The million-entry ORAM on MPC

- ORAM: Shi et al. (Parameters: Gentry et al.)
- MPC: “SPDZ” by Damgård et al.
- Access time:

The million-entry ORAM on MPC

- ORAM: Shi et al. (Parameters: Gentry et al.)
- MPC: “SPDZ” by Damgård et al.
- Access time: x seconds, $x \leq 30$?

The million-entry ORAM on MPC

- ORAM: Shi et al. (Parameters: Gentry et al.)
- MPC: “SPDZ” by Damgård et al.
- Access time: x seconds, $x \leq 30$?
  (estimate based on 1000-entry ORAM)

The million-entry ORAM on MPC

- ORAM: Shi et al. (Parameters: Gentry et al.)
- MPC: “SPDZ” by Damgård et al.
- Access time: x seconds, $x \leq 30$?
  (estimate based on 1000-entry ORAM)
  (not bug-free yet)