How to Use Indistinguishability Obfuscation: Deniable Encryption, and More

Amit Sahai

Brent Waters
Two Notions [BGIRSVY01]

- **Black Box Obfuscation**
  Learn no more than oracle interaction
  Natural, easy to use, but impossible for *some* functions

- **Indistinguishability Obfuscation**
  Cannot tell two equivalent circuits apart
  E.g. \( a (b+c) \) vs. \( ab + ac \)
  Application is less immediate
  Candidate! [GGHRSW13]
Vision: IO as hub for cryptography

Standard Assumption (e.g. LWE) (w/complexity leveraging?)

- Indistinguishability
- Obfuscation

“Most” of cryptography
Result 1: Building up crypto

Indistinguishability
Obfuscation

+ OWFs

PKE, short signatures, NIZK, OT, TDF, CCA-PKE

Punctured Programming:

Surgically remove key elements w/o changing input/output

Uses Confined PRFs [BW13, BGI13, KPTZ13]
Result 2: Deniable Encryption [CDNO97]

Claim a different message, even if attacker demands your random coins

MIT 1998

OMG NSYNC is kewl

“Hidden Trigger” Technique

Make any existing key deniable