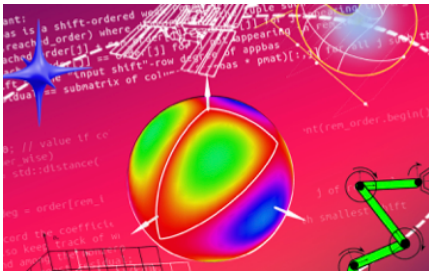

ID de Contribution: **31** Type: **Non spécifié**

# Applications of fast integer and polynomial lattice reduction in cryptography by Nadia Heninger

*jeudi 28 septembre 2023 09:30 (1 heure)*

Abstract. I will survey some concrete lattice computations that have appeared in the context of some recent papers in applied cryptography that I have been involved with, and pose some open problems and speculative improvements that arose in these contexts.