**Uselookup Analysis**

21st Jan 2021

**Problem:** Timing for similar phase 3(use of lookup table) in new protocol and wPRF with lokup(TCC’18) are not same. Both the protocols contains use\_lookup() function twice.

|  |  |
| --- | --- |
| **Uselookup(new protocol)** | **Uselookup(wPRF)** |
| 4.5 μsec | 16 μsec |

**Solution 1: Are variables used in uselookup function as local?**

**Observation:** The timings are still same, and no effect has been observed.

**Solution 2:** **Check if variable used in uselookup function are used in subsequent line. Since it runs for 1000 times, it may be skipping the part.**

**Observation:** The variables are accessed after the call to uselookup()

**Solution 3:** **Does PRF.cpp contains all the header files as newprotocol.cpp?**

**Observation:** All header files that were present in newprotocol.cpp were copied to PRF.cpp. But still the timing didn’t change.

**Solution 4:** Adding loop inside function PRF\_DM, declaring variables outside timing. Use proper declaration instead of auto.

**Observation:** The timing is still same. Uselookup takes more time 12.5 microseconds as opposed to similar use in newprotocol.cpp with 4.5 microseconds.

**Interesting Note:**

Uselookup()(called twice) took same time in both local and AWS in wPRF(16 μsec)

As discussed on 1/20/21, three timings were recorded:

1. wPRF(TCC’18) with lookup
2. newprotocol with lookup
3. centralized with lookup

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Phase/function()** | **AWS** | **Local** |
| wPRF(TCC’18) with lookup | Reformat\_input() | 1.27 | 1.6 |
| Uselookup | 13.43 | 16.07 |
| Subtract | 0.61 | 0.05 |
| Total | 17.71 | 17.87 |
| Centralized with lookup | Reformat\_input | 0.95 | 0.7 |
| Uselookup | 1.64 | 5.3 |
| Newprotocol with lookup | Mux+lookup | 4.11 | 10.86 |
| Phase3 total | 12.07 | 14.36 |

Note:

* All times are in μsec.
* Just phase 3 are timed since it contained the lookup table.