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

Marcel Keller

CSIRO's Data61

May 6, 2020

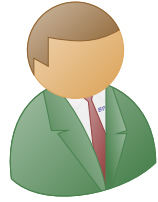
# Links

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

# Millionaire's Problem

$x

$x < y$?



$y

# MP-SPDZ

- 20+ protocols in several computation domains and security models (malicious/semi-honest, any degree of corruption)
- Unified high-level programming interface based on Python
- Extensive library including fractional number computation and mathematical functions