Rasta and Picnic

Christian Rechberger

In this talk I'll discuss recent developments in the area of design, analysis, and applications of primitives in symmetric cryptography with few multiplications. This includes 'Rasta', a design with an AND-depth of 2 (theoretical) and 4 (practical) that can be used to remove the huge ciphertext expansion in FHE schemes. This also includes 'Picnic', a new approach to longterm-secure signature schemes relying solely on the security of symmetric primitives.