

# Applications of Partial Difference Families to Partial Designs

Laura Johnson

lj68@st-andrews.ac.uk

University of St. Andrews

(This talk is based on joint work with Dr Sophie Huczynska.)

In 1939 Bose and Nair defined partially balanced incomplete block designs (PBIBDs). These are the partial analogue of BIBDs. More recently, in the early 2000s, Ogata et al. defined a new combinatorial design known as a splitting balanced incomplete block design (splitting BIBD). The motivation for defining splitting BIBDs was to construct AMD codes, a type of cryptographical tool used to protect against attacks from active adversaries.

In this talk I will discuss how two recently introduced combinatorial structures known as disjoint partial difference families (DPDFs) and external partial difference families (EPDFs) may be used to find constructions of these designs.