The hidden number problem revisited.

Nadia Heninger, University of Pennsylvania

In the hidden number problem, one wishes to recover a secret element α modulo p given the most significant bits of many multiples $t \alpha \bmod p$ for random t. One class of algorithms used to solve this problem uses lattice basis reduction, and is a popular tool in side channel cryptanalysis of ECDSA and DSA signature algorithm implementations. In this talk, I will show an alternative viewpoint on this problem, and give some experimental results for real-world cryptosystems.