

Let \mathcal{X} be a finite set and $x \in \mathcal{X}$. We use $x \leftarrow \mathcal{X}$ to denote that x is chosen uniformly at random from \mathcal{X} .

We show that the bound achieved in the Theorem 1.1 is asymptotically optimal. Let us define the following algorithm.

Algorithm Breaker $^{\Gamma_H^{(k)}}(r_B)$

Oracle: A hint circuit $\Gamma_H^{(k)}$ for the k -wise direct product of DWVP.

Input: A bitstring $r_B \in \{0, 1\}^*$.

$q \leftarrow Q$

for all $q \in Q \setminus \{q\}$ **do:**

ask a hint query using oracle Γ_H on q'

With probability $\delta^{(k)}$ ask a verification query $(q, (y_1, \dots, y_k))$

We define the following problem poser for a dynamic weakly verifiable puzzle.

Poser Π_{DWVP}

Input: A bitstring $r_\pi \in \{0, 1\}^n$.

Pick a random permutation $\pi : \{0, 1\}^n \rightarrow \{0, 1\}^n$

Generate hint and verification circuits such that:

$\Gamma_H(q)$ on input $q \in \{0, 1\}^n$ returns $\pi(q)$ or \perp if $q \notin \{0, 1\}^n$

$\Gamma_V(q, (y_1, \dots, y_k))$ on input $q \in \{0, 1\}^n$ returns 1 if for each $1 \leq i \leq k$ we have $\pi_i(q) = y_i$ and 0 otherwise.