

Judge J	Inverter I	virtual A
sample uniform $x \in \{0, 1\}^k$ $y := f(x)$	<div> <div> ▶ $J.y$ </div> <div> ▶ \tilde{m} </div> <div> unpack $\tilde{m} =: b_1 \ b_2 \ \dots \ b_k$ </div> <div> for $i = 1 \dots k$ do </div> <div> sample $r_i^0 \in \{0, 1\}^k$ </div> <div> sample $r_i^1 \in \{0, 1\}^k$ </div> <div> compute $f_i^0 := f(r_i^0)$ </div> <div> compute $f_i^1 := f(r_i^1)$ </div> <div> sample $j \in [k]$ </div> <div> reassign $f_j^{1-b_j} := J.y$ </div> <div> $\tilde{\sigma} := r_1^{b_1} \ r_2^{b_2} \ \dots \ r_k^{b_k}$ </div> <div> $pk := \begin{pmatrix} f_1^0 & f_2^0 & \dots & f_k^0 \\ f_1^1 & f_2^1 & \dots & f_k^1 \end{pmatrix}$ </div> <div> ▶ (m, σ) </div> <div> unpack $\sigma =: s_1 \ s_2 \ \dots \ s_k$ </div> <div> $x := s_j$ </div> </div>	<div> <div> select \tilde{m} </div> <div> ▶ $pk, \tilde{\sigma}$ forge (m, σ) </div> </div>
<div> ▶ $I.x$ </div> <div> return $y \stackrel{?}{=} f(I.x)$ </div>		