abstract

COMPUTER SCIENCE/DISCRETE MATH I
Topic:

Speaker:

Affiliation:

Date:

Time/Room:

We prove that every key exchange protocol in the random oracle model in which the honest users make at most n queries to the oracle can be broken by an adversary making $O(n^2)$ queries to the oracle. This improves on the previous $\Tilde{O}(n^6)$ query attack given by Impagliazzo and Rudich (STOC' 89). Our bound is optimal up to a constant factor since Merkle (CACM '78) gave an n query key exchange protocol in this model that cannot be broken by an adversary making $o(n^2)$ queries.

Our result extends to an $O(n^2)$ query attack in the random permutation model improving on the pervious $\Tilde{O}(n^{12})$ attack of Impagliazzo and Rudich. This bound again optimal up to a constant factor since Merkle's protocol can be adapted to this model as well.

Joint work with Boaz Barak