**Dark Matter Implmenetation**

**Configuration:**

**Platform:** Ubuntu Server 18.04

**Instance Type**: t2.medium

**Virtualization:** hvm

**vCPUs**: 2

**Memory:** 4GB

**Compiler:** G++ 7.5

**Code runs 1000 runs each time, time in document per run**

**Running environment: Amazon AWS**

**Code building notes:**

Currently, the flags needed to run the program are in the mains.hpp file.

Options:

**PACKED\_PRF\_CENTRAL = 1. - centralized packed PRF, both phases 2 and 3 are packed (no lookup table), key is Toeplitz:**

**UNPACKED\_PRF\_CENTRALIZED = 1. - Centralized naïve version**

**PACKED\_PRF\_CENTRAL\_LOOKUP = 1 , centralized using lookup table**

**Building the code:**

g++ -std=c++14 -O3 -o pDarkMatterPRF -I include/darkmatter/ src/\*.cpp tests/\*.cpp

**Runtimes**:

Runtime executed on Amazon AWS:

**Centralized version**:

**Centralized PRF Implementation (Using Packing)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase** | **sec (microsec)** | **Rounds/sec** | **Macbook Air (microsec)** |
| **P1**  (K \* X) | 2.67 |  | 1.782 |
| **P2** | 0.50 |  | 0.35 |
| **P3**  (multiply w 81x256 Rand matrix) | 12.12 |  | 53.214 |
| **Full Protocol** | 15.29 | 65,400 | 55.668 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase** | **sec (microseconds) (AWS)** | **Rounds per sec (AWS)** | **Local Macbook Air Machine** |
| **P1**  (K \* X) | 2.50 |  | 3.889 |
| **Generation of 81 X 256 randomization matrix** | 130.54 |  | 356 |
| **P3**  (Rmat\* (K\*X)) | 0.58 |  | 22.354 |
| **Full Protocol** | 136.13 |  | 28.448 |

**Centralized PRF Implementation (Using Packing+ Lookup Table)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Phase** | **milliseconds** | **Rounds per sec (AWS)** | **Local Macbook Air Machine** |
| **Calling Lookup function** | 1.64 |  | 14.786 |
| **Full Protocol** | 5.19 |  | 21.188 |

**Comparison of Timing of full protocol across unpacked, packed and packed lookup table**

**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 |

|  |  |
| --- | --- |
| **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 |