Judge J	**Adversary** B	**virtual** A
	▶ $m_1, \ldots, m_\ell$	select $m_1, \ldots, m_\ell$
	for $i = 0 \ldots \ell$**:** $(sk_i, pk_i) := \mathtt{gen}(1^k)$	
	sample $t \in [\ell]$	
	$\widetilde{m} := m_t \| pk_t$	
▶ $B.\widetilde{m}$		
$(sk, pk) := \mathtt{gen}(1^k)$		
$\widetilde{\sigma} := \mathtt{sgn}(sk, B.m_i)$		
	▶ $J.pk,\ J.\widetilde{\sigma}$	
	$pk_{t-1} := pk$	

	for $i = 1 \ldots \ell$**:**
	  if $i = t$ **then** $\eta_i := J.\widetilde{\sigma}$
	  else $\eta_i := \mathtt{sgn}(sk_{i-1}, m_i \| pk_i)$
	  $\sigma_i := (m_j \| pk_j \| \eta_j)_{1 \le j \le i}$	

		▶ $pk_0, \sigma_1, \ldots, \sigma_\ell$
		forge (m', σ')
	▶ (m', σ')	
	unpack $\sigma' =: (m'_j \| pk'_j \| \eta'_j)_{1 \le j \le i'}$	
	$m := m'_t \| pk'_t$	
	$\sigma := \eta'_t$	
▶ $B.m, B.\sigma$		
return $\mathtt{vrf}(pk, B.m, B.\sigma)$ $\wedge (B.m \neq B.\widetilde{m})$		