601.445/601.645
Practical Cryptographic Systems

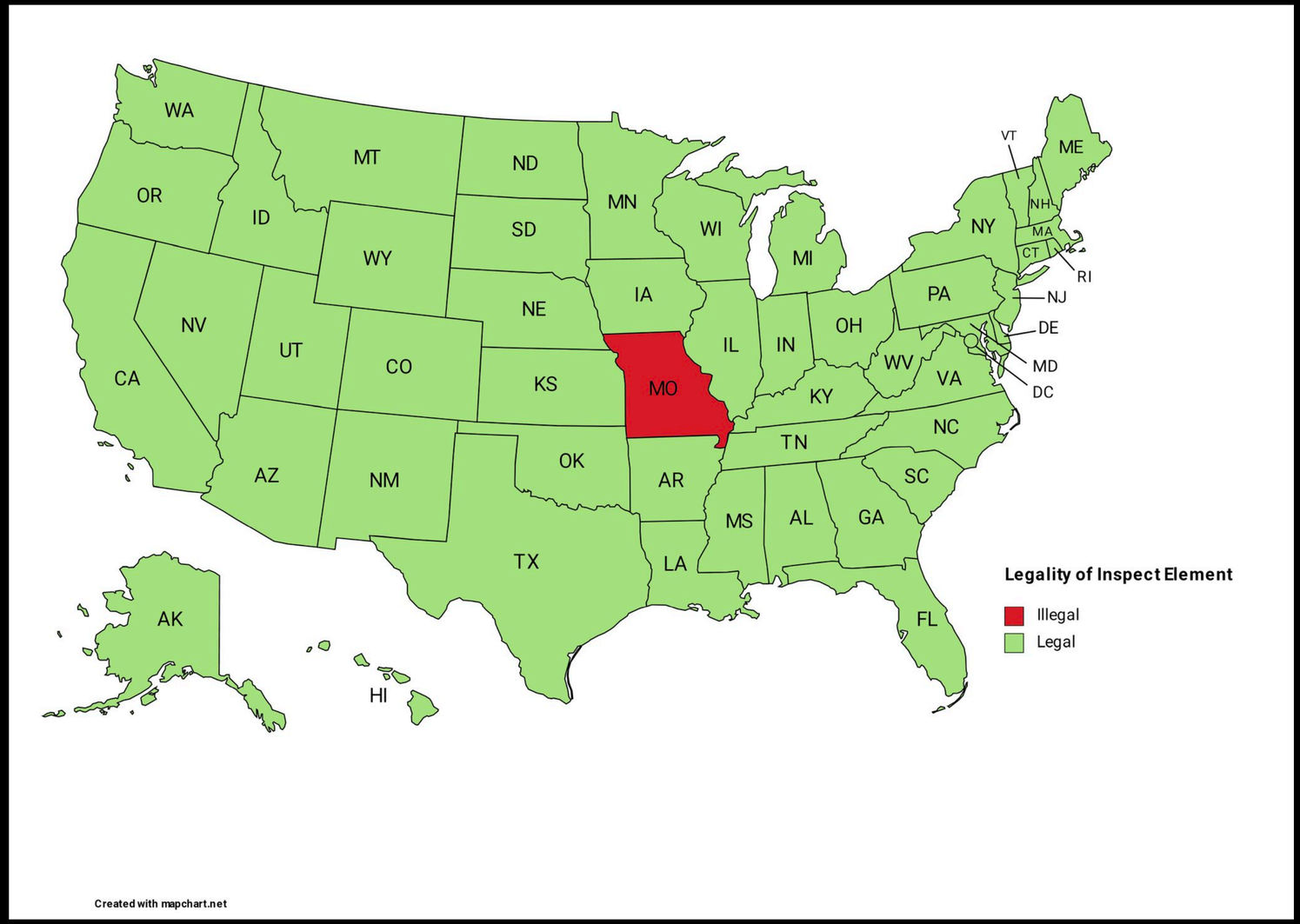
MPC and Private Computation

Instructor: Alishah Chator

Housekeeping

- Assignment 2 due Tuesday 10/26 at 11:59pm
- Weekly HW#3 coming out tonight
- Midterm 11/1
  - Will be covering all lecture and reading material so far

News


WA
OR
CA
ID
NV
MT
WY
UT
AZ
CO
NM
ND
SD
NE
KS
OK
TX
MN
IA
MO
AR
LA
WI
IL
MS
MI
IN
KY
TN
AL
OH
WV
GA
FL
SC
NC
VA
PA
NY
VT
NH
ME
MA
CT
RI
NJ
DE
MD
DC
AK
HI
Legality of Inspect Element
Illegal
Legal
Created with mapchart.net

NEWS

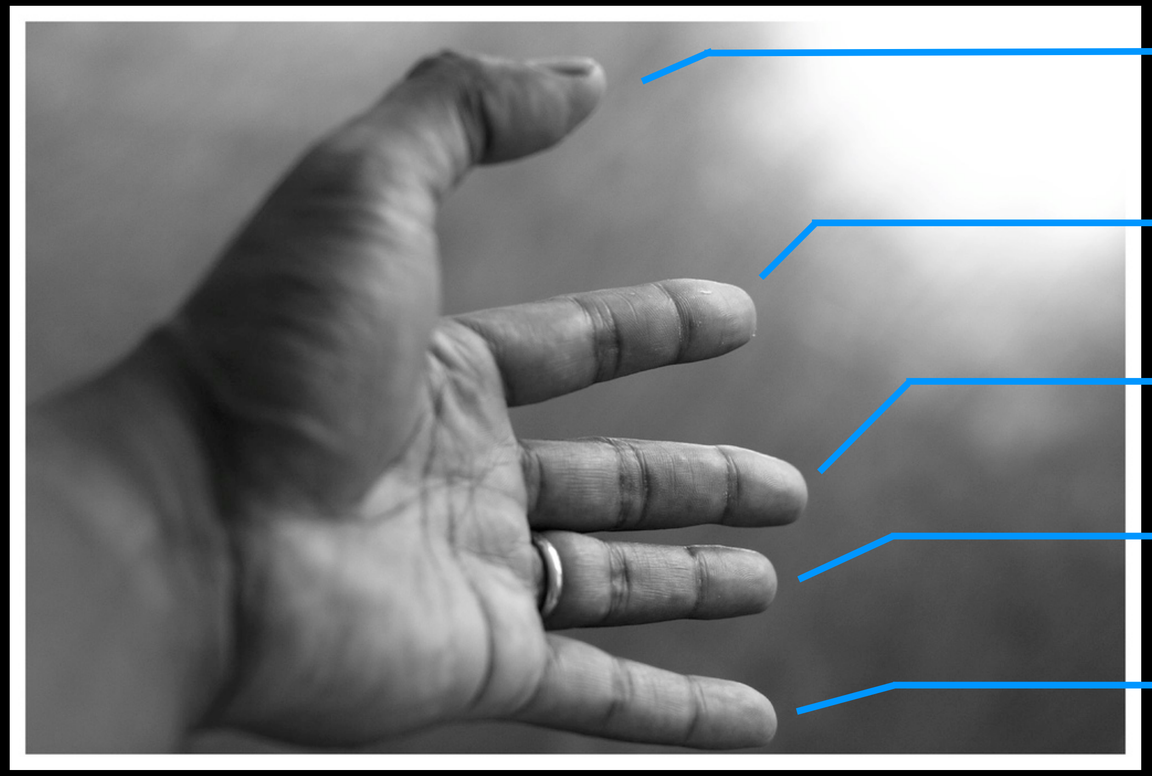
Minneapolis schools are spying on queer students & outing them to teachers and parents

The software has outed one student and also incorrectly notified a transgender teen's parents after they wrote about their past suicidal thoughts.

By LGBTQ Nation Saturday, October 16, 2021

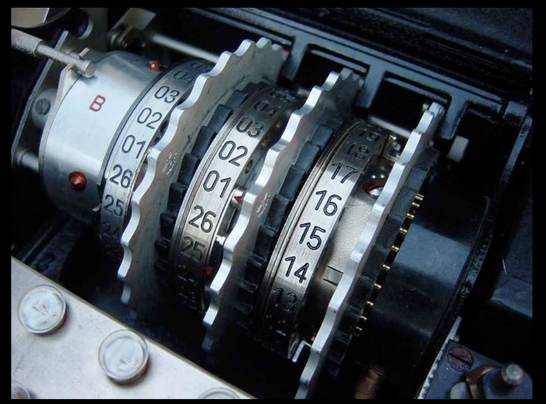
REvil ransomware shuts down again after Tor sites were hijacked

By Lawrence Abrams October 17, 2021 07:19 PM 2



Part 1

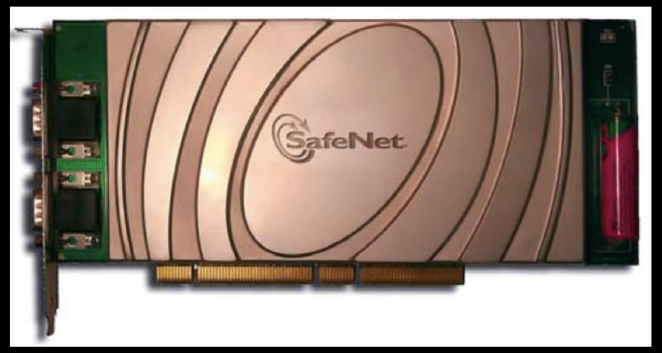
- (Re-)introduction to Crypto... at high speed:
  - Classical cryptography
  - Symmetric-key encryption & block ciphers
  - AES, ChaCha
  - Public-key cryptography
  - Diffie-Hellman, RSA, ECC



Enigma image from Wikipedia, used under GFDL.

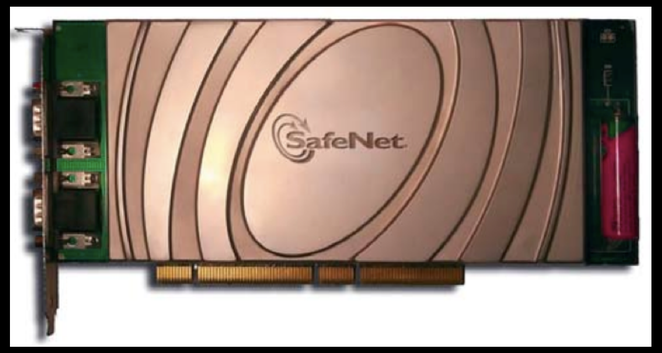
Part 2

- Exploiting Software:
  - Crypto vulnerabilities and where they turn up
- Privacy
  - Multi-party Computation
  - Tor and Anonymity
  - Zero Knowledge Proofs



Part 2

- Exploiting Software:
  - Crypto vulnerabilities and where they turn up
- **Privacy**
  - **Multi-party Computation**
  - **Tor and Anonymity**
  - **Zero Knowledge Proofs**



Today

- What is Multiparty Computation?
- How can we build an MPC system

MPC: the Classic Example

MPC: the Classic Example

I am the richest person around

MPC: the Classic Example

No, I am the richest!

I am the richest person around

MPC: the Classic Example

No, I am the richest!

I am the richest person around

What if neither party wants to disclose their net worth?

MPC More concretely

Technology preview: Private contact discovery for Signal

BWWC

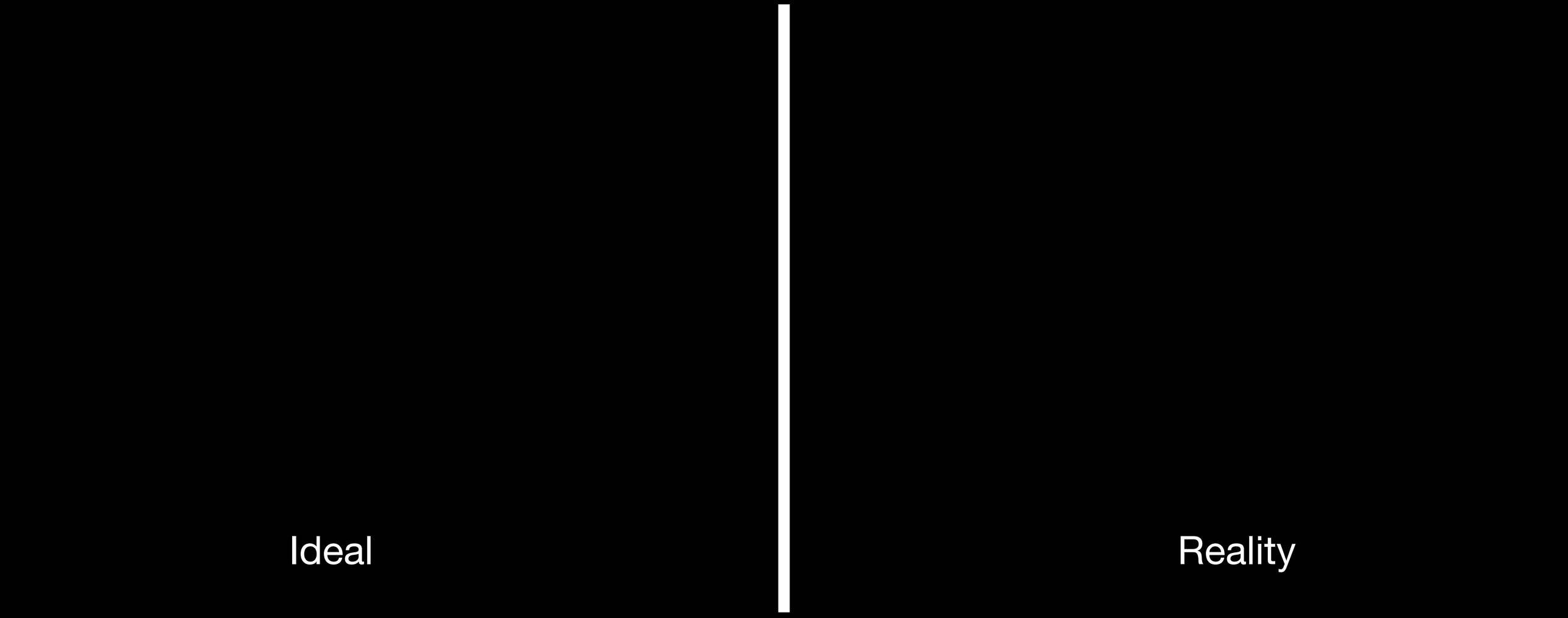
BOSTON WOMEN'S WORKFORCE COUNCIL

MPC Formally

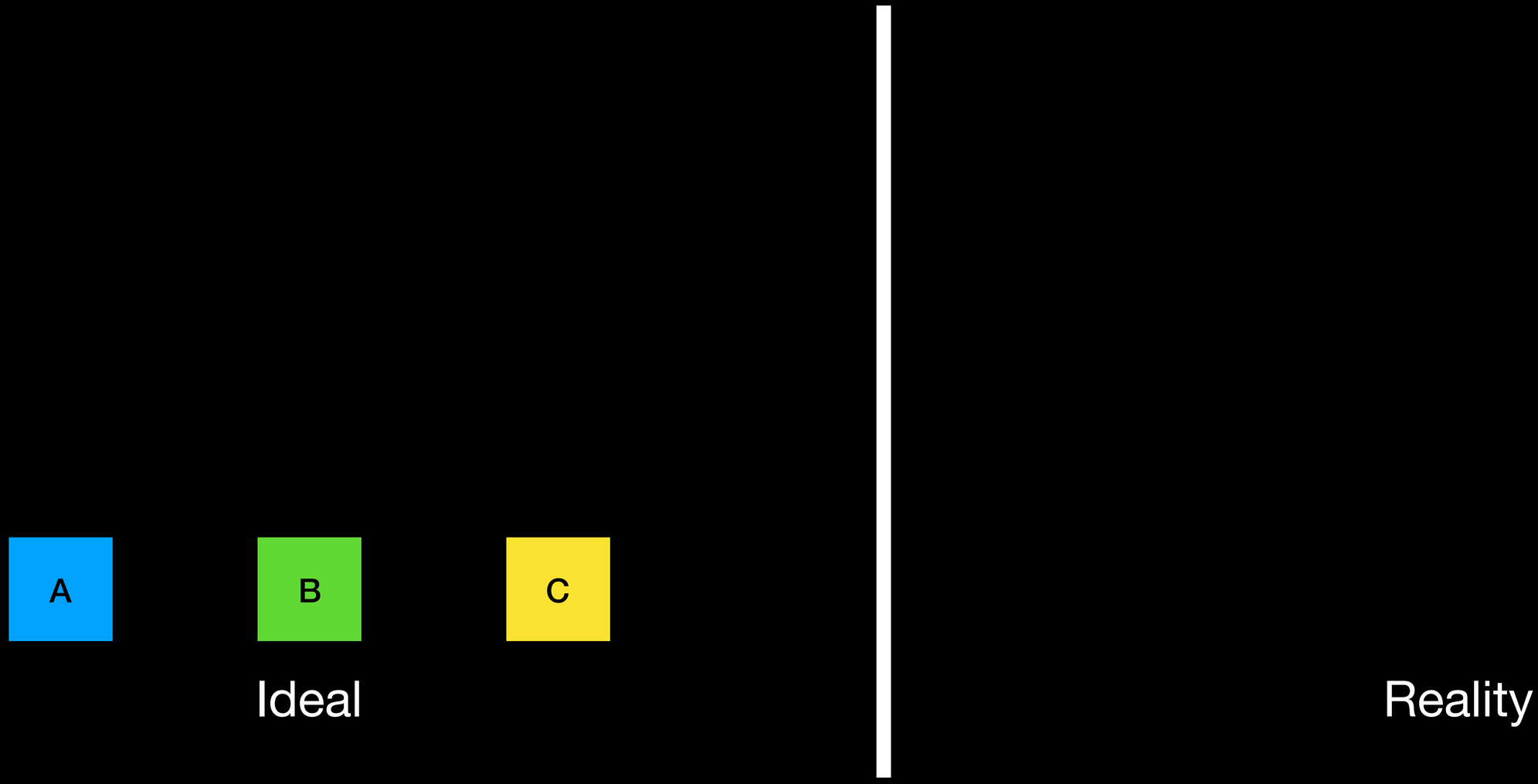
- A Multiparty Computation Protocol involves a set of parties $\{A, B, C, \dots\}$, a private input for each party $\{x_A, x_B, x_C, \dots\}$ and some functionality to jointly compute $f(x_A, x_B, x_C, \dots) = y$
  - Each party should learn nothing besides the output y
  - Crucially, that means the input of all other parties should be hidden

MPC: Ideal vs Reality

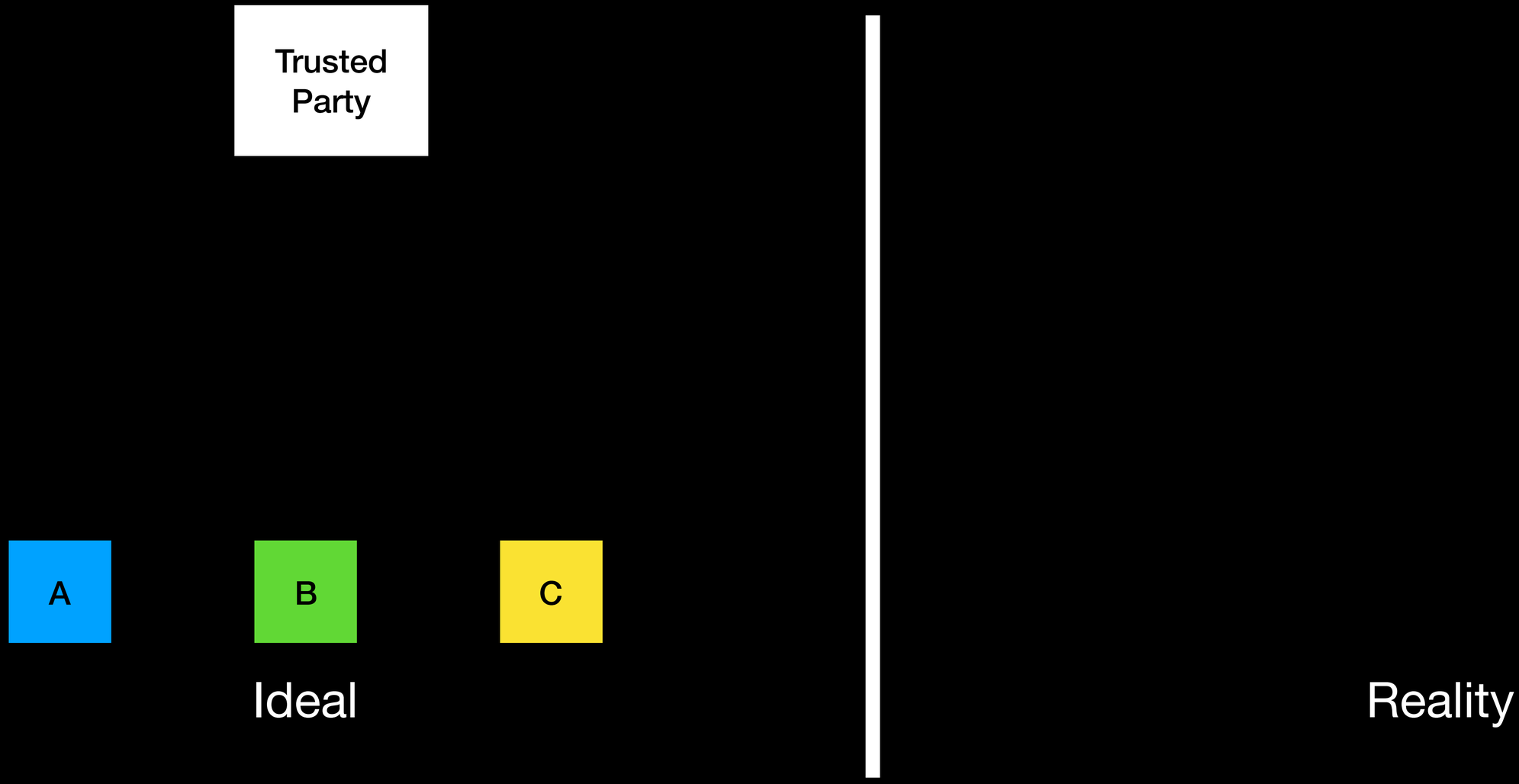
MPC: Ideal vs Reality



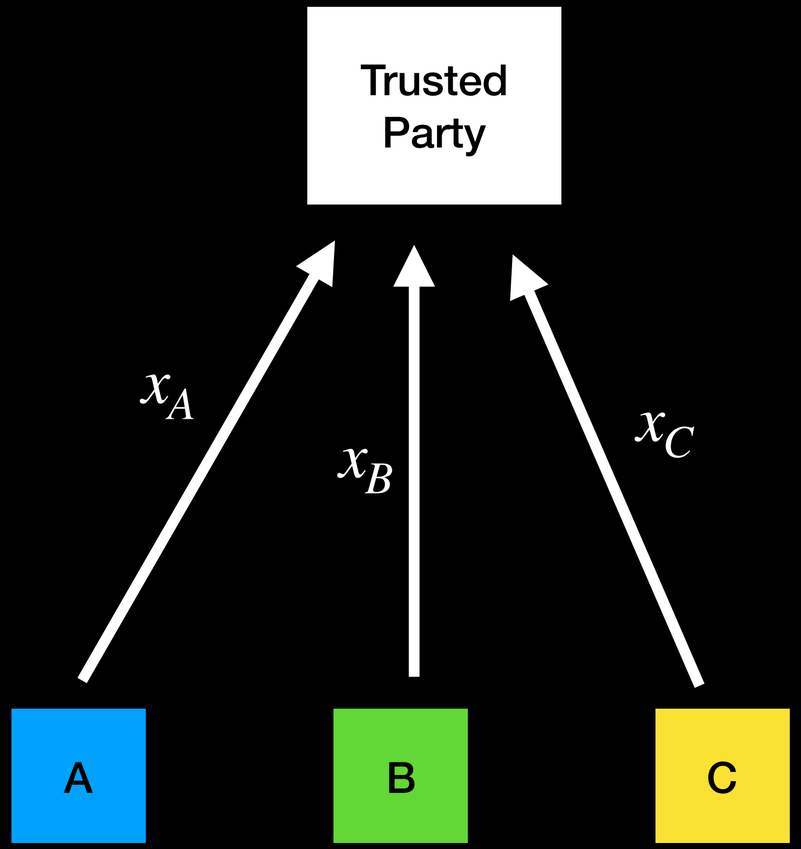
MPC: Ideal vs Reality



MPC: Ideal vs Reality



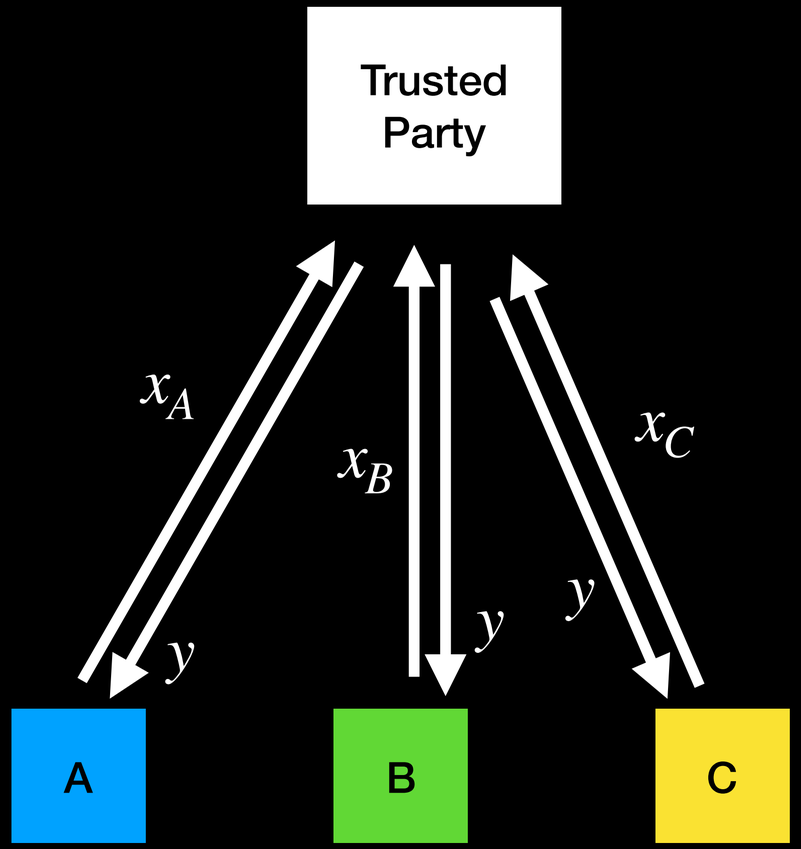
MPC: Ideal vs Reality



Ideal

Reality

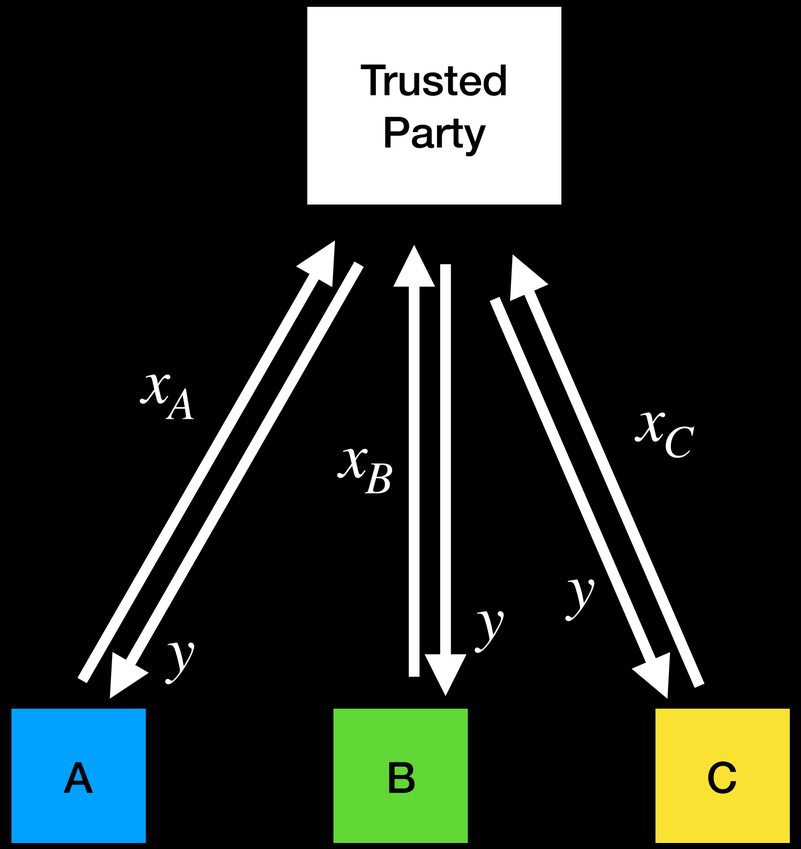
MPC: Ideal vs Reality



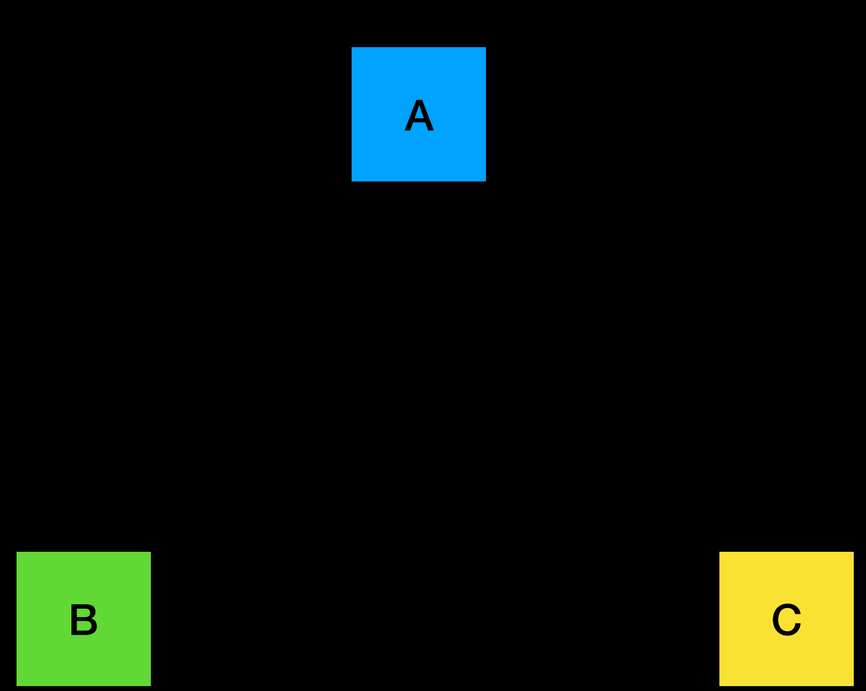
Ideal

Reality

MPC: Ideal vs Reality

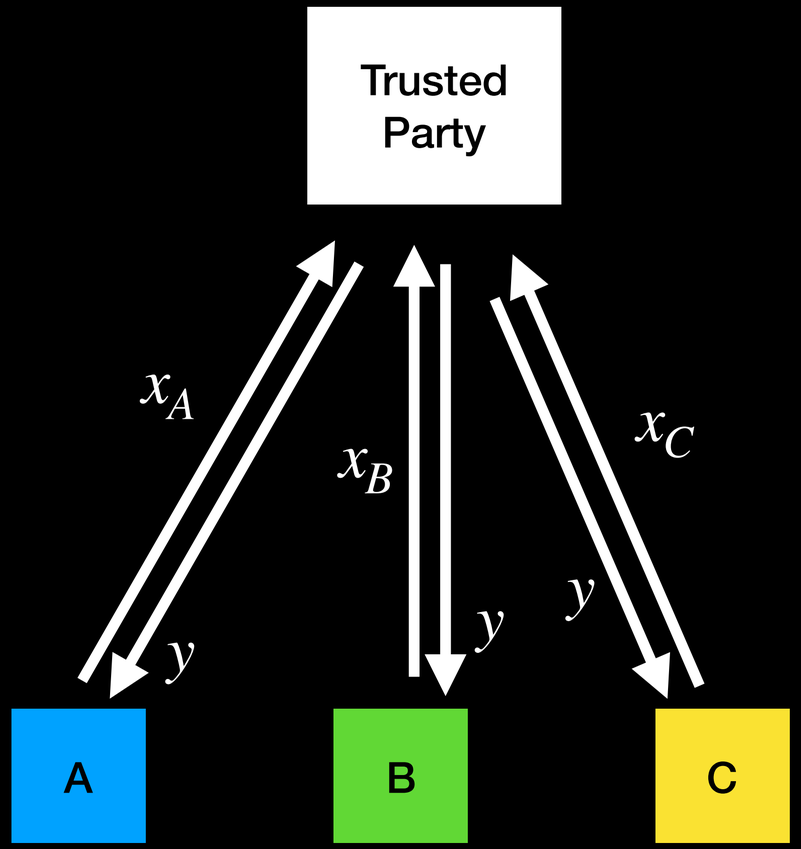


Ideal

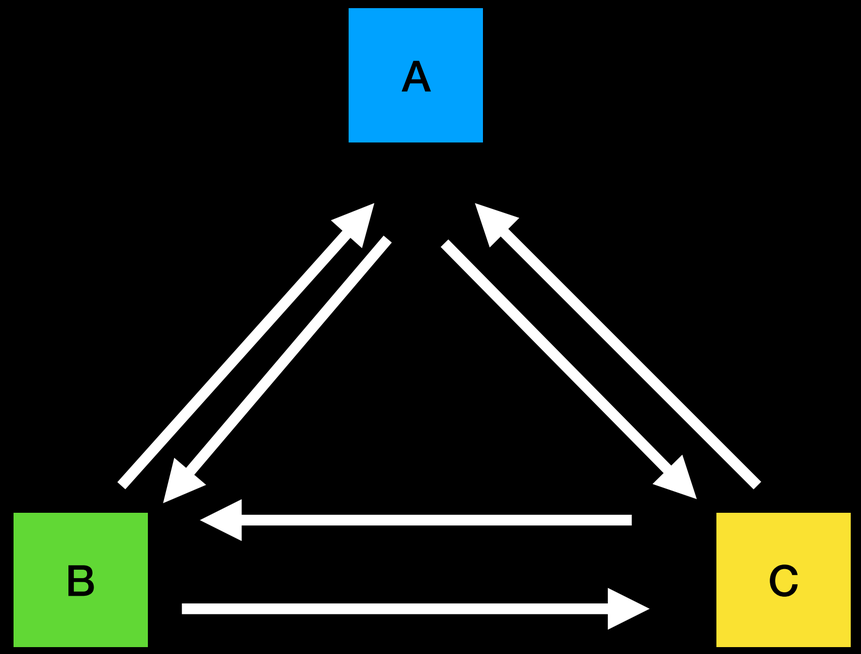


Reality

MPC: Ideal vs Reality

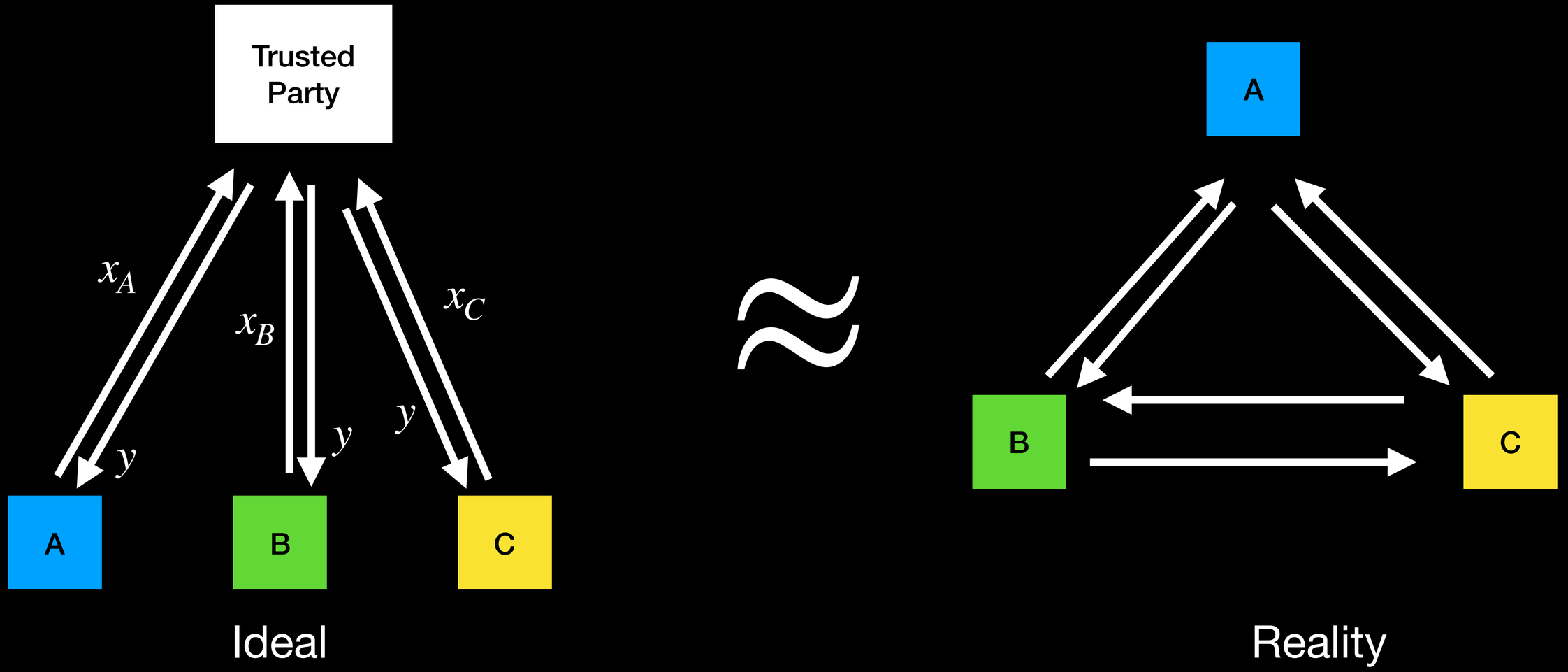


Ideal



Reality

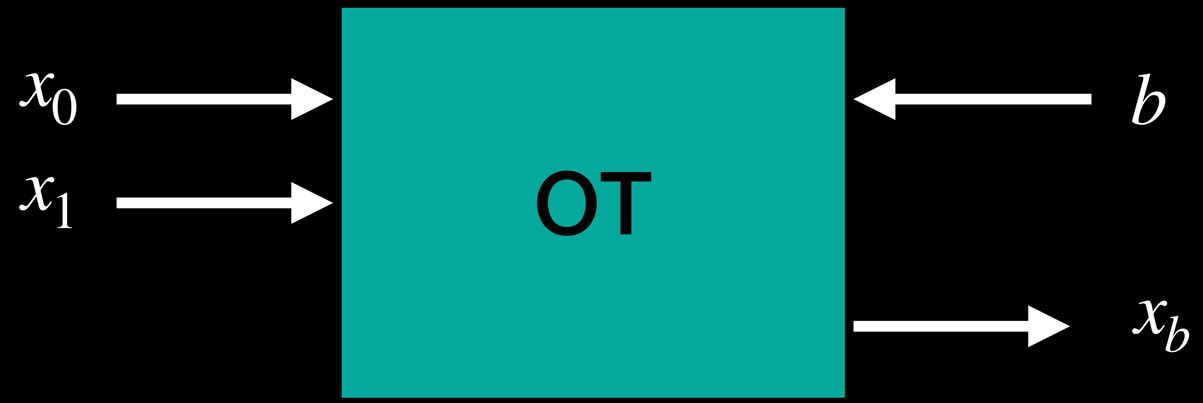
MPC: Ideal vs Reality



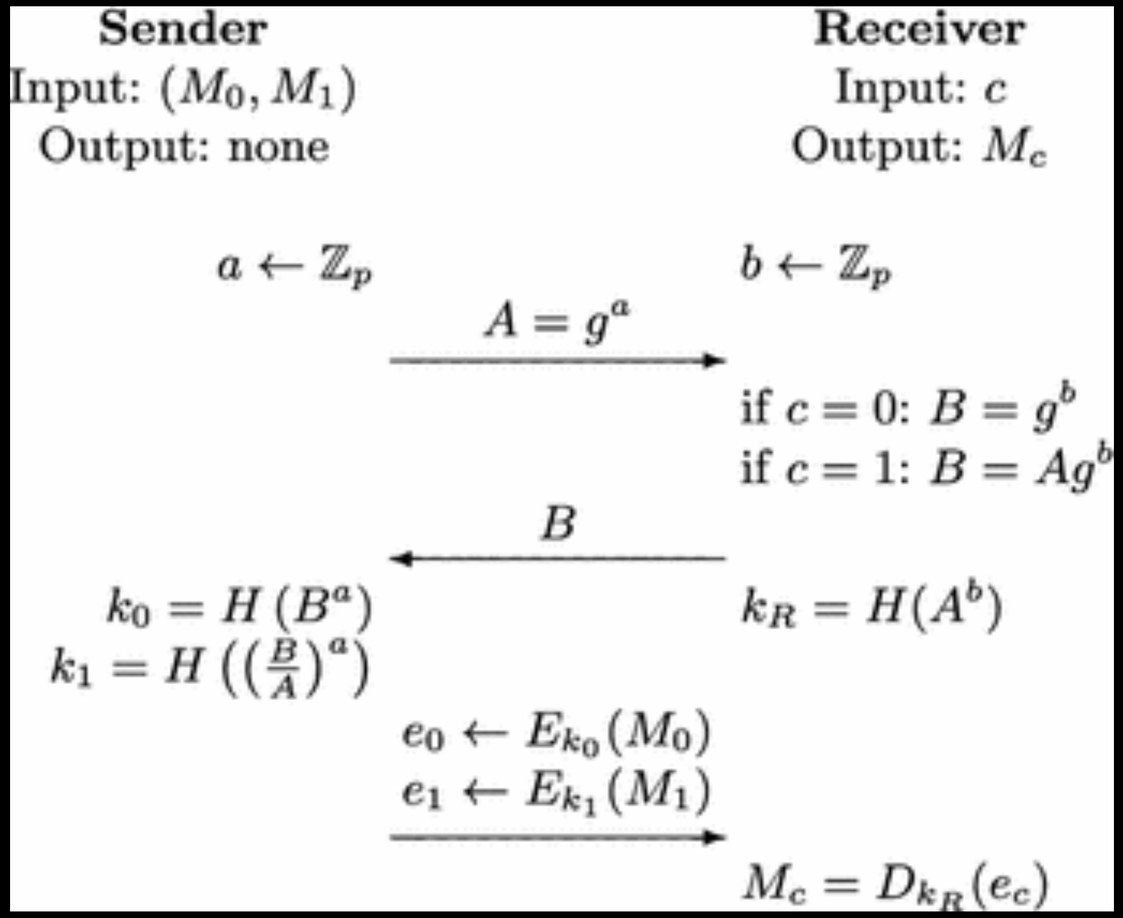
Building Block

- Consider a simple protocol for retrieving one of two values from a party

1-out-of-2 Oblivious Transfer



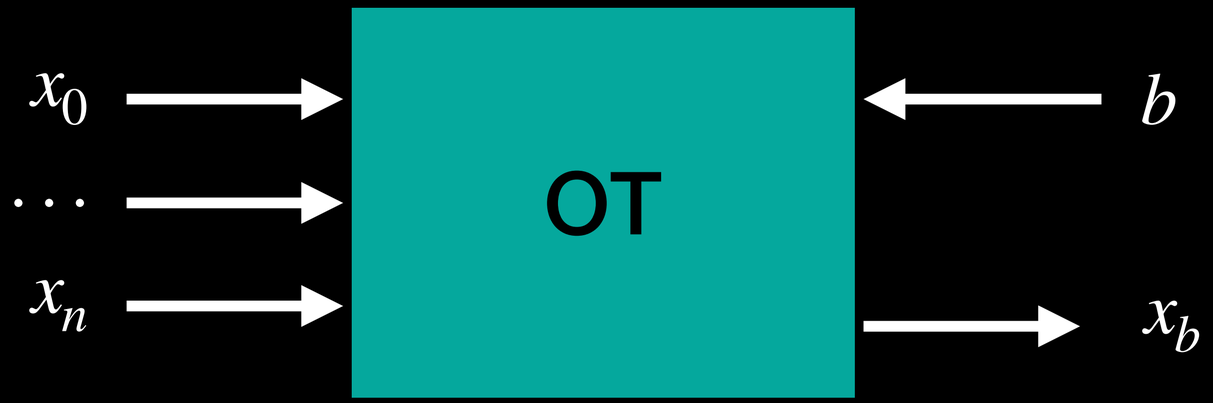
Oblivious Transfer



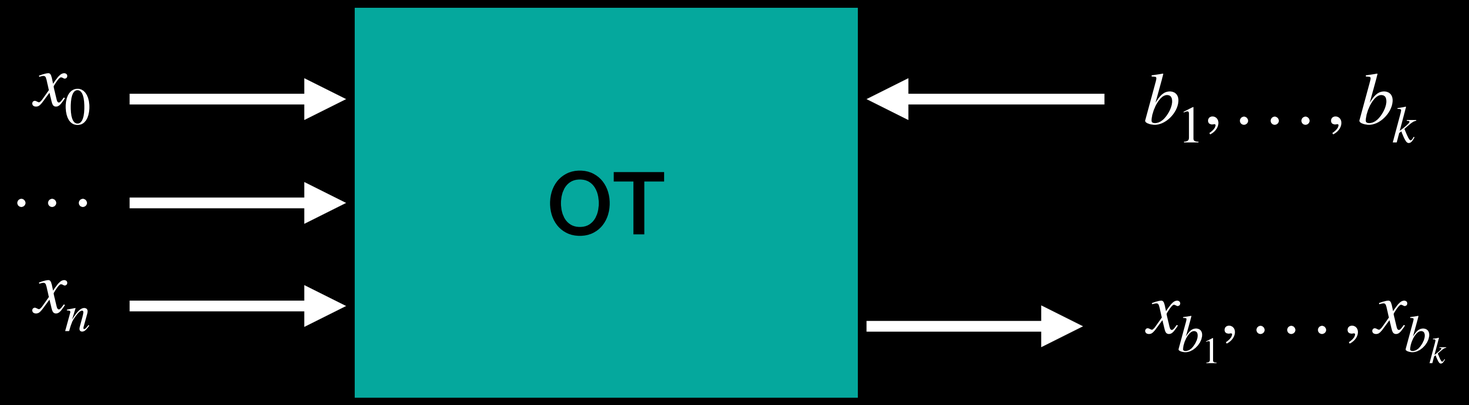
Oblivious Transfer and MPC

- Oblivious Transfer is complete for MPC!
- Note: the protocol we showed is only **semi-honest secure**: It only is secure against an adversary that may try to learn additional information but otherwise follows the protocol
  - Stronger security is possible but difficult so we will focus on semi-honest for now
- We saw 1-out-of-2 OT but we could also have 1-out-of-n OT or k-out-of-n OT

1-out-of-n Oblivious Transfer



k-out-of-n Oblivious Transfer



Private Information Retrieval (PIR)

- Goal: Query a server’s database without:
  - The server learning which entry was looked up
  - The client learning other entries of the database

Private Information Retrieval (PIR)

- Goal: Query a server's database without:
  - The server learning which entry was looked up
  - The client learning other entries of the database
- How might we do this naively?

Private Information Retrieval (PIR)

- Goal: Query a server's database without:
  - The server learning which entry was looked up
  - The client learning other entries of the database
- How might we do this naively?
- Can we use OT to build this?