Structural cryptanalysis of block ciphers

Sondre Rønjom

In this talk we present an overview of some recent progress in structural cryptanalysis of block ciphers with a focus on subspace cryptanalysis. We present some of the essential theory and present new attacks on concrete ciphers.