Involutions of F_q Obtained From Binomials of the Form $x^m(x^{\frac{q-1}{2}} + a)$

Lillian González-Albino*, University of Puerto Rico, Río Piedras Campus
Dr. Ivelisse Rubio, University of Puerto Rico, Río Piedras
Dr. Ariane Masuda, New York City College of Technology

Permutations over finite fields have many applications ranging from cryptography and combinatorics to theory of computation. For many of these applications it is important to find permutations with a small memory footprint that are easy to implement. A good option is to use permutations generated by polynomials that are their own inverse, called *involutions*. In 2017, Castro et al. gave explicit formulas for monomial involutions over F_q and their fixed points. The number of fixed points is important in applications in cryptography since it is related to the non-linearity of a permutation. In 2018, Zheng et al. characterized involutions of the form $x^m h(x^s)$ over F_q, but an explicit formula for m and the amount of fixed points were not given. In this talk we present results on explicit formulas for binomial involutions $x^m(x^{\frac{q-1}{2}} + a)$ over F_q, and their fixed points.

Keywords: permutation polynomials, involutions, fixed points, finite fields