From Auctions to ZK

An Educational Tour of MPC

Ais Connolly

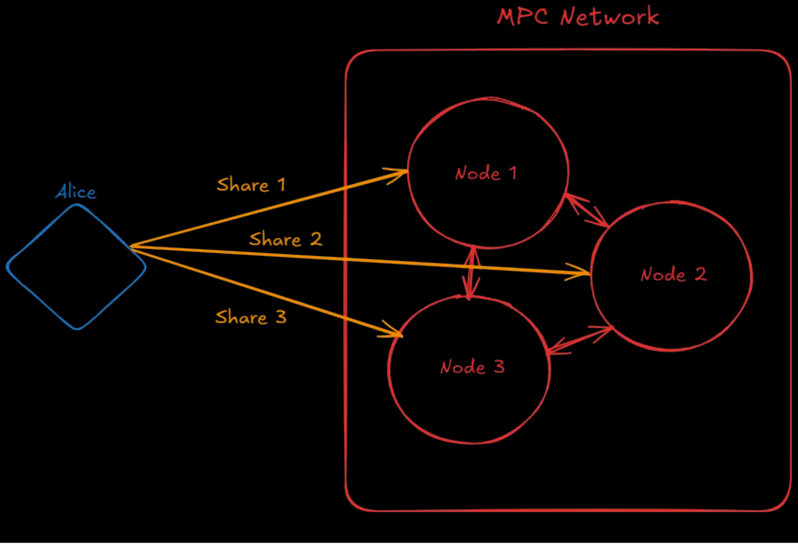
Head of Privacy, TACEO

Cryptographer ≠ Cypherpunk

So what has MPC been used for?

Computing on encrypted data

Started with coin flipping, mental poker and comparing integers



Sugar beet auction (2008)

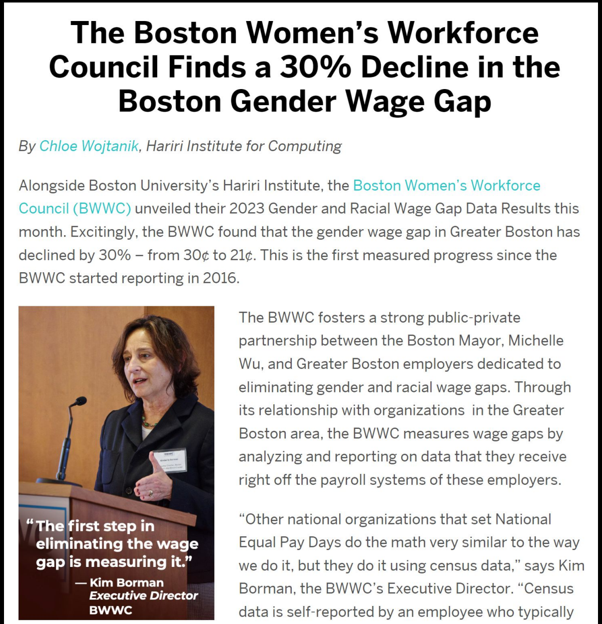
The first real commercial application

Double auction to determine market price of sugar beets

MPC run between farmers, sugar processor, and researchers

Boston wage study

Identifying salary gaps across gender and ethnicity



The Boston Women's Workforce Council Finds a 30% Decline in the Boston Gender Wage Gap

By Chloe Wojtanik, Hariri Institute for Computing

Alongside Boston University's Hariri Institute, the Boston Women's Workforce Council (BWWC) unveiled their 2023 Gender and Racial Wage Gap Data Results this month. Excitingly, the BWWC found that the gender wage gap in Greater Boston has declined by 30% – from 30¢ to 21¢. This is the first measured progress since the BWWC started reporting in 2016.

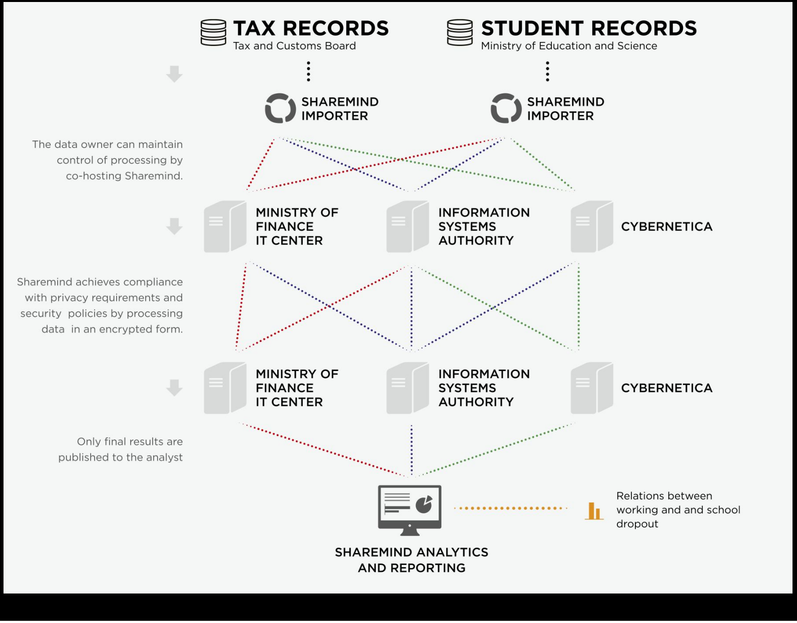
"The first step in eliminating the wage gap is measuring it."
— Kim Borman
Executive Director
BWWC

The BWWC fosters a strong public-private partnership between the Boston Mayor, Michelle Wu, and Greater Boston employers dedicated to eliminating gender and racial wage gaps. Through its relationship with organizations in the Greater Boston area, the BWWC measures wage gaps by analyzing and reporting on data that they receive right off the payroll systems of these employers.

"Other national organizations that set National Equal Pay Days do the math very similar to the way we do it, but they do it using census data," says Kim Borman, the BWWC's Executive Director. "Census data is self-reported by an employee who typically

Estonian student graduation

Investigating poor graduation rates in IT by computing over college data and tax data

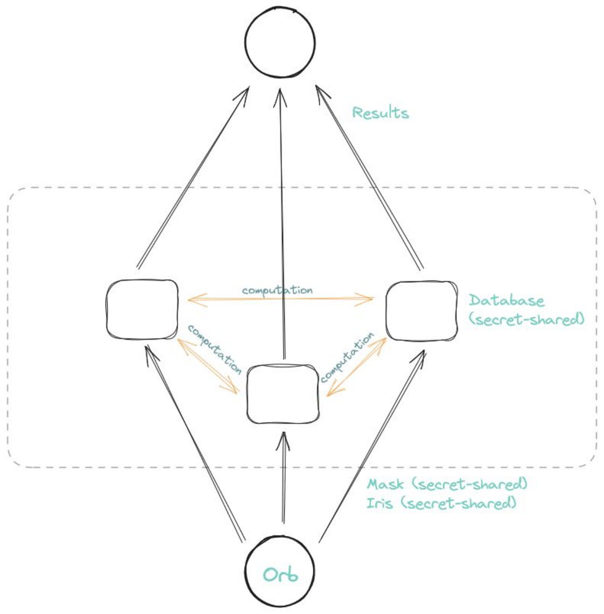

TAX RECORDS
Tax and Customs Board
STUDENT RECORDS
Ministry of Education and Science
SHAREMIND IMPORTER
SHAREMIND IMPORTER
The data owner can maintain control of processing by co-hosting Sharemind.
MINISTRY OF FINANCE IT CENTER
INFORMATION SYSTEMS AUTHORITY
CYBERNETICA
Sharemind achieves compliance with privacy requirements and security policies by processing data in an encrypted form.
MINISTRY OF FINANCE IT CENTER
INFORMATION SYSTEMS AUTHORITY
CYBERNETICA
Only final results are published to the analyst
SHAREMIND ANALYTICS AND REPORTING
Relations between working and and school dropout

Google ad conversion

Joint computation between Google and Mastercard

Worldcoin iris scanning

Uniqueness checks on iris scans from orbs



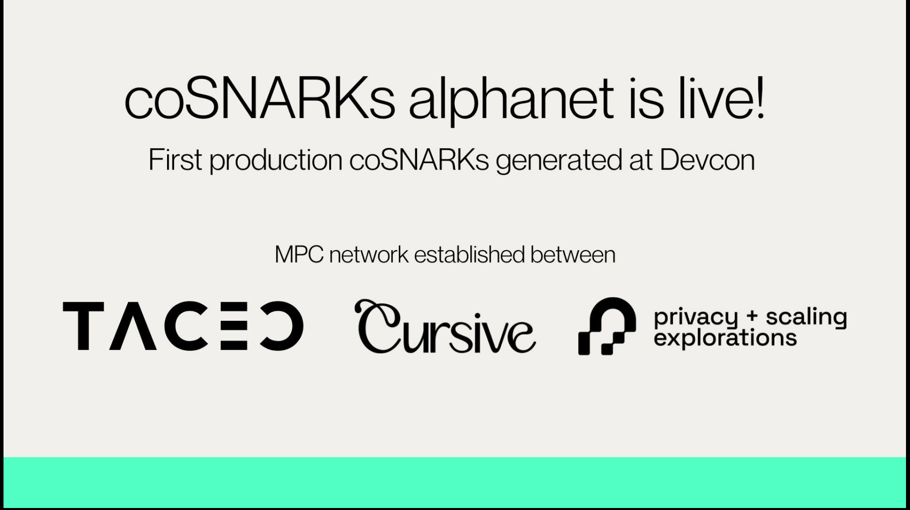
Just throw MPC at it.

Cursive private proof delegation

Large proofs are delegated in a privacy preserving way to MPC network

Cursive private proof delegation

Large proofs are delegated in a privacy preserving way to MPC network



coSNARKs alphanet is live!

First production coSNARKs generated at Devcon

MPC network established between

TACEO Cursive privacy + scaling explorations

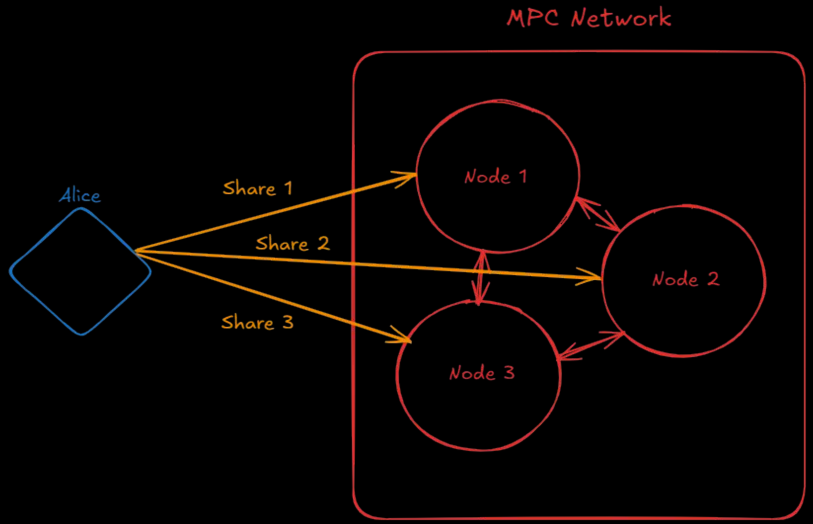
Collaborative SNARKs

ZK in MPC

Currently there is tooling for coCircom and coNoir (collaboratively gud)

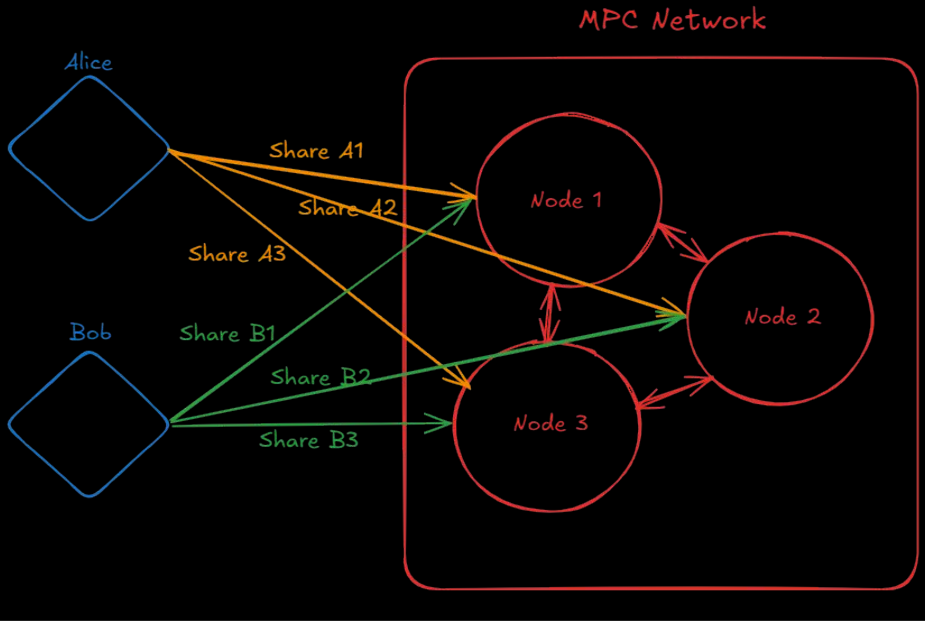
Private shared state

Collaboration on encrypted data



Private shared state

Collaboration on encrypted data



The privacy conversation is becoming beautifully nuanced

Who are your adversaries?

Collusion in the network

If parties collude, secrets can be reconstructed

How many parties need to be honest? Majority? Just one?

Semi-honest security

aka honest-but-curious

aka passive

Adversary can corrupt parties, but they follow protocol as normal

Malicious security

aka active

Adversary can corrupt parties, and they can deviate from the protocol

Adversary can control, manipulate, and arbitrarily inject messages on the network

What about efficiency?

State of the art

Deployed MPC protocols

Big difference between specialised protocols or general

World iris uniqueness checks - 40 billion per sec

Cursive coSNARK - 12 seconds each (11.9 is witness extension)

Thank you!

Ais Connolly

ais@taceo.io
@aisconnolly