COS522: Computational Complexity Fall 2011

Princeton University

Instructor: Sanjeev Arora

Lecture 9 notes Oct 13. Crypto contd.

1. Recap: Cryptography. How to define secure encryption? Strong property: encrypted msg looks indistinguishable from a random string. (Even this is not enough; chosen plaintext attack.)
2. Recap: Simplest system using shared random string. XOR. Satisfies most stringent defn of security.
3. How to share a random string (uses fast exponentiation): Alice picks a, sends over g^a. Bob pics b, sends over g^b. They both compute g^{ab}, which they now share. (Believed to be secure.)
4. One way function. Example: g^a. Random self-reducibility. One-way permutation. Lookahead: hardcore bit. (Intuition: if uncertain about even a single bit of a, then this bit is hard to guess.)
5. Another example: multiplication. Not known to be rsr.
6. One-way function formal defn. Weak/strong. Fact: can turn weak into strong (k-wise direct product). Hardness amplification.
7. Pseudorandom generator: Deterministic fn that stretches n bits to n^c, such that the output string is indistinguishable whp from random string.
8. Today: PRG from a oneway permutation.
9. Yao’s hybrid argument: fn is a PRG iff it passes the next bit test. Only if is clear: a next-bit test can be used to distinguish from random. So better pass it! If is harder.
10. Hybrid argument. Suppose distinguisher A has prob ½ + \delta of saying “1” on the pseudorandom string vs ½ on random string. Let P\_i = Pr[distinguisher says 1 when first i bits are from PRG and last n^c –i are random].
11. \delta = P\_{n^c} – P\_0. E\_i[P\_i –P\_{i-1}] is at least \delta/n^c.
12. Predictor: Given first i bits, add the I’th and then fill the remaining bits randomly. Run A. If it says 1, go with your guess otherwise with the other guess.
13. Analysis of correctness. Four possibilities: We guessed the right/wrong bit; A said 1/0. See which contribute to correct guess. Advantage is exactly p\_{i+1} – p\_i.
14. How to extend by 1 bit. Goldreich-Levin hardcore bit.