MP-SPDZ: A Versatile Framework for Multi-Party Computation

Marcel Keller

CSIRO's Data61

13 May 2020

MP-SPDZ

- 20+ MPC protocols in several computation domains and security models (malicious/semi-honest, any threshold corruption)
- Secret sharing, homomorphic encryption, oblivious transfer, garbled circuits
- Unified high-level programming interface based on Python
- Extensive library including fractional number computation and mathematical functions
- Binaries for Linux

Protocols

Security model	$\mathbb{F}_p$ / $\mathbb{F}_{2^n}$	$\mathbb{Z}_{2^k}$	$\mathbb{F}_2$ Sharing	Garbling
Malicious, dishonest majority	1	1	2	1
Covert, dishonest majority	2	0	0	0
Semi-honest, dishonest majority	3	1	1	2
Malicious, honest majority	3	4	2	1
Semi-honest, honest majority	2	1	2	1

Links

https://github.com/data61/MP-SPDZ
https://mp-spdz.readthedocs.io
https://gitter.im/MP-SPDZ/community
https://ia.cr/2020/521
https://twitter.com/mkskeller