Towards
A Unifying Framework of Computation on Encrypted Data

Shashank Agrawal
Shweta Agrawal
Manoj Prabhakaran
Exciting Times

• Explosion of primitives that enable computing on encrypted data
  • Identity based encryption, Functional encryption (FE), FHE, Obfuscation, Witness Encryption, Property Preserving encryption, Bilinear Groups/über assumption, …
Exciting Times, But..

- Each primitive has many different definitions of security
  - **FE**: IND \([BF01,SW05..]\), Non-adaptive SIM\(^{[ON'10]}\), Adaptive SIM\(^{[BSW'11]}\), Fully-adaptive security \(^{[MM'13]}\), SS2/SS3\(^{[BON'13]}\), Bounded-key IND/SIM\(^{[GVW'12]}\), Unbounded SIM \(^{[AGVW'13]}\), Relaxed SIM\(^{[AKS'14]}\), ...

- In addition, each primitive has many variants
  - **FE**: Symmetric key/Public key, With or without function hiding (function hiding has 3 different definitions!), public/private index, bounded/unbounded key…
Exciting Times, But..

• Each primitive has many different definitions of security
  • **FE**: IND $^{[BF01,SW05...]}$, Non-adaptive SIM$^{[O'N'10]}$, Adaptive SIM$^{[BSW'11]}$, Fully-adaptive security $^{[MM'13]}$, SS2/SS3$^{[BO'N'13]}$, Bounded-key IND/SIM$^{[GVW'12]}$, Unbounded SIM $^{[AGVW'13]}$, Relaxed SIM$^{[AKS'14]}$, …

• In addition, each primitive has many variants
  • **FE**: Symmetric key/Public key, With or without function hiding (function hiding has 3 different definitions!), public/private index, bounded/unbounded key…

What are the “best” achievable definitions? Are these primitives all that different from each other?
We present...

- **Unifying framework for “cryptographic objects”**
  - Models Obf., FE, FHE, (limited) Generic Group, …
    - Different “schemas” in the framework
  - Easy to define new variants
    - e.g., obtain iO, DiO as variants of Obf. schema
- **Indistinguishability-Preserving (IND-PRE) security**
  - Avoids many known impossibility results, but sometimes stronger than definitions in use today
  - Strong enough for composition (often)
We present…

- **Unifying framework for “cryptographic objects”**
  - Models Obf., FE, FHE, (limited) Generic Group, …
    - Different “schemas” in the framework
  - Easy to define new variants
    - e.g., obtain iO, DiO as variants of Obf. schema
- **Indistinguishability-Preserving (IND-PRE) security**
  - Avoids many known impossibility results, but sometimes stronger than definitions in use today
  - Strong enough for composition (often)