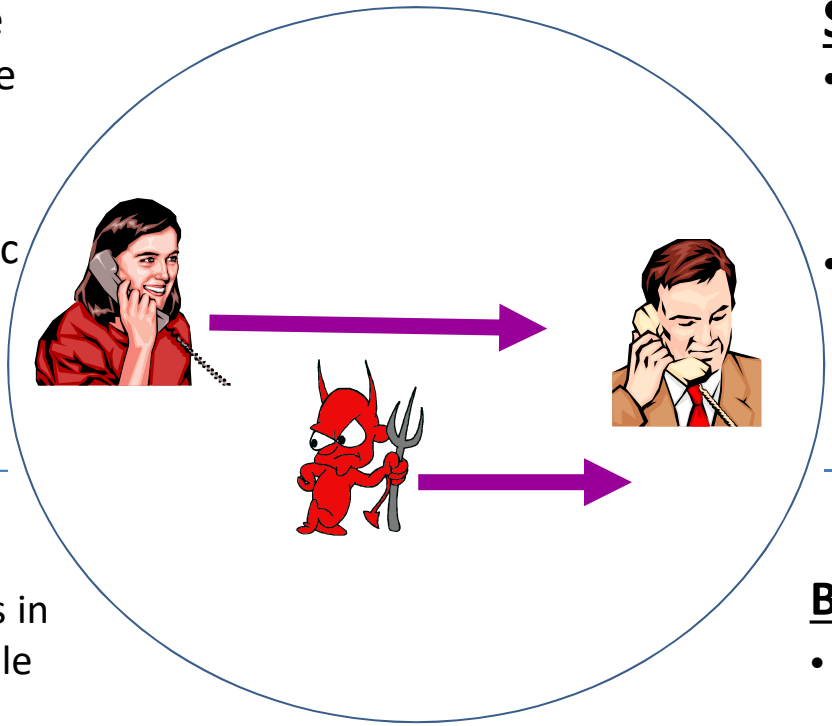
Transforming Non-Malleable Cryptography

Carnegie Mellon University

Challenge:

- Preventing tampering and man-in-the-middle attacks a core challenge in cryptography
- Affect the design of almost all cryptographic protocols



Scientific Impact:

- Will give an intellectual toolkit to secure against such attacks in larger cryptographic protocols
- Will lead to better secure multi-party computation protocols

Solution:

- Achieve breakthroughs in designing non-malleable commitments, non-malleable secret sharing and codes

Broader Impact:

- Train scientists and engineers in non-malleable cryptography (and crypto in general)
- Lead to better privacy preserving computation techniques

Award #1916939
Vipul Goyal (CMU)