**Computation Timings (Local machine)**

**Note:**

1. **All timings are in milliseconds(ms).**
2. **The timings are recorded for 1000 runs**
3. **Optimization flag was used -O3 while compiling**
4. **Preprocessing are excluded from timings.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Phases** | **1 (ms)** | **2 (ms)** | **3 (ms)** | **4 (ms)** |
| **AX + B**  **(Party 1)** | 5.815 | 5.623 | 5.626 | 5.669 |
| **AX + B**  **(Party 2)** | 5.650 | 5.239 | 5.461 | 5.321 |
| **Share Conversion (Party 1)** | 2.832 | 2.965 | 2.927 | 3.586 |
| **Share Conversion (Party 2)** | 1.086 | 1.132 | 1.113 | 1.354 |
| **Phase 3**  **(Randomization)** | 119.988 | 120.496 | 121.538 | 120.129 |
| **PRF**  **(entire PRF excluding preprocessing)** | 132.76 | 137.16 | 136.62 | 136.72 |

**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 PRF Implementation (Communication through shared variables/memory)**

|  |  |  |
| --- | --- | --- |
| **Phases** | **nanoseconds**  **(timing read as it is)** | **milliseconds**  **(for consistency)** |
| **AX + B**  **(Party 1)** | 10343218 | 10.34 |
| **AX + B**  **(Party 2)** | 11095472 | 11.09 |
| **Share Conversion (Party 1)** | 2768317 | 2.76 |
| **Share Conversion (Party 2)** | 3758289 | 3.75 |
| **Phase 3**  **(Randomization)** | 23508994 | 23.50 |
| **PRF**  **(entire PRF excluding preprocessing)** | 59086810 | 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 (ver 1.0) 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** (timings in seconds)

|  |  |
| --- | --- |
| **Rounds (1000 runs)** | **Time(ms)** |
| **Round 1** | 0.6 |
| **Round 2** | 11 |
| **Round 3** | 23 |

**Centralized PRF Implementation (Using Packing)**

|  |  |  |
| --- | --- | --- |
| **Phase** | **nanoseconds**  **(timing read as it is)** | **milliseconds**  **(for consistency)** |
| **P1**  (K \* X) | 2672543 | 2.67 |
| **P2**  (Share Conversion) | 598445 | 0.5 |
| **P3**  (multiply with 81 x 256 randomization matrix) | 12123630 | 12.12 |

**Centralized PRF Implementation (Naïve/ Unpacked implementation)**

|  |  |  |
| --- | --- | --- |
| **Phase** | **nanoseconds**  **(timing read as it is)** | **milliseconds**  **(for consistency)** |
| **P1**  (K \* X) | 2523520 | 2.67 |
| **P2**  (Share Conversion) | N.A. | N.A. |
| **P3**  (multiply with 81 x 256 randomization matrix) | 584529 | 0.5 |
| **Generation of 81 x 256 randomization matrix in Z3** | 130286799 | 130.28 |