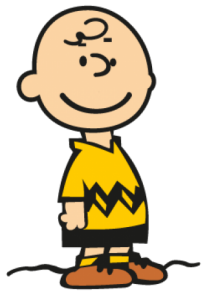
Three-Round Secure Multiparty Computation from Black-Box Two-Round Oblivious Transfer

Arpita Patra (IISc) and Akshayaram Srinivasan (TIFR)

CRYPTO 2021

Round complexity



.....

MPC: The Problem and Our setting

x_1

x_4

x_2

x_3

Problem:

- n parties $P_1,....,P_n$ with P_i holding **private** input x_i ; some corrupted by a centralized adversary

- Compute a common n-input function $f(x_1,x_2,..x_n)$ correctly (correctness), without leaking anything beyond (privacy).

Our Setting:

Setting

- Multi-party **(> 2)**
- Broadcast/public channel

Adversary

- Computationally-bounded, rushing, static
- Semi-honest/Active
- Majority corruption

Security

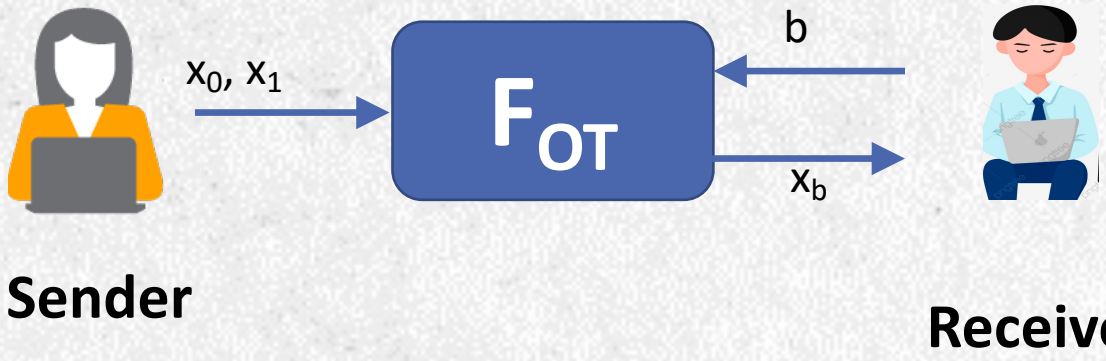
- Cryptographic
- With abort

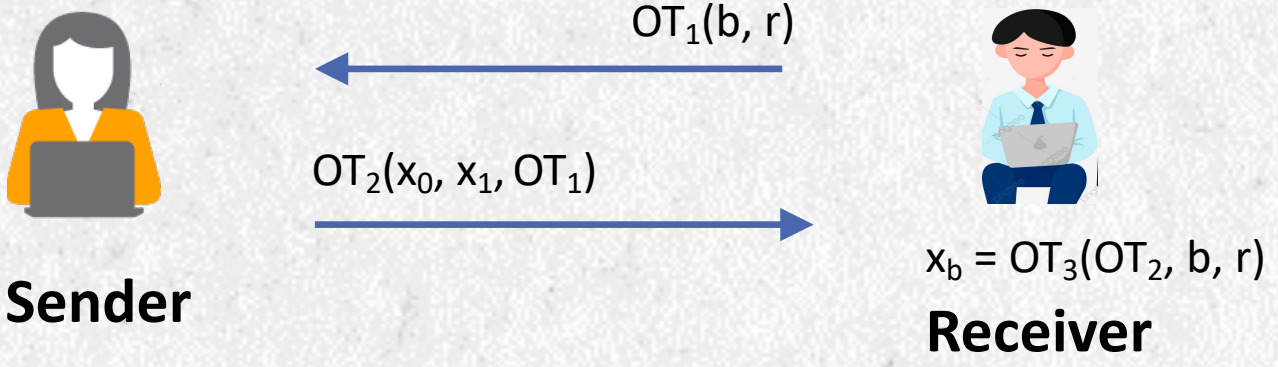
THE MINIMAL ASSUMPTION: 2-ROUND OBLIVIOUS TRANSFER

- The problem of securely computing a general n-party functionality f reduces to securely computing the elementary 2-party OT [Yao86, GMW87,Kil88,IPS08]!

- We are interested in the round complexity of MPC relying on the minimal assumption of 2-round OT

Oblivious Transfer (OT)





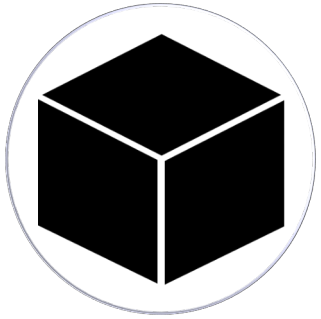
Black-box (BB) vs. Non-black-box (NBB) access

Black-box (BB)

- input/output access to the building blocks
- agnostic to how these building blocks are implemented
- Huge theoretical importance
- Huge potentially practical value, since BB tends to lead more efficient solutions

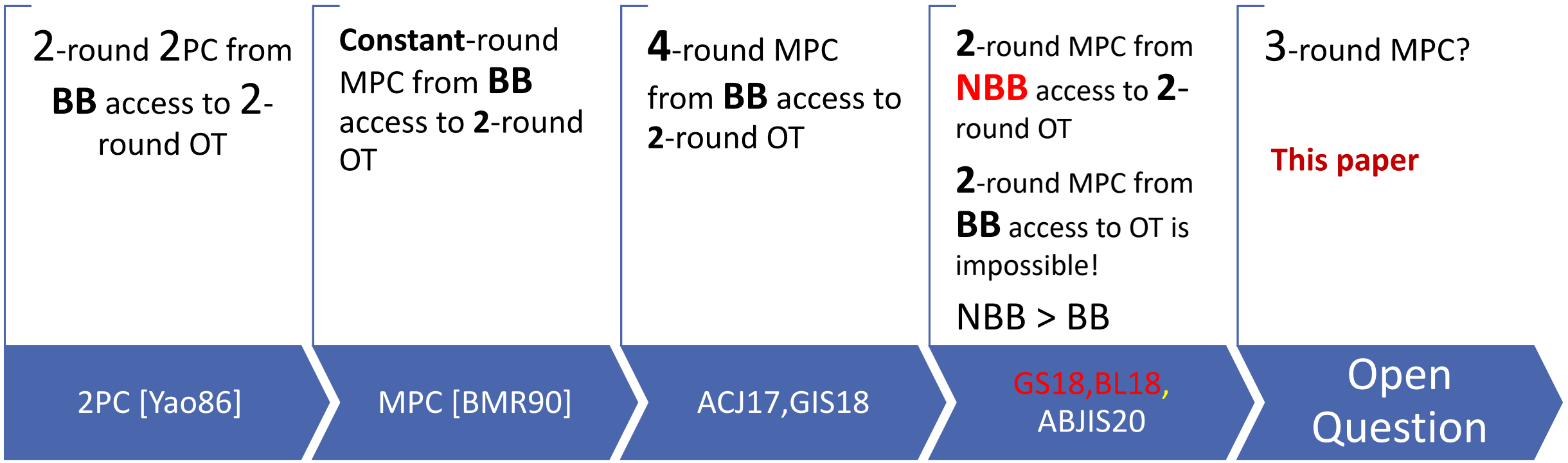
Non-black-box (NBB)

- Code of the building blocks are accessible
- Not as efficient as black-box solutions
- NBB access may lend more power than BB



We are interested in the **BB** round complexity of MPC!

History of round complexity



* 2 rounds are necessary -- folklore and formally proven in HLP14

Our Results

It’s a positive result!

Our (positive) results

Semi-honest

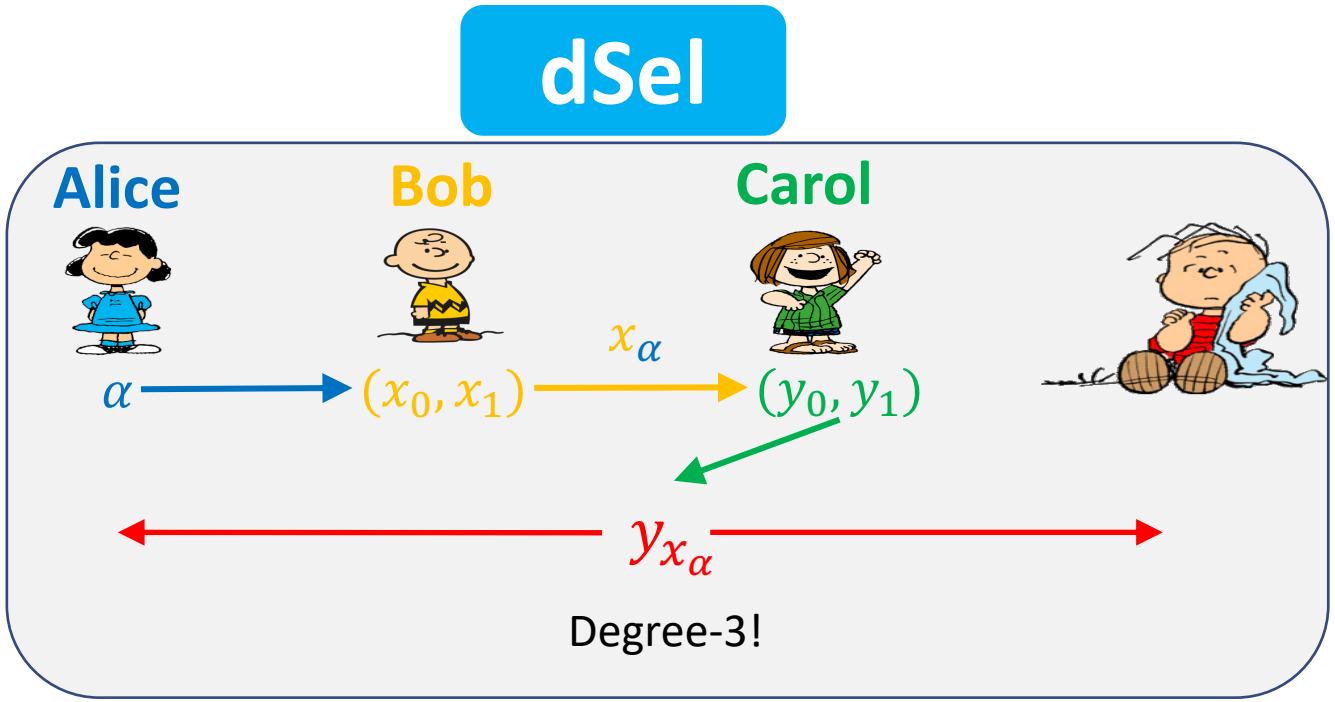
- There is 3-round protocol for computing every multiparty functionality against semi-honest adversaries making BB use of a 2-round semi-honest secure OT.
- This completely resolves the **BB** round complexity of **dishonest-majority** MPC in the **semi-honest** setting from **minimal assumption**.

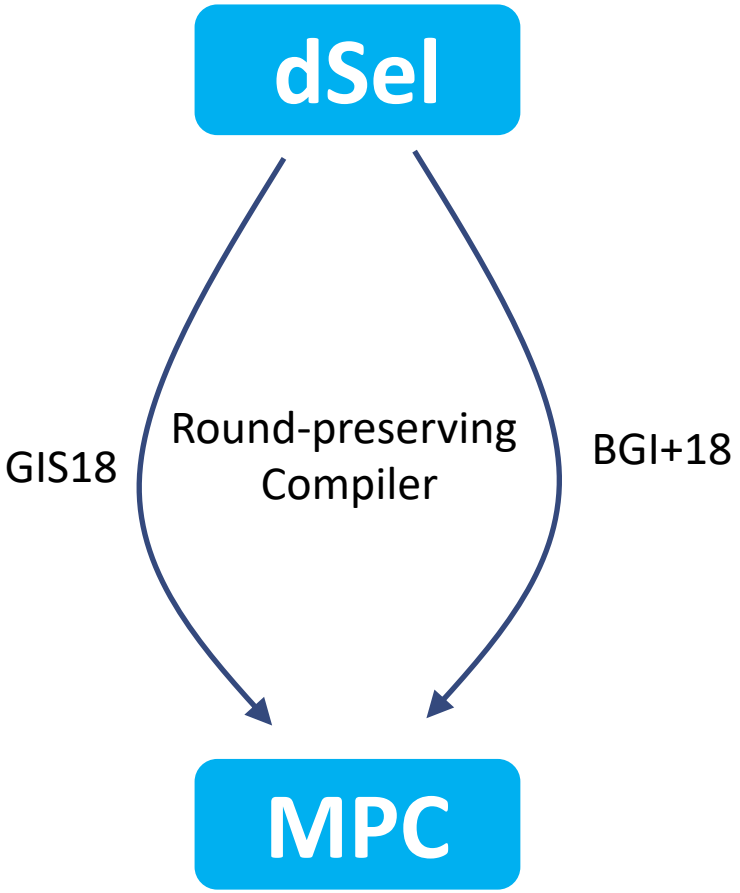
Malicious

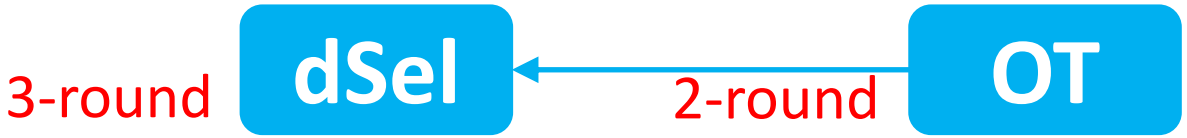
- There exists a 3-round protocol for computing every multiparty functionality against malicious adversaries (in the CRS model) making black-box use of a 2-round malicious secure OT with equivocal receiver security.
- **Equivocal receiver security:** The receiver's message OT_1 can be explained for both bits (0 and 1) in the simulation

Degree-3 computation in 2-rounds via cascading OT!

Our Contribution- Double Selection (dSel) Functionality



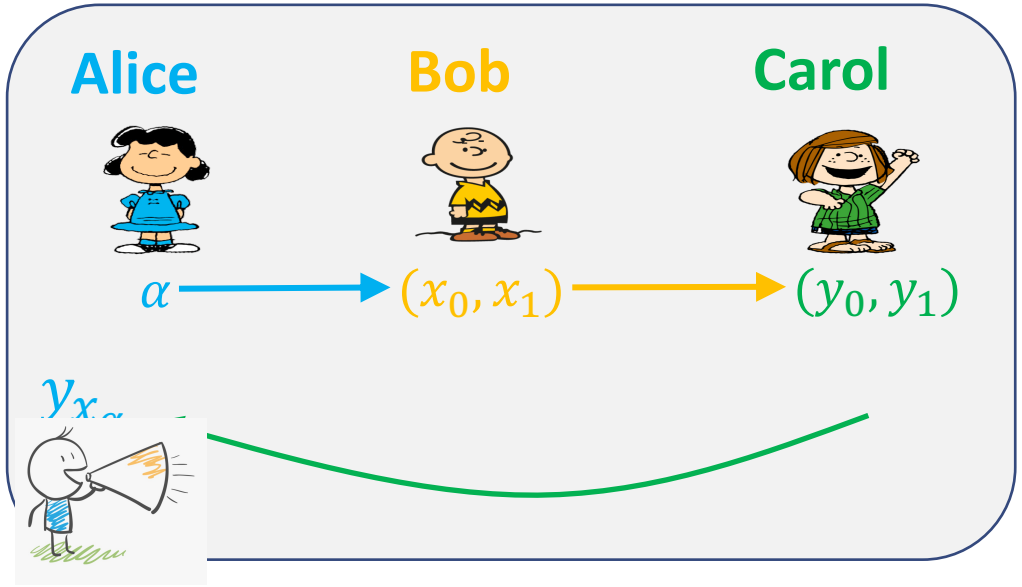




* Actual double selection functionality is a bit more involved.

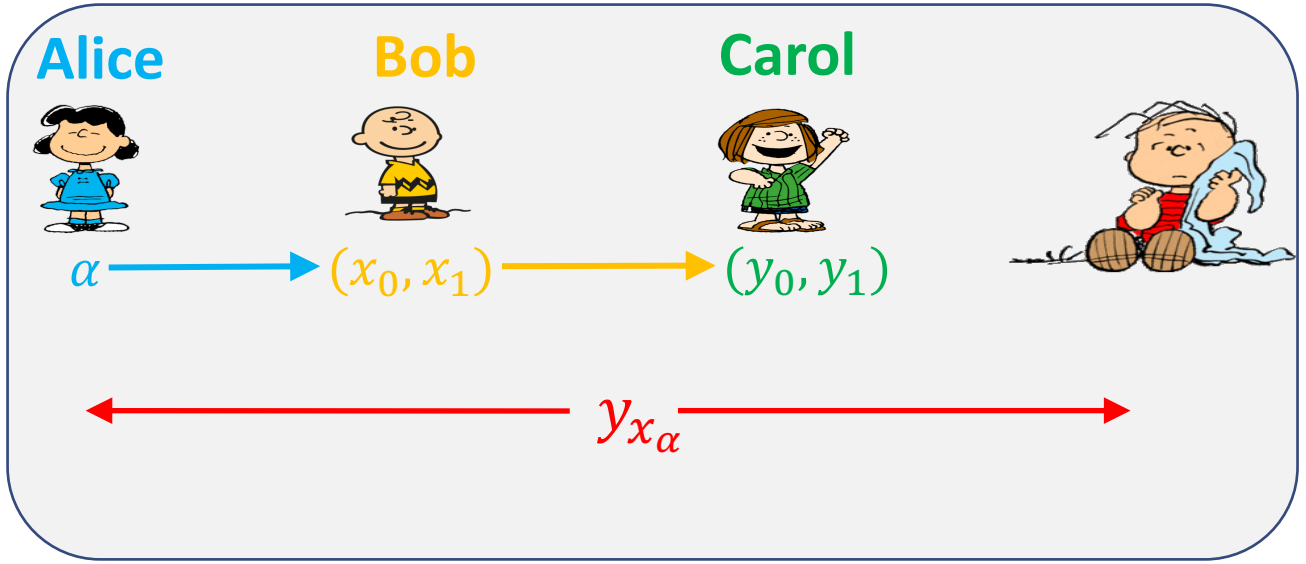
Double Selection: Public to Private

2-round **dSelP**



- Private output: Only Alice receives the output

3-round **dSel**

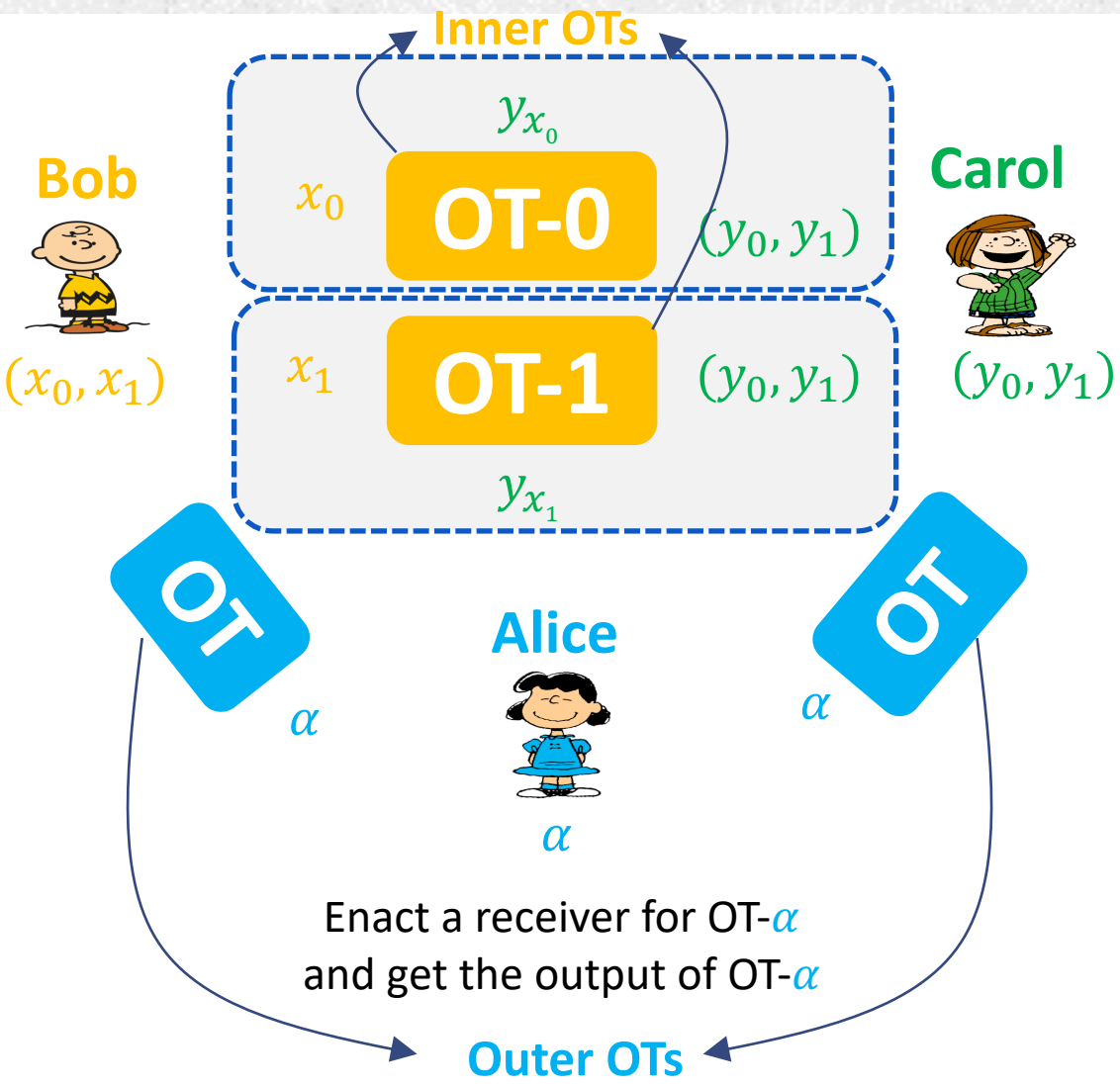


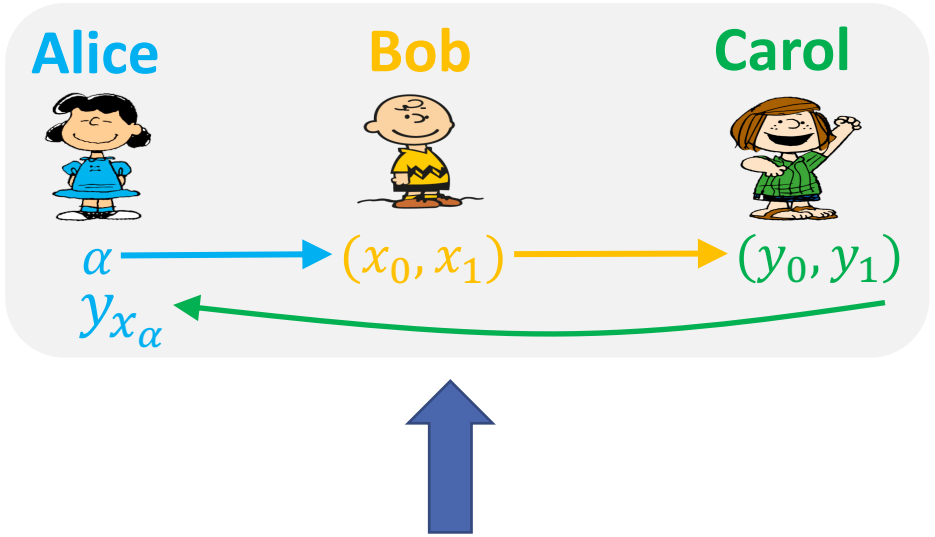
- Public output: Everyone receives the output

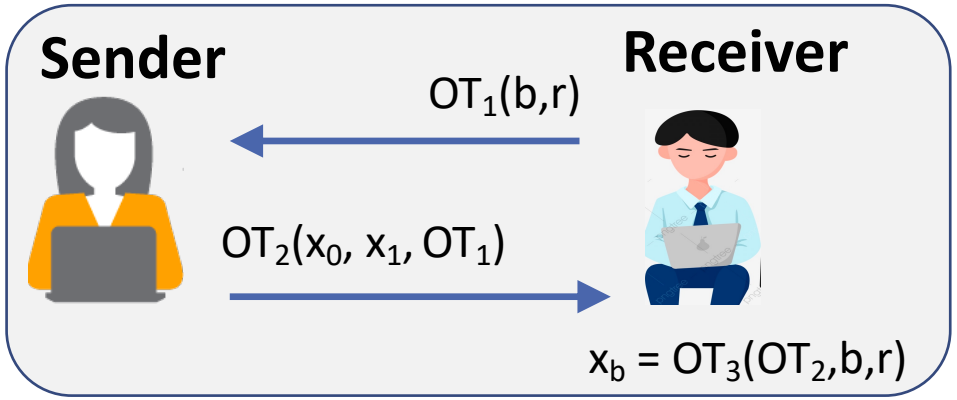
2-round **dSelP** ← 2-round **OT**

Challenging because dSelP is degree-3 and OT is degree-2!

Private Double Selection from OT– Selecting an OT via OTs

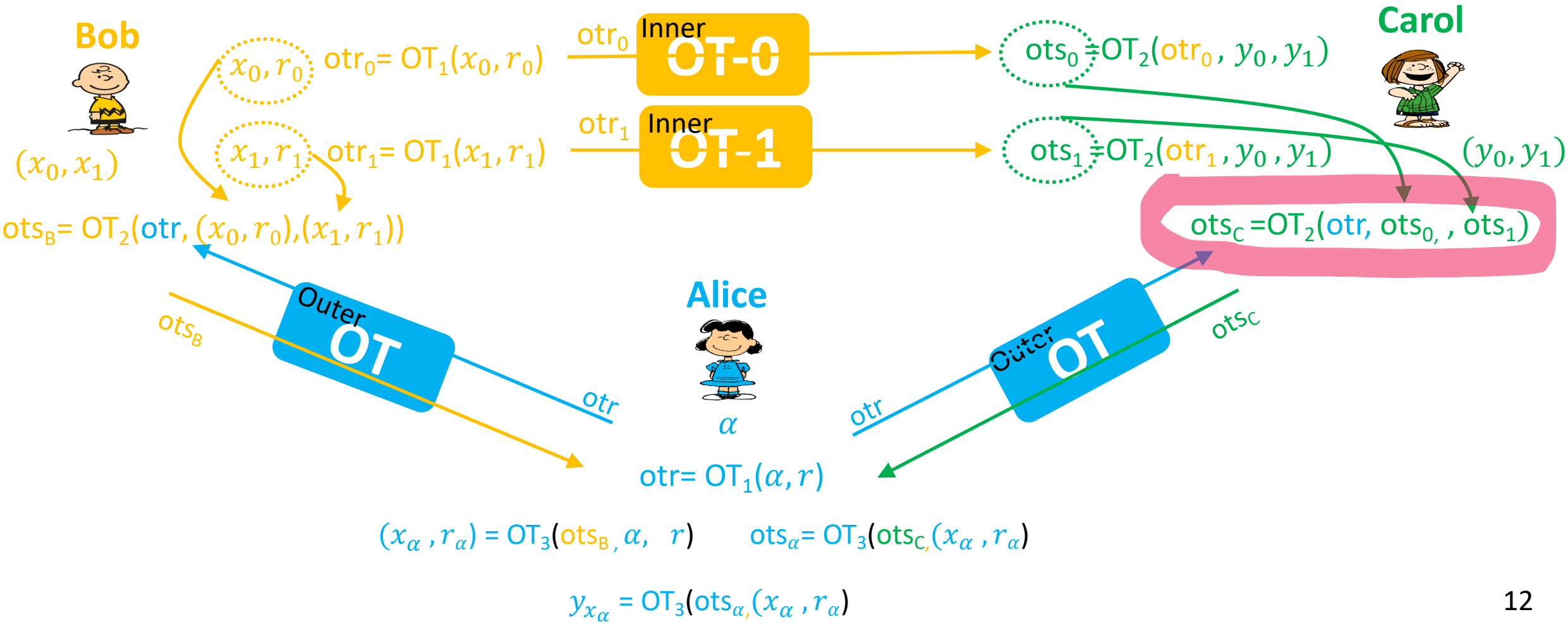






Private Double Selection from OT- Cascading OTs

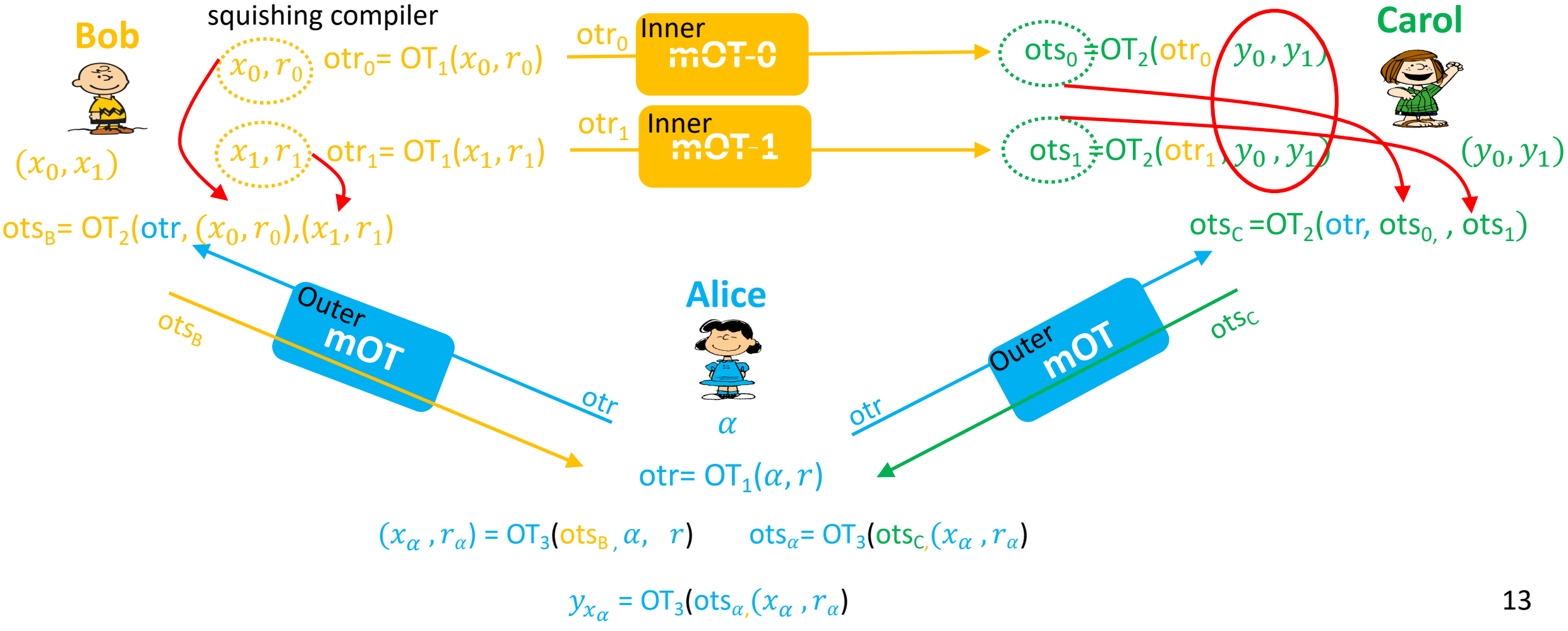
OT sender messages are OT sender messages themselves!



Cascading OTs– The malicious Case

Proof of correctness: OT Combiners + GIS18 round squishing compiler

Proof of correctness: "MPC-in-the-head" technique [IKOS07].



Conclusion and Open problems

- Resolved the black-box round complexity of MPC in the semi-honest setting under minimal assumptions.
- Gave a 3-round protocol in the malicious setting that made BB use of a two-round, malicious-secure OT that additionally satisfies a (mild)-variant of adaptive security for the receiver.
- Open Problems:
  - In the malicious setting, can we get rid of this additional adaptive security requirement.
  - Concrete efficiency?

THANK YOU!

https://eprint.iacr.org/2021/957

Arpita Patra, Akshayaram Srinivasan

arpita@iisc.acin, akshayaram@berkeley.edu

MPC-in-the-head style proof

m virtual parties

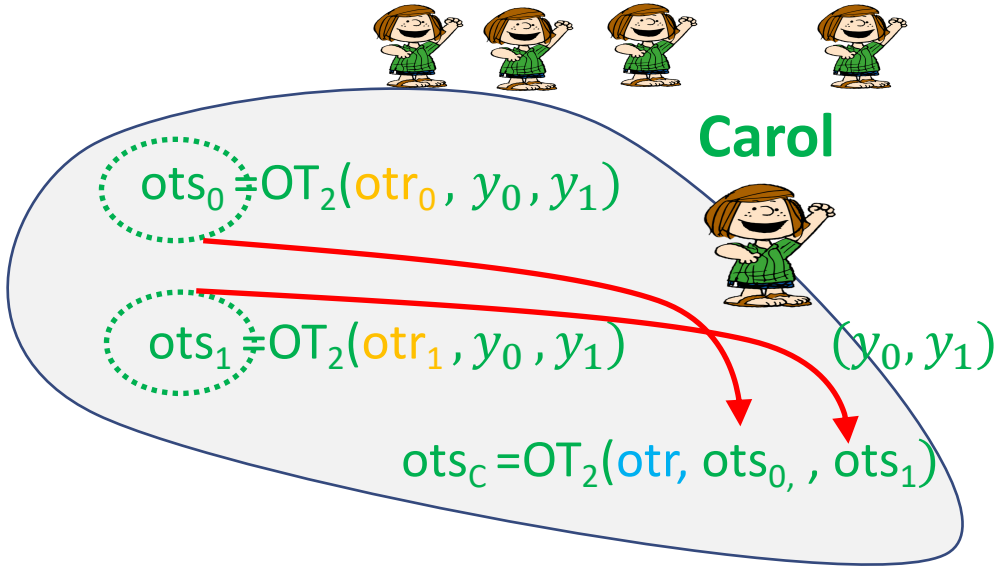
Secret-share the inputs using (m,t)-linear sharing scheme

i-th virtual party emulates Carol with with i-th shares of input instead of the inputs

k of the m virtual parties states are revealed to Alice for check

k is not enough (less than t) to breach privacy of Carol's input

k is large enough to either catch Carol or error correct the errors



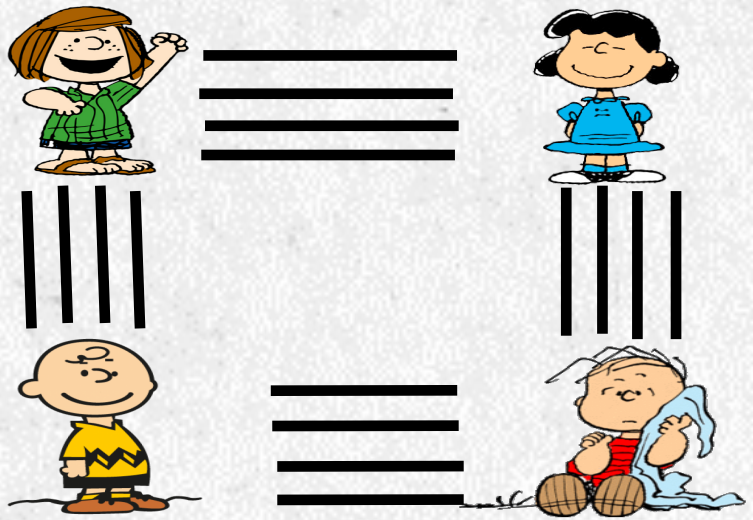
- All within 2 rounds

STARTING POINT (1)

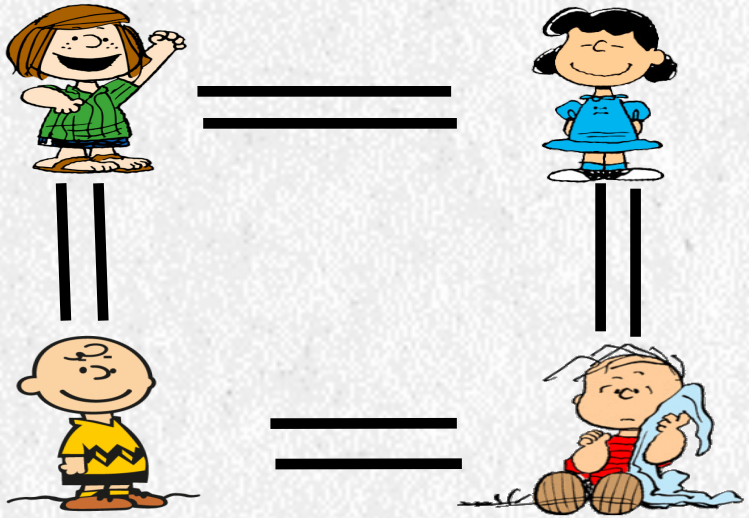
[GS18,BL18] Round squishing compiler: The 2-round protocol publishes garbled circuits for each round's computation of the arbitrary round protocol, and let them communicate via OT.

The garbled circuits use the code of the underlying arbitrary-round protocol. This makes the compiler use OT in NBB way

- Arbitrary-round protocol



- 2-round protocol via garbled circuit and OT



STARTING POINT (2)

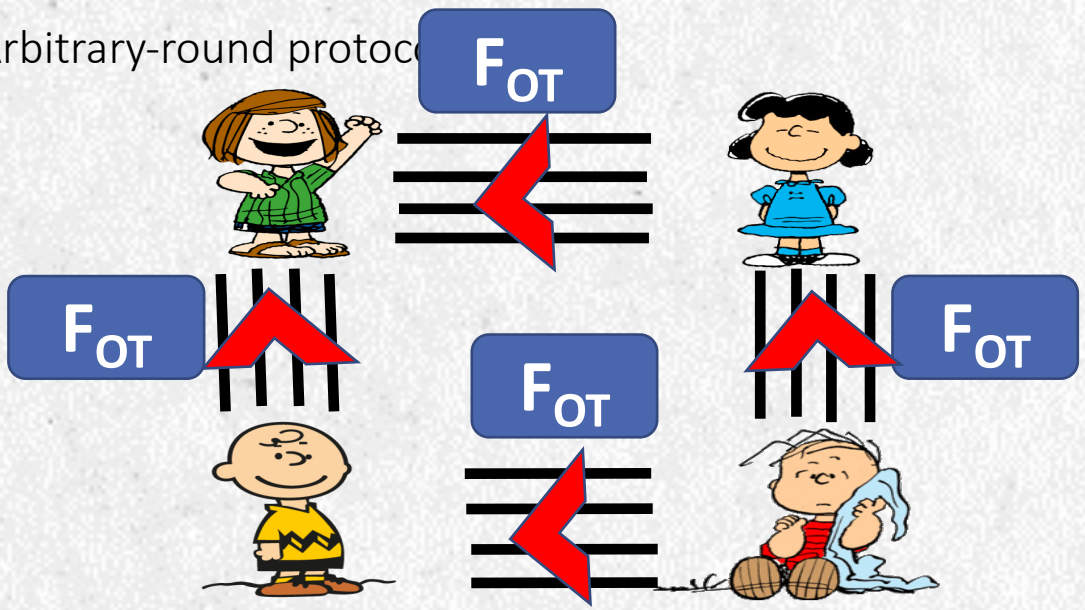
- [GIS18] Compiler: Uses an information-theoretic protocol that is OT-hybrid model

- By virtue of squishing an IT protocol, it avoids NBB usage of OT.

- But the OT correlations act as input to the squished protocol

- OT take 2 rounds and squishing needs 2 rounds. Results in a 4-round protocol

- Arbitrary-round protoc



- 2-round protocol via garbled circuit and OT