Cryptography

Boran Erol

March 2024

The Goldreich-Levin Theorem proves existence of probabilistic learning algorithms for linear functions.

1 Presentation in Katz and Lindell

Theorem 1.1. Assume OWFs exist. Then, there's a one-way function g and a hard-core predicate hc of g.

7.3.2 in Katz and Lindell

Notes about Claim 7.15 in Katz and Lindell

For $x \in S_n$, we're being careful with the size of the set and relaxing the success probability. For $x \notin S_n$, we're being careful with the success probability and relaxing the set size.

Notes about Claim 7.16 in Katz and Lindell

Union bound the failure probabilities for r and $r \oplus e_i$.

Finish the proof by using the Chernoff bound.