

Definition 1.1 (Dynamic weakly verifiable puzzle) A dynamic weakly verifiable puzzle (DWVP) is defined by a protocol between (P, S) , where P denotes a probabilistic algorithm that is a problem poser, and S is a probabilistic algorithm that solves the problem. The problem poser P outputs circuit Γ_V , which takes as input $q \in Q$ and a solution r , and a circuit Γ_H , which takes as input $q \in Q$. The circuit $\Gamma_V(q, r)$ is used to verify correctness of the solution r . Additionally, $\Gamma_H(q)$ is a circuit that evaluates a hint function. The solver S has oracle access to both circuits Γ_V and Γ_H . The calls to the circuit Γ_V are called verification queries, and the calls to the circuit Γ_H are hint queries. The solver S successfully solves a DWVP Π if it makes a successfully verification query for a $q \in Q$ when it has not previously asked for a hint query on this q .

Let $hash$ be a function $Q \rightarrow \{0, 2(h+v) - 1\}$ that partitions a query space Q into two sets P_{hash} and $Q \setminus P_{hash}$. The set P_{hash} contains elements $q \in Q$ such that $hash(q) = 0$. The elements of P_{hash} are called attacking queries. A *canonical success* with respect to set P_{hash} is a situation when the first successfully verification query is in P_{hash} and all previous hint or verification queries are not in P_{hash} .

Theorem 1.2 (Security amplification for DWVP (non unifrom version)). Let $g : \{0, 1\}^k \rightarrow \{0, 1\}$ be a monotone function, and $hash$ a function such that the probability of a canonical success of a problem solver S with respect to P_{hash} is at least $\frac{\varepsilon}{8(v+h)}$. If there exists a circuit C that makes at most v verification queries and h hint queries and succeeds with probability

$$\Pr[\Gamma_V^{(g)}(\langle P^{(g)}, C \rangle_C) = 1] \geq \Pr_{\mu \leftarrow \mu_\delta^k} [g(u) = 1] + \varepsilon, \quad (0.0.1)$$

where the probability is over random coins of P and C , then there exists a probabilistic algorithm $Gen(C, g, \varepsilon, \delta, n, hash)$ which takes as input a circuit C , a function g , parameters ε, δ, n , a function $hash$, and produce a circuit D such that with high probability it satisfies

$$\Pr[\Gamma^{(1)}(\langle P^1, D \rangle_D) = 1] \geq \frac{1}{8(h+v)} \left(\delta + \frac{\varepsilon}{6k} \right) \quad (0.0.2)$$

where the probability is taken over random coins of D and uniformly chosen random input puzzle.