**\* Secure version of PkNC**

\* n (DATA\_SIZE) = 2000, 4000, 6000, 8124

(n=\*, K=1024, k=1000, t=8.12)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Data size | 2000 | 4000 | 6000 | 8124 |
| Time | **8 m 41 s** | **11 m 13 s** | **24 m 5 s** | **m s** |

\* k (PARAM\_K) = 100, 400, 700, 1000

(n=1728, k=\*, K=1024, t=8.12)

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| K | 5 | 15 | 25 | 100 | 400 | 700 | **1000** |
| Time | **3 m 24 s** | **3 m 25 s** | **3 m 21 s** | **3 m 26 s** | **3 m 15 s** | **3 m 9 s** | **3 m 17 s** |

\* K (MOD\_SIZE) = 512, 1024, 2048

(n=1728, k=1000, K=\*, t=8.12)

|  |  |  |  |
| --- | --- | --- | --- |
| Key size | 512 | 1024 | 2048 |
| Time | **48 s** | **\*\*\*** | **35 m 56 s** |

\* t (NUM\_MAIN\_THREAD) = 1, 2, 4, 8, 12, 16

(n=1728, k=1000, K=1024, t=\*.\*)

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Thread | 1 | 2 | 4 | 8 | 12 | 16 |
| Time | **14 m 8 s** | **7 m 36 s** | **5 m 58 s** | **\*\*\*** | **2 m 57 s** | **m s** |

1. 다양한 query (input 변경)