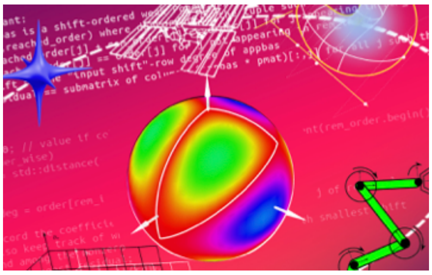

Contribution ID: **31**

Type: **not specified**

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

Thursday, September 28, 2023 9:30 AM (1 hour)

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.