MP-SPDZ
MPC Made in Australia

Marcel Keller

Data61

4 December 2018

MP-SPDZ: MPC made in Australia

Program once, execute in many protocols

`https://github.com/n1analytics/MP-SPDZ`

- Fork of Bristol Crypto's SPDZ-2
- Program in Python, execute in fast virtual machine
- Dishonest majority (any number of parties) and honest majority (3 parties)
- Malicious security and semi-honest
- Arithmetic (modulo prime and 2^{64}) and binary circuits
- Secret sharing and garbled circuits
- Protocols: SPDZ/MASCOT/Overdrive, 3-party replicated, Yao's garbled circuits, SPDZ-BMR