PN-secuencias entrelazadas de polinomios diferentes

Sara D. Cardell[1] Amparo Fúster Sabater[2] **Verónica Requena**[3]

[1] Instituto de Matemática, Estatística e Computação Científica
UNICAMP, Brazil
[2] Instituto de Tecnologías Físicas y de la Información
C.S.I.C., Spain
[3]Departamento de Matemáticas
Universidad de Alicante, Spain

RECSI 2022
19 de octubre de 2022

Índice

Índice

Criptografía ligera

- Conectividad de dispositivos de uso diario.

Criptografía ligera

- Conectividad de dispositivos de uso diario.
- El internet de las cosas (IoT): e-banking, e-govern, e-health, e-commerce.

Criptografía ligera

- Conectividad de dispositivos de uso diario.
- El internet de las cosas (IoT): e-banking, e-govern, e-health, e-commerce.
- Limitaciones dispositivos IoT: potencia de procesamiento, el tamaño, la memoria, el consumo de energía y la seguridad.

Criptografía ligera

- Conectividad de dispositivos de uso diario.
- El internet de las cosas (IoT): e-banking, e-govern, e-health, e-commerce.
- Limitaciones dispositivos IoT: potencia de procesamiento, el tamaño, la memoria, el consumo de energía y la seguridad.
- Los cifrados en flujo son la base de los protocolos de comunicación y dispositivos IoT.

Cifradores en flujo

- Los cifradores en flujo cifran bit a bit de forma individual.

Cifradores en flujo

- Los cifradores en flujo cifran bit a bit de forma individual.
- Cada bit de información se suma (XOR), con cada bit de la clave de cifrado.

Cifradores en flujo

- Los cifradores en flujo cifran bit a bit de forma individual.
- Cada bit de información se suma (XOR), con cada bit de la clave de cifrado.
- La clave debe ser lo más aleatoria posible.

Cifradores en flujo

- Los cifradores en flujo cifran bit a bit de forma individual.
- Cada bit de información se suma (XOR), con cada bit de la clave de cifrado.
- La clave debe ser lo más aleatoria posible.

Problema:

La clave de cifrado ha de ser tan grande como el mensaje.

Cifradores en flujo

- Los cifradores en flujo cifran bit a bit de forma individual.
- Cada bit de información se suma (XOR), con cada bit de la clave de cifrado.
- La clave debe ser lo más aleatoria posible.

Problema:

La clave de cifrado ha de ser tan grande como el mensaje.

Solución:

Generar una clave de cifrado lo más aleatoria posible a partir de una clave pequeña $\rightarrow$ Generadores de flujo de claves.

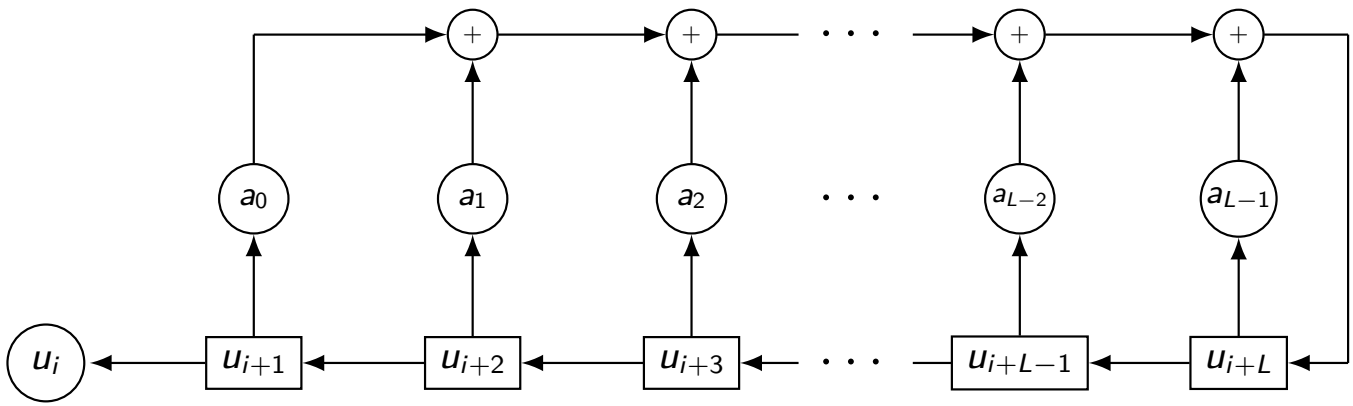
Índice

Linear feedback shift register

Definition

Es un registro de desplazamiento cuyo bit de entrada es una función lineal de su estado anterior.

Figure: LFSR de longitud L (o LFSR con L etapas)

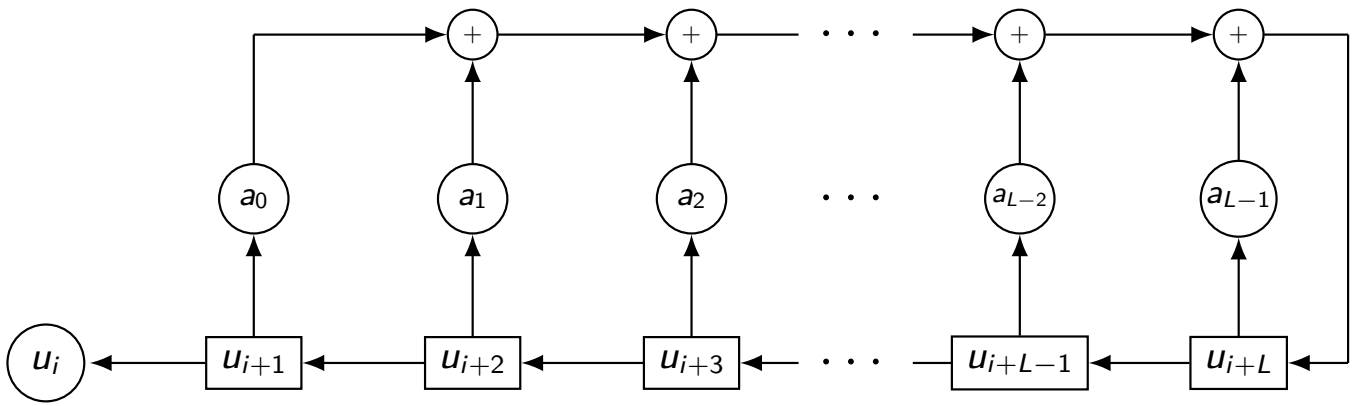


Linear feedback shift register

Definition

Es un registro de desplazamiento cuyo bit de entrada es una función lineal de su estado anterior.

Figure: LFSR de longitud L (o LFSR con L etapas)



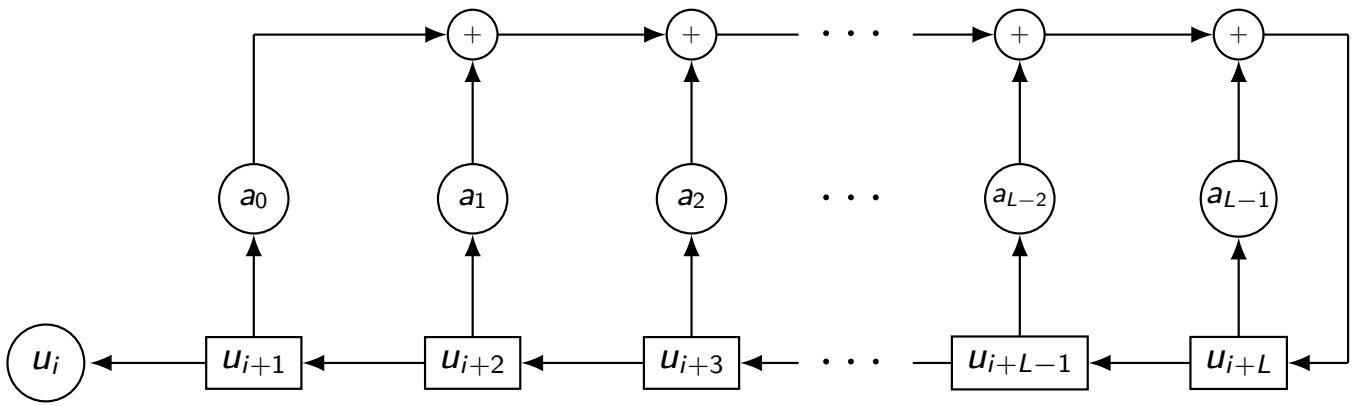
- Clave criptográfica (semilla) $\rightarrow$ secuencia pseudoaleatoria

Linear feedback shift register

Definition

Es un registro de desplazamiento cuyo bit de entrada es una función lineal de su estado anterior.

Figure: LFSR de longitud L (o LFSR con L etapas)



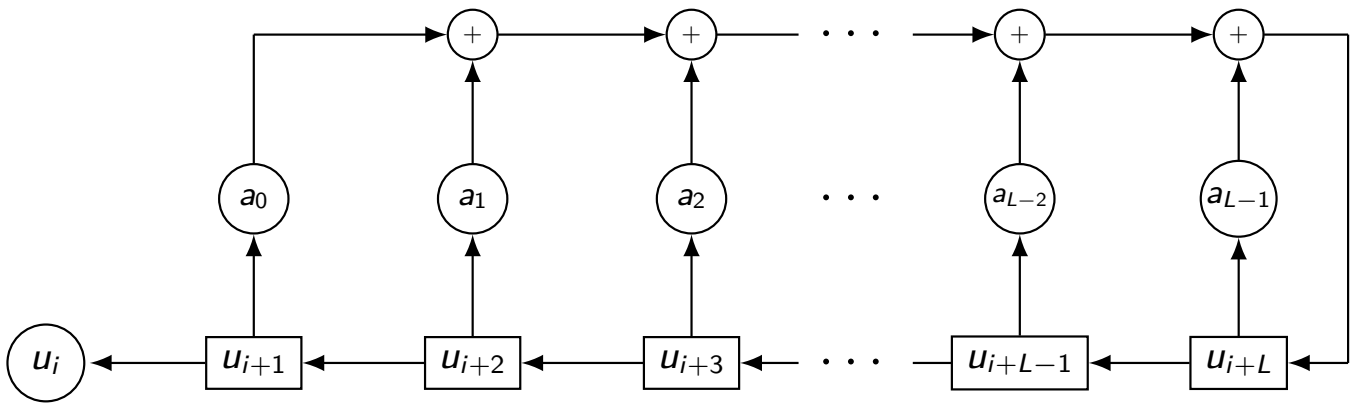
- Clave criptográfica (semilla) $\rightarrow$ secuencia pseudoaleatoria
- Si $p(x)$ primitivo grado $L \rightarrow$ LFSR de longitud máxima (PN-secuencia) $T = 2^L - 1$.

Linear feedback shift register

Definition

Es un registro de desplazamiento cuyo bit de entrada es una función lineal de su estado anterior.

Figure: LFSR de longitud L (o LFSR con L etapas)



- Clave criptográfica (semilla) $\rightarrow$ secuencia pseudoaleatoria
- Si $p(x)$ primitivo grado $L \rightarrow$ LFSR de longitud máxima (PN-secuencia) $T = 2^L - 1$.

Definition

La complejidad lineal de una secuencia es la longitud del mínimo LFSR que genera dicha secuencia.

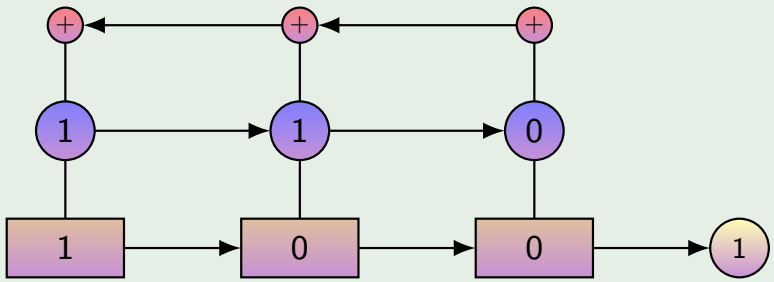
Linear feedback shift register

Example

Consideremos $p(x) = 1 + x + x^3$ un polinomio primitivo sobre $\mathbb{F}_2[x]$ y (100).

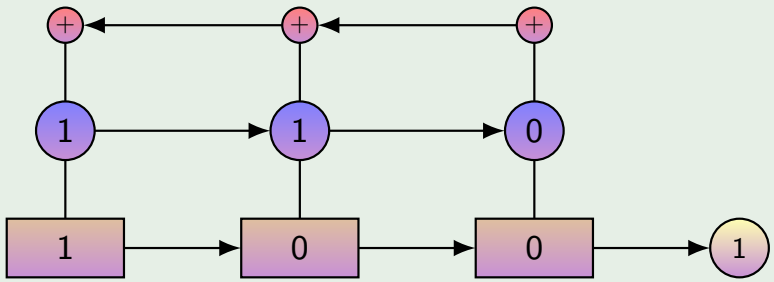
Example

Consideremos $p(x) = 1 + x + x^3$ un polinomio primitivo sobre $\mathbb{F}_2[x]$ y (100).



Example

Consideremos $p(x) = 1 + x + x^3$ un polinomio primitivo sobre $\mathbb{F}_2[x]$ y (100).



PN-secuencia: 1 0 0 1 0 1 1 . . .

Período: $T = 2^3 - 1 = 7$

Linear feedback shift register

LFSR NUNCA se utiliza como generador:

Linear feedback shift register

LFSR NUNCA se utiliza como generador:

- LFSR + NO LINEAL

Linear feedback shift register

LFSR NUNCA se utiliza como generador:

- LFSR + NO LINEAL
- combinación de LFSRs

Linear feedback shift register

LFSR NUNCA se utiliza como generador:

- LFSR + NO LINEAL
- combinación de LFSRs
- clock-controlled registers

Linear feedback shift register

LFSR NUNCA se utiliza como generador:

- LFSR + NO LINEAL
- combinación de LFSRs
- clock-controlled registers
- decimación, . . .

Índice

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

- Sean R_1 y R_2 LFSRs de máxima longitud L_1, L_2, con $\text{mcd}(L_1, L_2) = 1$.

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

- Sean R_1 y R_2 LFSRs de máxima longitud L_1, L_2, con $\text{mcd}(L_1, L_2) = 1$.
- Sean $p_1(x), p_2(x) \in \mathbb{F}_2[x]$, con grados L_1, L_2, los polinomios característicos de R_1, R_2.

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

- Sean R_1 y R_2 LFSRs de máxima longitud L_1, L_2, con $\text{mcd}(L_1, L_2) = 1$.
- Sean $p_1(x), p_2(x) \in \mathbb{F}_2[x]$, con grados L_1, L_2, los polinomios característicos de R_1, R_2.
- La PN-secuencia $\{a_i\}$ generada por R_1 decima la PN-secuencia $\{b_i\}$ producida por el otro registro R_2.

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

- Sean R_1 y R_2 LFSRs de máxima longitud L_1, L_2, con $\text{mcd}(L_1, L_2) = 1$.
- Sean $p_1(x), p_2(x) \in \mathbb{F}_2[x]$, con grados L_1, L_2, los polinomios característicos de R_1, R_2.
- La PN-secuencia $\{a_i\}$ generada por R_1 decima la PN-secuencia $\{b_i\}$ producida por el otro registro R_2.
- La regla de decimación satisface que:

$$\begin{cases} \text{Si } a_i = 1, \text{ entonces } s_j = b_i. \\ \text{Si } a_i = 0, \text{ entonces } b_i \text{ se descarta.} \end{cases}$$

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

- Sean R_1 y R_2 LFSRs de máxima longitud L_1, L_2, con $\text{mcd}(L_1, L_2) = 1$.
- Sean $p_1(x), p_2(x) \in \mathbb{F}_2[x]$, con grados L_1, L_2, los polinomios característicos de R_1, R_2.
- La PN-secuencia $\{a_i\}$ generada por R_1 decima la PN-secuencia $\{b_i\}$ producida por el otro registro R_2.
- La regla de decimación satisface que:

$$\begin{cases} \text{Si } a_i = 1, \text{ entonces } s_j = b_i. \\ \text{Si } a_i = 0, \text{ entonces } b_i \text{ se descarta.} \end{cases}$$

- $\{s_j\}$ se conoce como *secuencia shrunken* ($T = (2^{L_2} - 1)2^{L_1 - 1}$).

Generador Shrinking

Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.

- Sean R_1 y R_2 LFSRs de máxima longitud L_1, L_2, con $\text{mcd}(L_1, L_2) = 1$.
- Sean $p_1(x), p_2(x) \in \mathbb{F}_2[x]$, con grados L_1, L_2, los polinomios característicos de R_1, R_2.
- La PN-secuencia $\{a_i\}$ generada por R_1 decima la PN-secuencia $\{b_i\}$ producida por el otro registro R_2.
- La regla de decimación satisface que:

$$\begin{cases} \text{Si } a_i = 1, \text{ entonces } s_j = b_i. \\ \text{Si } a_i = 0, \text{ entonces } b_i \text{ se descarta.} \end{cases}$$

- $\{s_j\}$ se conoce como *secuencia shrunken* ($T = (2^{L_2} - 1)2^{L_1 - 1}$).
- $L_2 2^{L_1 - 2} < LC \leq L_2 2^{L_1 - 1}$ y su polinomio característico es $p(x)^m$, donde $2^{L_1 - 2} < m \leq 2^{L_1 - 1}$ y $p(x)$ es un polinomio primitivo de grado L_2.

Ejemplo generador Shrinking

Example

Sean R_1 y R_2, LFSRs con $p_1(x) = 1 + x + x^2$ y $p_2(x) = 1 + x^2 + x^3$, y estados iniciales (11) y (111).

Ejemplo generador Shrinking

Example

Sean R_1 y R_2, LFSRs con $p_1(x) = 1 + x + x^2$ y $p_2(x) = 1 + x^2 + x^3$, y estados iniciales (11) y (111).

$$
\begin{array}{rl}
R_1: & 1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0 \\
R_2: & 1\,1\,\cancel{1}\,0\,1\,\cancel{0}\,0\,1\,\cancel{1}\,1\,0\,\cancel{1}\,0\,0\,\cancel{1}\,1\,1\,\cancel{0}\,1\,0\,\cancel{0} \\
\{s_j\}: & \mathbf{1\,1}\quad\mathbf{0\,1}\quad\mathbf{0\,1}\quad\mathbf{1\,0}\quad\mathbf{0\,0}\quad\mathbf{1\,1}\quad\mathbf{1\,0}
\end{array}
$$

Ejemplo generador Shrinking

Example

Sean R_1 y R_2, LFSRs con $p_1(x) = 1 + x + x^2$ y $p_2(x) = 1 + x^2 + x^3$, y estados iniciales (11) y (111).

$$
\begin{array}{rl}
R_1: & 1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0\,1\,1\,0 \\
R_2: & 1\,1\,\cancel{1}\,0\,1\,\cancel{0}\,0\,1\,\cancel{1}\,1\,0\,\cancel{1}\,0\,0\,\cancel{1}\,1\,1\,\cancel{0}\,1\,0\,\cancel{0} \\
\{s_j\}: & \mathbf{1\,1}\quad\mathbf{0\,1}\quad\mathbf{0\,1}\quad\mathbf{1\,0}\quad\mathbf{0\,0}\quad\mathbf{1\,1}\quad\mathbf{1\,0}
\end{array}
$$

$T = 14 = (2^3 - 1)2^{2-1}$, $p(x)^2 = (1 + x + x^3)^2$ y $LC = 6$ es máxima.

Índice

Contexto

Definition

La **decimación** de la secuencia $\{s_i\}$ por (distancia) δ es la nueva secuencia $\{u_i\} = \{s_{\delta \cdot i}\}$, obtenida tomando cada δ-ésimo término de dicha secuencia.

Contexto

Definition

La **decimación** de la secuencia $\{s_i\}$ por (distancia) δ es la nueva secuencia $\{u_i\} = \{s_{\delta \cdot i}\}$, obtenida tomando cada δ-ésimo término de dicha secuencia.

Cardell, S.D., Fúster-Sabater, A.
Modelling the shrinking generator in terms of linear CA.
Adv. Math. Commun. vol.10, pp. 797–809, 2016.

Contexto

Definition

La **decimación** de la secuencia $\{s_i\}$ por (distancia) δ es la nueva secuencia $\{u_i\} = \{s_{\delta \cdot i}\}$, obtenida tomando cada δ-ésimo término de dicha secuencia.

Cardell, S.D., Fúster-Sabater, A.
Modelling the shrinking generator in terms of linear CA.
Adv. Math. Commun. vol.10, pp. 797–809, 2016.

Theorem

Las secuencias obtenidas decimando por (distancia) 2^{L_1-1} la secuencia shrunken son PN-secuencias con periodo T_2. A estas secuencias las llamamos PN-secuencias entrelazadas de la secuencia shrunken.

Contexto

Definition

La **decimación** de la secuencia $\{s_i\}$ por (distancia) δ es la nueva secuencia $\{u_i\} = \{s_{\delta \cdot i}\}$, obtenida tomando cada δ-ésimo término de dicha secuencia.

Cardell, S.D., Fúster-Sabater, A.
Modelling the shrinking generator in terms of linear CA.
Adv. Math. Commun. vol.10, pp. 797–809, 2016.

Theorem

Las secuencias obtenidas decimando por (distancia) 2^{L_1-1} la secuencia shrunken son PN-secuencias con periodo T_2. A estas secuencias las llamamos PN-secuencias entrelazadas de la secuencia shrunken.

Theorem

El polinomio primitivo $p(x)$ que genera las PN-secuencias entrelazadas de la secuencia shrunken es

$$p(x) = (x + \alpha^{T_1})(x + \alpha^{2T_1})(x + \alpha^{4T_1}) \cdots (x + \alpha^{2^{L_2-1}T_1}), \qquad (1)$$

donde $\alpha \in \mathbb{F}_{2^{L_2}}$ es una raíz primitiva del polinomio $p_2(x)$.

Example

Sean R_1 y R_2 dos LFSRs con polinomios característicos $p_1(x) = 1 + x^2 + x^3$ y $p_2(x) = 1 + x^3 + x^4$y estados iniciales (111) y (1111).

Example

Sean R_1 y R_2 dos LFSRs con polinomios característicos $p_1(x) = 1 + x^2 + x^3$ y $p_2(x) = 1 + x^3 + x^4$y estados iniciales (111) y (1111). La secuencia shrunken es

$$\{s_j\} = (1110110101110110001110100001010110011011010011000010111110000)$$

Example

Sean R_1 y R_2 dos LFSRs con polinomios característicos $p_1(x) = 1 + x^2 + x^3$ y $p_2(x) = 1 + x^3 + x^4$y estados iniciales (111) y (1111). La secuencia shrunken es

$$\{s_j\} = (111011010111011000111010000101$$
$$011001101101001100001011111000)$$

con $T = (2^{L_2} - 1)2^{L_1 - 1} = 60$ y $p(x)^4 = (1 + x + x^4)^4$, con $LC = 16$.

Example

Sean R_1 y R_2 dos LFSRs con polinomios característicos $p_1(x) = 1 + x^2 + x^3$ y $p_2(x) = 1 + x^3 + x^4$y estados iniciales (111) y (1111). La secuencia shrunken es

$$\{s_j\} = (1110110101110110001110100001010110011011010011000010111110000)$$

con $T = (2^{L_2} - 1)2^{L_1 - 1} = 60$ y $p(x)^4 = (1 + x + x^4)^4$, con $LC = 16$.
Si decimamos la secuencia shrunken por $\delta = 4$, obtenemos las 4 PN-secuencias

$$\begin{aligned} \{s_{4\cdot j}\}: &\quad (110001001101011) \\ \{s_{4\cdot j+1}\}: &\quad (111100010011010) \\ \{s_{4\cdot j+2}\}: &\quad (101111000100110) \\ \{s_{4\cdot j+3}\}: &\quad (011010111100010) \end{aligned}$$

Secuencia Shrunken - entrelazamientos de PN-secuencias

$$\{s_j\} = (1110110101110110001110100001010110011011010011000010111110000).$$

con las 4 PN-secuencias

$$\begin{aligned} \{s_{4\cdot j}\}: &\quad (110001001101011) \\ \{s_{4\cdot j+1}\}: &\quad (111100010011010) \\ \{s_{4\cdot j+2}\}: &\quad (101111000100110) \\ \{s_{4\cdot j+3}\}: &\quad (011010111100010) \end{aligned}$$

Secuencia Shrunken - entrelazamientos de PN-secuencias

$$\{s_j\} = (111011010111011000111010000101$$
$$011001101101001100001011111000)\,.$$

con las 4 PN-secuencias

$$\begin{aligned} \{s_{4\cdot j}\}: &\quad (110001001101011)\\ \{s_{4\cdot j+1}\}: &\quad (111100010011010)\\ \{s_{4\cdot j+2}\}: &\quad (101111000100110)\\ \{s_{4\cdot j+3}\}: &\quad (011010111100010) \end{aligned}$$

El polinomio característico de estas 4 PN-secuencias entrelazadas es

$$p(x) = \left(x+\alpha^7\right)\left(x+\alpha^{14}\right)\left(x+\alpha^{28}\right)\left(x+\alpha^{56}\right) = 1+x+x^4$$

donde $\alpha \in \mathbb{F}_{2^{L_2}}$ es una raíz de $p_2(x)$ y $p(x)$ es el polinomio recíproco de $p_2(x)$.

Secuencia Shrunken - entrelazamientos de PN-secuencias

$$\{s_j\} = (1110110101110110001110100001010110011011010011000010111110000).$$

con las 4 PN-secuencias

$$\begin{aligned} \{s_{4\cdot j}\}: &\quad (110001001101011) \\ \{s_{4\cdot j+1}\}: &\quad (111100010011010) \\ \{s_{4\cdot j+2}\}: &\quad (101111000100110) \\ \{s_{4\cdot j+3}\}: &\quad (011010111100010) \end{aligned}$$

El polinomio característico de estas 4 PN-secuencias entrelazadas es

$$p(x) = \left(x+\alpha^7\right)\left(x+\alpha^{14}\right)\left(x+\alpha^{28}\right)\left(x+\alpha^{56}\right) = 1+x+x^4$$

donde $\alpha \in \mathbb{F}_{2^{L_2}}$ es una raíz de $p_2(x)$ y $p(x)$ es el polinomio recíproco de $p_2(x)$.

NOTA:

- Las 4 PN-secuencias son versiones desplazadas de la misma PN-secuencia.

Secuencia Shrunken - entrelazamientos de PN-secuencias

$$\{s_j\} = (1110110101110110001110100001010110011011010011000010111110000).$$

con las 4 PN-secuencias

$$\begin{aligned} \{s_{4\cdot j}\}: &\quad (110001001101011) \\ \{s_{4\cdot j+1}\}: &\quad (111100010011010) \\ \{s_{4\cdot j+2}\}: &\quad (101111000100110) \\ \{s_{4\cdot j+3}\}: &\quad (011010111100010) \end{aligned}$$

El polinomio característico de estas 4 PN-secuencias entrelazadas es

$$p(x) = \left(x+\alpha^7\right)\left(x+\alpha^{14}\right)\left(x+\alpha^{28}\right)\left(x+\alpha^{56}\right) = 1+x+x^4$$

donde $\alpha \in \mathbb{F}_{2^{L_2}}$ es una raíz de $p_2(x)$ y $p(x)$ es el polinomio recíproco de $p_2(x)$.

NOTA:

- Las 4 PN-secuencias son versiones desplazadas de la misma PN-secuencia.
- El polinomio característico de las PN-secuencias se obtiene a partir de los polinomios del generador shrinking.

Secuencia Shrunken - entrelazamientos de PN-secuencias

$$\{s_j\} = (1110110101110110001110100001010110011011010011000010111110000).$$

con las 4 PN-secuencias

$$\begin{aligned} \{s_{4\cdot j}\}: &\quad (110001001101011) \\ \{s_{4\cdot j+1}\}: &\quad (111100010011010) \\ \{s_{4\cdot j+2}\}: &\quad (101111000100110) \\ \{s_{4\cdot j+3}\}: &\quad (011010111100010) \end{aligned}$$

El polinomio característico de estas 4 PN-secuencias entrelazadas es

$$p(x) = \left(x+\alpha^7\right)\left(x+\alpha^{14}\right)\left(x+\alpha^{28}\right)\left(x+\alpha^{56}\right) = 1+x+x^4$$

donde $\alpha \in \mathbb{F}_{2^{L_2}}$ es una raíz de $p_2(x)$ y $p(x)$ es el polinomio recíproco de $p_2(x)$.

NOTA:

- Las 4 PN-secuencias son versiones desplazadas de la misma PN-secuencia.
- El polinomio característico de las PN-secuencias se obtiene a partir de los polinomios del generador shrinking.
- Los desplazamientos de las secuencias desplazadas también se pueden obtener a través de los LFSRs de entrada.

Definition

Llamamos *secuencia t-entrelazada* a la secuencia $\{s_j\}$ obtenida entrelazando las sucesiones $\{u_i^{(1)}\}$, $\{u_i^{(2)}\}$, $\ldots$, $\{u_i^{(t)}\}$, todas ellas de periodo T,

$$\{s_j\} = \left(u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(t)}, u_1^{(1)}, u_1^{(2)}, \ldots, u_1^{(t)}, \ldots, u_{T-1}^{(1)}, u_{T-1}^{(2)}, \ldots, u_{T-1}^{(t)} \right).$$

Definition

Llamamos *secuencia t-entrelazada* a la secuencia $\{s_j\}$ obtenida entrelazando las sucesiones $\{u_i^{(1)}\}$, $\{u_i^{(2)}\}$, $\ldots$, $\{u_i^{(t)}\}$, todas ellas de periodo T,

$$\{s_j\} = \Big(u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(t)}, u_1^{(1)}, u_1^{(2)}, \ldots, u_1^{(t)}, \ldots, u_{T-1}^{(1)}, u_{T-1}^{(2)}, \ldots, u_{T-1}^{(t)}\Big).$$

Theorem

Consideremos un polinomio primitivo $p(x)$ de grado L. Si entrelazamos t secuencias trasladadas de una PN-secuencia de periodo $T = 2^L - 1$, entonces la secuencia t-entrelazada resultante cumple que: $LC \leq t \cdot L$ y $T \leq t \cdot \left(2^L - 1\right)$.

Definition

Llamamos *secuencia t-entrelazada* a la secuencia $\{s_j\}$ obtenida entrelazando las sucesiones $\{u_i^{(1)}\}$, $\{u_i^{(2)}\}$, ..., $\{u_i^{(t)}\}$, todas ellas de periodo T,

$$\{s_j\} = \left(u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(t)}, u_1^{(1)}, u_1^{(2)}, \ldots, u_1^{(t)}, \ldots, u_{T-1}^{(1)}, u_{T-1}^{(2)}, \ldots, u_{T-1}^{(t)}\right).$$

Las secuencias t-entrelazadas obtenidas con PN-secuencias del mismo polinomio primitivo son estudiadas en

Cardell, S.D., Fúster-Sabater, A., Requena, V.
Interleaving Shifted Versions of a PN-Sequence,
Mathematics, vol. 9, n.68, pp. 1–23, 2021.

Entrelazando PN-secuencias con polinomios diferentes

Sean $p_1(x)$, $p_2(x), \ldots, p_t(x)$ polinomios característicos de grado L de los LFSRs R_1, R_2,..., R_t. Dadas las PN-secuencias $\{a_i^{(k)}\}$, generadas por R_k, para $k = 1, 2, \ldots, t$, definimos la **secuencia t-entrelazada** $\{s_j\}$ como

$$\{s_j\} = \left(a_0^{(1)}, a_0^{(2)}, \ldots, a_0^{(t)}, a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(t)}, \ldots, a_{L-1}^{(1)}, a_{L-1}^{(2)}, \ldots, a_{L-1}^{(t)}, \ldots\right).$$

Entrelazando PN-secuencias con polinomios diferentes

Sean $p_1(x), p_2(x), \ldots, p_t(x)$ polinomios característicos de grado L de los LFSRs R_1, R_2,..., R_t. Dadas las PN-secuencias $\{a_i^{(k)}\}$, generadas por R_k, para $k = 1, 2, \ldots, t$, definimos la **secuencia t-entrelazada** $\{s_j\}$ como

$$\{s_j\} = \left(a_0^{(1)}, a_0^{(2)}, \ldots, a_0^{(t)}, a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(t)}, \ldots, a_{L-1}^{(1)}, a_{L-1}^{(2)}, \ldots, a_{L-1}^{(t)}, \ldots\right).$$

Theorem

Sea $\{s_j\}$ la secuencia t-entrelazada obtenida a partir de t PN-secuencias producidas por diferentes polinomios primitivos $p_1(x), \ldots, p_t(x)$ de grado L. Tenemos que

$$LC = t^2 L \quad y \quad p(x) = \prod_{i=1}^{t} p_i(x^t).$$

Entrelazando PN-secuencias con polinomios diferentes

Sean $p_1(x), p_2(x), \ldots, p_t(x)$ polinomios característicos de grado L de los LFSRs R_1, R_2,..., R_t. Dadas las PN-secuencias $\{a_i^{(k)}\}$, generadas por R_k, para $k = 1, 2, \ldots, t$, definimos la **secuencia t-entrelazada** $\{s_j\}$ como

$$\{s_j\} = \left(a_0^{(1)}, a_0^{(2)}, \ldots, a_0^{(t)}, a_1^{(1)}, a_1^{(2)}, \ldots, a_1^{(t)}, \ldots, a_{L-1}^{(1)}, a_{L-1}^{(2)}, \ldots, a_{L-1}^{(t)}, \ldots\right).$$

Theorem

Sea $\{s_j\}$ la secuencia t-entrelazada obtenida a partir de t PN-secuencias producidas por diferentes polinomios primitivos $p_1(x), \ldots, p_t(x)$ de grado L. Tenemos que

$$LC = t^2 L \quad y \quad p(x) = \prod_{i=1}^{t} p_i(x^t).$$

Corollary

Sea $t = 2^r$, con $r \in \mathbb{N}$. El polinomio característico de una secuencia t-entrelazada, generada a partir de t polinomios primitivos distintos $p_1(x), \ldots, p_t(x)$ de grado L, es

$$p(x) = [p_1(x) \cdot p_2(x) \cdots p_{t-1}(x) \cdot p_t(x)]^t.$$

Entrelazando PN-secuencias con polinomios diferentes

Example

Sean $p_1(x) = 1 + x^2 + x^5$, $p_2(x) = 1 + x + x^2 + x^4 + x^5$ y $p_3(x) = 1 + x + x^2 + x^3 + x^5$, y los estados iniciales $\{11101\}$, (10001) y (10101).

Entrelazando PN-secuencias con polinomios diferentes

Example

Sean $p_1(x) = 1 + x^2 + x^5$, $p_2(x) = 1 + x + x^2 + x^4 + x^5$ y $p_3(x) = 1 + x + x^2 + x^3 + x^5$, y los estados iniciales $\{11101\}$, (10001) y (10101). Las correspondientes PN-secuencias son

$$\{a_i^{(1)}\} : (11101010000100101100111111000110)$$
$$\{a_i^{(2)}\} : (10001001010110000111001101111110)$$
$$\{a_i^{(3)}\} : (10101000111011111001001100000101)\,.$$

Entrelazando PN-secuencias con polinomios diferentes

Example

Sean $p_1(x) = 1 + x^2 + x^5$, $p_2(x) = 1 + x + x^2 + x^4 + x^5$ y $p_3(x) = 1 + x + x^2 + x^3 + x^5$, y los estados iniciales $\{11101\}$, (10001) y (10101). Las correspondientes PN-secuencias son

$$\{a_i^{(1)}\} : (11101010000100101100111110001 10)$$
$$\{a_i^{(2)}\} : (10001001010110000111001101111 10)$$
$$\{a_i^{(3)}\} : (10101000111011111001001100001 01)\,.$$

La secuencia 3-entrelazada:

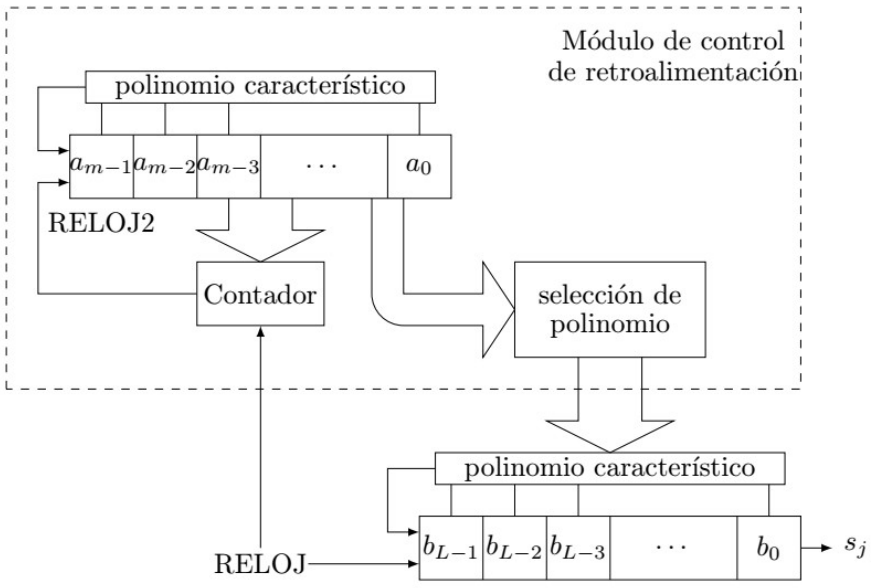
$$(11110010100011100010001000101100111001100 1101$$
$$00110111001001110010011111110001001001011111 0001)$$

tiene periodo $T = 3(2^5 - 1) = 93$, $LC = 3^2 \cdot 5 = 45$ y

$$\begin{aligned} p(x) &= 1 + x^9 + x^{24} + x^{27} + x^{39} + x^{42} + x^{45} \\ &= (1 + x^6 + x^{15})(1 + x^3 + x^6 + x^{12} + x^{15})(1 + x^3 + x^6 + x^9 + x^{15}) \\ &= p_1(x^3) \cdot p_2(x^3) \cdot p_3(x^3) \end{aligned}$$

Dynamic Linear Feedback Shift Register

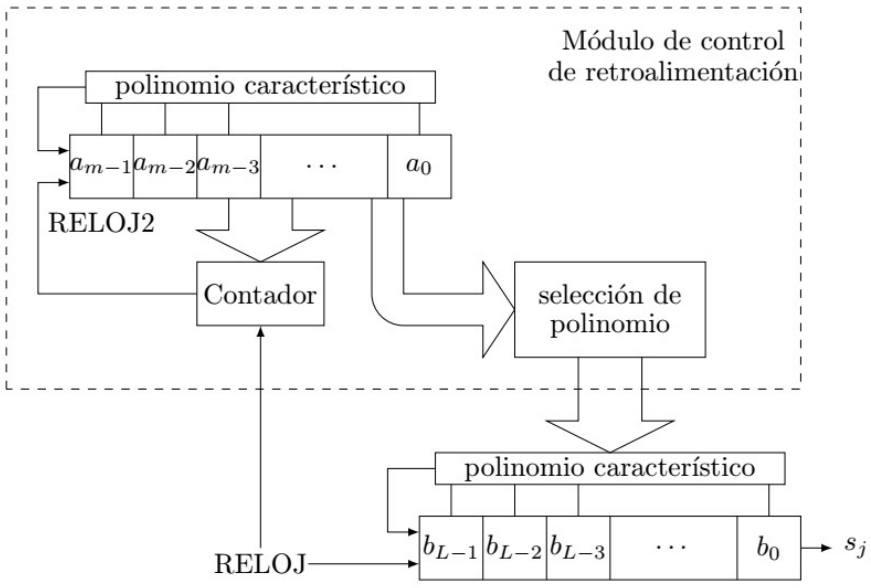
Figure: DLFSR



- Un DLFSR es un tipo de LFSR en el que el polinomio característico cambia en cierto instante.

Dynamic Linear Feedback Shift Register

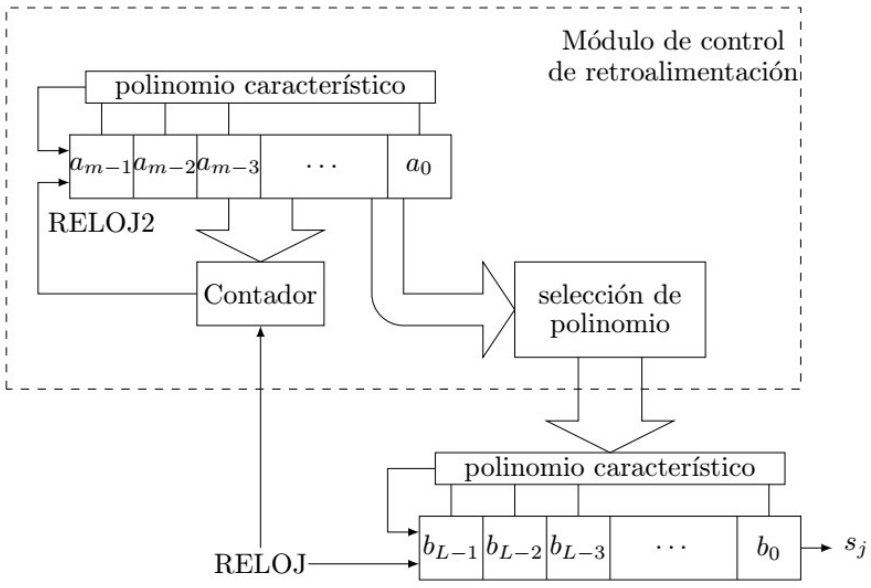
Figure: DLFSR



- Un DLFSR es un tipo de LFSR en el que el polinomio característico cambia en cierto instante.
- Las secuencias generadas son la concatenación de segmentos de diferentes PN-secuencias.

Dynamic Linear Feedback Shift Register

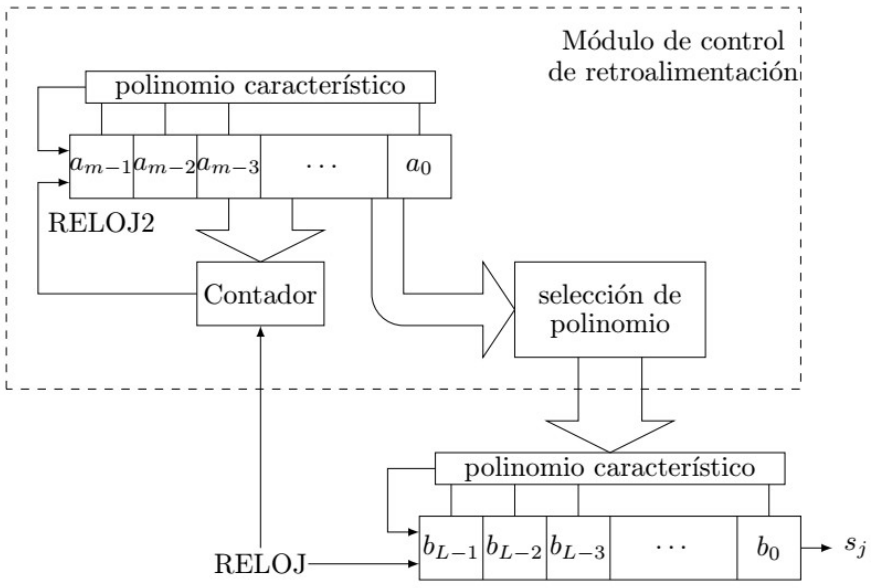
Figure: DLFSR



- Un DLFSR es un tipo de LFSR en el que el polinomio característico cambia en cierto instante.
- Las secuencias generadas son la concatenación de segmentos de diferentes PN-secuencias.
- Objetivo: generar secuencias con mayor periodo y complejidad lineal.

Dynamic Linear Feedback Shift Register

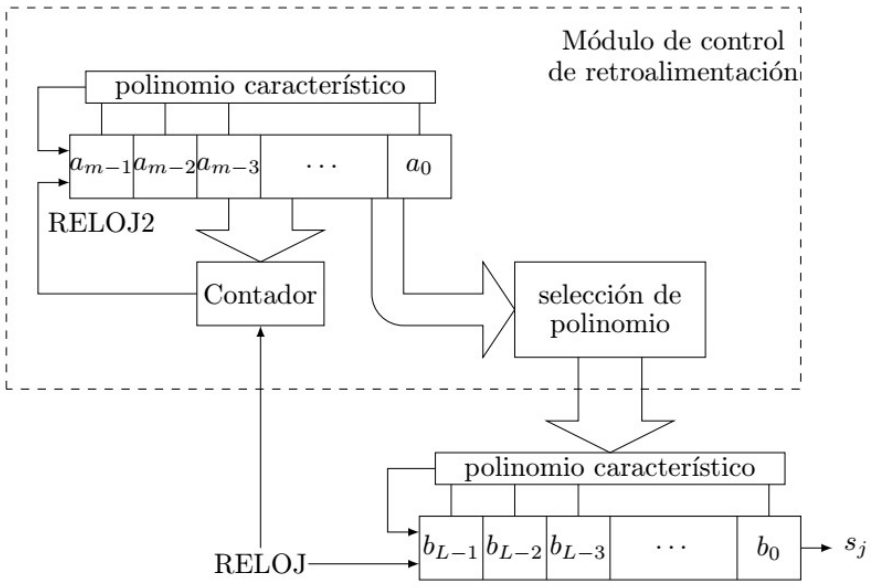
Figure: DLFSR



- Un DLFSR es un tipo de LFSR en el que el polinomio característico cambia en cierto instante.
- Las secuencias generadas son la concatenación de segmentos de diferentes PN-secuencias.
- Objetivo: generar secuencias con mayor periodo y complejidad lineal.
- Método de entrelazado = la concatenación de la salida de t LFSRs en cada instante de tiempo.

Dynamic Linear Feedback Shift Register

Figure: DLFSR



- Un DLFSR es un tipo de LFSR en el que el polinomio característico cambia en cierto instante.
- Las secuencias generadas son la concatenación de segmentos de diferentes PN-secuencias.
- Objetivo: generar secuencias con mayor periodo y complejidad lineal.
- Método de entrelazado = la concatenación de la salida de t LFSRs en cada instante de tiempo.

Figure: Generar una secuencia 4-entrelazada a partir de un DLFSR

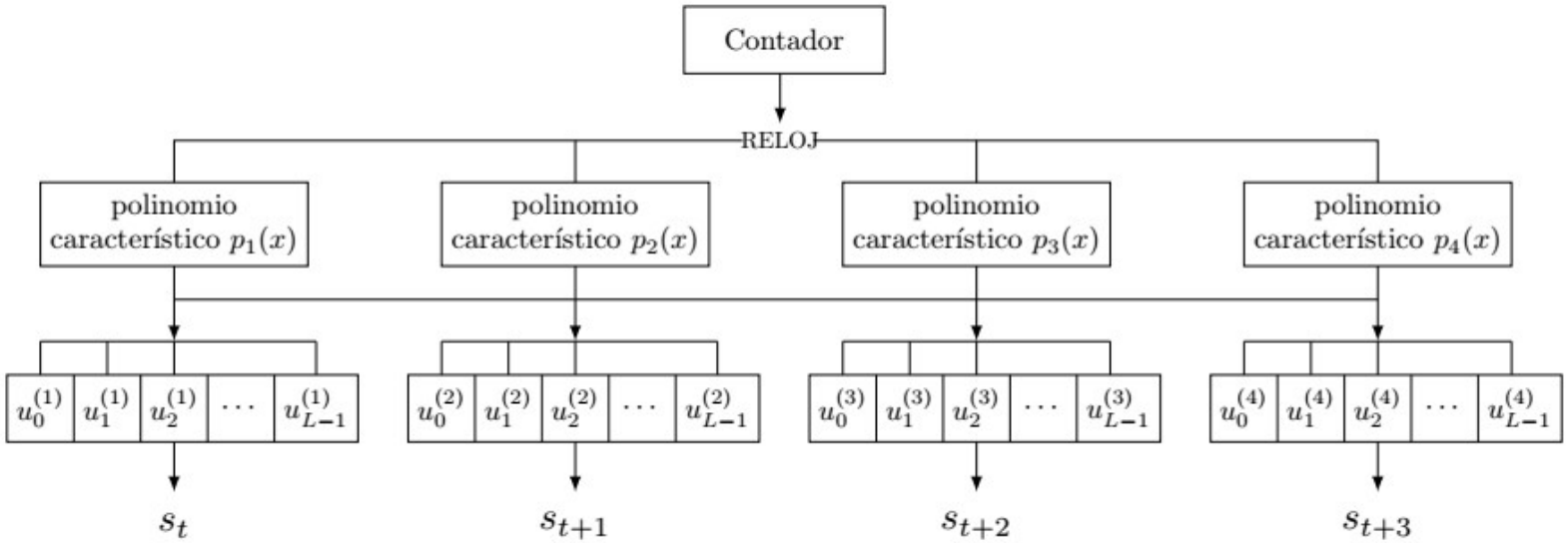
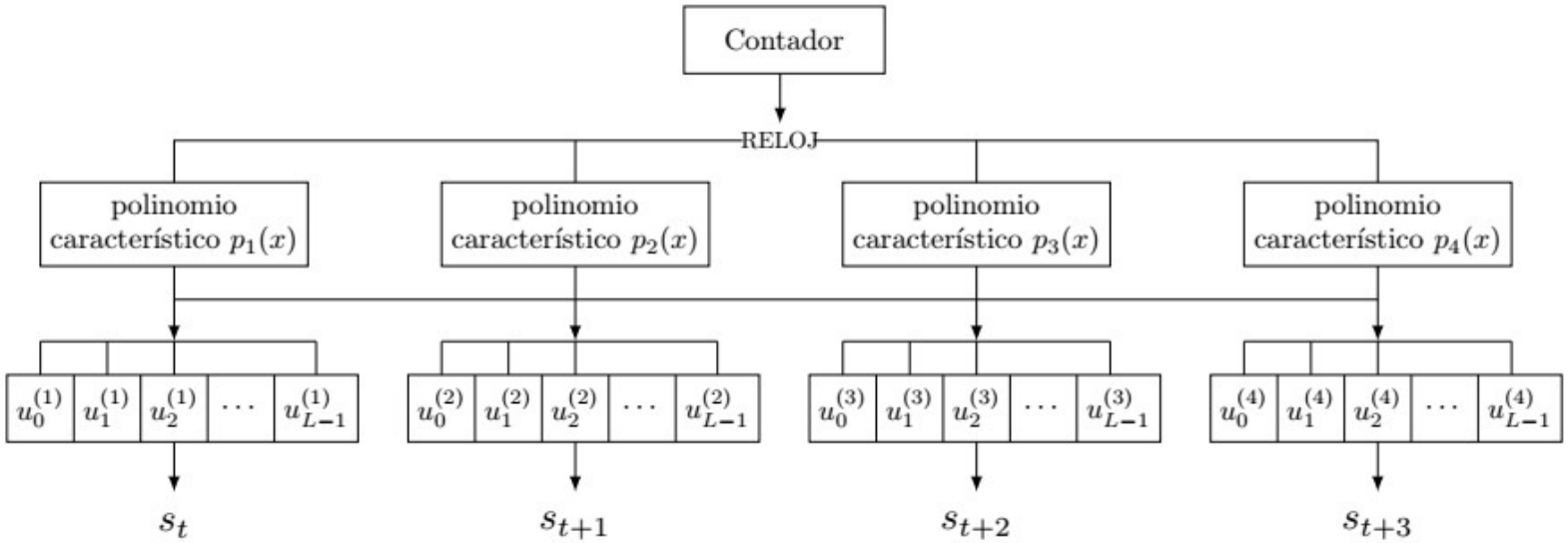


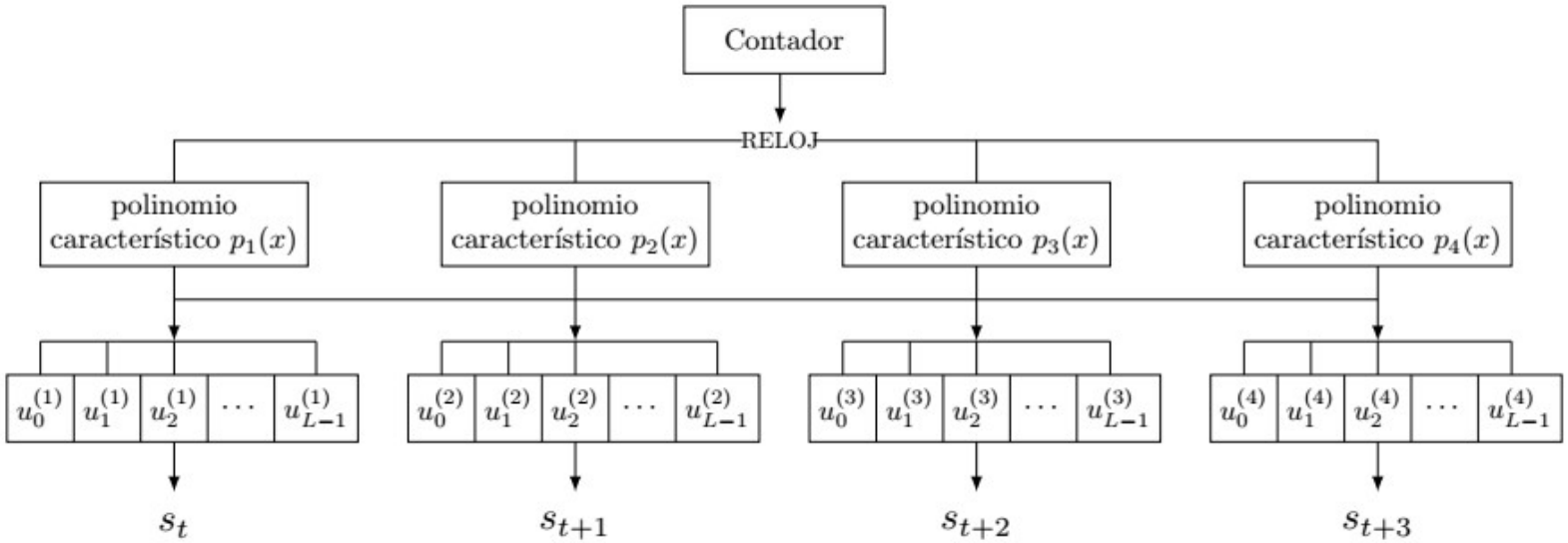
Figure: Generar una secuencia 4-entrelazada a partir de un DLFSR



- Método de entrelazado $\approx$ método de generación de un DLFSR.

Dynamic Linear Feedback Shift Register

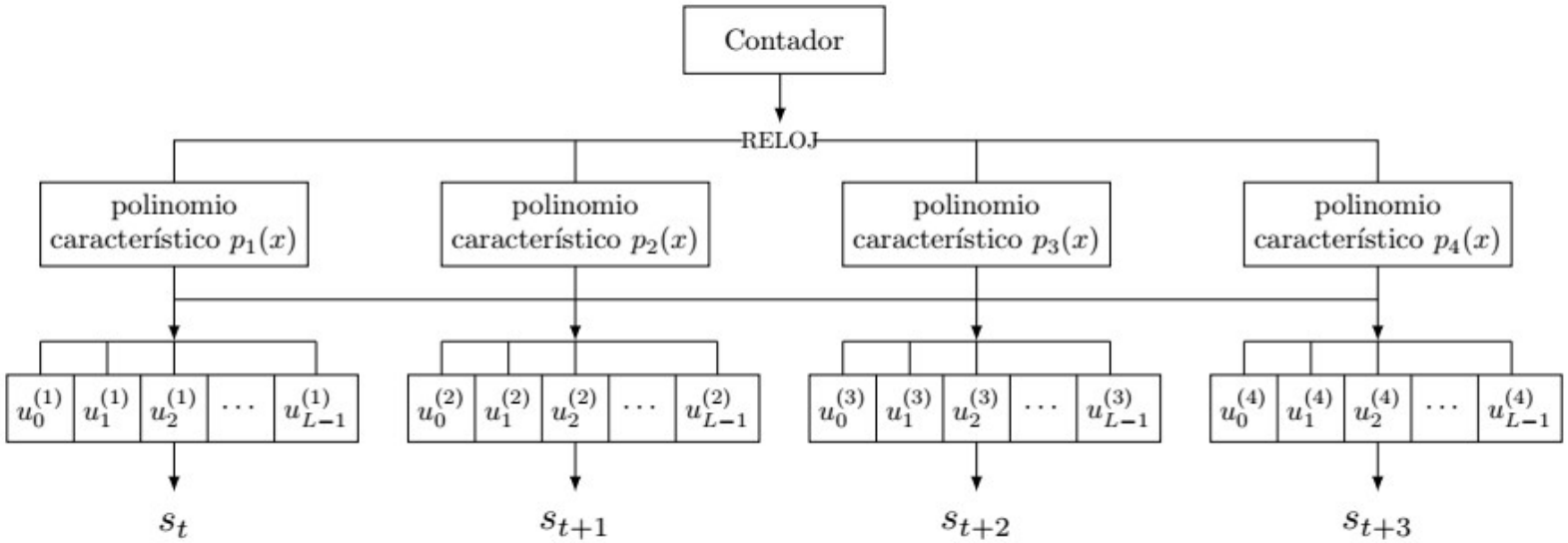
Figure: Generar una secuencia 4-entrelazada a partir de un DLFSR



- Método de entrelazado $\approx$ método de generación de un DLFSR.
- El polinomio característico cambia según el módulo contador.

Dynamic Linear Feedback Shift Register

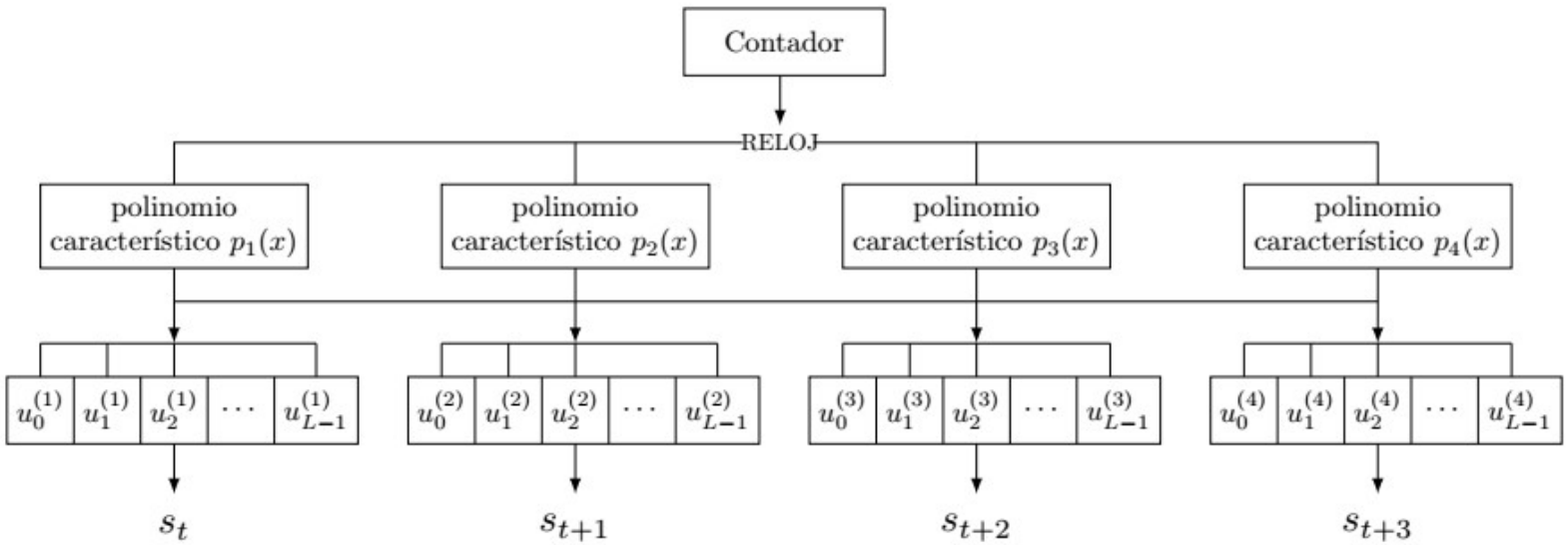
Figure: Generar una secuencia 4-entrelazada a partir de un DLFSR



- Método de entrelazado $\approx$ método de generación de un DLFSR.
- El polinomio característico cambia según el módulo contador.
- En cada pulso de reloj consideramos un polinomio primitivo diferente.

Dynamic Linear Feedback Shift Register

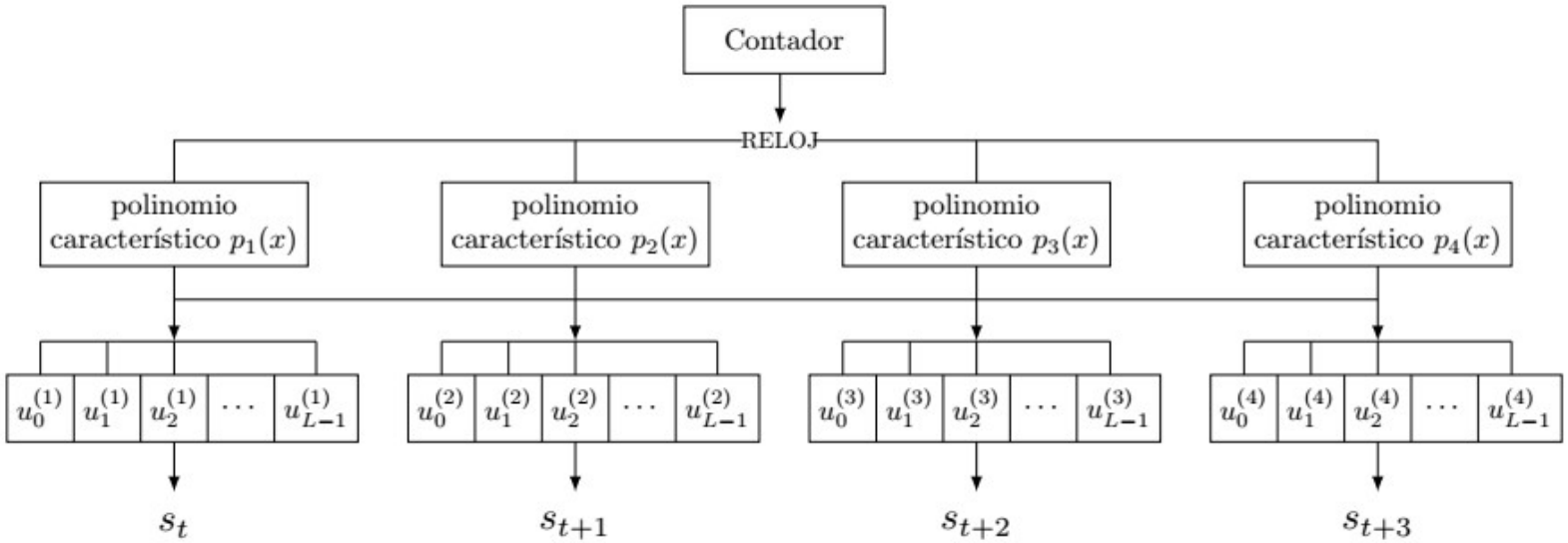
Figure: Generar una secuencia 4-entrelazada a partir de un DLFSR



- Método de entrelazado $\approx$ método de generación de un DLFSR.
- El polinomio característico cambia según el módulo contador.
- En cada pulso de reloj consideramos un polinomio primitivo diferente.
- Se genera un bit del LFSR correspondiente en ese instante y saltamos del polinomio actual al siguiente.

Dynamic Linear Feedback Shift Register

Figure: Generar una secuencia 4-entrelazada a partir de un DLFSR



- Método de entrelazado $\approx$ método de generación de un DLFSR.
- El polinomio característico cambia según el módulo contador.
- En cada pulso de reloj consideramos un polinomio primitivo diferente.
- Se genera un bit del LFSR correspondiente en ese instante y saltamos del polinomio actual al siguiente.
- Secuencia entrelazada = concatenación de la salida de t LFSRs en cada instante de tiempo.

Entrelazando t-secuencias con algún polinomio igual

Example

Sean $p_1(x) = p_2(x) = 1 + x^2 + x^5$, $p_3(x) = 1 + x + x^2 + x^3 + x^5$ y $p_4(x) = 1 + x^2 + x^3 + x^4 + x^5$ y los estados iniciales $\{10111\}$, $\{11010\}$, $\{00011\}$ y $\{10110\}$.

Entrelazando t-secuencias con algún polinomio igual

Example

Sean $p_1(x) = p_2(x) = 1 + x^2 + x^5$, $p_3(x) = 1 + x + x^2 + x^3 + x^5$ y $p_4(x) = 1 + x^2 + x^3 + x^4 + x^5$ y los estados iniciales $\{10111\}$, $\{11010\}$, $\{00011\}$ y $\{10110\}$. La secuencia 4-entrelazada:

$$\{11010100100111111010011110000010101000100111001100000011000011011100001110111101010101011001111100110111010010001100001111 0\}$$

Entrelazando t-secuencias con algún polinomio igual

Example

Sean $p_1(x) = p_2(x) = 1 + x^2 + x^5$, $p_3(x) = 1 + x + x^2 + x^3 + x^5$ y $p_4(x) = 1 + x^2 + x^3 + x^4 + x^5$ y los estados iniciales $\{10111\}$, $\{11010\}$, $\{00011\}$ y $\{10110\}$. La secuencia 4-entrelazada:

$$\{1101010010011111010011110000101010001001110011000000110000110111000011101111010101011100111110011011101001000110000111110\}$$

con $T = 124$ y $LC = 60$, i.e, $LC \leq 80$. Su polinomio característico

$$\begin{aligned} p(x) =& [p_1(x)p_3(x)p_4(x)]^4 \\ =& 1 + x^4 + x^8 + x^{16} + x^{20} + x^{24} + x^{36} + x^{56} + x^{60}. \end{aligned}$$

NO es el producto de los 4 polinomios ($p_1(x) = p_2(x)$).

Índice

Secuencias shrunken VS t-entrelazadas con polinomios diferentes

NOTA:

- La secuencia shrunken se obtiene entrelazando 2^{L_1-1} PN-secuencias desplazadas con polinomio primitivo de grado L_2.

Secuencias shrunken VS t-entrelazadas con polinomios diferentes

NOTA:

- La secuencia shrunken se obtiene entrelazando 2^{L_1-1} PN-secuencias desplazadas con polinomio primitivo de grado L_2.
- Tomaremos $t = 2^{L_1-1}$ PN-secuencias generadas por diferentes polinomios primitivos de grado L_2.

Secuencias shrunken VS t-entrelazadas con polinomios diferentes

NOTA:

- La secuencia shrunken se obtiene entrelazando 2^{L_1-1} PN-secuencias desplazadas con polinomio primitivo de grado L_2.
- Tomaremos $t = 2^{L_1-1}$ PN-secuencias generadas por diferentes polinomios primitivos de grado L_2.

Table: Comparación de los valores de LC y T de secuencias shrunken y t-entrelazadas.

	Secuencias shrunken	t polinomios diferentes
LC	$2^{L_1-2} < LC \leq L_2 \cdot 2^{L_1-1}$	$L_2 \cdot 2^{2(L_1-1)}$
T	$(2^{L_2}-1)2^{L_1-1}$	$(2^{L_2}-1)2^{L_1-1}$

t-entrelazadas con un único polinomio VS t-entrelazadas con polinomios diferentes

Table: Comparación de los valores de LC y T de secuencias t-entrelazadas con un único polinomio y con polinomios distintos.

	t polinomios diferentes		un único polinomio	
(t, L)	LC	T	LC	T
(8,16)	1024	524280	128	524280
(8,17)	1088	1048568	136	1048568
(8,18)	1152	2097144	144	2097144
(8,19)	1216	4194296	152	4194296
(8,20)	1280	8388600	160	8388600

Conclusiones y trabajo futuro

- Entrelazar secuencias es una forma de aumentar la complejidad lineal de las secuencias y de romper la linealidad.

Conclusiones y trabajo futuro

- Entrelazar secuencias es una forma de aumentar la complejidad lineal de las secuencias y de romper la linealidad.
- Análisis comparativo entre t-secuencias de un mismo polinomio primitivo y t-secuencias de polinomios primitivos diferentes.

Conclusiones y trabajo futuro

- Entrelazar secuencias es una forma de aumentar la complejidad lineal de las secuencias y de romper la linealidad.
- Análisis comparativo entre t-secuencias de un mismo polinomio primitivo y t-secuencias de polinomios primitivos diferentes.
- Gran potencial uso de estas secuencias para propósitos criptográficos.

Conclusiones y trabajo futuro

- Entrelazar secuencias es una forma de aumentar la complejidad lineal de las secuencias y de romper la linealidad.
- Análisis comparativo entre t-secuencias de un mismo polinomio primitivo y t-secuencias de polinomios primitivos diferentes.
- Gran potencial uso de estas secuencias para propósitos criptográficos.
- Análisis de la aleatoriedad de las secuencias t-entrelazadas.

Conclusiones y trabajo futuro

- Entrelazar secuencias es una forma de aumentar la complejidad lineal de las secuencias y de romper la linealidad.
- Análisis comparativo entre t-secuencias de un mismo polinomio primitivo y t-secuencias de polinomios primitivos diferentes.
- Gran potencial uso de estas secuencias para propósitos criptográficos.
- Análisis de la aleatoriedad de las secuencias t-entrelazadas.
- Estudio del entrelazamiento de PN-secuencias con polinomios diferentes y de distintos grados.

References


S. W. Golomb, Shift Register-Sequences.Laguna Hill, California: Aegean Park Press, 1982.


Coppersmith, D., Krawczyk, H., Mansour, Y.
The shrinking generator,
Advances in Cryptology—CRYPTO '93, Lecture Notes in Computer Science, vol. 773, pp. 22–39, 1994.


Xiong, H., Qu, L., Li, C., Fu, S.
Linear complexity of binary sequences with interleaved structure,
IET Communications, vol. 7, n. 15, pp.1688-1696, 2013.


Cardell, S.D., Fúster-Sabater, A.
Modelling the shrinking generator in terms of linear CA.
Adv. Math. Commun. vol.10, pp. 797–809, 2016.


Cardell, S.D., Fúster-Sabater, A., Requena, V.
Interleaving Shifted Versions of a PN-Sequence,
Mathematics, vol. 9, n.68, pp. 1–23, 2021.

¡¡MUCHAS GRACIAS!!

PN-secuencias entrelazadas de polinomios diferentes

Sara D. Cardell[1] Amparo Fúster Sabater[2] **Verónica Requena**[3]

[1] Instituto de Matemática, Estatística e Computação Científica
UNICAMP, Brazil
[2] Instituto de Tecnologías Físicas y de la Información
C.S.I.C., Spain
[3]Departamento de Matemáticas
Universidad de Alicante, Spain

RECSI 2022
19 de octubre de 2022