Cifrado de comunicaciones de alta velocidad

Amparo Fúster Sabater

Abstract: La Dra. Fúster, científica titular del CSIC, experta en Criptografía de clave secreta, presenta los procedimientos de cifrado en flujo que permiten el diseño, evaluación y posterior criptoanálisis, de generadores de secuencia cifrante para su aplicación en los actuales estándares de comunicación que exigen altas velocidad de transmisión, y en consecuencia, altas tasas de rendimiento de las implementaciones hardware y/o software. De modo particular, presenta diseños de secuencias cifrantes basados en Registros de desplazamiento realimentados linealmente (LFSR) a los que se les añaden no-linealidades mediante combinaciones no lineales con otros LFSR o mediante filtrados no lineales de las secuencias generadas. Por último, presenta las líneas de investigación más recientes centradas en la utilización de LFSR definidos sobre cuerpos extendidos de Galois, especialmente orientados para el aprovechamiento de las longitudes de palabra con las que trabajan los actuales procesadores.