Evolución de los sistemas de cifrado caótico

Gonzalo Álvarez Marañón

Instituto de Física Aplicada
Consejo Superior de Investigaciones Científicas
C/ Serrano, 144 28006 Madrid
gonzalo@iec.csic.es

Desde principios de los años 90, se han propuesto numerosos sistemas de comunicaciones basados en la sincronización de osciladores caóticos usando una gran variedad de técnicas, con resultados diversos. Muchos de estos sistemas fueron presentados además presumiendo su seguridad frente a la intercepción por terceros. El análisis posterior de estos criptosistemas demostraba en todos los casos que los mecanismos de transmisión segura de la información propuestos eran fácilmente atacables. A medida que nuevos criptosistemas eran creados, nuevas técnicas de criptoanálisis fueron inventadas capaces de romperlos, hasta nuestros días, en que puede asegurarse con confianza que no existe sistema de comunicaciones caóticas pretendidamente seguro capaz de resistir el criptoanálisis.

A la vista de este desalentador panorama en el campo de las comunicaciones analógicas, se exploró la posibilidad de aplicar las prometedoras ideas del caos a la criptografía en el dominio de los criptosistemas digitales, funcionando en tiempo discreto. En esta nueva modalidad se han propuesto asimismo numeros criptosistemas, la mayoría de ellos igualmente débiles. Sin embargo, existen algunos criptosistemas basados en el cifrado de bloques que resisten con éxito todos los ataques.

En esta comunicación se repasa la evolución de los criptosistemas analógicos y digitales, reseñándose los hitos más destacables y resaltando la importancia de las nuevas tendencias.