Modelo de secuencias entrelazadas para la generación de secuencias cifrantes

Alberto Peinado Domínguez

Dept. Ingeniería de Comunicaciones
E.T.S.I. Telecomunicación, Universidad de Málaga
Campus Teatinos. 29071-Málaga
apeinado@ic.uma.es

El diseño y análisis de los sistemas de cifrado en flujo se centra en la generación de secuencias pseudoaleatorias cifrantes. Tal es la importancia de dichas secuencias, que la seguridad del sistema completo depende fuertemente de las características aleatorias que presentan [3]. Debido a la rapidez y eficiencia de los sistemas de cifrado en flujo, se continua considerando su utilización hasta en los más recientes sistemas móviles de tercera y cuarta generación, como es el caso de UMTS (Universal Mobile Telecommunication System). En este sentido, las investigaciones en este campo han producido y continuan produciendo numerosas propuestas de generadores de secuencias pseudoaleatorias. Estas secuencias deben cumplir unos requisitos mínimos como, por ejemplo, un período de repetición elevado, una buena distribución de ceros y unos así como de rachas, una autocorrelación bivaluada (véase Criterios de Golomb en [1]) y una baja correlación cruzada entre secuencias producidas por el mismo generador usando distintas semillas.

En [2] Gong presenta un modelo basado en secuencias entrelazadas que permite estudiar bajo un mismo marco un buen número de generadores propuestos en la literatura. Este modelo es también aplicable al generador DLFSR basado en un registro de desplazamiento realimentado linealemente con realimentación dinámica) presentado por Mita et al. [4]. Este trabajo presenta los resultados de aplicar este modelo al DLFSR y a los autómatas celulares que determinan las funciones cuadráticas iteradas sobre cuerpos de caraterística 2 [5].

Referencias

[1] Golomb, S.W., *Shift Register Sequences*, Revised edition, Aegean Park Press, Laguna Hills, California, 1982

[2] Gong, G., "Theory and Applications of q-ary Interleaved Sequences", I*EEE Trans. on Information Theory*, **41**, (1995), pp. 400-411

[3] Menezes, A., Oorschot, P, Vanstone, S.A., *Handbook of Applied Cryptography*, CRC Press, 1996

[4] Mita, R., Palumbo, G., Pennisi, S., Poli, M., "Pseudorandom bit generator based on dynamic linear feedback topology", *Electronic Letters*, **38** (2002), pp 1097-1098

[5] Montoya, F., Muñoz, J., Peinado, A., "Iterated Quadratic functions in $\mathbb{F}_{2^n}$", *International Journal of Applied Mathematics*, **5** (1), (2001), pp 65-83.