DELARAM KAHROBAEI, The City University of New York, QC, GC, University of York (UK)
Post-quantum hash functions using $SL_n(F_p)$

We define new families of Tillich-Zémor hash functions, using higher dimensional special linear groups over finite fields as platforms. The Cayley graphs of these groups combine fast mixing properties and high girth, which together give rise to good preimage and collision resistance of the corresponding hash functions. We justify the claim that the resulting hash functions are post-quantum secure. Joint work with Corentin Le Coz, Christopher Battarbee, Ramón Flores, Thomas Koberda.