Optimal verification

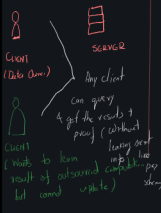
Time complexity of verifier depends only on
- Description → How big is the query
- Outcome → How big is the result
of Query

Doesn't depend on how big of a set the query is run on

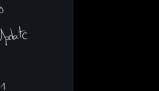
Example
$|y_1| \cap s_2 \cap s_3 \cap \ldots \cap s_n$ $|s_i| = \delta$
Complexity of verifier is
$O(t + \delta)$
↓ ↓
no of bits in Query — Size of Proof Π

Previous works provide Optimal verification but without
- Public Verifiability
- Dynamic Updates

Public Verifiability



Dynamic Updates

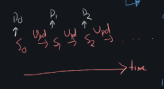


Can still query over updated DB // Previous schemes fixed description of circuit at Initialization
↳ ???

SETTING

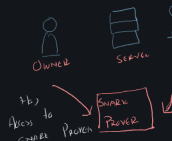
Three Party Model

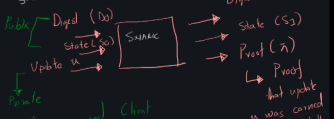
Trust Assumptions



↳ He is conducting queries on Data with appropriate digest i.e he trusts the digests he receives after updates to the DB are true(???)

(Random Idea)





↳ Proof that update U was carried out successfully

- Owner and Client can issue Updates Privately (Owner doesn't see Client's update and vice-versa)

But they can be assured that the digest D_1 actually came out of private update U made by either party

Trivial Scheme

- Owner also gives the update to the client that the Digest client verifies transition $D_0 \to D_1$ by applying Update U to state S_0.

Novelty with SNARKs?!

- Can either party carry out private Updates with still being convinced that the updated digest arose out of the pvt. update