RANDOMNESS AND COMPUTATION

- Foundations of Cryptography
  - "Secrets" → randomness
  - "publicly verifiable secrets" → intractability
    \[≈\text{compt. hardness}\]

- Pseudorandomness
  \[\Rightarrow\text{Computational Indistinguishability}\]
  \[\text{(of distant distributions)}\]

- Probabilistic Proof Systems
  = Randomized verification procedure
  \[+\text{Probability of error}!\]

- Property Testing
  = A notion of approximation for decision problems
  \[\text{focused at sublinear-time algorithms}\]
  \[\text{must be randomized}\]
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 $\Rightarrow$ Comput. Indistinguishability

- "PERFECT"
  - RANDOM OBJECT
- Efficiently constructible
  - "RANDOM APPROXIMATION"

Comput. Limited Observer

General paradigm

- instabilities
  - "anti-typical"
    - generation in Poly-time
    - observer $\not\in$ Poly-time
  - "derandomization"
    - generation in exp-time
    - observer = fixed poly-time
  - vs space
  - special properties
    - k-wise indpand.
    - small bias
    - extra conditions
Probabilistic 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.
  \[ \text{THM: } \text{IP} = \text{PSPACE} \]

- Zero-Knowledge (interactive) Proofs
  \[ \text{= Proving without teaching anything} \]
  \[ \text{= beyond the validity of the assertion.} \]
  \[ \text{THM: Anything provable is provable in zero-knowledge} \]
  \[ \text{provided one-way functions.} \]

- Probabilistically Checkable Proofs
  \[ \text{= Written proofs, partially read.} \]
  \[ \text{(Indeed proofs are in redundant form)} \]
  \[ \text{THM: } \text{NP} = \text{PCP}[\log, O(1)] \]