Amazon AWS

Configuration:
Platform: Ubuntu Server 18.04
Instance Type: t2.medium
Virtualization: hvm
vCPUs: 2
Memory: 4GB
Compiler: G++ 7.5
Number of Runs: 1000

Distributed Dark Matter PRF Implementation

Phases	milliseconds (for consistency)
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)	23.50
PRF (entire PRF excluding preprocessing)	59.08

Phases	milliseconds (for consistency)
Round 1	21.43
Round 2	6.51
Phase 3 (Randomization)	23.50
PRF (entire PRF excluding preprocessing)	59.08

New Protocol Computation Timings (Amazon AWS)

Note:

1. **Optimization flag was used -O3 while compiling**
2. **Preprocessing are excluded from timings.**

Note: The following timings are for **1000 runs**

Rounds (1000 runs)	Time(ms)
Round 1	0.69
Round 2	11.68
Round 3	24.2

New Protocol Z3 Lookup table Computation Timings (AWS)

Note:

1. **Optimization flag was used -O3 while compiling**
2. **Preprocessing are excluded from timings.**

Note: The following timings are for **1000 runs**

Rounds (1000 runs)	Time(ms)
Round 1	0.69
Round 2	11.68
Round 3	6.11

Centralized PRF Implementation (Using Packing)

Phase	milliseconds (for consistency)
P1 (K * X)	2.67
P2 (Share Conversion)	0.5
P3 (multiply with 81 x 256 randomization matrix)	12.12

Centralized PRF Implementation (Naïve/ Unpacked implementation)

Phase	milliseconds (for consistency)
P1 (K * X)	2.67

P2 (Share Conversion)	N.A.
P3 (multiply with 81 x 256 randomization matrix)	0.5
Generation of 81 x 256 randomization matrix in Z3	130.28