Definition 1.1 ***(Weakly verifiable puzzle.)*** *A system for weakly verifiable puzzles consists of algorithms for generating random puzzles and for verifying solutions to these puzzles. The pair of algorithms $Z = (G, V)$ where*

- *The puzzle generator algorithm G, on security parameter k, outputs a random puzzle p along with some check information c, $(p, c) \leftarrow G(1^k)$*
- *The puzzle verifier V is a deterministic efficient algorithm that on input a puzzle p, check information c, and answer a, outputs either zero or one, $V(p, c, a) \in \{0, 1\}$*

A solver for the above puzzle system is an efficient algorithm S that gets a puzzle p as input and outputs an answer a, outputs either zero or one, $V(p, c, a) \in \{0, 1\}$

Definition 1.2 *Dynamic weakly verifiable puzzle A dynamic weakly verifiable puzzle consists of two algorithms P and S. Where S is a problem solver and P is a problem poser. The poser P outputs circuits $\Gamma^V(q, r)$ and $\Gamma^H(q, r)$ where $q \in Q$ (for some well defined set Q). The circuit $\Gamma^V(q, r)$ is used to verify correctness of the solutions r. Additionally, $\Gamma^H(q)$ is a circuit that evaluates a hint function. A solver can make a number of verification and hint queries. A solver successfully solves a DWVP if it makes a successfully verification query for a q when it has not previously asked for verification or hint query on q.*

Definition 1.3 *Interactive weakly verifiable puzzle*

Definition 1.4 *Dynamic interactive weakly verifiable puzzle*