SaTC: CORE: Small

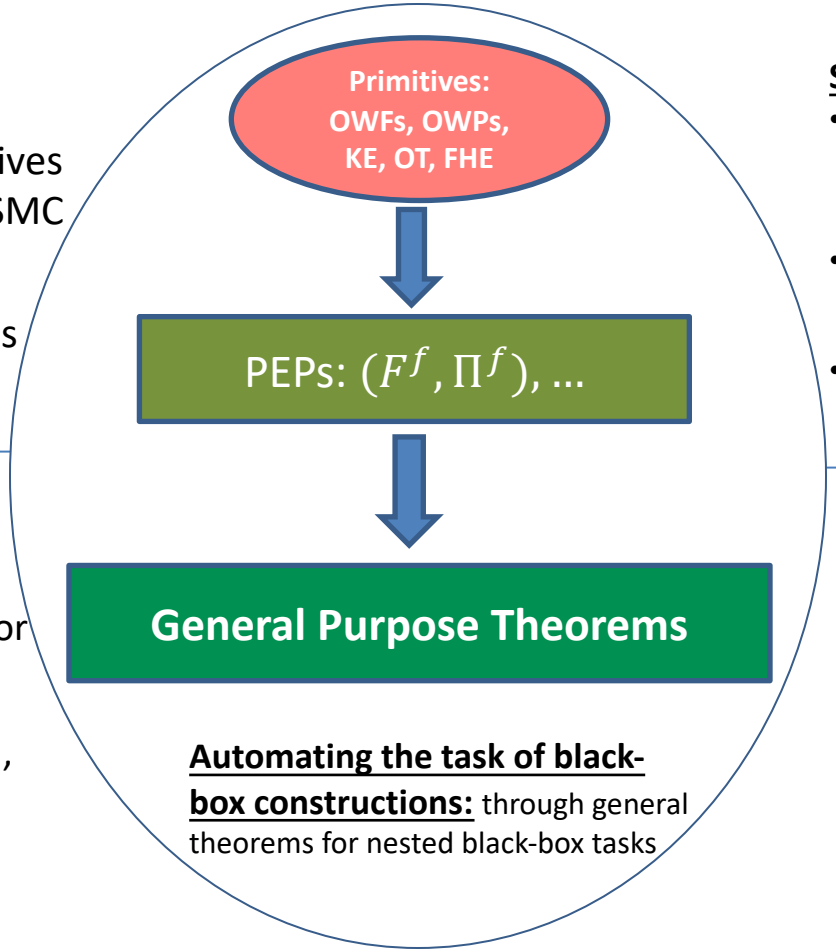
Nested Black-Box Constructions in Cryptography

Challenges:

- Protocol-equip. primitives (PEPs): black-box, ZK/SMC
- Composition
- Gen-purpose theorems

Solution:

- Key innovation: GL style def., cut-&-choose inspired constructions for core primitives
- Methods for composing PEPs, and through them, development of GMW style theorems



Scientific Impact:

- Provide a unified theory of black-box (BB) constructions, particularly in ZK and secure computation
- Enable a fundamentally new understanding of BB constructions
- Potential to yield new and improved BB constructions

Broader Impact and Broader Participation:

- New techniques that advance the area of secure computation
- Training several graduate students through research and curriculum
- Exposure to cutting edge research for young minds

Award# 2028920, Stony Brook University, Omkant Pandey, omkant@cs.stonybrook.edu