$\exists\mathsf{CM}^-$ attack on Σ

J	B	virtual A
	▶ $m_1, \ldots, m_l$	select $m_1, \ldots, m_l$
▶ $B.m_1, \ldots, B.m_l$		
$(sk, pk) := \mathtt{gen}(1^k)$		
for $i = 1 \ldots l$:		
$\quad \sigma_i := \mathtt{sgn}(sk, B.m_i)$		
	▶ $J.pk$	
	▶ $J.\sigma_1, \ldots, J.\sigma_l$	
	sample $a \in \{0,1\}^k$	
	sample $b \in \{0,1\}^k \setminus \{a\}$	
	$pk' := J.pk \| a \| b$	
	for $i = 1 \ldots l$:	
	$\quad$ **if** $m_i = a$ **then fail**	
	$\quad$ **else** $\sigma'_i := \sigma_i \| \mathbf{0}$	
		▶ pk'
		▶ $\sigma'_1, \ldots, \sigma'_l$
	▶ (m, σ')	forge (m, σ')
	unpack $\sigma' =: \sigma \| \eta$	
▶ $B.m, B.\sigma$		
return $\mathtt{vrf}(pk, B.m, B.\sigma)$		
$\quad \wedge (\forall i \in [l],\ B.m \neq B.m_i)$		

$\exists\mathsf{CM}^-$ attack on Σ'