

**Definition 1.1 (Dynamic weakly verifiable puzzle.)** A dynamic weakly verifiable puzzle (DWVP) is defined by a probabilistic algorithm  $P$  called a problem poser. We denote the randomness  $P$  uses by  $\pi$ . A problem solver  $S = (S_1, S_2)$  is a probabilistic two phase algorithm. The randomness used by  $S$  is denoted by  $\rho$ . In the first phase  $P(\pi)$  interacts with  $S_1(\rho)$ . As the result of the interaction  $P(\pi)$  outputs circuits  $\Gamma_V, \Gamma_H$ , a puzzle  $x \in \{0, 1\}^*$ . The solver  $S_1(\rho)$  produces no output. The circuit  $\Gamma_V$  takes as input  $q \in Q$ , an answer  $y \in \{0, 1\}^*$ , and outputs 1 if  $y$  is a correct solution of  $x$  for  $q$  and 0 otherwise. The circuit  $\Gamma_H$  on input  $q \in Q$  outputs a hint such that  $\Gamma_V(q, \Gamma_H(q)) = 1$ . In the second phase  $S_2$  takes as input  $x$ , and has oracle access to  $\Gamma_V$  and  $\Gamma_H$ . The execution of  $S_2$  with the input  $x$  and the randomness  $\rho$  is denoted by  $S_2(x, \rho)$ . The queries of  $S_2$  to  $\Gamma_V$  are called verification queries, and to  $\Gamma_H$  hint queries. The algorithm  $S_2$  can ask at most  $h$  hint queries,  $v$  verification queries, and successfully solves the puzzle if and only if it makes a verification query  $(q, y)$  such that  $\Gamma_V(q, y) = 1$ , when it has not previously asked for a hint query on  $q$ .

**Definition 1.2 ( $k$ -wise direct-product of DWVPs.)** Let  $g : \{0, 1\}^k \rightarrow \{0, 1\}$  be a monotone function and  $P^{(1)}$  a problem poser as in Definition 1.1. The  $k$ -wise direct product of  $P^{(1)}$  is a DWVP defined by a probabilistic algorithm  $P^{(g)}$ . Let  $\pi^{(k)} := (\pi_1, \dots, \pi_k)$  be the randomness used by  $P^{(g)}$ , and  $P^{(g)}(\pi^{(k)})$  denote the execution of  $P^{(g)}$  with the randomness  $\pi^{(k)}$ . A solver  $S := (S_1, S_2)$  is a probabilistic algorithm. In the first phase  $P$  interacts with  $S_1$ . As the result of the interaction  $P^{(g)}$  outputs: a verification circuit

$$\Gamma_V^{(g)}(q, y_1, \dots, y_k) := g(\Gamma_V^1(q, y_1), \dots, \Gamma_V^k(q, y_k)),$$

a hint circuit

$$\Gamma_H^{(k)}(q) := (\Gamma_H^1(q), \dots, \Gamma_H^k(q)),$$

and a puzzle  $x^{(k)} := (x_1, \dots, x_k)$ , where the  $i$ -th instance  $(x_i, \Gamma_V^i, \Gamma_H^i) := \langle P^{(1)}(\pi_i), S_1(\rho) \rangle_{P^{(1)}}$ .