analysis

June 27, 2023

0.1 AES in CTR mode using SIMD (Memory)

0.1.1 Excluding Setup

Current benchmarks don't include memory for ABY excluding setup, as I first needed to implement this functionality in ABY.

0.1.2 Including Setup

0.2 AES in CTR mode using SIMD (Runtime)

0.2.1 Online (LAN)

0.2.2 Online (WAN)

0.2.3 Setup (LAN)

Excluding MP-SPDZ as its setup time can't be recorded separately.

0.2.4 Total (LAN)

0.3 AES in CBC mode (Memory)

- `seec_aes_cbc_no_setup_sc_static_layers`: Uses sub-circuits and static layers which are precomputed
- `seec_aes_cbc_no_setup_sc`: Uses sub-circuits and dynamic layers computed on the fly during execution
- `seec_aes_cbc_no_setup`: No sub-circuits, uses dynamic layers

All without setup, as this impacts memory consumption majorly

0.4 AES in CBC mode (LAN Online Runtime)

0.5 SHA-256 SIMD (Memory)

0.5.1 Excluding Setup

TODO: run MOTION bench for 100k as well

0.6 SHA-256 SIMD (Memory)

0.6.1 Including Setup

Majority of memory consumption in normal evaluation is due to single batch computation of OTs.

0.7 SHA-256 SIMD (Online Runtime)

TODO: Benchmark MOTION for 100k (500k?)