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