivo produzca un número aleatorio, medios conectados al dispositivo para comunicarse con una estación de comunicación alejada del aparato y medios para utilizar el número aleatorio en la determinación de una clave de comunicación criptográfica segura para comunicarse con la estación de comunicación alejada.

La invención se describirá ahora a modo de ejemplo con referencia al dibujo adjunto.

Según la invención, el aparato de comunicación con vehículos espaciales para comunicarse o bien con otro vehículo espacial, por ejemplo un satélite, o bien una estación terrestre en la Tierra u otro planeta puede hacerse funcionar desde un satélite en órbita para generar, cuando se requiera, un número aleatorio para su uso en una clave numérica criptográfica para permitir la comunicación segura desde el satélite.

La invención se basa en un aparato y método para generar tal número aleatorio y para generar la clave criptográfica segura para permitir la comunicación segura mencionada anteriormente. La parte de generación de número aleatorio de la invención se ilustra en el dibujo en forma de diagrama de bloques. Una máquina de estado algorítmica (ASM, *algorithmic state machine*) está unida operativamente a una memoria de acceso aleatorio (RAM) de 4 megabits, un registro de desplazamiento con retroalimentación lineal (LFSR) y un contador. Los enlaces de lectura y escritura entre la RAM y la ASM, por una parte, y la RAM y el contador, por otra parte, pueden verse en el dibujo. Además, puede verse la retroalimentación del LFSR, a través de la ASM a la RAM.

La invención está diseñada para usar inversiones de bits experimentadas por la RAM cuando está en el espacio para producir números aleatorios verdaderos, es decir números cuyo patrón no puede determinarse por un observador. El LFSR se implementa en lógica secuencial en un micro-chip y se usa junto con la RAM para garantizar que se propagan las redisposiciones de evento simple (SEU) de inversión de bit.

En funcionamiento, se lee cada ubicación de memoria en la RAM por turnos y se carga en el LFSR. El LFSR se temporiza entonces una vez y se combina cada valor con los datos en otra ubicación de RAM y se escribe de vuelta en la RAM. El LFSR es lo suficientemente grande en cuanto al almacenamiento de bits de manera que puede leerse cualquier número de bits requerido práctico del mismo antes de que empiece a repetirse el patrón (incluso suponiendo que no se han producido SEU en la RAM mientras tanto).

Cada dirección de RAM tendrá un valor semilla escrito en la misma inicialmente (cualquier valor distinto de cero). Entonces se leerá cada dirección por turnos y se almacenará en registros de un LFSR, de manera conveniente un LFSR de 36 bits. Tras temporizarse el LFSR, se combina la salida (mediante una puerta XOR) con los datos en la siguiente dirección de RAM sucesiva y se escribe de vuelta en la dirección de RAM original. Este procedimiento es continuo y tras un tiempo dado, los datos en la RAM serán completamente impredecibles y por tanto aleatorios. Siempre que se requiera que se emita un número aleatorio del aparato, se detiene el procedimiento anterior y se leen tantos bits como se requieran del LFSR. Con un LFSR de 36 bits, pueden emitirse aproximadamente 68 billones de bits antes de que se produzca una repetición (incluso sin producirse SEU). Tales salidas pseudoaleatorias también son eficazmente aleatorias sin que se produzca ninguna inversión de bits en la RAM siempre que se desconozca el momento exacto en que la secuencia se inició y terminó y además de modo que el aparato funcione a una alta tasa de reloj.

Tal como puede observarse a partir de los dibujos, la ASM también comprueba constantemente la condición de todo

cero en la RAM. Si se produce esta condición, la RAM no funcionará. Si se detecta una condición de este tipo, la ASM reinicia la ubicación de la RAM a un valor distinto de cero conocido.

Cuando está en funcionamiento, el aparato actúa como un generador de número aleatorio grande y complejo. Cada vez que se produce un SEU en la RAM, cambia el patrón de los datos almacenados en la RAM. Cuando se emiten estos datos al LFSR, un pequeño cambio en la salida de datos desde la RAM tiene un efecto muy grande sobre los datos que se emiten desde el LFSR.

A continuación, se expone como Anexo cierto código informático de muestra que usa una pequeña RAM interna para llevar a cabo el método de la invención.

ANEXO

```
library IEEE;
use IEEE.std_logic_1164.all;
use IEEE.numeric_std.all;
use IEEE.std_logic_unsigned.all;
entity Top_level_RNG is
  port (Sysclock : in std_logic;
       Resetz : in std_logic;
       Data_out_RD : in std_logic;
       Random_data_out : out std_logic);
end Top_level_RNG;
architecture rtl of Top_level_RNG is
component RAM_128_36
  port(Data in std_logic_vector(35 downto 0);
       Q : out std_logic_vector(35 downto 0);
     WAddress : in std_logic_vector (6 downto 0);
     RAddress : in std_logic_vector (6 downto 0);
       WE : in std_logic;
       RE : in std_logic;
       WClock : in std_logic;
       RClock : in std_logic);
       end component;
       signal

Wr_data,Rd_data,LFSR_data_in,LFSR_data_out,LF SR_data,Wr_data_int :
       std_logic_vector (35 downto 0);
       signal count,count_plus_1 :
std_logic_vector (6 downto 0);
       signal current_state,next_state :
std_logic_vector (1 downto 0);
       signal WE,RE,count_en : std_logic;
       Begin
       --RAM port map
       Actel_RAM_128_36 : RAM_128_36 port
map(Data=>Wr_data,Q=>Rd_data,

WAddress=>count,RAddress=>count=>plus_1,WE=>W E,RE=>RE,
    WClock=>Sysclock,RClock=>Sysclock);
    --7 bit address counter
    Process (sysclock,resetz)
    Begin
    if resetz = '0' then
  count <= (others=>'0');
  elsif rising_edge(sysclock) then
  if count_in = '1' then
    count <= count_plus_1;
  end if;
  end if;
  end process;
  count_plus_1 <= count + '1';
  --LFSR registers
  process (sysclock,resetz)
  Begin
  if resetz = '0' then
```

```
    LFSR_data <= (others=>101);
  elsif rising_edge(sysclock) then
    LFSR_data <= LFSR_data_in;
  end if;
  end process;
  --LFSR Feedback taps
  LFSR_data_out(35 downto 1) <= LFSR_data(34 downto 0);
  LFSR_data_out(0) <= LFSR_data(35) Xor LFSR_data(24);
  --The output is combined with the next input, with an xor gate
  Wr_data_int <= LFSR_data_out xor Rd_data;
  --state machine registers - 2 bit
  process (sysclock,resetz)
  Begin
  if resetz = '0' then
  current_state <= (others=>'0');
  elsif rising_edge(sysclock) then
  current_state <= next_state;
  end if;
  end process;
  --Main state machine
  process

  (current_state,count,Rd_data,LFSR_data_out,Data_out_RD,LFSR_data,Wr_data_int)
  begin
  next_state <= "00";
  WE <= '0';
  RE <= '0';
  count_en <= '0';
  LFSR_data_in <= (others=>'0');
  Wr_data <= (others=>'0');
  Random_data_out <= '0';
  case current_state is
  --All locaciones in RAM are set to the default number
    when "00" =>
    count_en <= '1';
    WE <= '1';
    Wr_data <=
    "00101000010110100010100100000101111";
    if count = "1111111" then
    next_state <= "01";
    else
    next_state <= "00";
    end if;
    --Allow a clock for the first read back data to be output from the RAM
    when "01" =>
    RE <= '1';
    next_state <= "10";
    --Allow a clock for the read back data to propagate through the LFSR
    when "10" =>
    RE <= '1';
    LFSR_data_in <= Rd_data;
    next_state <= "11";
    --Loop back continously monitoring for the very unlikely all zero
    condition
    --unless the output is being read then hold until it has finished
    when "11" =>
    next_state <= "11";
    if Data_out_RD = '1' then
    Random_data_out <= LFSR_data(35);
    LFSR_data_in <= LFSR_data_out;
    else
    count_en <= '1';
    WE <= '1';
    RE <= '1';
    LFSR_data_in <= Rd_data;
    if Wr_data_int =
```

```
“00000000000000000000000000000000” then
Wr_data <= “00101000010110100010100100000101111”;
else
  Wr_data <= Wr_data_int:
end if;
end if;
when others =>
null;
end case;
end process;
end RTL;
```

REIVINDICACIONES

1. Método de generación de un número aleatorio en un vehículo espacial que incluye las etapas de:

- proporcionar una RAM que tiene una salida que puede emitir una serie de bits

en el que la serie de bits de salida es susceptible al cambio tras el impacto sobre la RAM de partículas de radiación que se producen libremente en espacio;

exponer la RAM a dicha radiación durante un periodo suficiente para cambiar al menos uno de los bits, y

leer de la salida la serie de bits tal como cambia mediante dicha radiación, mediante lo cual se produzca el número aleatorio.

2. Método según la reivindicación 1, que incluye la etapa de proporcionar un generador de número pseudoaleatorio para propagar una secuencia de bits legible como salida y conectar la RAM a una entrada del generador de número pseudoaleatorio, mediante lo cual cada cambio en la salida de la RAM se propagará mediante el generador de número pseudoaleatorio.

3. Método según la reivindicación 2, en el que la etapa de proporcionar el generador de número pseudoaleatorio implica proporcionar un LFSR y en el que la etapa de propagación del cambio en la salida de la RAM incluye retroalimentar la salida del LFSR a la RAM.

4. Método según la reivindicación 3, en el que la etapa de propagación del cambio en la salida de la RAM incluye las etapas de:

a) leer de una primera dirección de RAM los bits almacenados en la misma;

b) usar los bits almacenados como valores semilla del LFSR;

c) temporizar el LFSR;

d) leer de una segunda dirección de RAM los bits almacenados en la misma;

e) leer los bits emitidos desde el LFSR tras dicha temporización de los mismos;

f) combinar los bits almacenados de la segunda dirección de RAM con los bits emitidos desde el LFSR e introducir el resultado en la primera dirección de RAM;

g) leer de la segunda dirección de RAM los bits almacenados en la misma e introducir los bits almacenados en la entrada del LFSR;

h) temporizar el LFSR;

repetir las etapas c) a h) para direcciones de RAM sucesivas hasta que se alcanza una dirección de RAM final, tras lo cual leer la primera dirección de RAM como la siguiente dirección de RAM sucesiva y, cuando se requiera,

interrumpir las etapas c) a h) para temporizar sucesivamente el LFSR un número requerido de veces para leer una serie de bits de longitud requerida de la salida del LFSR.

5. Método según la reivindicación 4, que incluye ajustar la tasa de temporización del LFSR y un periodo de tiempo durante el que se hace funcionar el método antes de que se lea un número aleatorio, mediante lo cual se garantice un grado de cambio deseado de un valor semilla existente en el LFSR al comienzo del método.

6. Método según cualquier reivindicación anterior, en el que la RAM proporcionada se selecciona del grupo: electrónica y óptica y se selecciona además del grupo: analógica y digital.

7. Método según cualquier reivindicación anterior, cuando depende de la reivindicación 4, en el que la RAM y el LFSR se proporcionan en un único microchip o en el que la RAM y el LFSR se proporcionan cada uno en forma de un microchip.

8. Método según cualquier reivindicación anterior, cuando depende de la reivindicación 4, que incluye la etapa de proporcionar el LFSR con suficiente almacenamiento de bits de manera que el número total de bits que puede generarse por el LFSR antes de repetir es de mayor longitud que cualquier número individual que se

requiere que se lea del LFSR.

9. Método de obtención, mientras se está en un vehículo espacial, de una clave criptográfica segura que incluye las etapas de:

proporcionar, en el vehículo espacial, una RAM que puede producir información aleatoria cuando se somete a radiación que se produce libremente en espacio;

exponer la RAM a dicha radiación durante un periodo suficiente para cambiar al menos uno de los bits;

obtener dicha información aleatoria y producir un número aleatorio a partir de la misma, y

ejecutar un algoritmo que utiliza dicho número aleatorio, mediante lo cual se establece la clave segura.

10. Aparato de comunicación con vehículos espaciales que incorpora una RAM para generar números aleatorios, teniendo la RAM una salida que puede emitir una serie de bits en el que la serie de bits de salida es susceptible al cambio tras el impacto sobre la RAM de paquetes de radiación que se producen libremente en espacio para permitir que la RAM produzca un número aleatorio, medios conectados a la RAM para comunicarse con una estación de comunicación alejada del aparato y medios para utilizar el número aleatorio en la determinación de una clave de comunicación criptográfica segura para comunicarse con la estación de comunicación alejada.

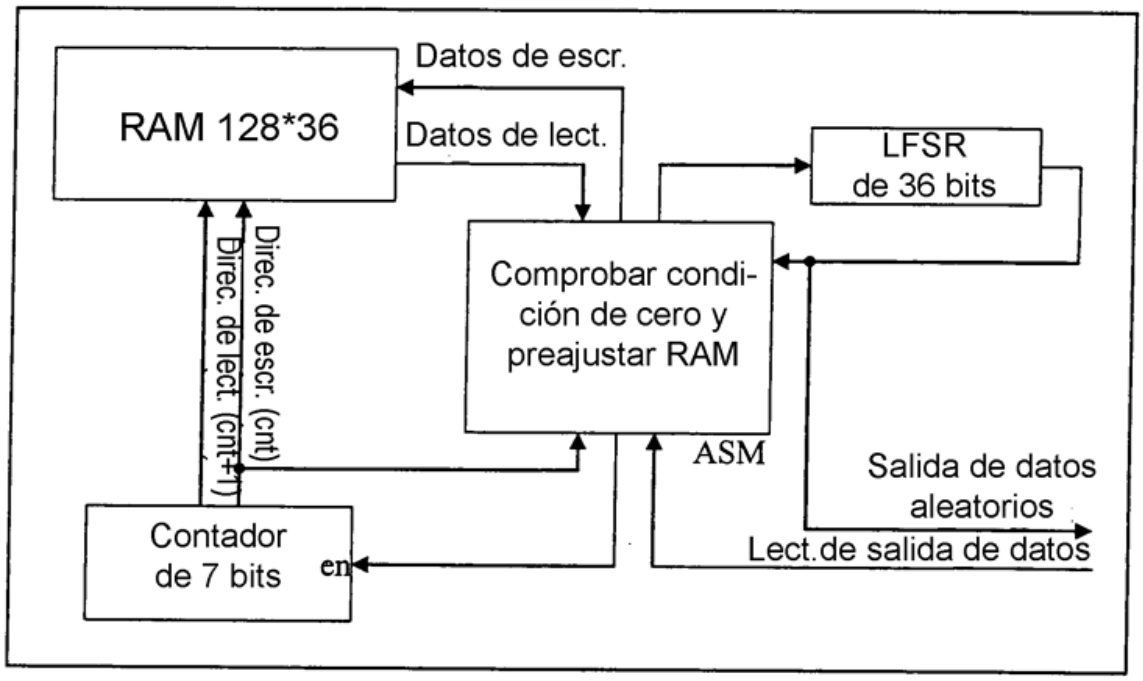
11. Aparato de comunicación con vehículos espaciales según la reivindicación 10, que incluye un generador de número pseudoaleatorio para propagar una secuencia de bits en su salida basándose en una secuencia de bits diferente aplicada a su entrada, teniendo dicho generador de número pseudoaleatorio una entrada que puede conectarse a la salida de la RAM mediante lo cual cada cambio en la salida de la RAM se propagará mediante el generador de número pseudoaleatorio.

12. Aparato de comunicación con vehículos espaciales según la reivindicación 11, en el que el generador de número pseudoaleatorio comprende un LFSR.

13. Aparato de comunicación con vehículos espaciales según la reivindicación 12, en el que el LFSR tiene una capacidad de almacenamiento de bits mayor que cualquier secuencia de bits individual que va a leerse del mismo.

14. Aparato de comunicación con vehículos espaciales según cualquiera de las reivindicaciones 10 a 13, en el que la RAM se selecciona del grupo: electrónica y óptica y se selecciona además del grupo: analógica y digital.

15. Aparato de comunicación con vehículos espaciales según cualquiera de las reivindicaciones 12 a 14, en el que la RAM y el LFSR están comprendidos ambos en un único microchip o la RAM y el LFSR están comprendidos cada uno en un microchip.



Generador de número aleatorio

FIG 1