$\exists$CM attack on Σ

Judge J	**Adversary** B	virtual A
▶ $m_1, \ldots, m_\ell$	▶ $m_1, \ldots, m_\ell$	select $m_1, \ldots, m_\ell$
$(sk, pk) := \texttt{gen}(1^k)$ **for** $i = 1 \ldots \ell$: $\sigma_i := \texttt{sgn}(sk, m_i)$		
	▶ $pk, \sigma_1, \ldots, \sigma_\ell$	

	sample $a \in \{0,1\}^k$
	sample $b \in \{0,1\}^k \setminus \{a\}$
	$pk' := pk \| a \| b$
	for $i = 1 \ldots \ell$:
	    if $m_i = a$ **then fail**
	    else $\sigma_i' := \sigma_i \| \mathbf{0}$	

		▶ $pk', \sigma_1', \ldots, \sigma_\ell'$
	▶ (m, σ')	forge (m, σ')
	unpack $\sigma' =: \sigma \| \eta$	
▶ m, σ		
return $\texttt{vrf}(pk, m, \sigma)$ $\wedge(\forall i \in [\ell],\ m \neq m_i)$		

$\exists$CM attack on Σ'