LEARNING FROM NOISY PARITIES VIA NEAREST-NEIGHBOR SEARCH

Antonio R. Nicolosi
Computer Science Department
Stevens Institute of Technology
e-mail: nicolosi@cs.stevens.edu

Carleton J. Bosley
Computer Science Department
Stevens Institute of Technology
e-mail: bosley@cs.stevens.edu

Miaomiao Zhang
Computer Science Department
Stevens Institute of Technology
e-mail: miaomiao@cs.stevens.edu

SAMS Classification: 15

Learning Parity with Noise (LPN) is a fundamental problem from computational learning theory that has recently been suggested as the basis for cryptographic applications. Roughly speaking, the \((n, \epsilon)\)-LPN problem amounts to recovering an unknown \(s \in \mathbb{Z}_2^n\) from a random collection of its noisy parities, i.e., dot-products of \(s\) with several known \(a \in \mathbb{Z}_2^n\), each perturbed with independent Bernoulli noise of rate \(\epsilon\). We design an exponential-time algorithm to solve the \((n, \epsilon)\)-LPN problem using tools from approximation algorithms, namely Nearest Neighbor Search. We then compare our algorithm with existing solutions to the problem, and discuss its relation to a classic approach toward attacking coding-based cryptography known as Information-Set Decoding.