PROPUESTA DE TRABAJO DE FIN DE MÁSTER
MÁSTER EN MATEMÁTICAS AVANZADAS

Director(es): Yago Antolín Pichel, María Isabel González Vasco

Tutor UCM: (sólo en caso de que no haya ningún director de la UCM)

Alumno(a): Irene María Urrutia Calvo

Curso: 2024-2025

Título: Análisis de Construcciones Criptográficas Basadas en Grupos de Matrices

Resumen:

Desde el trabajo seminal de Tillich y Zémor para diseñar funciones hash usando grupos de matrices, existen diferentes propuestas interesantes en la literatura. La idea de estos diseños es combinar la agilidad computacional de estos grupos con la dificultad de resolución de ciertos problemas de la palabra asociados. Así, dada una cadena de bits, su resumen o hash se calcula en última instancia como un producto de matrices con arreglo a una cierta codificación. La robustez de dicho hash depende de lo difícil que sea encontrar colisiones, i.e., cadenas de bits que se resuman como el mismo elemento del grupo.
En este trabajo se investigará el estado del arte de este tipo de construcciones, analizando en profundidad al menos una propuesta reciente y evaluando su seguridad y eficiencia en función de la estructura del grupo que se utilice como plataforma.

Referencias

Rainer Steinwandt, Markus Grassl, Willi Geiselmann, y Thomas Beth. Weaknesses in the SL2(F2n) Hashing Scheme. In Advances in Cryptology–CRYPTO 2000, volume 1880 of Lecture Notes in Computer Science, pages 287–299. Springer-Verlag, 2000.

Jean-Pierre Tillich and Gilles Zemor. Group-theoretic hash functions. In Algebraic Coding, First French-Israeli Workshop, volume 781 of Lecture Notes in Computer Science, pages 90–110. Springer-Verlag, 1994.

Jean-Pierre Tillich and Gilles Zemor. Hashing with SL2. In Advances in Cryptology– CRYPTO ’94, volume 839 of Lecture Notes in Computer Science, pages 40–49, 1994.

Gilles Zemor. Hash Functions and Graphs With Large Girths. In Advances in Cryptology– EUROCRYPT ’91, volume 547 of Lecture Notes in Computer Science, pages 508–511. Springer-Verlag, 1991.

Gilles Zemor. Hash Functions and Cayley Graphs. Designs, Codes and Cryptography, 4(4):381–394, October 1994.