

J
<p>► $B.m_1, \dots, B.m_\ell$ $(sk, pk) := \text{gen}(1^k)$ for $i = 1 \dots \ell$: $\sigma_i := \text{sgn}(sk, B.m_i)$</p> <p>► $B.m, B.\sigma$ return $\text{vrf}(pk, B.m, B.\sigma)$ $\wedge (\forall i \in [\ell], B.m \neq B.m_i)$</p>

B	virtual A
► m_1, \dots, m_ℓ	select m_1, \dots, m_ℓ
► $J.pk$ ► $J.\sigma_1, \dots, J.\sigma_\ell$ sample $a \in \{0, 1\}^k$ sample $b \in \{0, 1\}^k \setminus \{a\}$ $pk' := J.pk \ a \ b$ for $i = 1 \dots \ell$: if $m_i = a$ then fail else $\sigma'_i := \sigma_i \ 0$	
	► pk' ► $\sigma'_1, \dots, \sigma'_\ell$
► (m, σ') unpack $\sigma' =: \sigma \ \eta$	forge (m, σ')