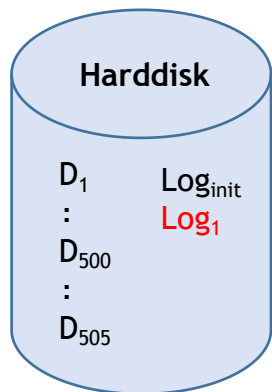




ZURICH[®]

1. train($n = 500$)



3a. load* Log_{init} and
 $D_1 \dots D_{500}$ into enclave

DP-GBDT Enclave

2a. ensure n is valid training size

2b. $c_q := \text{Read}()$

2c. ensure $c_q \geq n$

4. (prng-)derive s_1 from s_m

5a. Inc()

5b. $c_{\text{log}} := \text{Read}()$

6. $\text{Log}_1 := \text{seal}(\{ \text{"Log"}, \text{id}_{\text{LC}}, c_{\text{log}}, 1, 500, s_1 \})$

7. start_training($D_1 \dots D_{500}, s_1$)

8. output model

Questionnaire
Counter

[val = 505]

Log Counter (id_{LC})

[val = 1]
[val = 2]