OPRF construction-2

Analysis of Timing

Components in OPRF construction-2

- R0: matrix multiplication
- R1, R2 : matrix vector multiplication + vector addition

- Here, R0 is the **Key update phase.**
- R1, R2 and computation of y=Mz is the **evaluation phase.**

Key Update phase timing

- R and K are two circulant matrix of size n bits.
- R*K is the matrix vector multiplication, which can be performed with the help of lookup table. Since $R \in \mathbb{Z}_3$and K $\in \mathbb{Z}_2$, it is same as the time taken in centralized Lookup table implementation(1.8 μsec)
- So, Key update phase timing = 1.8 μsec(approximate)

Evaluation phase timing

- Server performs R2
- Client performs R1 + compute y=Mz

- R2 is similar to phase 3 of OPRF construction 1: **4.84 µsec**
- Client performing $R_1\ and\ (y = Mz) = 4.82 + 4.02 = \mathbf{8.84}$ **µsec**

- **Parallel Implementation(OPRF construction 2): 8.84 + (server key update) = 10.64 µsec**