TOC

↳ RANDOMNESS AND COMPUTATION

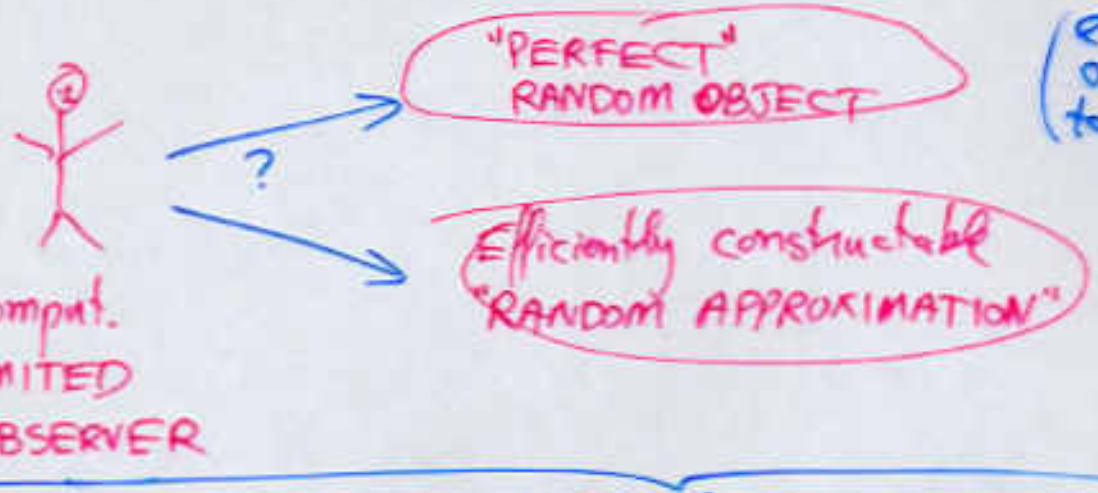
- FOUNDATIONS OF CRYPTOGRAPHY
  - "Secrets" ⟹ randomness
  - "publically verifiable secrets" ⟹ intractability ≡ compt. hardness
- PSEUDORANDOMNESS
  ⟹ Computational Indistinguishability (of distant distributions)
- PROBABILISTIC PROOF SYSTEMS
  = Randomized verification procedure (+ probability of error!)
- PROPERTY TESTING
  = A notion of approximation for decision problems focused at sublinear-time algorithms
  ↓ must be randomized

FOUNDATIONS OF CRYPTOGRAPHY

= PARADIGMS, APPROACHES & TECHNIQUES
used to CONCEPTUALIZE, DEFINE
& PROVIDE SOLUTIONS
to "natural security concerns"

- Study of existing paradigms, techniques, ...
  (e.g. conc. & reset. ZK)
  [ROSEN, B., L.]
- Introduction of new paradigms
  (e.g. non-black-box simulation)
  [BARAK]
- Identification (or rigorous treat.) of new problems
  (e.g. "passwd-based security")
  [LINDELL]

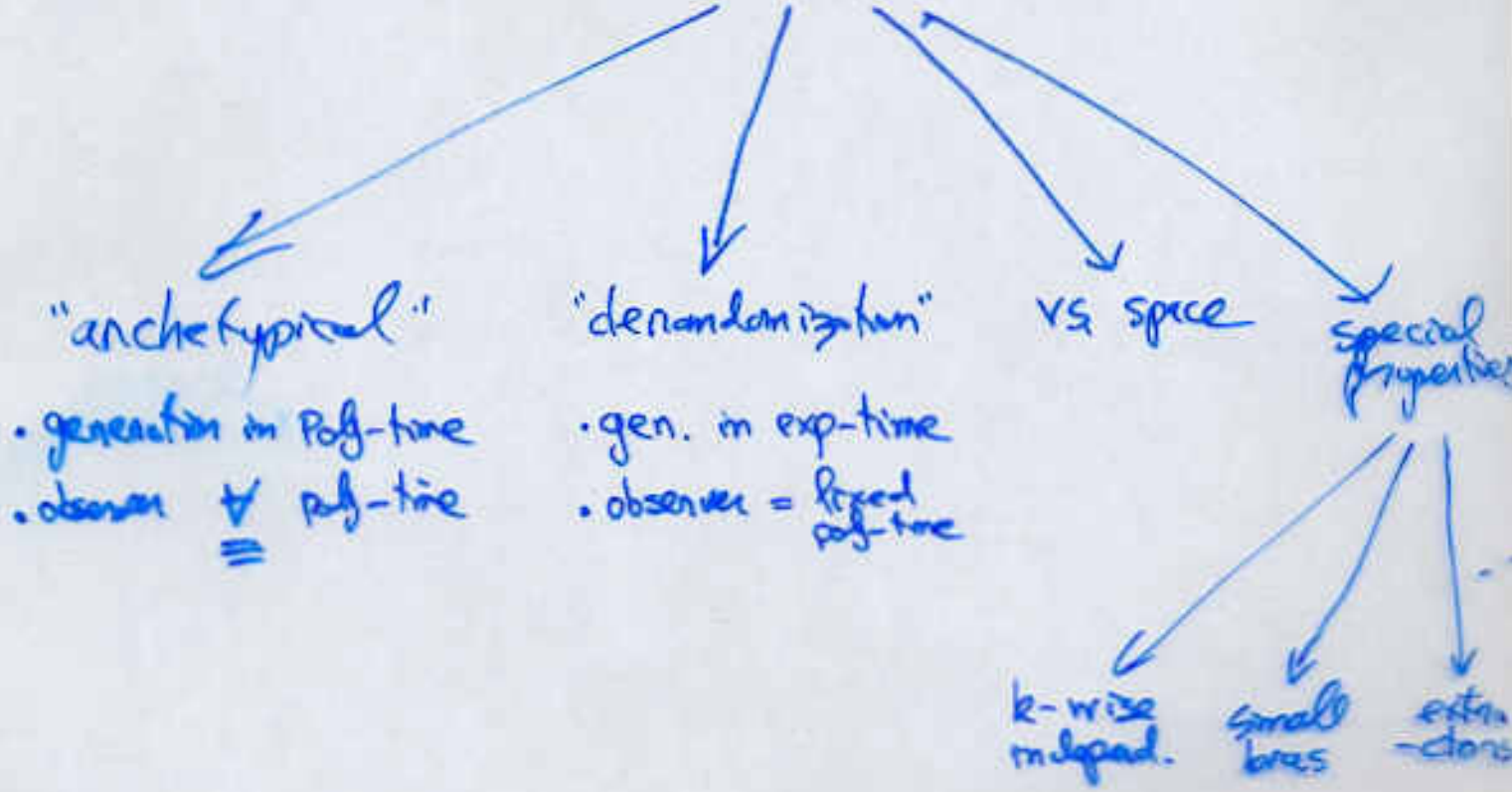
PSEUDORANDOMNESS ⟹ Comput. Indistng.



General paradigm

⇓

instantiations



PROBABILSTIC PROOF Systems

= RANDOMIZED & "INTERACTIVE" VERIFICATION PROCEDURE
+ PROBABILITY OF ERROR (BOUNDED by a parameter).

- INTERACTIVE PROOFS (vs. "written proofs")

  ALLOW more efficient verification (than via written proofs);
  e.g., proof of NON-ISOMORPHISM.

  THM: IP = PSPACE

- ZERO-KNOWLEDGE (interactive) PROOFS

  ≡ Proving without teaching anything
  (beyond the validity of the assertion).

  THM: Anything provable is provable in zero-knowledge
  provided one-way functions.

- Probabilistically Checkable Proofs

  ≡ Written proofs, partially read.
  (INDEED proofs are in redundant form)

  THM: NP = PCP[log, O(1)]