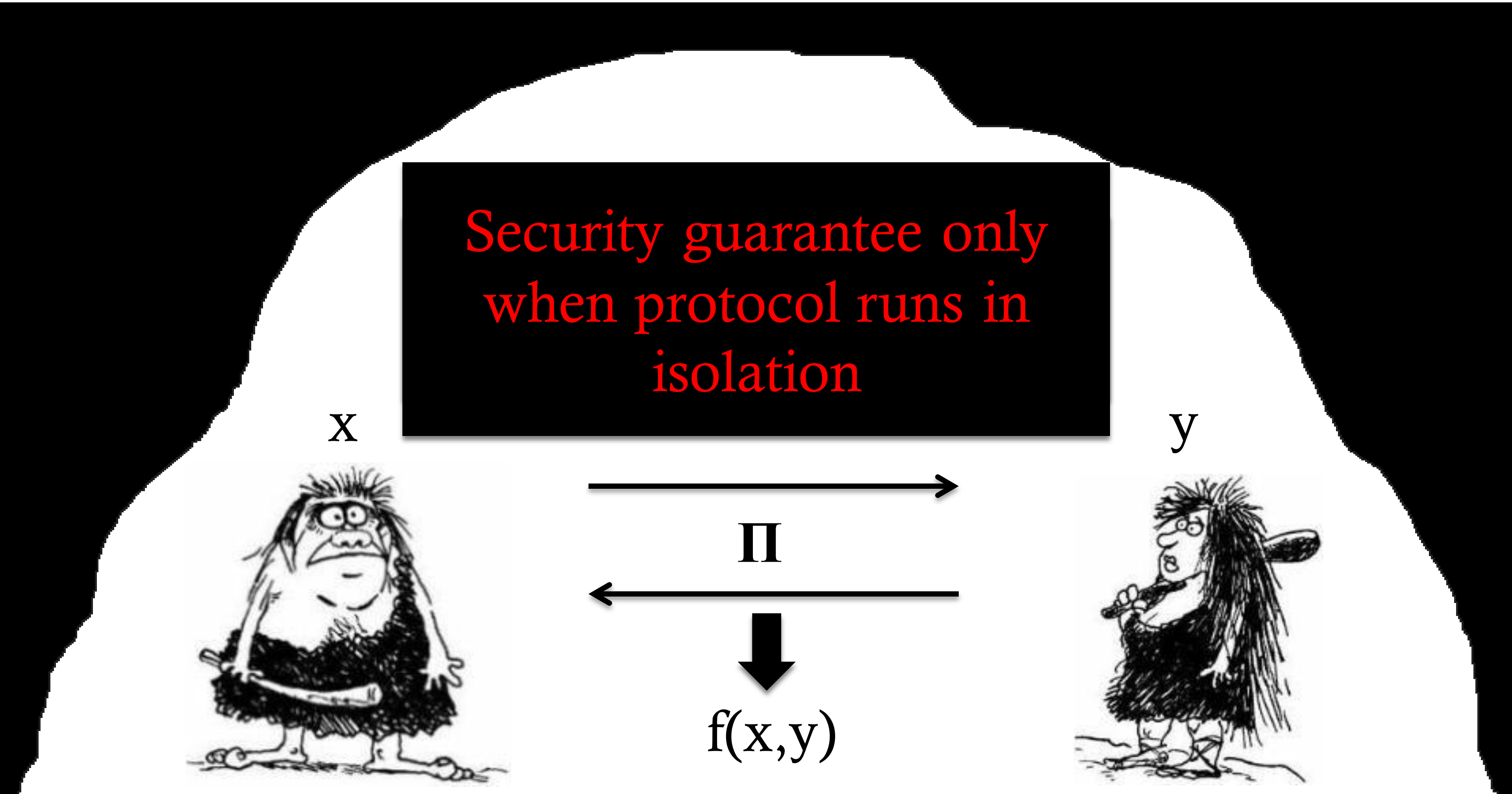
New Impossibility Results for Concurrent Composition and a Non-Interactive Completeness Theorem for Secure Computation

Shweta Agrawal Vipul Goyal Abhishek Jain
Manoj Prabhakaran Amit Sahai

Impossibility Results for Static Input Secure Computation

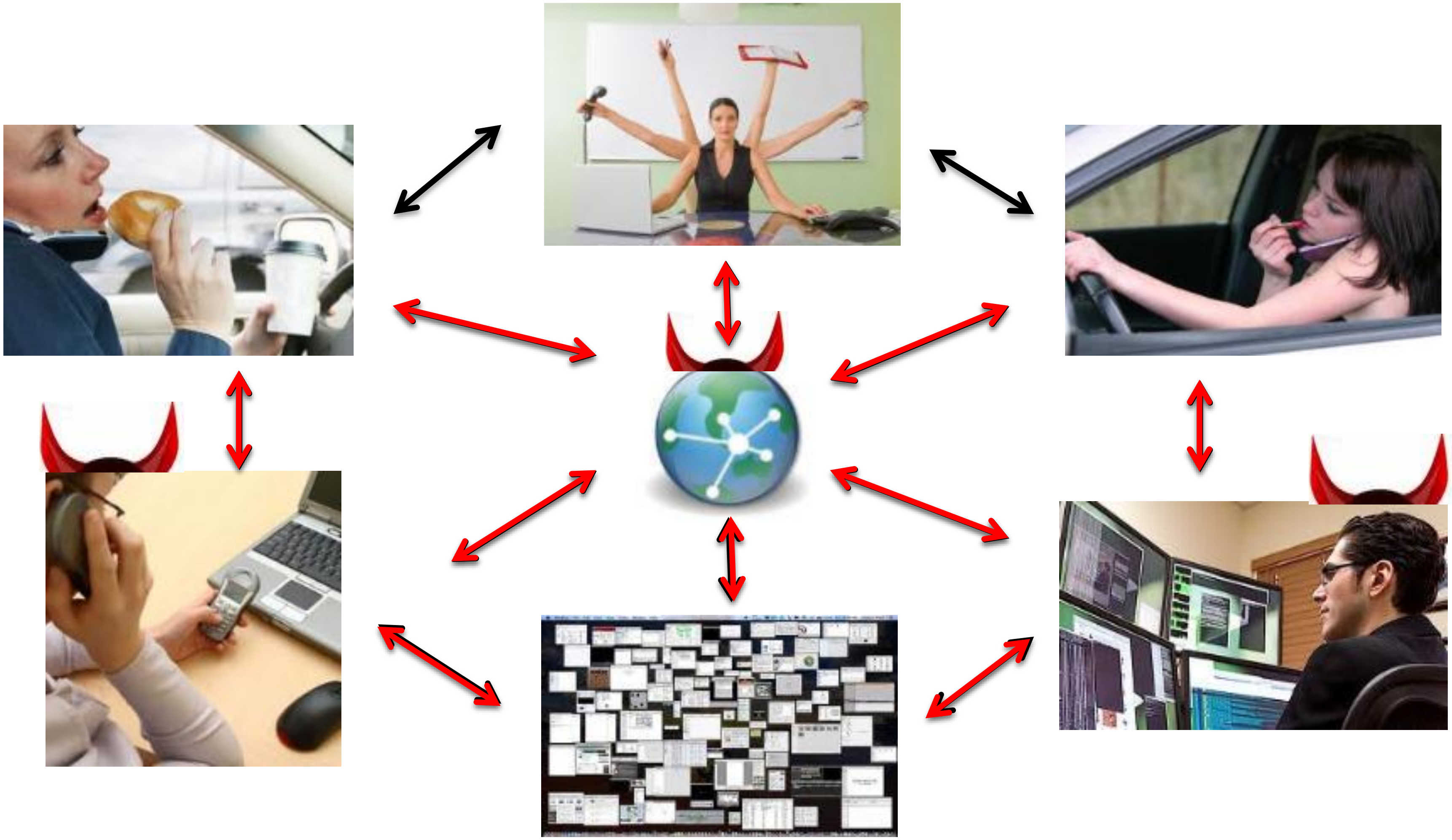
Sanjam Garg Abishek Kumarasubramanian Rafail Ostrovsky
Ivan Visconti

Secure Computation [Yao,GMW]



Security guarantee only when protocol runs in isolation

Today's World is *Concurrent*



Overall Question

Can we design protocols that remain secure even when executed concurrently?

Stand-alone security does *not* imply security under concurrent composition [DDN92,DNS98]

Positive Results

- If we are willing to make global trust assumptions, then general positive results known [CF01,CLOS…]
- Alternatively, can relax the security definition to obtain positive results [Pass03,PS04,BS05,MPR06]

No general positive result in the plain model

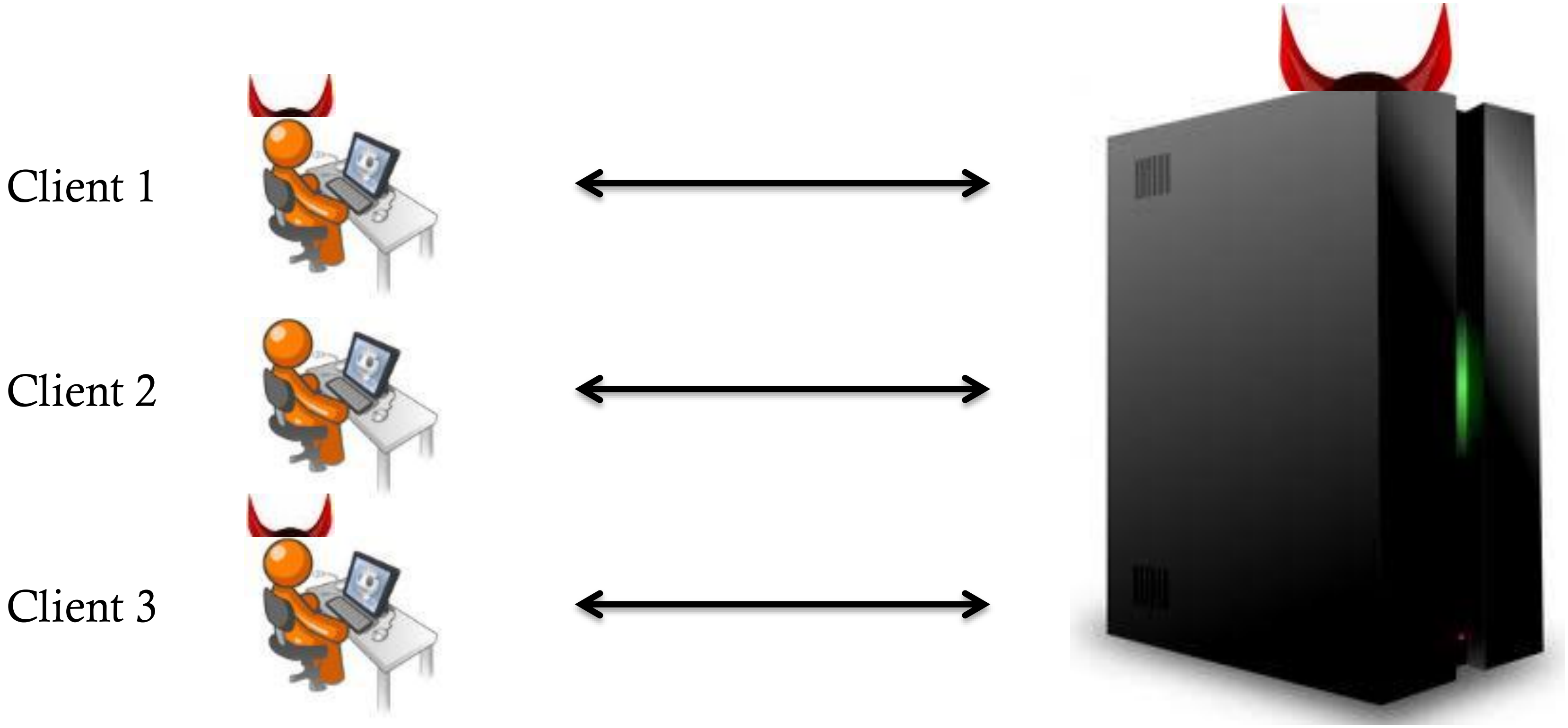
Negative Result?

- Broad impossibility results known in the plain model [CF01, CKL03, Lin03, Lin04, BPS06]

There are still important gaps in our understanding

Paper 1 - [Agrawal-Goyal-Jain-Prabhakaran-Sahai]

Motivation – Fixed Roles

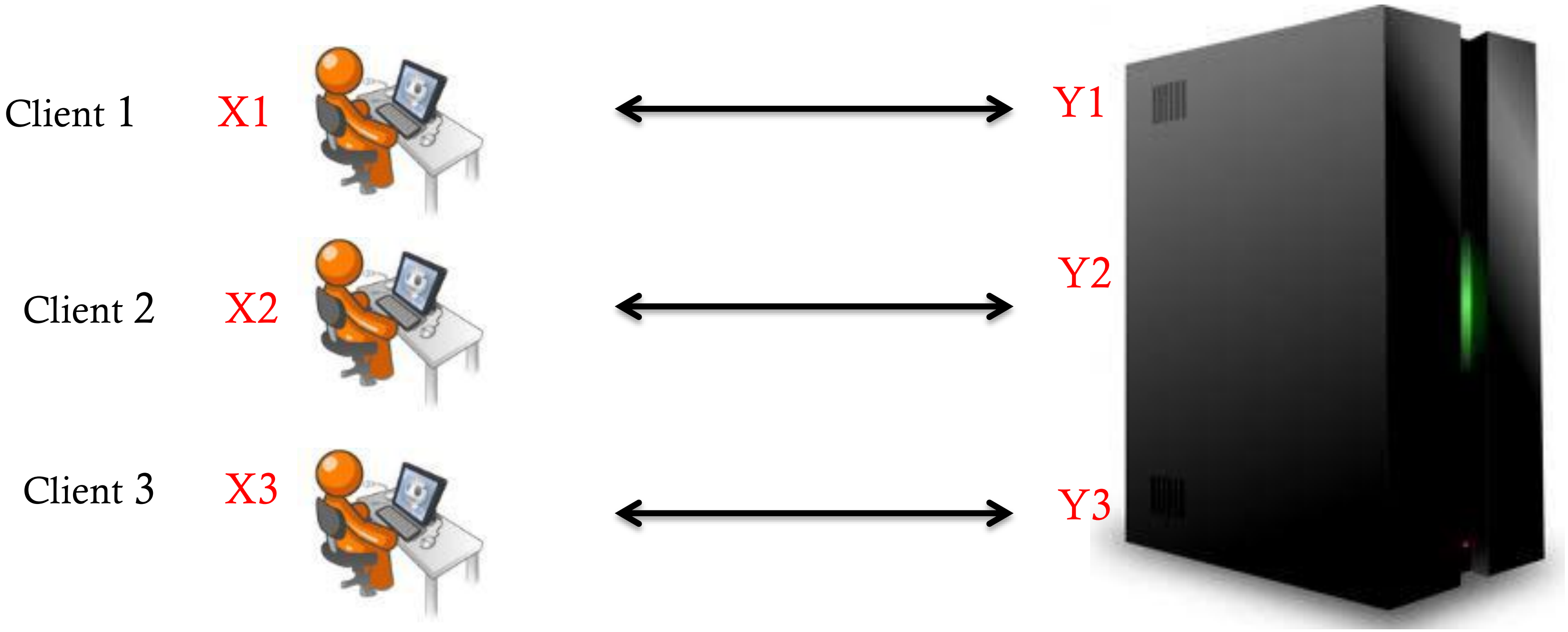


- Positive results for concurrent zero-knowledge [RK99,KP01,PRS02]
- Impossibility for some functionalities [Lin04]

Is concurrently secure **Oblivious Transfer** possible? [Lin08]

Paper 2 - [Garg-K-Ostrovsky-Visconti]

Motivation – Fixed Input



Client 1 X1 Y1

Client 2 X2 Y2

Client 3 X3 Y3

Impossibility results for two very specific (somewhat contrived) functionalities [BPS06,Goy12]

Core Result

[Agrawal-Goyal-Jain-Prabhakaran-Sahai]
[Garg-K-Ostrovsky-Visconti]

- Concurrent self composition impossible for Oblivious Transfer
  - in both fixed input, fixed role settings

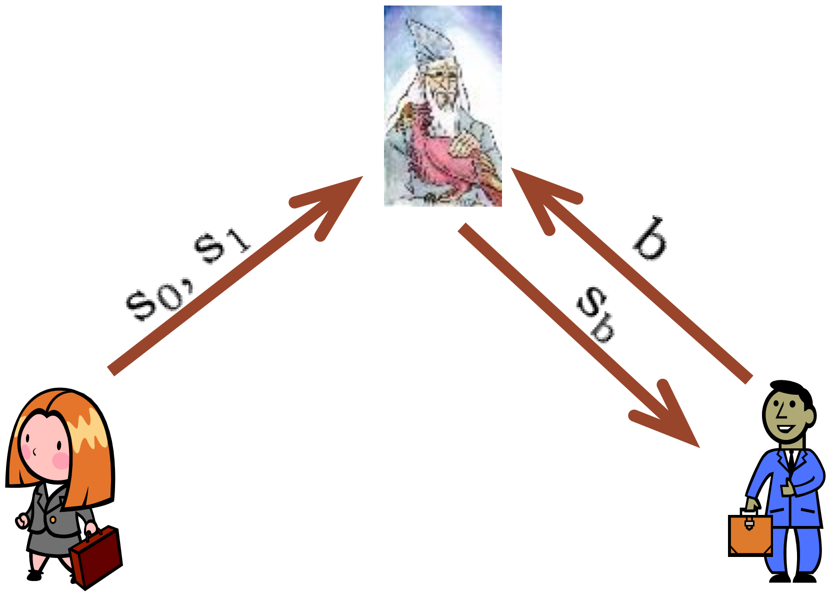
Extensions

- [Garg-K-Ostrovsky-Visconti]
  - Concurrent composition impossible for all non trivial asymmetric and symmetric functionalities
  - General stateless secure computation [GS09,GM11] is impossible

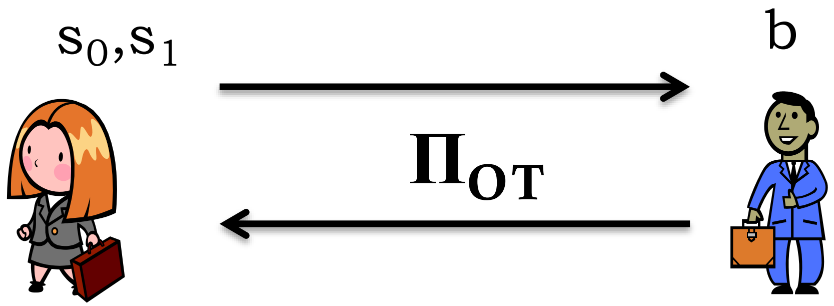
- [Agrawal-Goyal-Jain-Prabhakaran-Sahai]
  - Non-interactive completeness theorem for non trivial asymmetric functionalities
    - subsumes result of [Kil00]
    - corollary: concurrent composition impossibility for non trivial asymmetric functionalities

Oblivious Transfer

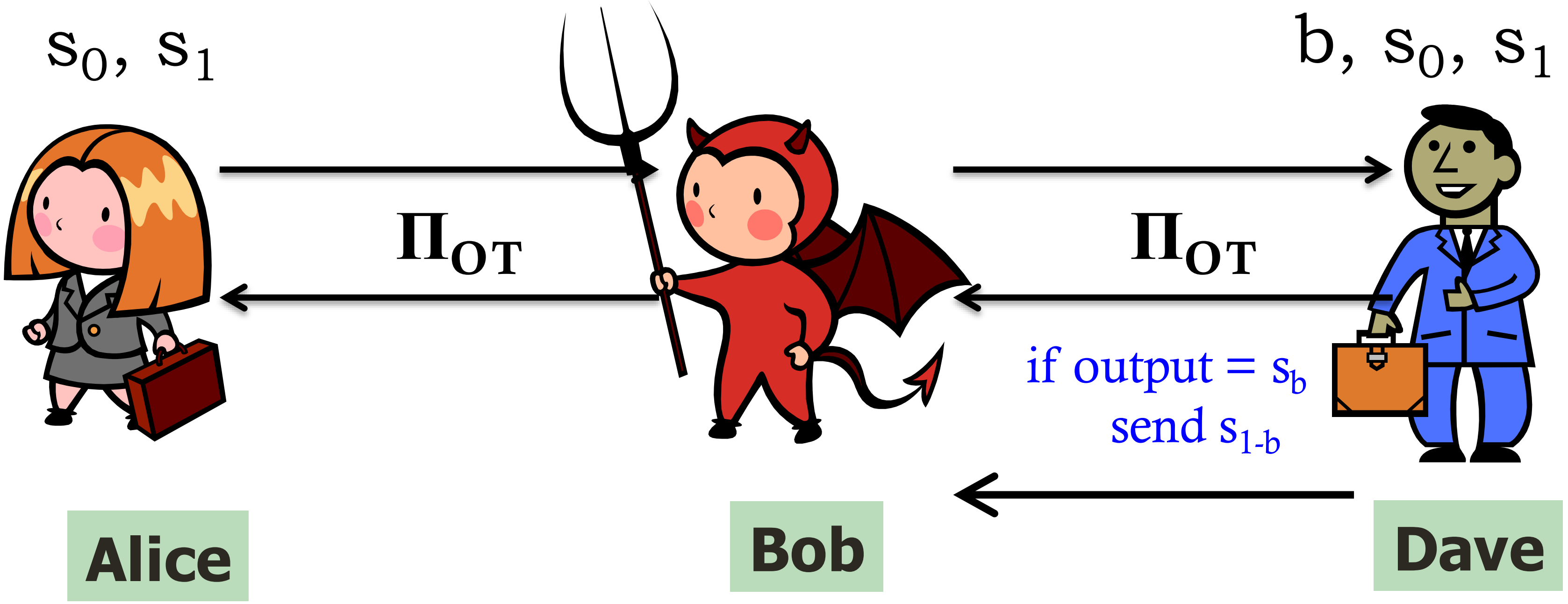
Ideal World



Real world



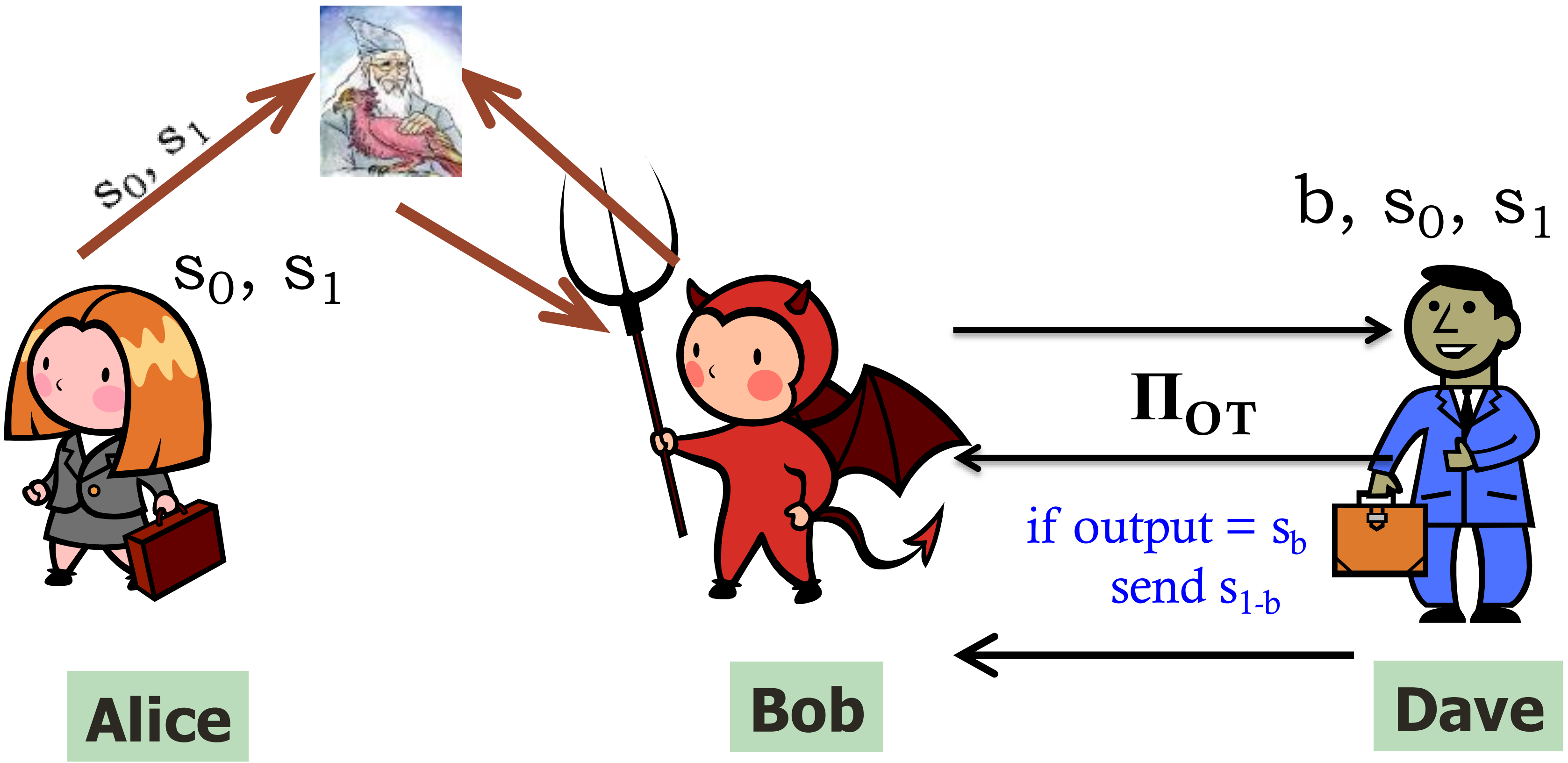
Chosen Protocol Attack



if output = s_b send $s_{1\text{-}b}$

Bob merely forwards messages; successfully learns $s_{1\text{-}b}$ always

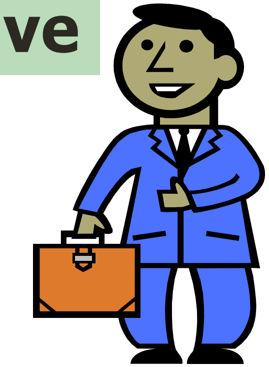
Chosen Protocol Attack…



Bob fails Dave's test with prob. 1/2 ; so learns s_{1-b} with prob. 1/2

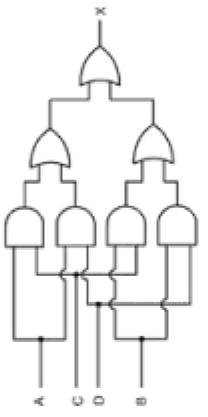
From Chosen Protocol Attack to Impossibility of Concurrent OT

replace

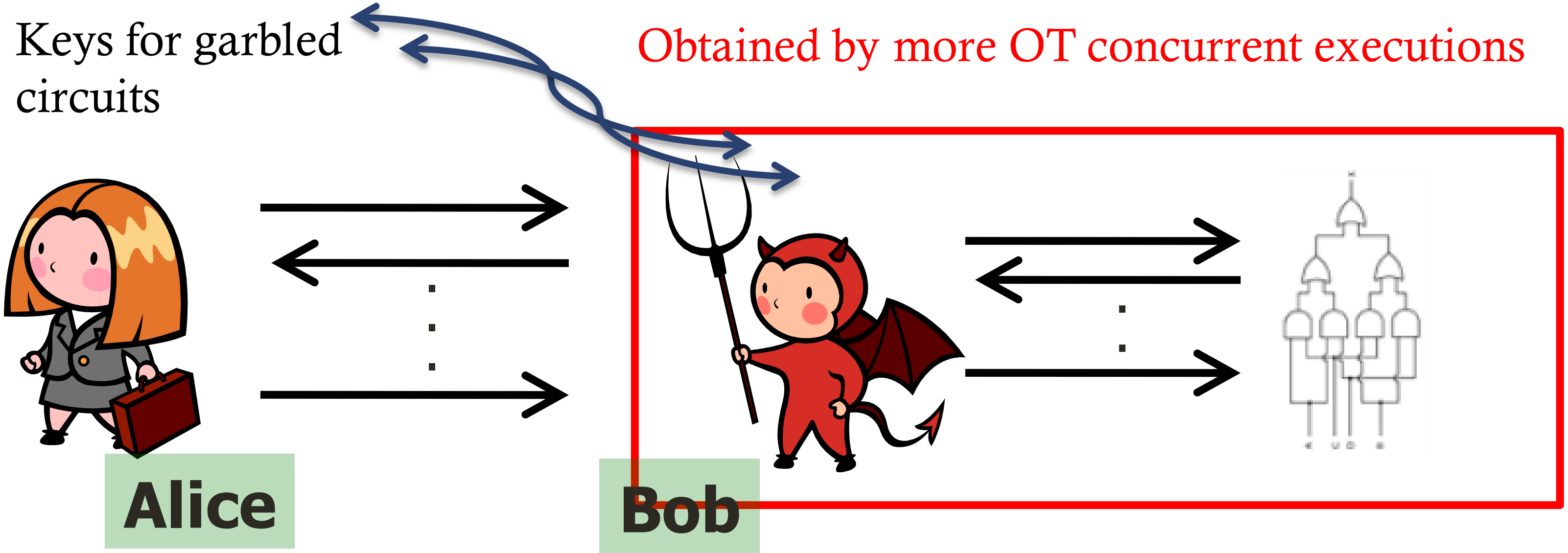


Dave

with



garbled circuits computing his next msg function



Keys for garbled circuits

Obtained by more OT concurrent executions

Alice

Bob

Complete Proof

210 Full versions!

Thank you! And Questions!

Many thanks to Abhishek Jain and Shweta Agrawal for the slides
Only 1/3 of the blame goes to me!