**Computation Analysis**

**centralized implementation (packed)**:

Phase 1: ~28 x 256 operations

Phase 2: 16 operations

Phase 3: 30 X 256 operations

**Centralized version (unpacked):**

Phase 2: 0 operations

Phase 3:

**Distributed implementation (packed)**:

Phase 1: 112 x 256 + 36

Phase 2: 28 + OT’s = 28 + 26 x 4

Phase 3: 60 x 256

**Communication Analysis (distributed, packed)**:

Ax+b:

Mx = 256 bits

Ma = 512 bits

Mb = 256 bits

Phase 1: 8 x 256

OT:

3 x 256 vectors

**Runtime in MS (1000 runs)**:

**Centralized version**:

Phase 1: 1985

Phase 2: 58

Phase 3: 61213

**Distributed version**

Phase 1 – AX+B:

Party 1: 4028

Party 2: 3781

Phase 2: Share Conversion:

Party 1: 1907

Party 2: 828

Phase 3 (both parties combined): 115783

Overall PRF=132851

Runtimes do not match computation analysis right now, probably because of a compiler issue. We will start working on AWS for this.