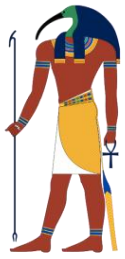

Píldora nº 32: ¿Qué son los postulados de Golomb?

Escena 1: Solomon Golomb

Solomon Golomb es un matemático norteamericano nacido en 1932 y actualmente profesor en la Universidad del Sur de California. En 1967 publica la primera edición del libro Secuencias de Registros de Desplazamiento, en el que analiza dichos registros y plantea las propiedades de aleatoriedad que debe poseer la secuencia cifrante para ser segura.

Escena 2: Características de las secuencias cifrantes

Para que una secuencia binaria de ceros y unos sea considerada una clave adecuada para la cifra en flujo, esto es que sea robusta y se parezca lo más posible a una secuencia aleatoria, deberá cumplir las siguientes condiciones: a) Tener un período muy elevado, tanto o más que el mensaje, para que la clave no se repita durante la operación de cifrado del mensaje; b) Generarse a partir de una semilla conocida por emisor y receptor, que hará las veces de clave secreta o de sesión. Deberá tener un tamaño suficientemente grande, sobre los cien bits para generar períodos del orden de 2^{100} bits; c) Ser de fácil implementación para obtener algoritmos rápidos; d) Ser imprevisible, de forma que aunque se conozca una parte de la secuencia, la probabilidad de predecir el próximo bit no sea ser superior al 50%.

Escena 3: Rachas de bits y autocorrelación fuera de fase

Para entender los postulados de Golomb, definiremos previamente rachas de bits como un conjunto de bits iguales entre bits distintos. Por ejemplo, 101 indica una racha de longitud uno de ceros y 01110 indica una racha de longitud tres de unos. Por otra parte, la autocorrelación fuera de fase de una secuencia es la comparación bit a bit de la secuencia original con la misma secuencia desplazada a la izquierda desde 1 hasta n-1 bits. En dicha comparación bit a bit, contamos los aciertos de bits iguales en las dos secuencias y los fallos debidos a bits distintos.

Escena 4: Postulados de Golomb G1, G2 y G3

El primer postulado de Golomb G1, indica que la secuencia cifrante deberá tener mitad de unos y mitad de ceros, aceptándose una diferencia de una unidad y en este caso siempre habrá más unos que ceros al provenir ésta de registros de desplazamiento lineales, donde está prohibida la secuencia de todos ceros. Esto quiere decir que la probabilidad de adivinar un bit de la secuencia en cualquier lugar de la misma es del 50%.

El segundo postulado de Golomb G2, nos dice que las rachas deben seguir una distribución geométrica, habiendo más rachas cortas que largas. Así, en un período T, la mitad de las rachas serán de longitud 1, la cuarta parte de longitud 2, la octava de longitud 3, etc. Eso quiere decir que la probabilidad de adivinar el siguiente bit de la secuencia conociendo incluso los bits anteriores, sigue siendo de un 50%. Esto es debido a que la secuencia pasa por todos sus restos.

Por último, el tercer postulado de Golomb G3, indica que la autocorrelación fuera de fase deberá tener el mismo número de aciertos que de fallos para todos los desplazamientos aplicados a la secuencia, desde 1 hasta n-1 bits. Esto significa que, independientemente de la zona en la que comencemos a analizar dicha secuencia cifrante, no obtendremos una mayor información o ventaja para su análisis ni tampoco datos de su comportamiento.

Escena 5: ¿Es suficiente con cumplir los postulados de Golomb para cifrar?

Las secuencias cifrantes que cumplen con los tres postulados de Golomb, generadas por registros lineales y conocidas como m-secuencias, son interesantes pero desgraciadamente muy fáciles de predecir, por el hecho de que el registro pasa por todos sus restos. El ataque conocido como de Berlekamp Massey rompe una clave de 2^n bits con tan sólo conocer 2n bits consecutivos de la secuencia, razón por la cual no sirven como claves para la cifra. Esto se soluciona añadiendo alguna operación entre dos o más registros de desplazamiento que generan dichas secuencias, siendo recomendable utilizar una función or exclusivo. La secuencia cifrante final por lo general ya no cumplirá con los postulados de Golomb, pero será una clave segura para la cifra. Recuerda que la cifra bit a bit entre mensaje y clave, se realiza

con esta secuencia cifrante y no con la clave secreta o semilla intercambiada previamente entre emisor y receptor.

Madrid, marzo de 2015

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*