ARIANE MASUDA, New York City College of Technology, CUNY
Involutions over finite fields

In the context of memory-limited environments, involutions are desirable because they allow for efficient use of limited memory resources. Specifically, in many applications, both the permutation and its inverse must be stored in memory, which can be a challenge in resource-constrained environments. By using an involution as the interleaver, the same structure and technology used for encoding can be used for decoding as well. Fixed points are points that remain unchanged under the permutation. In cryptographic applications, such as the design of S-boxes, it is desirable to have permutations with a small number of fixed points to increase the security of the system. Therefore, understanding the number of fixed points and how to construct involutions with few fixed points is an important area of research. In this talk we will present some families of involutions over finite fields, including some explicit constructions based on a prescribed number of fixed points.