Chemical OT:

On the (Im)possibility of Basing Oblivious Transfer on Chemical Assumptions

Bernardo David

Anderson C. A. Nascimento

University of Brasilia, Brazil

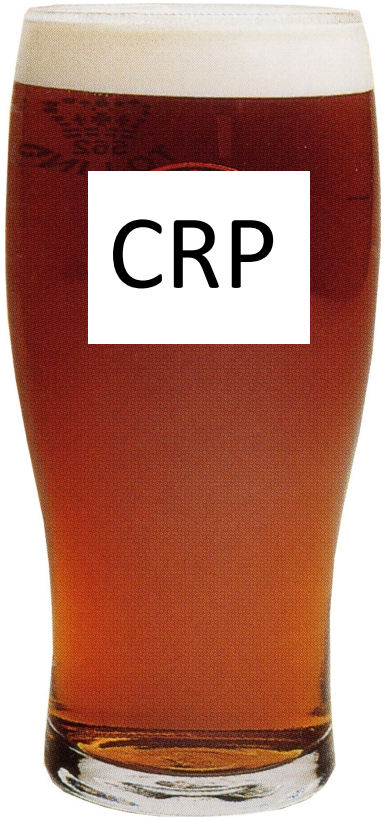
Practical MPC

- Current assumptions are complicated
- Getting a common reference string in the real world is hard!!!
- How are we gonna perform MPC during the Euro Cup?

Who's richer???

Chemical Assumptions Are Practical!

- The Common Reference Pint:

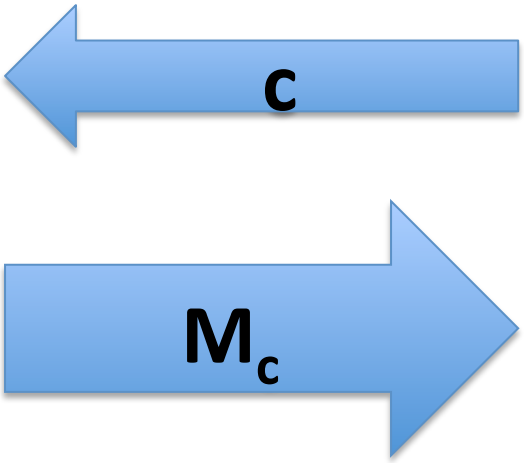


- Easily obtainable in any football game!

Composable OT from the CRP

- Step 1: The sender has two messages m1,m2 and accesses the CRP

- Step 2: Receiver queries sender



- Step 3: Sender terminates the protocol

Impossibility

- The sender is wasted after accessing the CRP
- Solution: Share the CRP among friends

Summary

- The Common Reference Pint achieves: OT and Secure Erasures.
- Bonus: Random Walks and True Random Number Generators!

Implementing Chemical OT in Aarhus

- Tir na nog, Frederiksgade
- Ris Ras Filliongongong, Mejlgade
- Escobar, Skolegade
- Cassino Bar, Skolegade
- Heidi's Beer Bar, Klostergade
- Cafes at Åboulevarden (eg. Cross Café)
- Local Friday Bars, every Friday around the campus
- Meatpackers, Skolegade
- Under Masken, Bispegade