Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Cifrado en Flujo

DSIC-UPV

Contenido

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

1. Características del cifrado en flujo
2. Clasificación de sistemas
3. Secuencias binarias pseudoaleatorias
4. Generación de secuencias pseudoaleatorias
5. Cifrado basado en generadores pseudoaleatorios

Bibliografía

- Handbook of applied crytography. *A. J. Menezes, P. C. van Oorshot and S. A. Vanstone*. CRC Press. 1996. (Capítulo 6)
- A Graduate Course in Applied Cryptography. *D. Boneh and V. Shoup* (Borrador disponible en la página de D. Boneh) (Capítulo 3)
- Specification of the 3GPP Confidentiality and Integrity Algorithms UEA2 & UIA2. Document 5: Design and Evaluation Report. *ETSI/SAGE Technical report*. 2006.
- Análisis e Implementación del Generador SNOW 3G Utilizado en las Comunicaciones 4G. *J. Molina-Gil, P. Caballero-Gil y A. Fúster-Sabater*. Actas de la RECSI 2014. pp 51–56. 2014.
- Salsa20 - Design, Specification, Security and Speed. *ECRYPT II eSTREAM portfolio. (March 2012)*.

Características del cifrado en flujo

Cifrado en flujo
Propiedades

Cifrado en Flujo

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

- Cifrado de símbolos individuales mediante una transformación que varía con el tiempo
- Fácilmente implementables en hardware (rápidos)
- Útiles en determinados casos (telecomunicaciones) donde el almacenamiento temporal está limitado
- Poco sensibles a errores en la transmisión
- El diseño de los sistemas de cifrado en flujo se basa en generadores de claves pseudoaleatorias (no seguros incondicionalmente pero computacionalmente seguros)

Cifrado en flujo
Cifrado Autoclave

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Cifra el texto en bloques de símbolos $(m_1, m_2, ..., m_n)$
- Se utiliza una clave primaria para cifrar los m primeros símbolos, sirviendo el própio mensaje como clave de cifrado

Cifrado en flujo
Cifrado Autoclave

- Cifra el texto en bloques de símbolos $(m_1, m_2, ..., m_n)$
- Se utiliza una clave primaria para cifrar los m primeros símbolos, sirviendo el própio mensaje como clave de cifrado

x:	R	E	U	N	I	O	N	D	I	A	...
k:	c	l	a	v	e						
x:	18	4	21	13	8						
k:	2	11	0	22	4						
y:	20	15	21	8	12						
y:	T	O	U	I	M						

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

- Cifra el texto en bloques de símbolos $(m_1, m_2, ..., m_n)$
- Se utiliza una clave primaria para cifrar los m primeros símbolos, sirviendo el própio mensaje como clave de cifrado

x:	R	E	U	N	I	O	N	D	I	A	...
k:	c	l	a	v	e	r	e	u	n	i	...
x:	18	4	21	13	8	15	13	4	8	0	...
k:	2	11	0	22	4	18	4	21	13	8	...
y:	20	15	21	8	12	6	17	24	21	8	...
y:	T	O	U	I	M	G	Q	X	U	I	...

Cifrado en flujo
Cifrado Vernam (*One Time Pad*)

Cifrado en Flujo

Propiedades

Clasificación
Cifrado síncrono
Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G

PRGs
Salsa20/x
ChaCha20/x

Algoritmo:

- Obtener una codificación binaria del mensaje y la clave
- El mensaje cifrado aparece cuando se opera un "O exclusivo" bit a bit sobre el mensaje y la clave
- El mismo proceso sirve como descifrado del mensaje

Cifrado en flujo
Cifrado Vernam (*One Time Pad*)

Cifrado en Flujo

Propiedades

Clasificación
Cifrado síncrono
Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G

PRGs
Salsa20/x
ChaCha20/x

Algoritmo:

- Obtener una codificación binaria del mensaje y la clave
- El mensaje cifrado aparece cuando se opera un "O exclusivo" bit a bit sobre el mensaje y la clave
- El mismo proceso sirve como descifrado del mensaje

Propiedades:

- Incondicionalmente seguro si:
  - Clave compuesta por una secuencia binaria de la misma longitud que el mensaje
  - Clave única para cada mensaje

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Clasificación de sistemas

Cifrado en flujo síncrono
Descripción

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Flujo de claves generado independientemente del mensaje y del criptograma Función de cambio de estado:

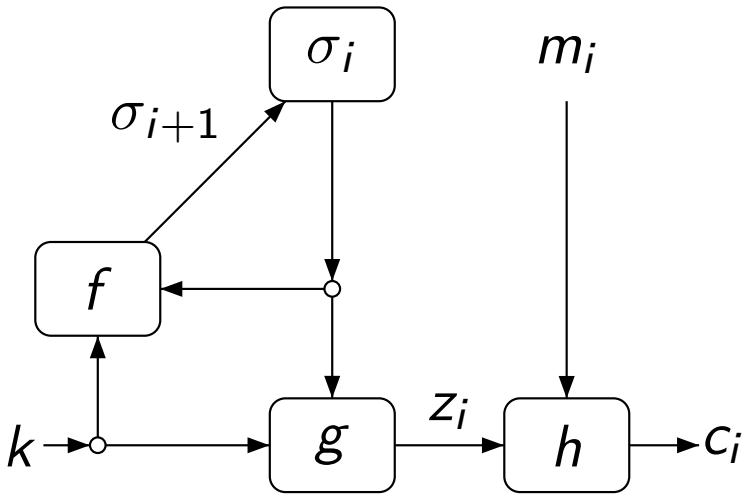
  $\sigma_{i+1} = f(\sigma_i, k)$
  Función de generación de clave: $z_i = g(\sigma_i, k)$
  Función de cifrado: $c_i = h(z_i, m_i)$

Cifrado en flujo síncrono
Descripción

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

- Flujo de claves generado independientemente del mensaje y del criptograma Función de cambio de estado:

  $\sigma_{i+1} = f(\sigma_i, k)$
  Función de generación de clave: $z_i = g(\sigma_i, k)$
  Función de cifrado: $c_i = h(z_i, m_i)$

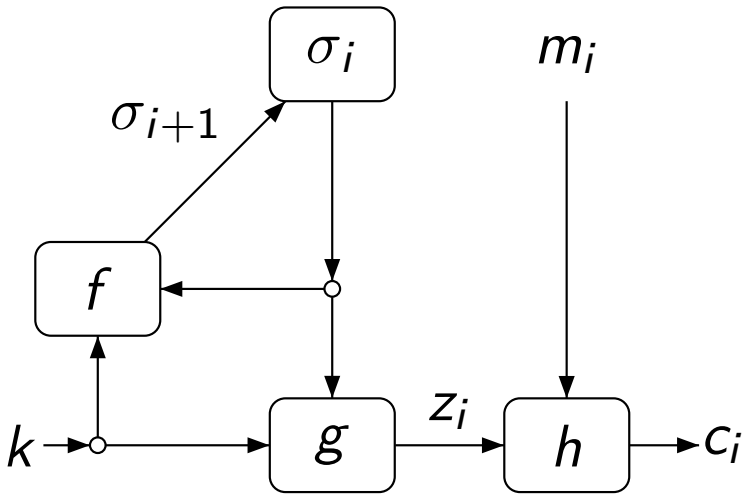


CIFRADO

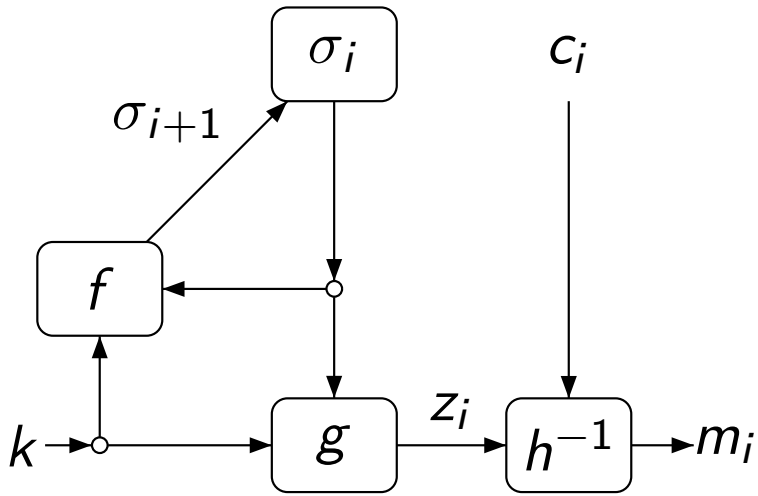
Cifrado en flujo síncrono
Descripción

- Flujo de claves generado independientemente del mensaje y del criptograma Función de cambio de estado:

  $\sigma_{i+1} = f(\sigma_i, k)$
  Función de generación de clave: $z_i = g(\sigma_i, k)$
  Función de cifrado: $c_i = h(z_i, m_i)$



CIFRADO



DESCIFRADO

Cifrado en flujo síncrono
Propiedades

- Necesidad de sincronización entre EMISOR y RECEPTOR. Incorporación de marcas a intervalos regulares (reinicialización)
- No sensible a errores en la transmisión. Los errores provocan únicamente errores locales en el descifrado
- Sensible a ataques activos (inserción, borrado o repetición de símbolos en el criptograma)

Cifrado en flujo síncrono
Propiedades

- Necesidad de sincronización entre EMISOR y RECEPTOR. Incorporación de marcas a intervalos regulares (reinicialización)
- No sensible a errores en la transmisión. Los errores provocan únicamente errores locales en el descifrado
- Sensible a ataques activos (inserción, borrado o repetición de símbolos en el criptograma)

Binary additive stream cipher: Sistema de cifrado en flujo síncrono donde:

- El mensaje, la clave y el criptograma son secuencias binarias
- La función de cifrado y descifrado (h) es la función XOR

Cifrado en flujo autosíncrono
Descripción

Cifrado en Flujo

Propiedades

Clasificación
Cifrado síncrono
Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G

PRGs
Salsa20/x
ChaCha20/x

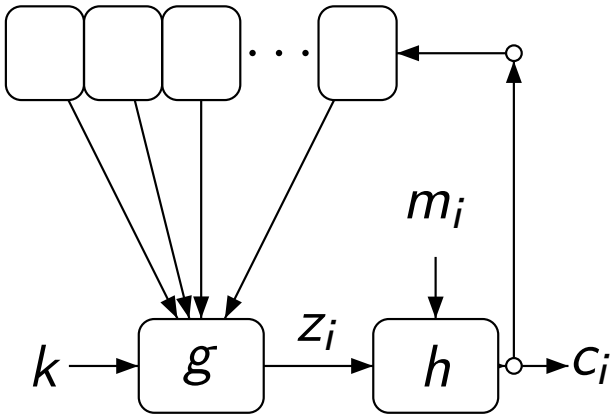
- Flujo de claves generado como una función de la clave de cifrado y un número prefijado de los últimos símbolos del criptograma

  Estado del sistema: $\sigma_i = (c_{i-t}, c_{i-t+1}, c_{i-t+2}, \ldots, c_{i-1})$
  Función de generación de clave: $z_i = g(\sigma_i, k)$
  Función de cifrado: $c_i = h(z_i, m_i)$

Cifrado en flujo autosíncrono
Descripción

- Flujo de claves generado como una función de la clave de cifrado y un número prefijado de los últimos símbolos del criptograma

  Estado del sistema: $\sigma_i = (c_{i-t}, c_{i-t+1}, c_{i-t+2}, \ldots, c_{i-1})$
  Función de generación de clave: $z_i = g(\sigma_i, k)$
  Función de cifrado: $c_i = h(z_i, m_i)$

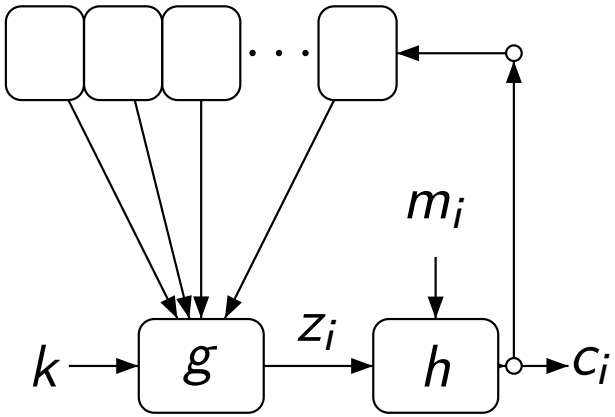


CIFRADO

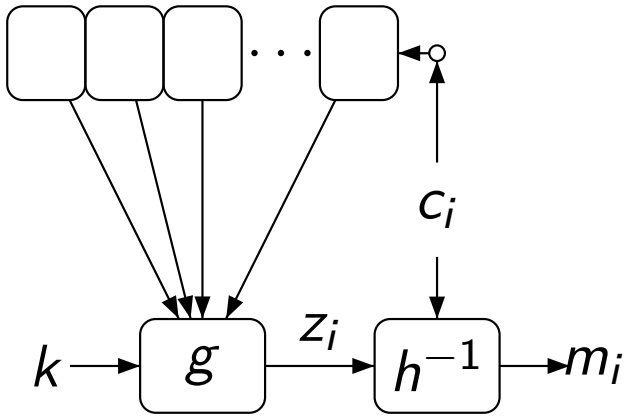
Cifrado en flujo autosíncrono
Descripción

- Flujo de claves generado como una función de la clave de cifrado y un número prefijado de los últimos símbolos del criptograma

  Estado del sistema: $\sigma_i = (c_{i-t}, c_{i-t+1}, c_{i-t+2}, \ldots, c_{i-1})$
  Función de generación de clave: $z_i = g(\sigma_i, k)$
  Función de cifrado: $c_i = h(z_i, m_i)$



CIFRADO



DESCIFRADO

Cifrado en flujo autosíncrono
Propiedades

- *Autosincronización*. El descifrado depende de los últimos símbolos del criptograma, así, la perdida de sincronización se corrige una vez se analiza una secuencia suficientemente larga
- Propagación limitada de errores: debida a la modificación (insertado o borrado)
- Menos sensible a ataques activos. El efecto de un ataque activo provoca una secuencia limitada de errores
- Debido a la influencia del mensaje en el cifrado de los símbolos siguientes, se desvirtuan las propiedades estadisticas del texto en el criptograma. Menos sensibles a ataques basados en redundancias en el texto del mensaje

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Secuencias binarias pseudoaleatorias

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

- El *periodo* de una cadena pseudoaleatoria debe ser muy grande
- *Racha*: Una racha de longitud k en una secuencia de bits es un segmento de longitud k del mismo bit entre dos bits distintos
- *Función de autocorrelación*: medida de similitud entre una secuencia periódica $x = x_0, x_1, x_2, ..., x_T$ de periodo T y la secuencia y resultante de desplazar d posiciones la secuencia x ($y_i = x_{(i+d) mod T}$). Para $k = 1...T$ se define:

$$AC_T(k) = \frac{A - F}{T}$$

donde A y F denotan respectivamente el número de coincidencias y fallos en las secuencias x e y. Si x es una secuencia aleatoria, se esperan valores de $AC_T(k)$ pequeños para $0 < k < T$

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

Ejemplo:

010110010001111

- *periodo*
- *Rachas*
- *Función de autocorrelación*

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

Ejemplo:

$$010110010001111$$

- *periodo* 15
- *Rachas*: 4 de longitud 1; 2 de longitud 2; una de longitud 3; 1 de longitud 4
- *Función de autocorrelación*: $AC^{15}(4) = \frac{7-8}{15}$

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Postulados de Golomb:

- P1: En un periodo, la diferencia entre el número de bits distintos (0s y 1s) ha de ser a lo sumo 1
- P2: Denotando el total de rachas con r, el número de rachas de longitud l en el periodo debe ser igual o superior a $\frac{r}{2^l}$
- P3: Para cualquier valor de k no múltiplo de T (fuera de fase) el valor de $AC_T(k)$ es constante.

  (Nótese que en caso que k sea múltiplo de T, $AC_T(k) = 1$)

Las secuencias que cumplen los Postulados de Golomb presenta una distribución uniforme, denomiandose *pseudo-noise* (PN)

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Generación de secuencias pseudoaleatorias

Cifrado en Flujo

Propiedades

Clasificación
Cifrado síncrono
Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G

PRGs
Salsa20/x
ChaCha20/x

La generación se realiza mediante una ecuación del tipo:

$$x_{i+1} = ax_i + b \pmod{n}$$

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

La generación se realiza mediante una ecuación del tipo:

$$x_{i+1} = ax_i + b \pmod{n}$$

- Los valores a, b y n caracterizan el generador (clave secreta)
- La generación considera el valor anterior en la secuencia. El valor x_0 se denomina semilla
- Es posible obtener los parámetros del generador teniendo en cuenta un fragmento de la secuencia generada
- No se consideran de utilidad en aplicaciones criptográficas

Cifrado en Flujo

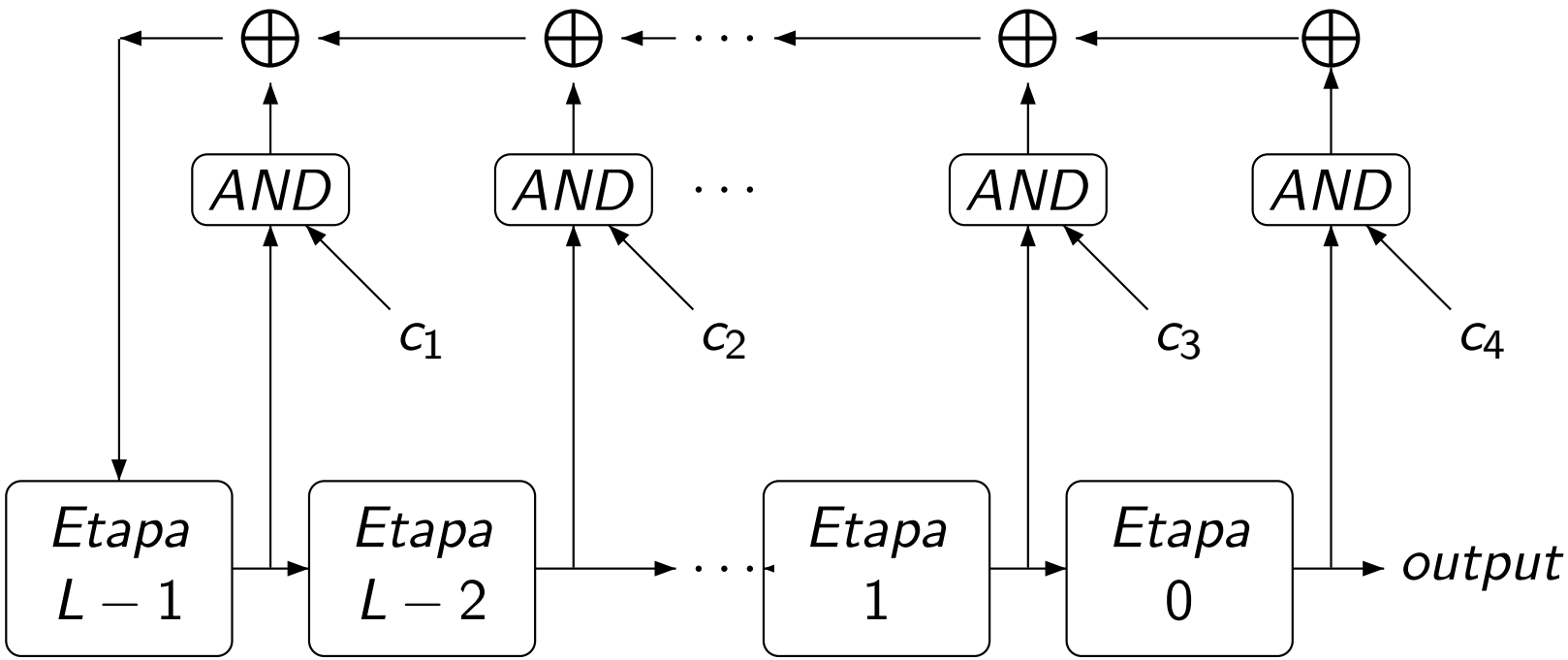
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Descripción:

- La Etapa 0 da lugar a un valor de la secuencia de salida
- El contenido de la Etapa i-esima se desplaza a la Etapa $(i-1)$-esima $(1 \leq i \leq L-1)$
- El contenido de la Etapa $L-1$ se obtiene como combinación lineal (módulo 2) de los contenidos de (algunos de) los registros en el estado precedente

Generadores pseudoaleatorios de claves
LFSR

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x



Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

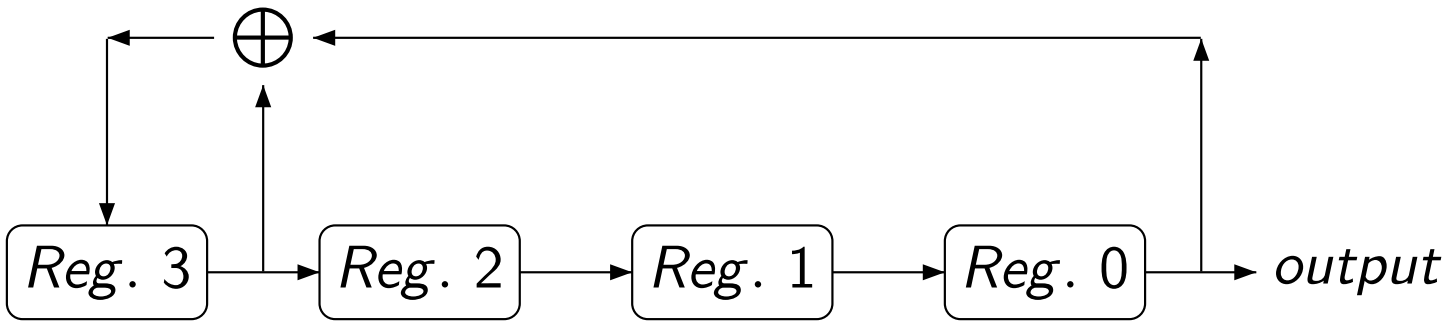
Snow 3G

PRGs

Salsa20/x

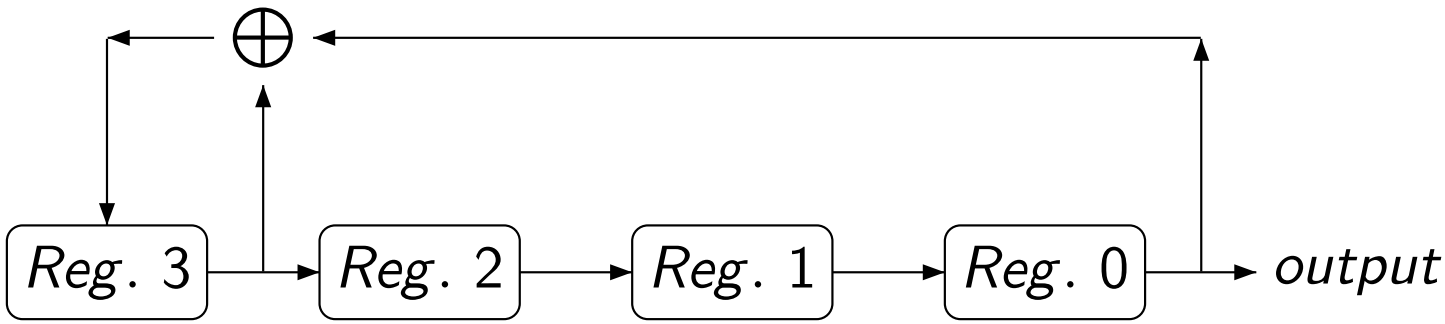
ChaCha20/x

Ejemplo:



Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Ejemplo:



t	R_3	R_2	R_1	R_0
0	0	1	1	0
1	0	0	1	1
2	1	0	0	1
3	0	1	0	0
4	0	0	1	0
5	0	0	0	1
6	1	0	0	0
7	1	1	0	0

t	R_3	R_2	R_1	R_0
8	1	1	1	0
9	1	1	1	1
10	0	1	1	1
11	1	0	1	1
12	0	1	0	1
13	1	0	1	0
14	1	1	0	1
15	0	1	1	0

Generadores pseudoaleatorios de claves
Linear Feedback Shift Registers (LFSR)

Cifrado en Flujo

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Propiedades:

- Capaces de proporcionar secuencias pseudoaleatorias con gran periodo
- Capaces de proporcionar secuencias con buenas propiedades estadísticas
- Fácilmente implementables en hardware
- Posibilidad de analizarlos algebraicamente: La realimentación de un LFSR se caracteriza por un polinómio módulo 2

Generadores pseudoaleatorios de claves
Linear Feedback Shift Registers (LFSR)

Tipos de polinómios (n denota el número de etapas del LFSR)

Factorizables:

Irreducibles:

Primitivos:

Cifrado en Flujo

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Tipos de polinómios (n denota el número de etapas del LFSR)

Factorizables:

- El polinomio puede descomponerse en polinomios más simples
- El periodo depende del estado inicial
- El periodo máximo varía, $n \geq T \geq 2^n - 1$
- Puede haber periodos de longitud divisor del principal

Irreducibles:

Primitivos:

Cifrado en Flujo

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Tipos de polinómios (n denota el número de etapas del LFSR)

Factorizables:

Irreducibles:

- La longitud del periodo no depende del estado inicial
- El periodo es un factor de $2^n - 1$

Primitivos:

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

Tipos de polinómios (n denota el número de etapas del LFSR)

Factorizables:

Irreducibles:

Primitivos:

- Además de ser irreducible, el polinomio genera el conjunto completo de configuraciones
- El periodo no depende del estado inicial y es máximo, igual a $2^n - 1$
- el número de polinomios primitivos de grado n es $\phi(2^n - 1)/n$ (crece exponencialmente con n)

Generadores pseudoaleatorios de claves

Linear Feedback Shift Registers (LFSR)

Tipos de polinómios (n denota el número de etapas del LFSR)

Factorizables:

Irreducibles:

Primitivos:

Puede romperse un LFSR considerando un segmento de $2n$ valores de la secuencia generada

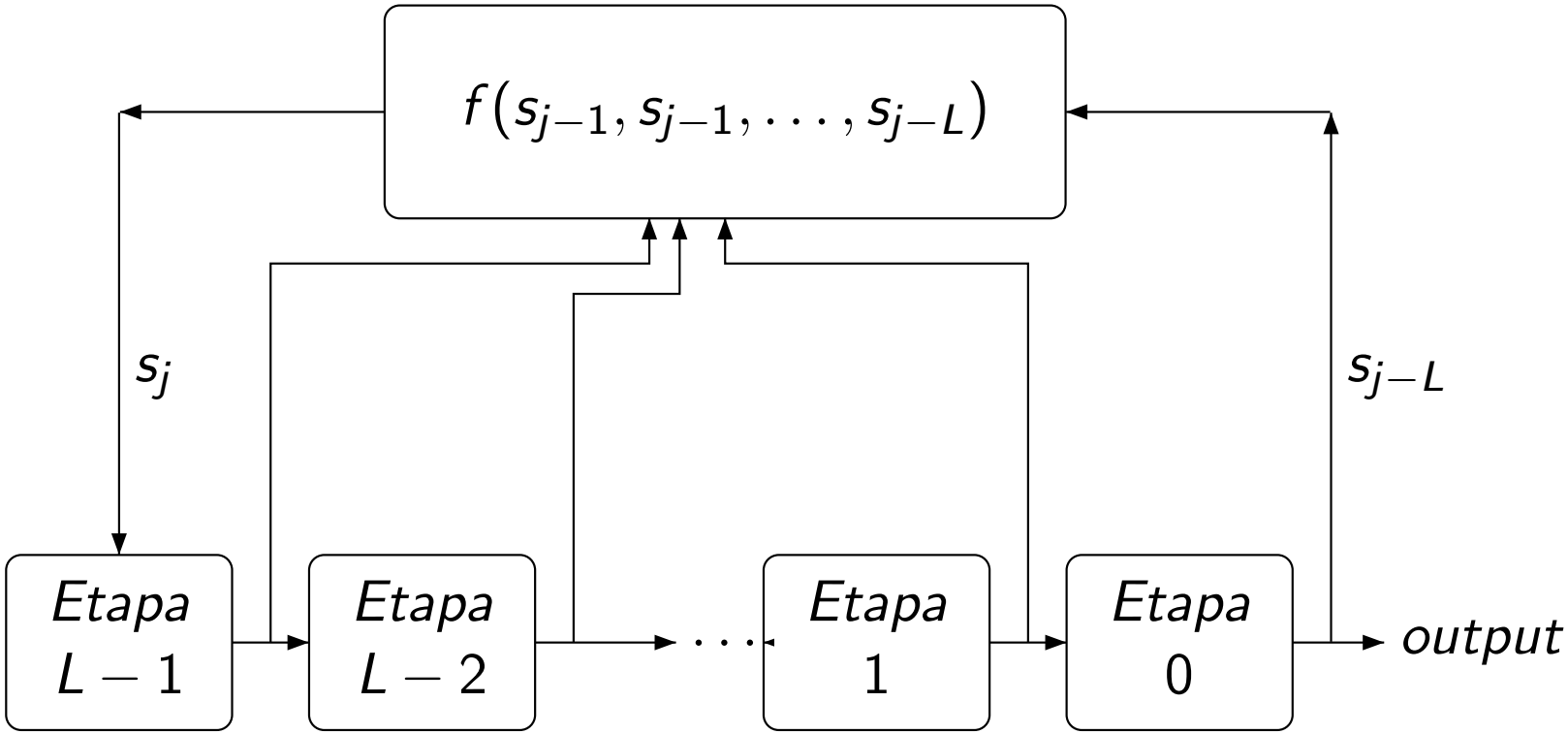
Cifrado en Flujo

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Descripción:

- La Etapa 0 da lugar a un valor de la secuencia de salida
- El contenido de la Etapa i-esima se desplaza a la Etapa $(i-1)$-esima $(1 \leq i \leq L-1)$
- El contenido de la Etapa $L-1$ es el resultado de una función booleana f que toma como entrada los valores en la etapa anterior de todos los registros

Generadores pseudoaleatorios de claves
FSR



Cifrado en Flujo

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Propiedades:

- Basados en funciones booleanas
  - *función booleana*: función con n entradas y una salida, todas ellas binarias
  - Existen 2^{2^n} funciones booleanas distintas de n variables
  - Pueden tener pequeños ciclos que se repiten indefinidamente
  - Son más lentos que los sistemas lineales

Generadores pseudoaleatorios de claves
Feedback Shift Registers (FSR)

Propiedades:

- Basados en funciones booleanas
  - *función booleana*: función con n entradas y una salida, todas ellas binarias
  - Existen 2^{2^n} funciones booleanas distintas de n variables
  - Pueden tener pequeños ciclos que se repiten indefinidamente
  - Son más lentos que los sistemas lineales

Por su diseño, no existe un método sistemático de análisis

Combinaciones de LFSR

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Las secuencias de un LFSR son fácilmente predecibles

Combinaciones de LFSR

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Las secuencias de un LFSR son fácilmente predecibles
- Con objeto de romper la linealidad de las secuencias, se plantean tres aproximaciones:

Combinaciones de LFSR

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Las secuencias de un LFSR son fácilmente predecibles
- Con objeto de romper la linealidad de las secuencias, se plantean tres aproximaciones:
  - Combinando la salida de varios LFSR mediante una función no lineal

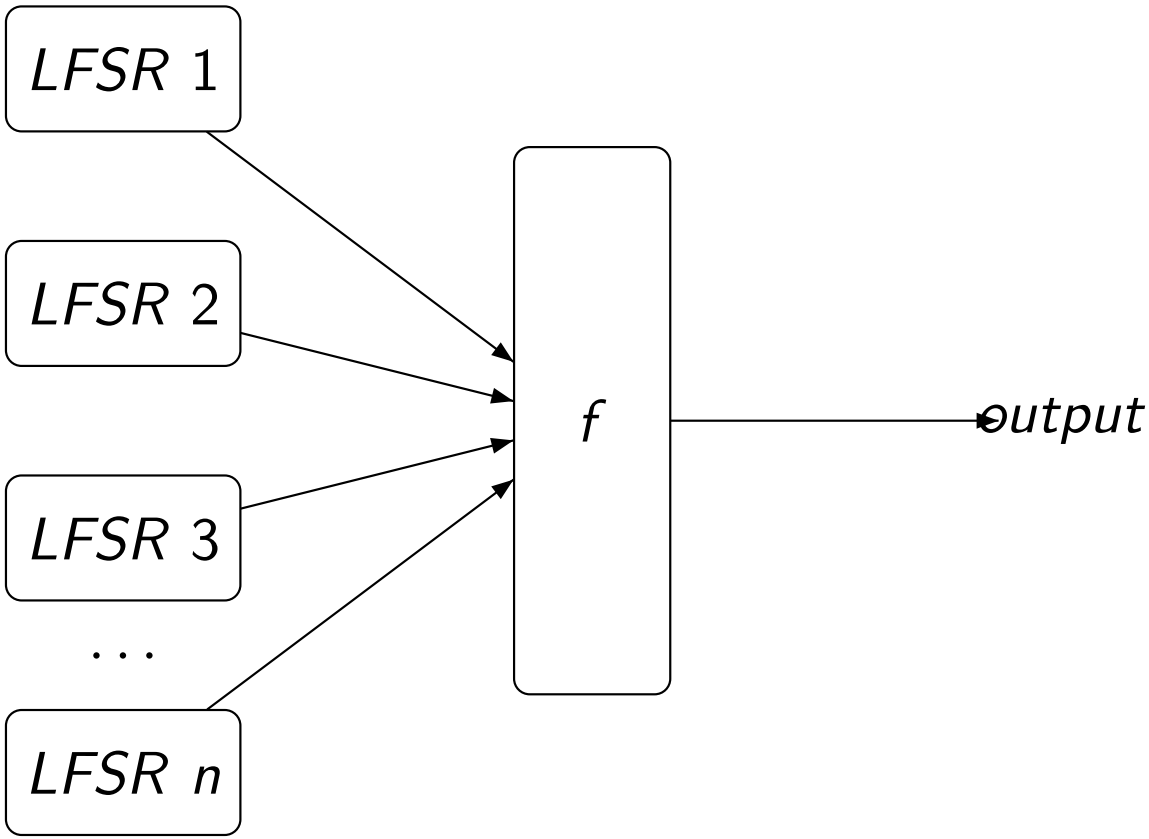
Combinaciones de LFSR

- Las secuencias de un LFSR son fácilmente predecibles
- Con objeto de romper la linealidad de las secuencias, se plantean tres aproximaciones:
  - Combinando la salida de varios LFSR mediante una función no lineal
  - Utilizando una función de filtrado sobre los registros de un único LFSR (*Nonlinear filter generators*)

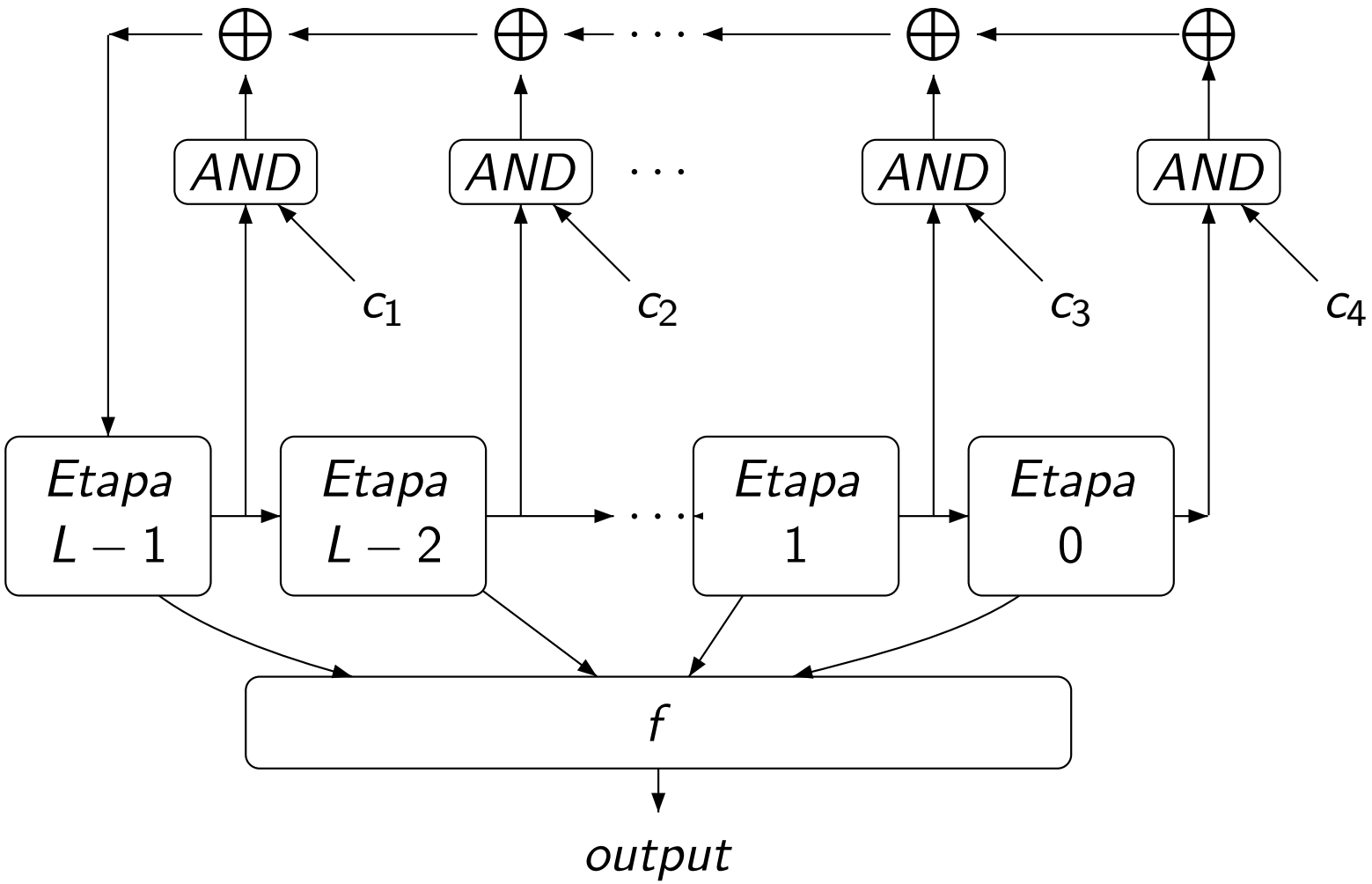
Combinaciones de LFSR

- Las secuencias de un LFSR son fácilmente predecibles
- Con objeto de romper la linealidad de las secuencias, se plantean tres aproximaciones:
  - Combinando la salida de varios LFSR mediante una función no lineal
  - Utilizando una función de filtrado sobre los registros de un único LFSR (*Nonlinear filter generators*)
  - Utilizando un LFSR para controlar el reloj de uno (o más) LFSR (*Clock controlled generators*)

Combinaciones de LFSR
Función de salida booleana



Combinaciones de LFSR
Nonlinear filter generators



Cifrado en Flujo

Propiedades

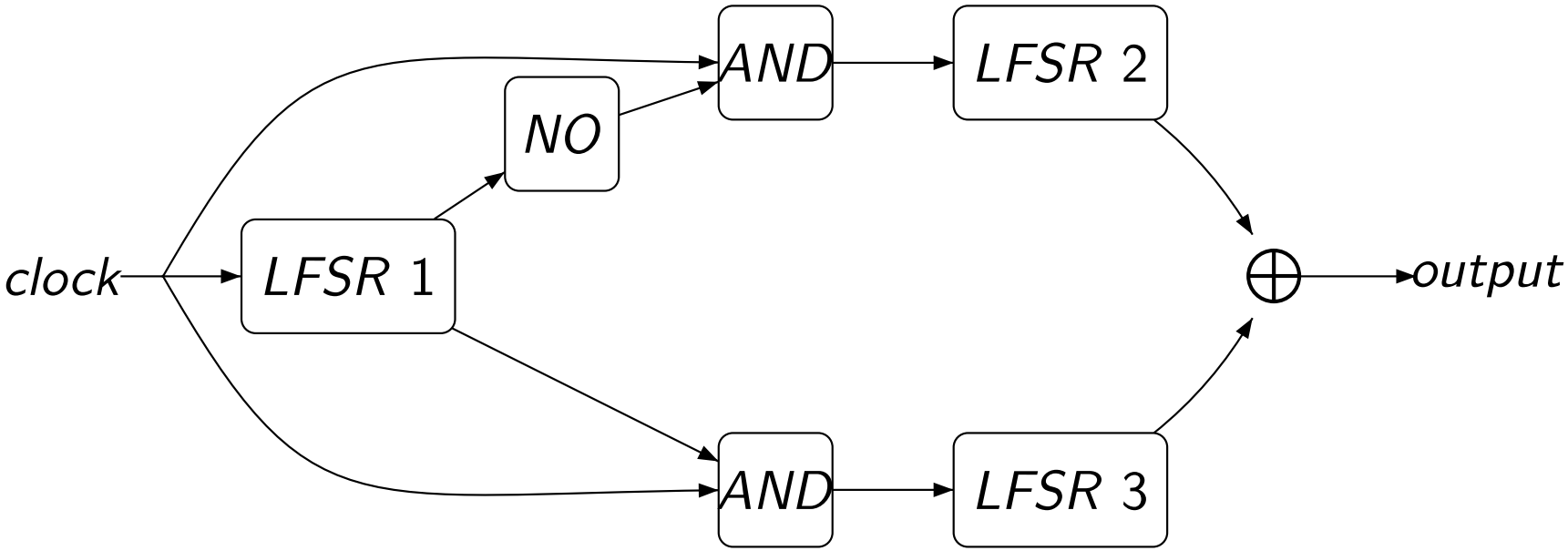
Clasificación
Cifrado síncrono
Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G

PRGs
Salsa20/x
ChaCha20/x

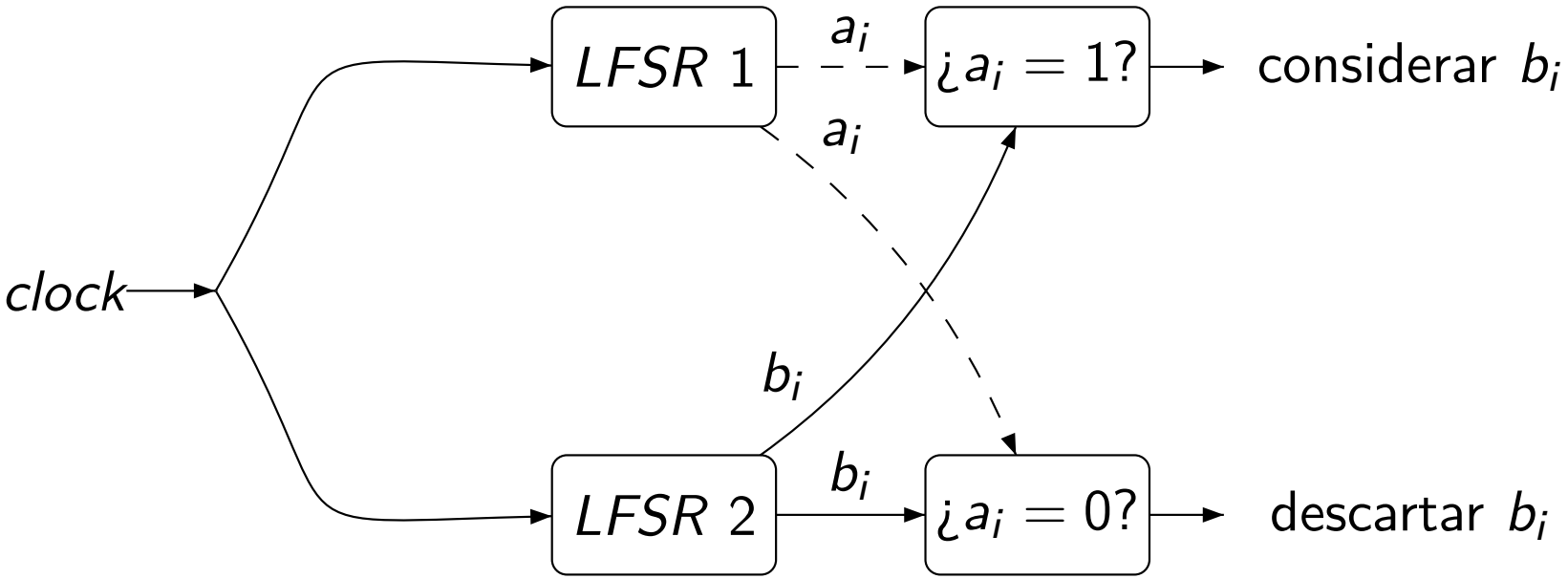
Alternating step generator



Combinaciones de LFSR
Clock controlled generators

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Shrinking generator



Cifrado A5/1
Descripción

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Algoritmo de cifrado en flujo desarrollado en 1987 para el estandar GSM e inicialmente secreto. Se desarrolla A5/2 en 1989 para paises de *baja confianza*
- Considera tres LFSR de 19, 22 y 23 estados
- El sistema no desplaza todos los LFSR en cada paso de generación. Considera un registro de cada uno de los LFSR (*clocking bits*) para determinar, mediante un criterio de mayoría, los LFSR que se desplazan
- Después de inicializado el sistema, genera secuencias pseudoaleatorias de 114 bits (característica del estandar GSM)
- Se publican debilidades del sistema en 1994

Cifrado A5/1
Arquitectura

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

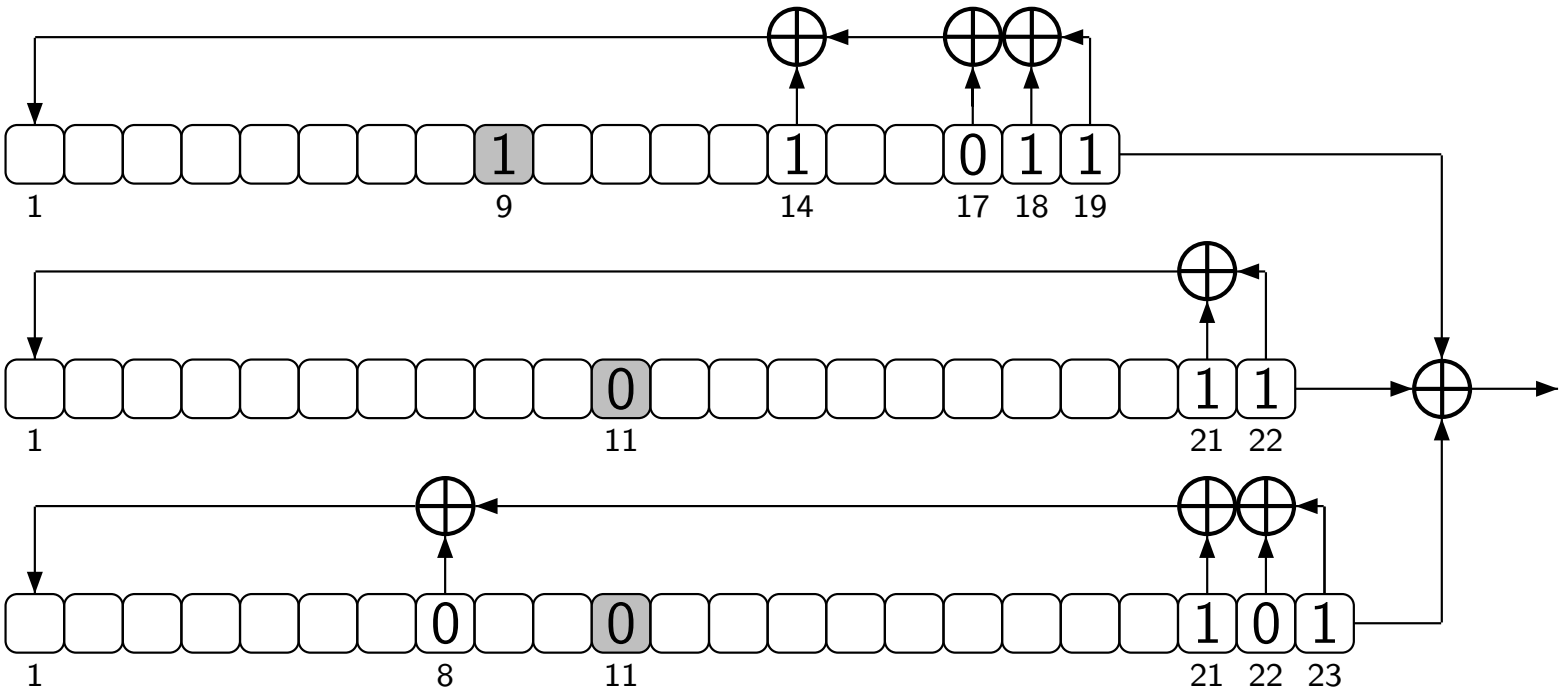
A5/1

Snow 3G

PRGs

Salsa20/x

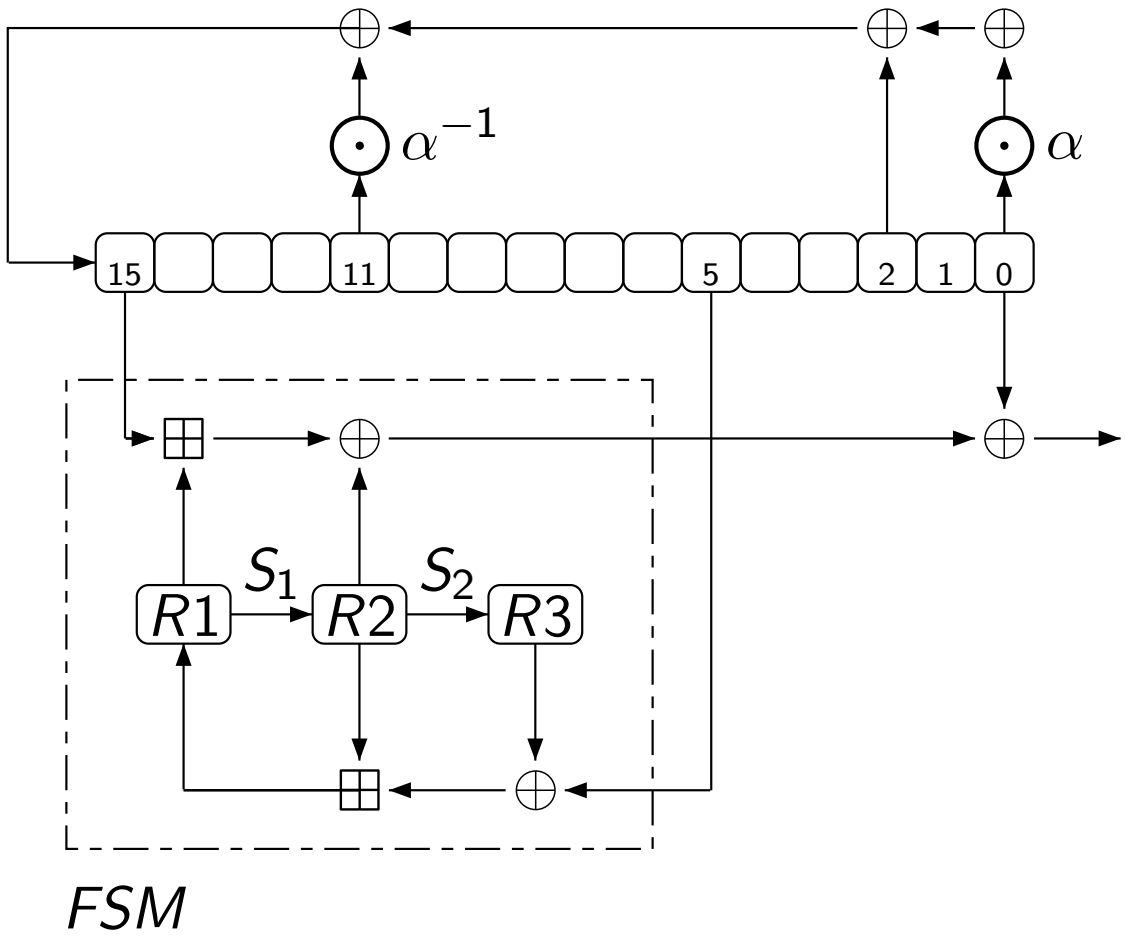
ChaCha20/x



Cifrado 4G
Snow3G: Descripción

- Basado en el diseño de SOSEMANUK, uno de los cuatro cifrados finalistas incluídos en eSTREAM Portfolio 1.
- Generador orientado a palabras basado en un LFSR de 16 registros y una FSM.
- La FSM modifica dos de los tres registros utilizando dos *S-boxes*, una de ellas basada en AES y otra especialmente diseñada.
- El sistema considera distintas operaciones sobre registros de 32 bits. Sistema orientado a palabras.
- Sistema robusto frente a ataques habituales a los sistemas LFSR.
- Se han reportado ataques basados en que determinadas operaciones se implementan utilizando tablas de búsqueda.

Cifrado 4G
Snow3G: Arquitectura



Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Cifrado basado en generadores pseudoaleatorios

Cifrado basado en generadores pseudoaleatorios
Descripción

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- En esencia, realizan el cifrado considerando una secuencia de números aleatorios como clave que se combina con el mensaje (xor u otra función).
- Distintas aproximaciones permiten combinar generadores más simples.
- El Proyecto eStream incluye Salsa20/12 (uno de estos sistemas) como uno de los cuatro sistemas de su Portfolio 1.

Cifrado basado en generadores pseudoaleatorios
Salsa20/x: Descripción

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

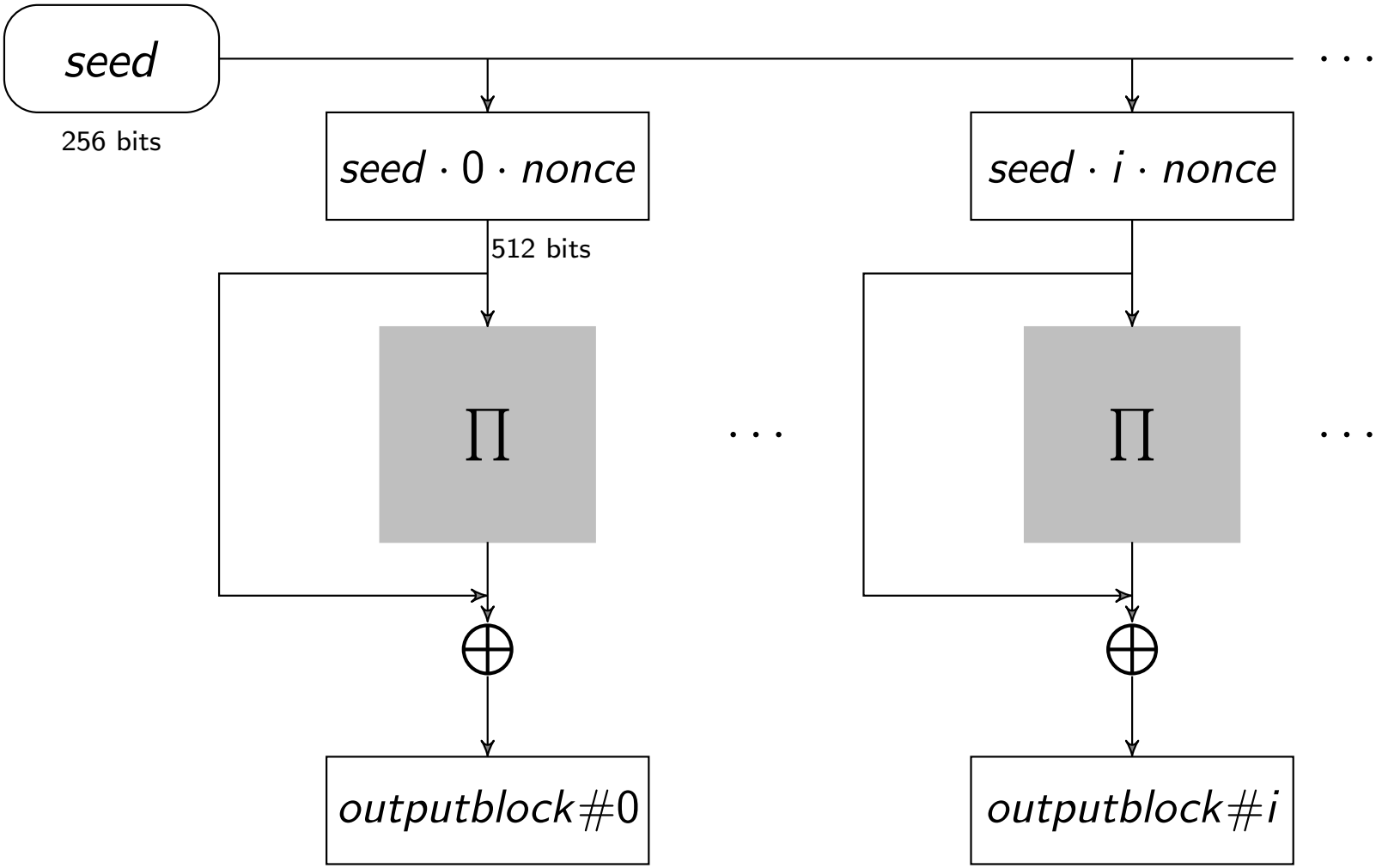
PRGs

Salsa20/x

ChaCha20/x

- Ganador de la competición eSTREAM (2007).
- Cada bloque del flujo proviene de un hash de la clave (256 bits) un nonce (id. único de mensaje de 64 bits) y un contador de posición (64 bits).
- El uso de la posición permite acceder a posiciones determinadas de la secuencia generada en tiempo constante.
- La función resumen utilizada en la generación está basada en una permutación fija de 512 bits.
- El comité eSTREAM sugiere el uso de Salsa 20/12. Se han propuesto distintas variantes (Salsa 20/8, Salsa 20/20) para equilibrar necesidades de seguridad/velocidad.
- No se conocen ataques eficientes a versiones *mayores* de estos sistemas.

Cifrado basado en generadores pseudoaleatorios
Salsa20/x: Arquitectura



Cifrado basado en generadores pseudoaleatorios

Salsa20/x: Implementación

$c_0 = 61707865_{HEX} \quad c_1 = 3320646E_{HEX}$ //Constantes

$c_2 = 79622D32_{HEX} \quad c_3 = 6B206574_{HEX}$

$k_0, k_1, \ldots, k_7 \in \{0,1\}^{32}$ //Clave

$j_0, j_1 \in \{0,1\}^{32}$ //Contador de posición

$n_0, n_1 \in \{0,1\}^{32}$ //Nonce

$$\omega = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{pmatrix} \Longleftarrow \begin{pmatrix} c_0 & k_0 & k_1 & k_2 \\ k_3 & c_1 & n_0 & n_1 \\ j_0 & j_1 & c_2 & k_4 \\ k_5 & k_6 & k_7 & c_3 \end{pmatrix}$$

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Permutación $\prod$ de Salsa 20

Require: $x_1x_2x_3 \ldots x_{15} \in \{0,1\}^{512}$ $//x_i \in \{0,1\}^{32}$
Require: Salsa20 $QRound(a,b,c,d,t)$

1: **Método**
2: **for** $i = 1$ **to** 10 **do**
3: $QRound(x_0, x_4, x_8, x_{12}, 1)$; $QRound(x_1, x_5, x_9, x_{13}, 2)$;
4: $QRound(x_2, x_6, x_{10}, x_{14}, 3)$; $QRound(x_3, x_7, x_{11}, x_{15}, 4)$;
5: $QRound(x_0, x_1, x_2, x_3, 1)$; $QRound(x_4, x_5, x_6, x_7, 2)$;
6: $QRound(x_8, x_9, x_{10}, x_{11}, 3)$; $QRound(x_{12}, x_{13}, x_{14}, x_{15}, 4)$;
7: **end for**
8: **FinMétodo.**

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Salsa 20 QuarterRound

Require: $a, b, c, d \in \{0,1\}^{32}$
Require: $t \in \{1,2,3,4\}$

Método

Ejecuta las operaciones de forma circular empezando por la t-esima.

(i) $b \oplus = (a \boxplus d) <<< 7;$
(ii) $c \oplus = (b \boxplus a) <<< 9;$
(iii) $d \oplus = (c \boxplus b) <<< 13;$
(iv) $a \oplus = (d \boxplus c) <<< 18;$

FinMétodo.

Cifrado basado en generadores pseudoaleatorios
ChaCha20/x: Descripción

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

- Versión de Salsa20/x.
- Existe una implementación estandarizada (RTF-7539).
- Habitualmente utilizado para sustituir AES (más rápido en CPUs no especializadas).
- Actualmente utilzadas en protocolos muy utilizados (TLS, SSH, etc.) sustituyendo RC4.
- Mantiene la arquitectura de Salsa20.
- Cada bloque de la secuencia generada proviene de un hash de la clave (256 bits) un nonce (id. único de mensaje de 96 bits) y un contador de posición (32 bits).

Cifrado basado en generadores pseudoaleatorios

ChaCha20/x: Implementación

$$c_0 = 61707865_{HEX} \quad c_1 = 3320646E_{HEX} \qquad //\text{Constantes}$$
$$c_2 = 79622D32_{HEX} \quad c_3 = 6B206574_{HEX}$$
$$k_0, k_1, \ldots, k_7 \in \{0,1\}^{32} \qquad //\text{Clave}$$
$$j_0 \in \{0,1\}^{32} \qquad //\text{Contador de posición}$$
$$n_0, n_1, n_2 \in \{0,1\}^{32} \qquad //\text{Nonce}$$

$$\omega = \begin{pmatrix} x_0 & x_1 & x_2 & x_3 \\ x_4 & x_5 & x_6 & x_7 \\ x_8 & x_9 & x_{10} & x_{11} \\ x_{12} & x_{13} & x_{14} & x_{15} \end{pmatrix} \Longleftarrow \begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ k_0 & k_1 & k_2 & k_3 \\ k_4 & k_5 & k_6 & k_7 \\ j_0 & n_0 & n_1 & n_2 \end{pmatrix}$$

Cifrado en Flujo
Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x

Permutación $\prod$ de ChaCha 20

Require: $x_1 x_2 x_3 \ldots x_{15} \in \{0,1\}^{512}$ $//x_i \in \{0,1\}^{32}$
Require: ChaCha20 $QRound(a,b,c,d)$

1: **Método**
2: **for** $i = 1$ **to** 10 **do**
3: $QRound(x_0, x_4, x_8, x_{12})$; $QRound(x_1, x_5, x_9, x_{13})$;
4: $QRound(x_2, x_6, x_{10}, x_{14})$; $QRound(x_3, x_7, x_{11}, x_{15})$;
5: $QRound(x_0, x_5, x_{10}, x_{15})$; $QRound(x_1, x_6, x_{11}, x_{12})$;
6: $QRound(x_2, x_7, x_8, x_{13})$; $QRound(x_3, x_4, x_9, x_{14})$;
7: **end for**
8: **FinMétodo.**

Cifrado en Flujo

Propiedades

Clasificación

Cifrado síncrono

Cifrado asíncrono

Secuencias pseudoaleat.

Generación secuencias pseudoaleat.

LFSR

FSR

Combinación de sistemas

A5/1

Snow 3G

PRGs

Salsa20/x

ChaCha20/x

ChaCha20 QuarterRound

Require: $a, b, c, d \in \{0,1\}^{32}$

1: **Método**
2: $a \boxplus = b; \quad d \oplus = a; \quad d <<< 16;$
3: $c \boxplus = d; \quad b \oplus = c; \quad b <<< 12;$
4: $a \boxplus = b; \quad d \oplus = a; \quad d <<< 8;$
5: $c \boxplus = d; \quad b \oplus = c; \quad b <<< 7;$
6: **FinMétodo.**

Propiedades
Clasificación
Cifrado síncrono
Cifrado asíncrono
Secuencias pseudoaleat.
Generación secuencias pseudoaleat.
LFSR
FSR
Combinación de sistemas
A5/1
Snow 3G
PRGs
Salsa20/x
ChaCha20/x