

# Positive Results for Concurrently Secure Computation in the Plain Model

**Vipul Goyal**  
Microsoft Research, India

# Concurrently Secure Computation (in plain model)

Impossible!! ☹ Impossible !! ☹ Impossible!! ☹

Lin'03

BPS'06

Lin'04

AGJPS'12

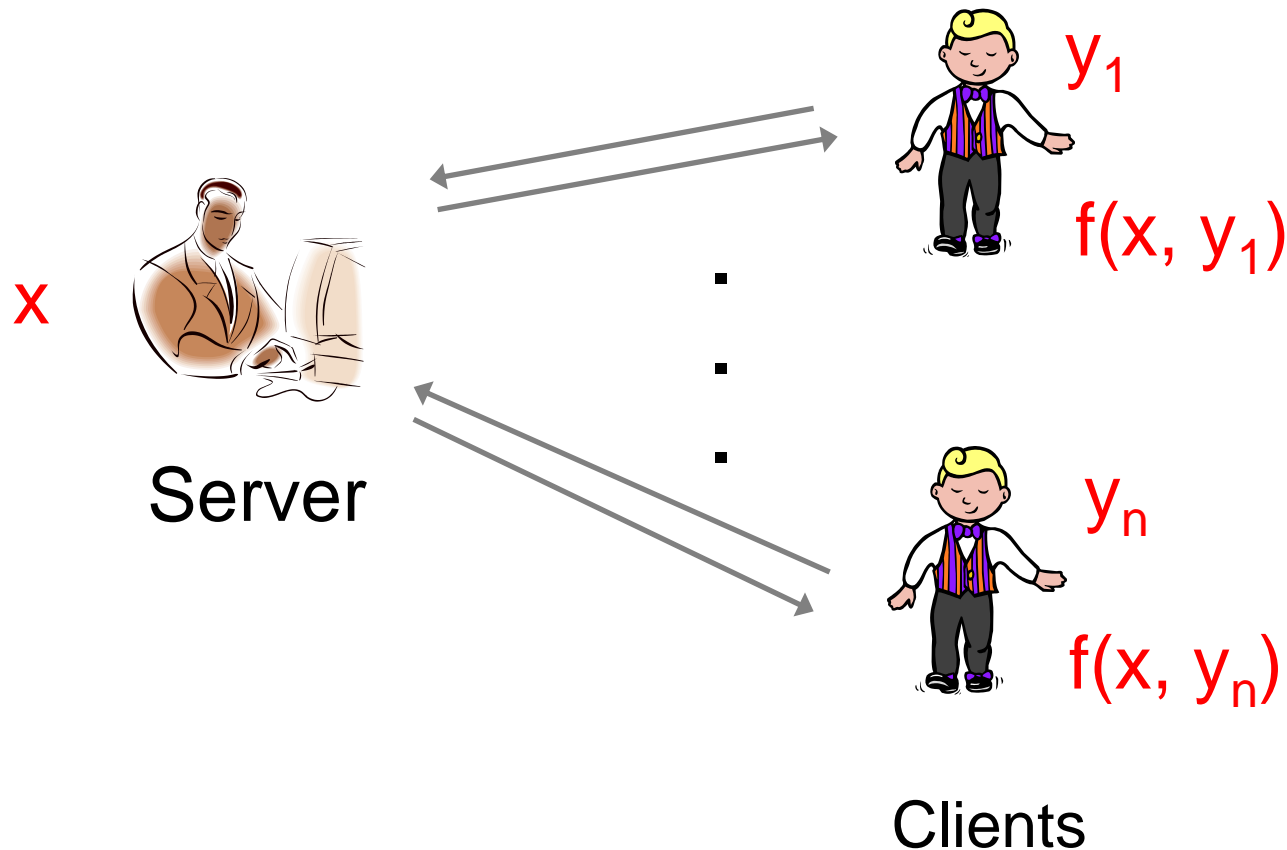
CF'01

GKOV'12

CKL'03

# Single Input Setting: Minimal Clean Model of CSC

Various clients, concurrently interacting with a server, **holding a single fixed input  $x$**



# Positive Results!!

- Almost all functionalities can be securely realized in the single input setting
  - Plain model, standard defn (no SPS etc), no bound on the number of concurrent sessions
- More precisely: all except where ideal functionality behaves as a PRF
  - For PRF: impossibility result ☹️

# Implications of our results

- Concurrent protocols for
  - private information retrieval
  - privacy preserving data-mining
  - secure set intersection
  - etc
- Improved concurrent password based key exchange

# Prior to our work

- Only known positive results in the plain model, fully concurrent setting:
  - zero-knowledge functionality [RK'99, ...]

# Generalizations

- Results can be generalized significantly beyond the single input setting
- Several interesting corollaries of our techniques:
  - first bounded concurrent MPC with BB sim,
  - unified construction of concurrent ZK and bounded concurrent MPC, etc

# Various Open Problems

- Bounded Pseudoentropy Conjecture: open
- Round complexity? Right now depends even upon the functionality (not just security parameter)



# Thank You!!

More details in FOCS 2012  
(paper on eprint)