**PRF Program**

**Computation Analysis**

N = 256, K = 81 (Z3), nWords (for packing) = 4;

**centralized implementation (packed)**:

Phase 1: ~28 x N operations

Phase 2: 16 operations

Phase 3: 30 X N operations

**Centralized version (unpacked):**

Phase 1: N^2

Phase 2: 0 operations

Phase 3: N\*K\*2 + K\*2

**Distributed implementation (packed)**:

Phase 1: 132 x N + 9\*nWords ~= 132 X 256

(4 \* toeplitzbyVec + 9 additions

Phase 2: 28 + OT’s = 28 + 26 x nWords

OT2\_1 : 1 X nWords

OT1: 17 X nWords

OT2\_2:8 X nWords

Phase 3: 78 x N.

(functions used for calculations: At: 8 operations, ToeplitzbyVec: N\*(5+nWords\*7) = 256\*33)

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

Ax+b:

Mx = N bits

Ma = 2\*N bits. (a Toeplitz matrix)

Mb = N bits

Phase 1: 2 \* Ax+B = 8 x N

OT: 3 x N

**Runtime**:

in milliseconds for 1000 runs on AWS, instance medium type)

|  |  |
| --- | --- |
| **AX + B**  **(Party 1)** | 10.34 |
| **AX + B**  **(Party 2)** | 11.09 |
| **Share Conversion (Party 1)** | 2.76 |
| **Share Conversion (Party 2)** | 3.75 |
| **Phase 3**  **(Randomization – both parties together)** | 23.50 |
| **PRF**  **(entire PRF excluding preprocessing)** | 59.08 |