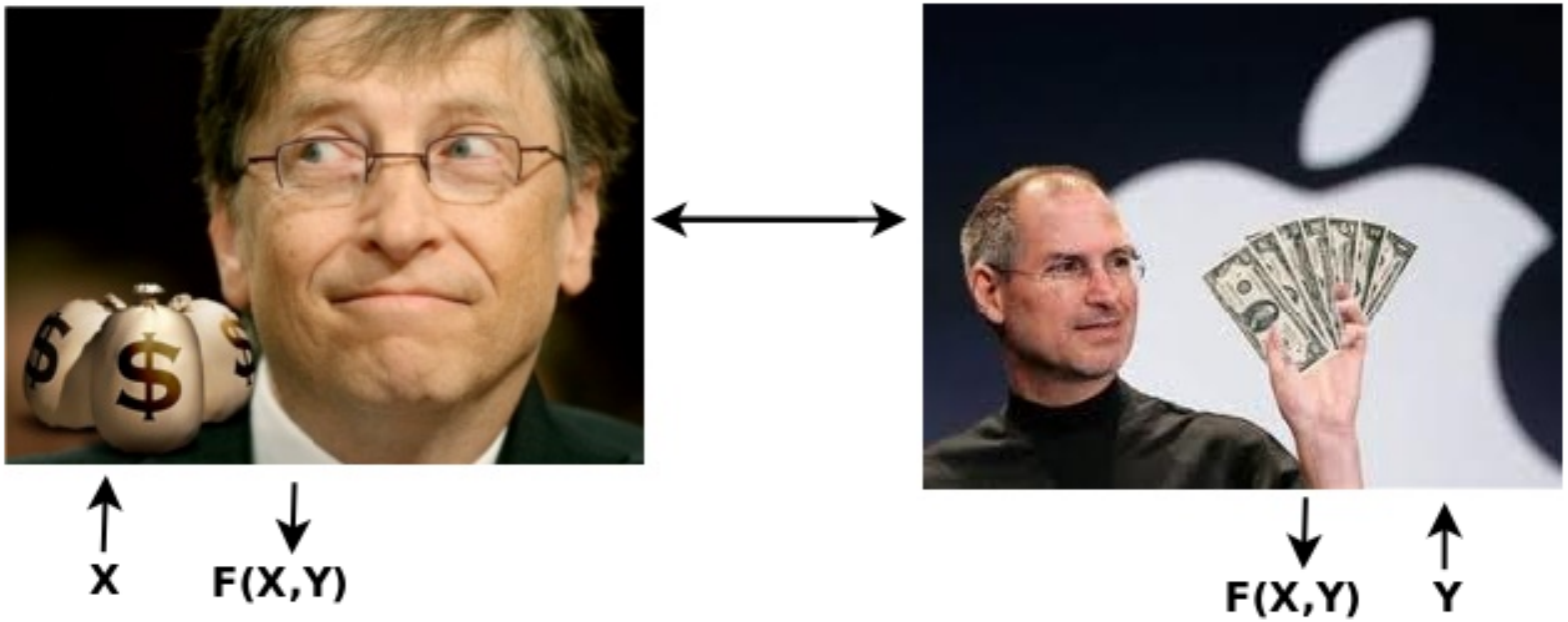
Asymptotically Optimal and Concretely Fast UC Commitments From Any Linear Error Correcting Codes

Ignacio Cascudo, Ivan Damgård,
Bernardo David, Irene Giacomelli,
Jesper Buus Nielsen, Roberto Trifiletti
Aarhus University

Commitment Schemes

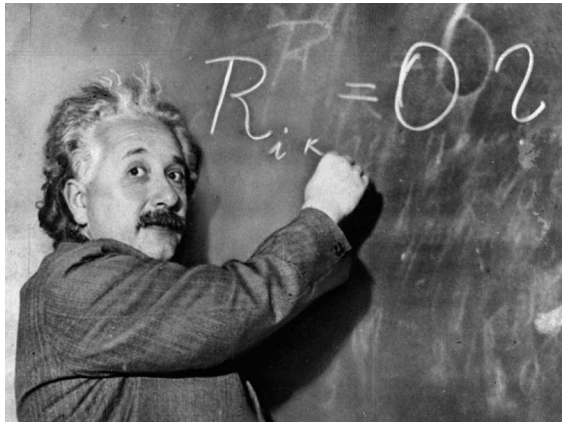
Why are commitments cool?

- The Millionaires' Problem



- In the UC framework commitments are complete [CLOS02]
- Basic building blocks in many different protocols.

What do we do in theory?



- Optimal communication
- Additively Homomorphic
- Optimal computation 
- No need for general secret sharing 

How do we do it?

ECC + PRG + OT

Basic Structure

- Setup Phase: Create efficient watchlists!

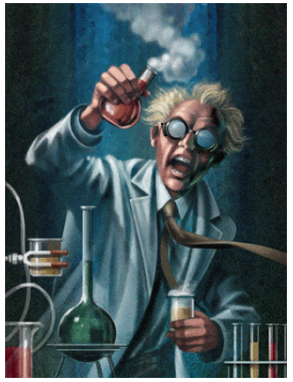
PRG + OT

  - Independent of the length or number of commitments
- Online Phase (commit/open):

ECC + PRG

  - No public key operations!
  - Only an error correcting code and a PRG are needed!
  - Round optimal!

What do we do in practice?



- Online Phase:

BCH [796,256,>=121] + PRG

2 Encodings: 1.5 µs

VS.

[Lindell11,BCPV13] -> 22 exponentiations: 8250 µs

II

- Practical scheme runs 5500 times faster

Practical Trade Offs…

- No additive homomorphism.

- Setup phase cost:

796 OTs

8756 exponentiations using [PVW08]

398 [Lindell11,BCPV13] commitments

THANK YOU!

READ THE FULL PAPER:

https://eprint.iacr.org/**2014/829**