GUIONES DE CRIPTOGRAFÍA

SECUENCIAS PSEUDO-ALEATORIAS

Ejercicio 1. Escribe una función que determine si una secuencia de bits cumple los postulados de Golomb ([2, §3.5]).

Ejercicio 2. Implementa registros lineales de desplazamiento con retroalimentación (LFSR, [1, Chapter 6]). La entrada son los coeficientes del polinomio de conexión, la semilla, y la longitud de la secuencia de salida.

Ilustra con ejemplos la dependencia del periodo de la semilla en el caso de polinomios reducibles, la independencia en el caso de polinomios irreducibles, y la maximalidad del periodo en el caso de polinomios primitivos.

Comprueba que los ejemplos con polinomios primitivos satisfacen los postulados de Golomb (en [1, §4.5.3] hay tablas de polinomios primitivos).

Ejercicio 3. Un polinomio en varias variables con coeficientes en $\mathbb{Z}_2$ se puede expresar como suma de monomios, simplemente usando la propiedad distributiva. Cualquier monomio $x_1^{e_1}\cdots x_n^{e_n}$, $e_i \in \mathbf{N}$, es, como función, equivalente a un monomio de la forma $x_{i_1}\cdots x_{i_r}$ ($x^2 = x$ para todo $x \in \mathbb{Z}_2$, los i_j son precisamente los índices tales que $e_{i_j} \neq 0$). Por ejemplo, $1 + x^2(y + x) = 1 + x^3 + x^2 y$, es esta expresión es equivalente a $1 + x + xy$, por lo que la representamos mediante $[[0,0],[1,0],[1,1]]$, que se corresponde con la lista de exponentes en las dos variables: $x^0y^0 + x^1y^0 + x^1y^1$. Así un polinomio en $\mathbb{Z}_2$ se puede representar por una lista monomios. Y cada monomio como una lista de 0 y 1, que corresponden con los exponentes de cada una de las variables que intervienen en el polinomio.

Escribe una función que toma como argumentos una función polinómica f, una semilla s y un entero positivo k, y devuelve una secuencia de longitud k generada al aplicar a s el registro no lineal de desplazamiento con retroalimentación asociado a f.

Encuentra el periodo de la NLFSR $((x \wedge y) \vee \overline{z}) \oplus t$ con semilla 1011.

Ejercicio 4. Implementa el generador de Geffe ([1, 6.50]).

Encuentra ejemplos donde el periodo de la salida es $p_1p_2p_3$, con p_1, p_2 y p_3 los periodos de los tres LFSRs usados en el generador de Geffe.

Usa este ejercicio para construir un cifrado en flujo. Con entrada un mensaje m, construye una llave k con la misma longitud que m, y devuelve $m \oplus k$ (donde $\oplus$ significa suma componente a componente en $\mathbb{Z}_2$).

El descifrado se hace de la misma forma: $c \oplus k$ (nótese que $c \oplus k = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m$, ya que $x \oplus x = 0$ en $\mathbb{Z}_2$).

Ejercicio 5. Dada una sucesión de bits periódica, determina la complejidad lineal de dicha sucesión, y el polinomio de conexión que la genera. Para esto, usa el algoritmo de Berlekamp-Massey ([1, Algorithm 6.30]).

Haz ejemplos con sumas y productos de secuencias para ver qué ocurre con la complejidad lineal.

REFERENCES

[1] A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.

[2] P. J. Cameron, Notes on cryptography.