How Useful are Random Oracles?

Mohammad Mahmoody
Hemanta K. Maji
Manoj Prabhakaran
How Useful are Random Oracles in Secure Function Evaluation

Mohammad Mahmood
Hemanta K. Maji
Manoj Prabhakaran
In 2-party deterministic Secure Function Evaluation, Random Oracle is useful *ONLY* as Commitment.
Semi-honest Setting

- Commitment is **Trivial**

- So, Random Oracles are **USELESS** for Secure Function Evaluation!
Malicious Setting

- Access to Random Oracle EQUIVALENT to the Commitment-hybrid
Highlights
Highlights

• Implies black-box separations (a la Impagliazzo-Rudich-89)
Highlights

• Implies **black-box separations** (a la **Impagliazzo-Rudich-89**)

• Techniques: **Barak-Mahmoody-09** and **Maji-Prabhakaran-Rosulek-09** on steroids
Highlights

- Implies **black-box separations** *(a la Impagliazzo-Rudich-89)*

- Techniques: **Barak-Mahmoody-09** and **Maji-Prabhakaran-Rosulek-09** on steroids

- Cannot “securely compile away” the RO from any arbitrary protocol
Highlights

• Implies **black-box separations** (a la **Impagliazzo-Rudich-89**)

• Techniques: **Barak-Mahmoody-09** and **Maji-Prabhakaran-Rosulek-09** on steroids

• Cannot “securely compile away” the RO from any arbitrary protocol

• Relies on the structure of the SFE function
Next?

- Commitment got its oracle
Next?

- Commitment got its oracle
- Conjecture: Every functionality has its own oracle
Next?

- Commitment got its oracle
- Conjecture: Every functionality has its own oracle
- Infinitely many NEW (natural) distinct computational assumptions