SaTC: CORE: Small: Optimal Coin-flipping Protocols

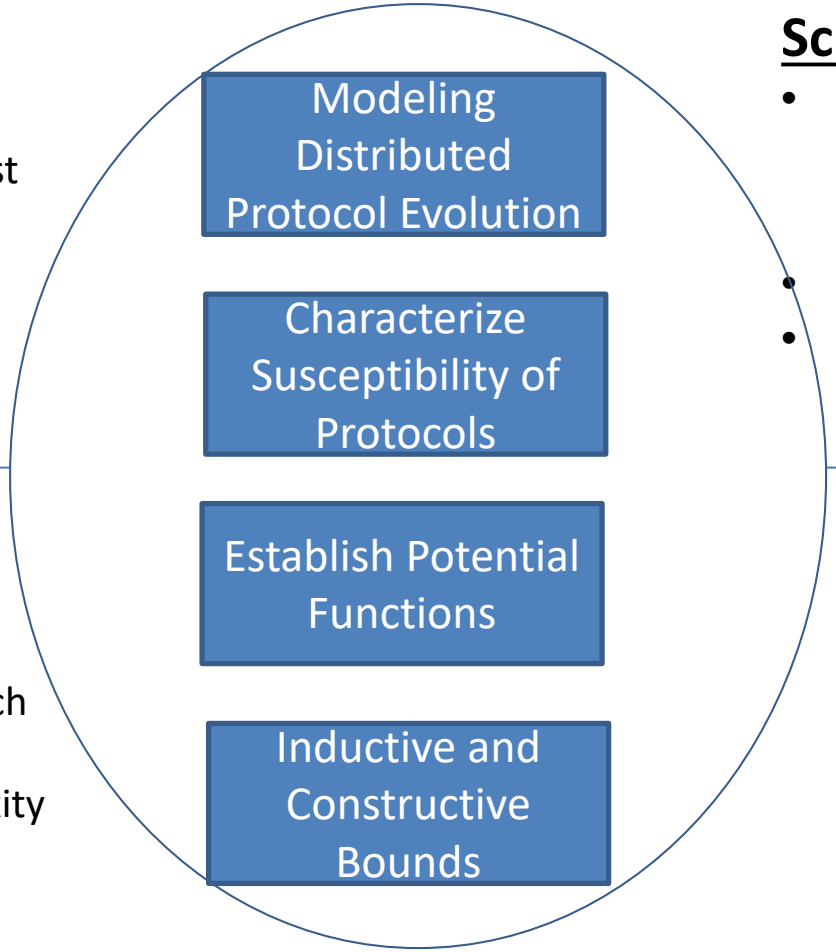
PURDUE UNIVERSITY

Challenge:

- Characterize the most secure protocol for a computation (for example, the coin-tossing functionality)

Solution:

- Inductive and (inherently) constructive approach
- Develop tools for information complexity of secure protocols



Scientific Impact:

- Consequences to distributed and cryptographic protocol design
- Characterize attack strats
- New Isoperimetric inequalities and ML applications

Broader Impact and Broader Participation:

- New secure computation techniques
- New optimal distributed consensus protocols
- Training of undergraduates and students from minority demographics in mathematical topics

Project info (2055605, Purdue University, PI: Hemanta K. Maji)