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 are interested whether it is possible to improve bound stated in Theorem 1.1. We show that the bound achieved in Theorem 1.1 is asymptotically optimal.

Definition 1.1 *(Black-box reduction)*

Definition 1.2 *(One way permutation) How to generate random permutation in the fly? How to efficiently find a permutation using only n bits of randomness*

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

Poser $\Pi_{DWVP}(r_\pi)$

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

Send 1^n to the problem solver.
Pick a random permutation $\pi : \{0,1\}^n \to \{0,1\}^n$
Generate hint and verification circuits such that:
$\Gamma_H(q)$ on input $q \in \{0,1\}^n$.
$\Gamma_V(q,y)$ on input $q \in \{0,1\}^n$ returns 1 if $\pi(q) = y$ and 0 otherwise.

We denote by $\Pi^{(k)}_{DWVP}$ the k-wise direct product of Π_{DWVP}. Furthermore, let the hint circuit for $\Pi^{(k)}_{DWVP}$ be as follows

$$\Gamma^{(k)}_H(q) := (\Gamma^1_H(q), \ldots, \Gamma^k_H(q))$$

and the verification circuit

$$\Gamma^{(k)}_V(q,(y_1,\ldots,y_k)) := \prod_{i=1}^{k} \Gamma^i_V(q,y_i).$$

We give the description of the following inefficient algorithm Breaker that helps to break the k-wise direct product of Π_{DWVP}.

Algorithm Breaker$^{\Gamma^{(k)}_H}(x, r_B)$

Oracle: A hint circuit $\Gamma^{(k)}_H$ for the k-wise direct product of DWVP.
Input: A bitstring $r_B \in \{0,1\}^*$ and $x \in \{0,1\}^n$.

$q \leftarrow \{0,1\}^n$
for all $q'_i \in \{0,1\}^n \setminus \{q\}$ **do:**
    Ask a hint query on q' using oracle Γ_H
    Let $(y'_1,\ldots,y'_k) := \Gamma^{(k)}_H(q_i)$
    if $(y'_1,\ldots,y'_k) \notin \{0,1\}^n$ **then**
        return $\perp$
    if $\exists j < i : \Gamma^{(k)}_H(q_i) = \Gamma^{(k)}_H(q_j)$ **then**
        return $\perp$
With probability δ^k ask a verification query $(q,(y_1,\ldots,y_k))$ where $(y_1,\ldots,y_k)$ is such that $\forall q' \in \{0,1\}^n \setminus q : \Gamma^k_H(q_i) \neq (y_1,\ldots,y_k)$.

Finally, we define the following polynomial time algorithm A with oracle access to Breaker that solves the k-wise direct product of Π_{DWVP}.

Solver algorithm $A^{\text{Breaker},\Gamma_H^{(k)},\Gamma_V^{(k)}}$

Oracle: A hint circuit $\Gamma_H^{(k)}$ and a verification circuit $\Gamma_V^{(k)}$ for $\Pi_{DWVP}^{(k)}$, an algorithm Breaker.
Input: Bitstrings $x \in \{0,1\}^n$ and $\rho \in \{0,1\}^*$

Let $(q, (y_1, \ldots, y_k)) := \text{Breaker}^{\Gamma_H^{(k)}}(x, \rho)$.
if $(q, (y_1, \ldots, y_k)) \neq \perp$ **then**
ask a verification query $(q, (y_1, \ldots, y_k))$ to $\Gamma_V^{(k)}$.

It is clear that the success probability of A in solving a puzzle defined by $\Pi_{DWVP}^{(k)}$ is δ^k.

Theorem 1.3 *There exists no black-box reduction from solving the k-wise direct product $\Pi_{DWVP}^{(k)}$ with probability δ^k to solving a dynamic weakly verifiable puzzle defined by Π_{DWVP} with probability at least δ.*

Lemma 1.4 *Let S be a solver for Π_{DWVP} with oracle access to Breaker and hint and verification oracles for*