MPC Tooling or How to create MPC apps

Rasul Ibragimov // MPC Research @ PSE

privacy + scaling explorations

Contents

➔ What is MPC?

➔ Applications of MPC

➔ Circom-MPC

➔ Summon

➔ Circom-MP-SPDZ

➔ 2PC is for Lovers

What is MPC?

MPC – interactive protocol that allows parties to jointly compute a function over their inputs while keeping those inputs private.

App-Specific vs General Purpose MPC

App-Specific

- Threshold signatures
- Shamir's Secret Sharing
- PSI

General Purpose

Any function, including all the app-specific protocols

Applications

- MPC-ML
  Privacy Preserving Machine Learning
- coSNARKS
  Collaboratively compute ZKP
- MPC Stats
  Privacy Preserving stats on data

etc.

Circom-MPC

Fork of Circom. Compiles to universal MPC format called Bristol Fashion Circuit/Format, that can describe boolean & arithmetic circuits.

Advantages:

- zk/cryptography devs know Circom;
- big number of circuits written in Circom, that can be reused, e.g. circomlib-ml

github.com/namnc/circom-2-arithc

Summon

A language for collaboratively summoning computations.

TypeScript-like DSL, similar to Circom-MPC, with a goal for user-friendliness. Can be used in TypeScript => allows to build everything end-to-end in TypeScript

github.com/voltrevo/summon

Circom-MP-SPDZ

Transpiler from Bristol format to .mpc representation that is required to run the circuit in MP-SPDZ backend.

The project shows an example of running circomlib-ml Machine Learning circuits in MP-SPDZ.

The same tool can be used to transpile circuits generated by Summon.

github.com/namnc/circom-mp-spdz

2PC is for Lovers

Matching game for friends & lovers, built with Summon.

If you choose **love** but the result is **friendship**, only you will know about your feelings. Even if your friend knows advanced cryptography.

You can try it here!

github.com/voltrevo/2pc-is-for-lovers

Thanks for coming

find me: @curryrasul