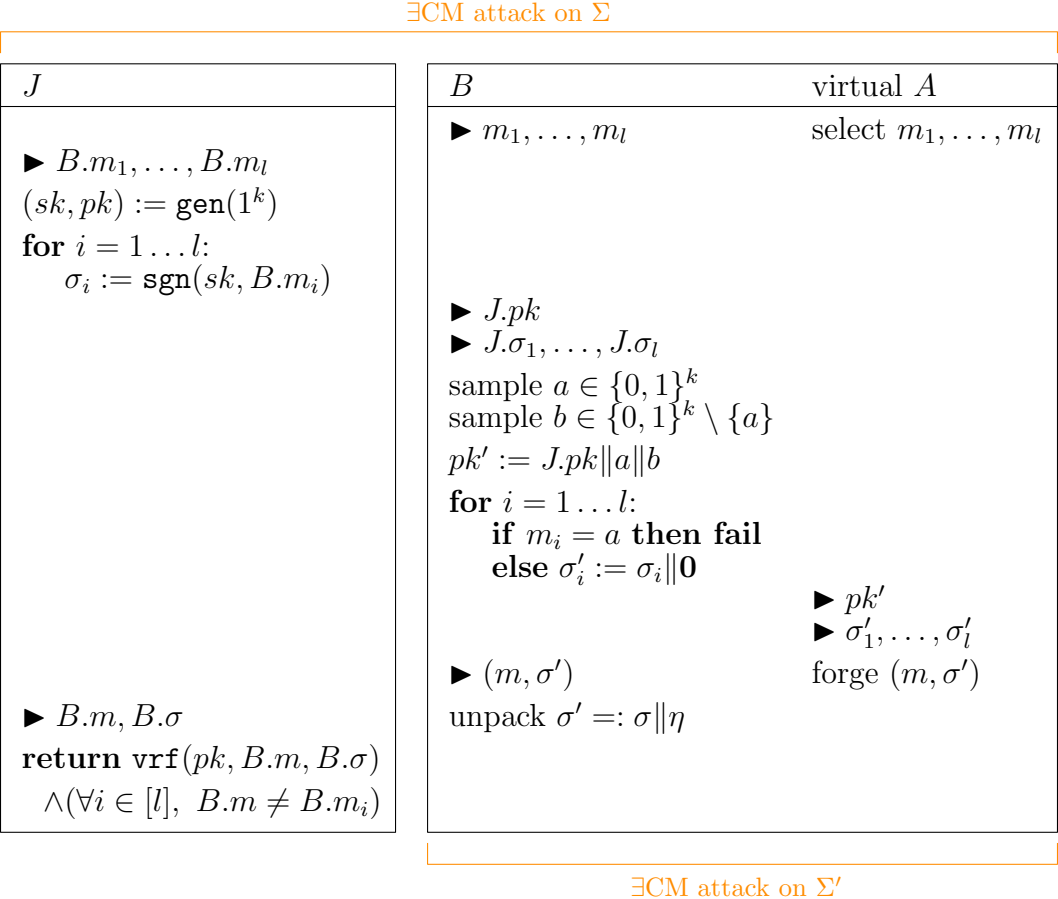
∃CM attack on Σ
J
B
virtual A
▶ m1, . . . , ml
select m1, . . . , ml
▶ B.m1, . . . , B.ml
(sk, pk) := gen(1^k)
for i = 1 . . . l:
σi := sgn(sk, B.mi)
▶ J.pk
▶ J.σ1, . . . , J.σl
sample a ∈ {0, 1}^k
sample b ∈ {0, 1}^k \ {a}
pk′ := J.pk‖a‖b
for i = 1 . . . l:
if mi = a then fail
else σ′i := σi‖0
▶ pk′
▶ σ′1, . . . , σ′l
▶ B.m, B.σ
return vrf(pk, B.m, B.σ)
∧(∀i ∈ [l], B.m ≠ B.mi)
▶ (m, σ′)
forge (m, σ′)
unpack σ′ =: σ‖η
∃CM attack on Σ′