Resemblance

Robert S. Coulter

Department of Mathematical Sciences
University of Delaware

joint work with Li-An Chen

One of the main problems in our area is that of constructing bijections with low differential uniformity. Indeed, the "Big APN problem" is familiar to all of us. In this talk we will introduce the notion of *resemblance*, which is a way of comparing how close two functions are from each other. One can apply the concept in a variety of situations. We will concentrate mostly (if not exclusively) on the concept of *permutation resemblance* (P-Res), which provides a new way of measuring how close a function is to being a permutation. P-Res provides some advantages over historical tools for measuring a function's "bijectiveness", especially in the case where one is concerned about constructing bijections with low differentially uniformity. However, it also offers some disadvantages, perhaps most notably being that it is not immediately clear how to compute the P-Res of a function. To this end, we will describe a linear programming method showing how to resolve this issue. We will also present some computational and theoretical results.