**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 1: 256X258

Phase 2: 0 operations

Phase 3: 256X81+2\*81+258\*81 ~= 163\*256

**Distributed implementation (packed)**:

Phase 1: 132 x 256 + 36 ~= 132 X 256

4 \* toeplitzbyVec + 9 additions

Phase 2: 28 + OT’s = 28 + 26 x 4

OT2\_1 : 1 X 4

OT1: 17 X 4

OT2\_2:8 X 4

Phase 3: 78 x 256.

(1+26+(2\* 6))\*256 = 39 \* 256

At: 8 operations

ToeplitzbyVec: 256\*(5+4\*7) = 256\*33

**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 microsecond (1000 runs)**:

**Centralized version (packed)**:

Phase 1: 1985

Phase 2: 58

Phase 3: 61213

**Centralized version (phase 3 unpacked)**:

Phase 1: 55730

Phase 3: 132148

**Distributed version** (packed)

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.