Aproximaciones periódicas de automorfismos y sus aplicaciones al diseño de sustituciones

José María Amigó

Dpto. de Estadística y Matemática Aplicada
Universidad Miguel Hernández
Avda. del Ferrocarril s/n, 03202-Elche
jm.amigo@umh.es

La idea de usar aplicaciones caóticas en criptografía puede encontrarse ya en los artículos fundacionales de Shannon alrededor de 1950. Aunque en aquella época la palabra caos no estaba en circulación, Shannon se refiere claramente a este concepto al proponer la construcción de criptosistemas seguros mediante aplicaciones con medidas invariantes y la propiedad de mezcla, que dependan de sus argumentos de una forma 'sensible'. No es, por tanto, de extrañar que, cuando en las décadas de los años 70 y 80 floreció el estudio del caos en la dinámica discreta, no tardaron en aparecer aplicaciones a la criptografía digital, tanto en la definición misma de criptosistemas como en el diseño de sustituciones de bits —investigaciones que continúan con igual vigor en la actualidad. El caos está siendo también utilizado para encriptación analógica mediante circuitos sincronizados, si bien estos sistemas pertenecen más bien al campo de la esteganografía.

En esta comunicación exploramos, siguiendo la sugerencia de Shannon, la posibilidad de diseñar sustituciones criptográficamente seguras mediante aproximaciones periódicas de aplicaciones caóticas. La expectativa detrás de esta propuesta es, por supuesto, que las aproximaciones puedan heredar las propiedades de mezcla de tales aplicaciones, al menos si la velocidad de convergencia es la adecuada y las particiones correspondientes son lo suficientemente finas. Nuestros resultados corroboran esta expectativa, mostrando que, en principio, se pueden diseñar de esta manera criptosistemas con resistencia al criptoanálisis lineal y diferencial cercana al valor óptimo. Mostraremos también algunas implementaciones parciales de esta metodología, con la correspondiente evidencia numérica.