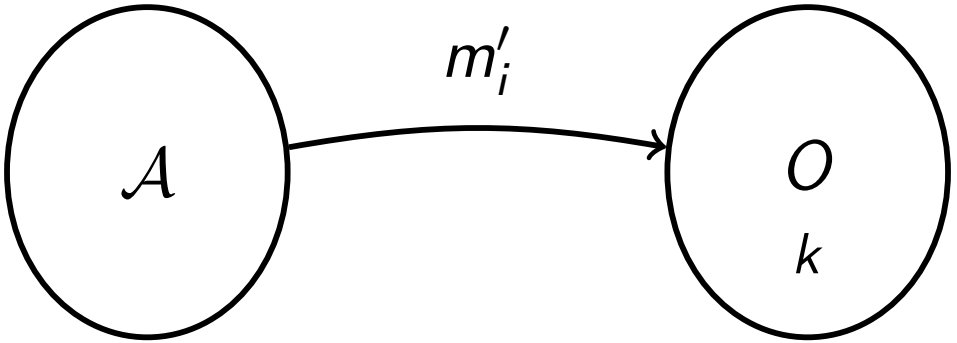
What does the adversary look like?

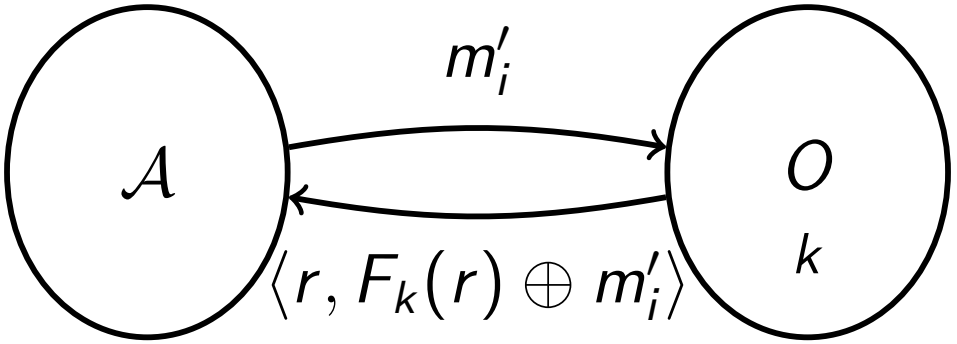
What does the adversary look like?

Query phase 1

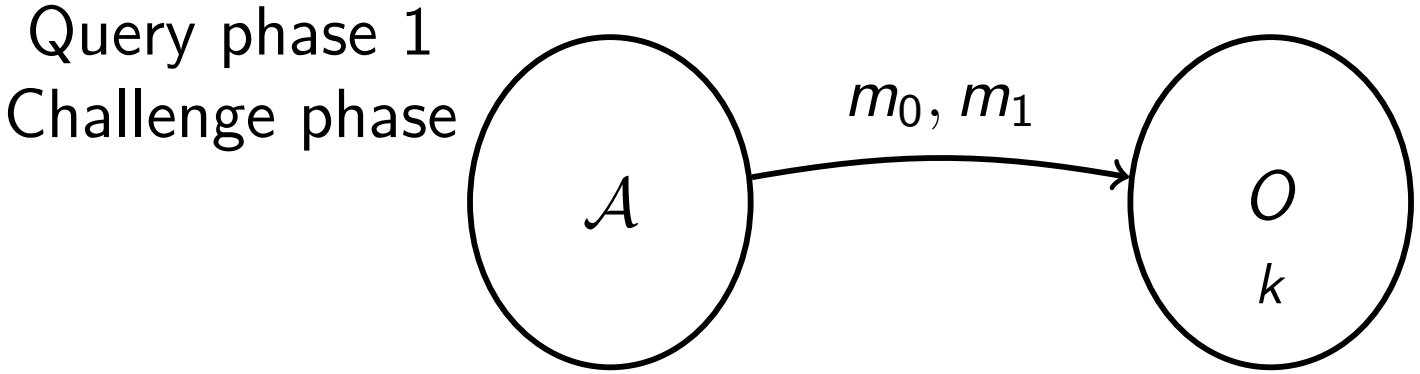


What does the adversary look like?

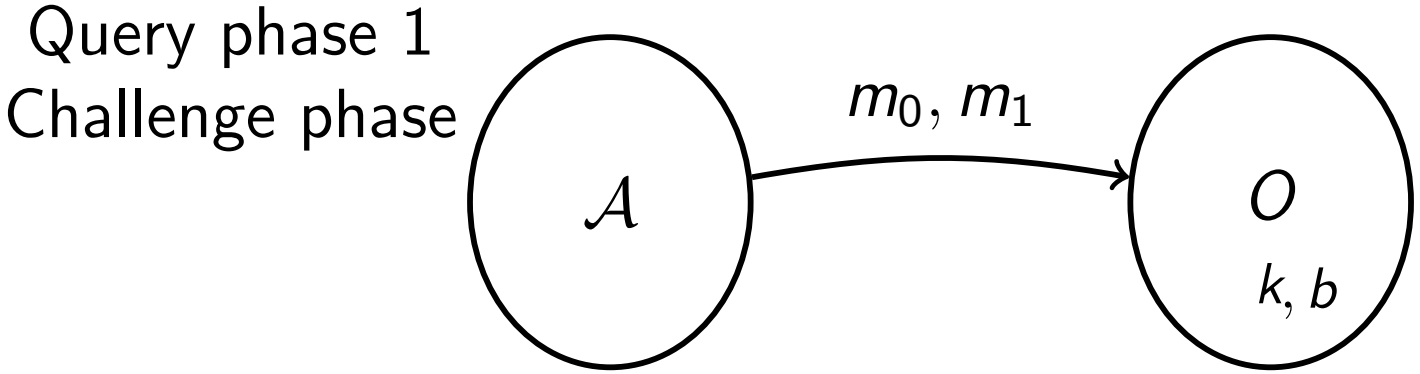
Query phase 1



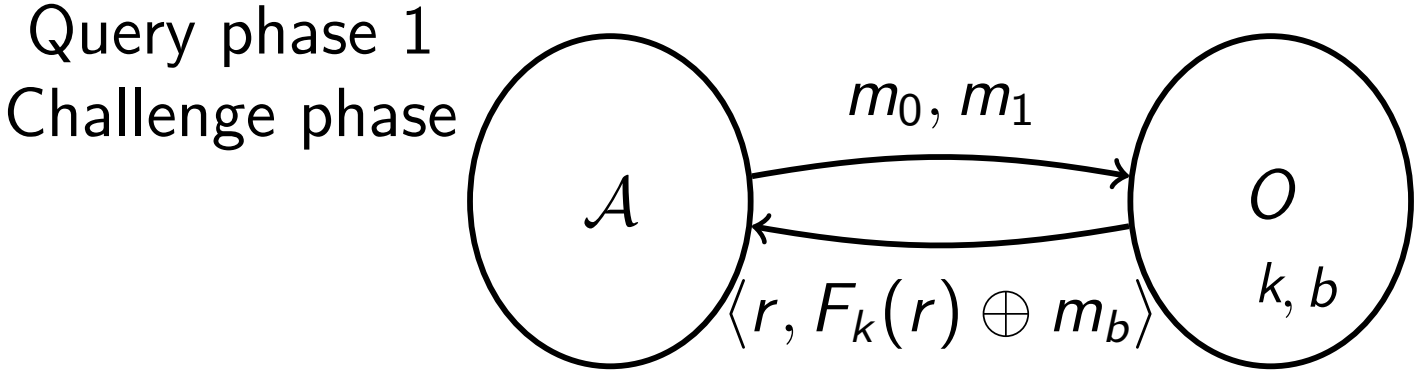
What does the adversary look like?



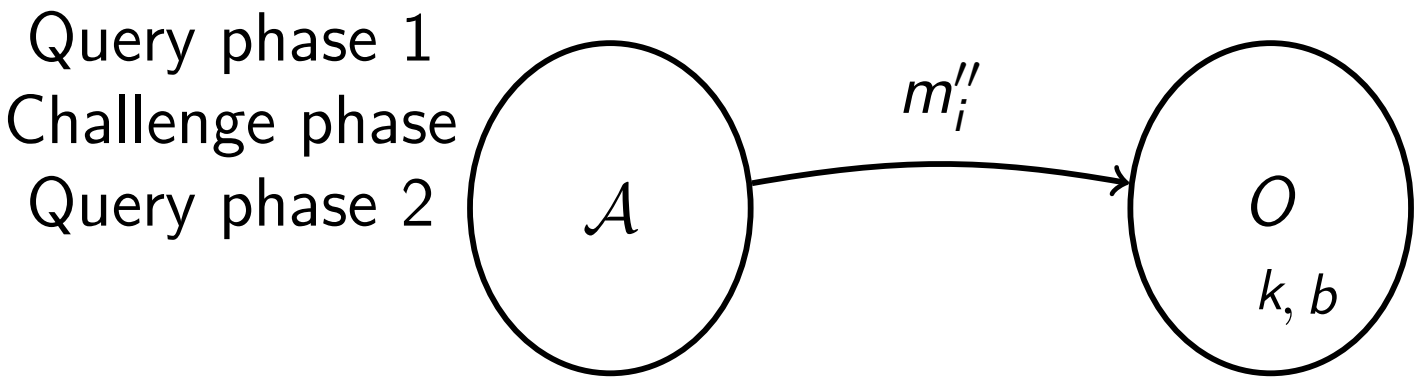
What does the adversary look like?



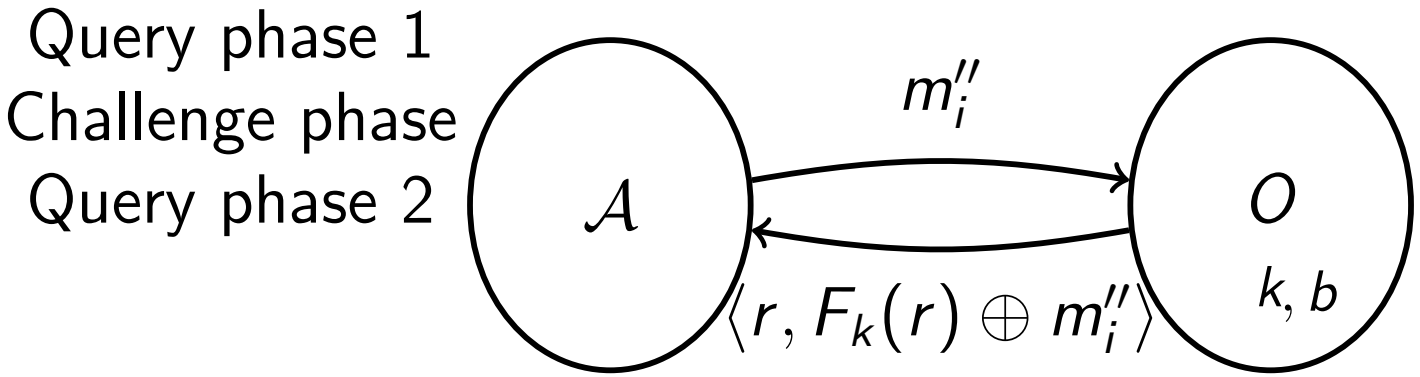
What does the adversary look like?



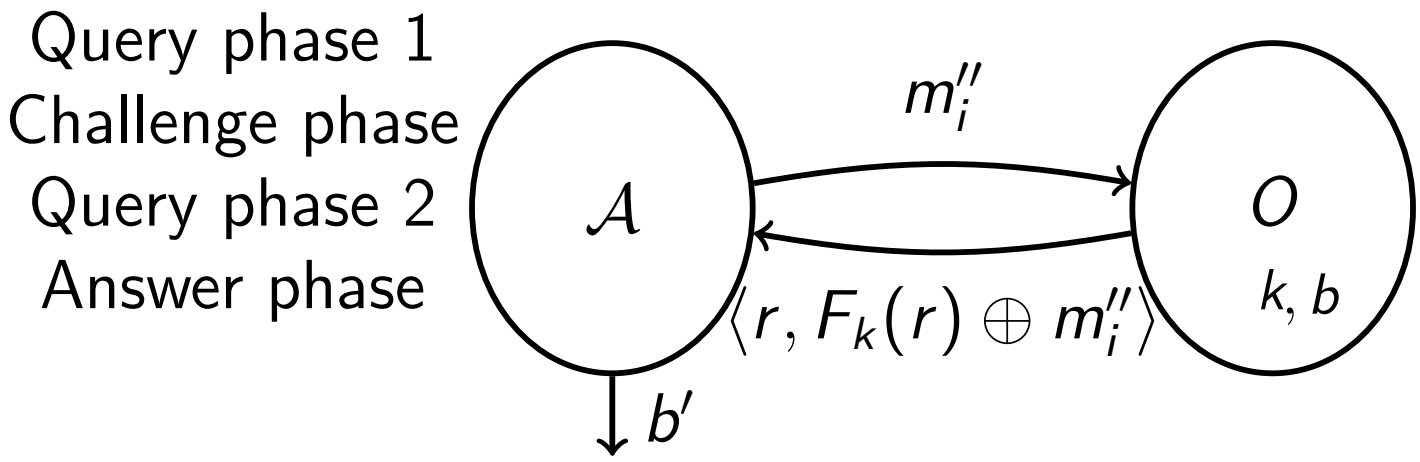
What does the adversary look like?



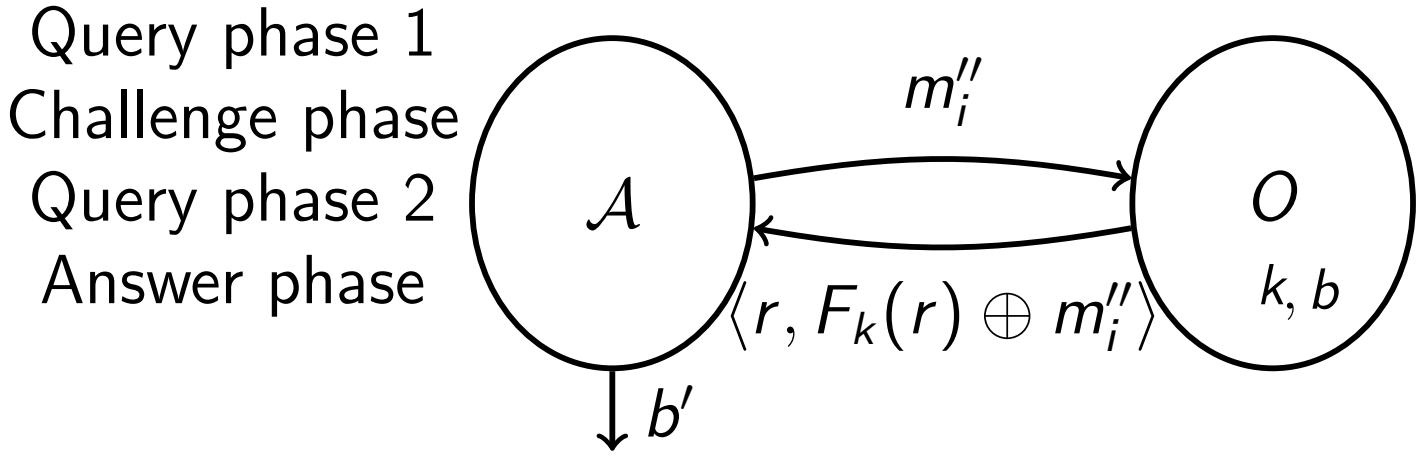
What does the adversary look like?



What does the adversary look like?

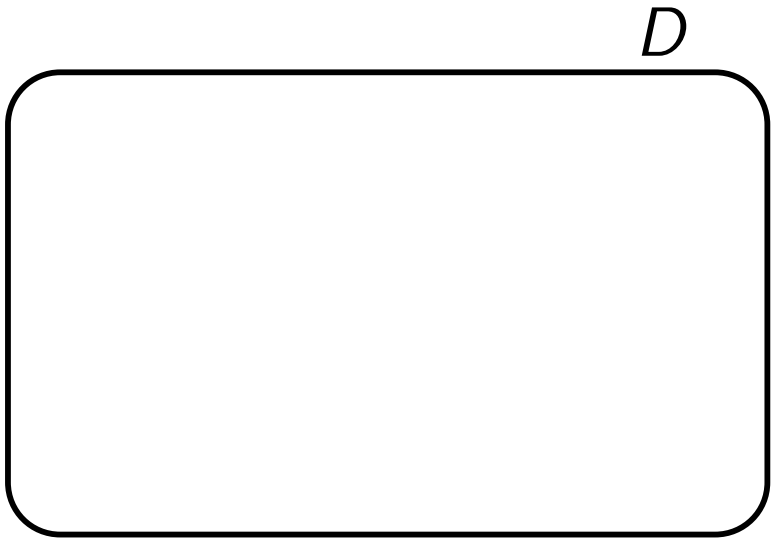


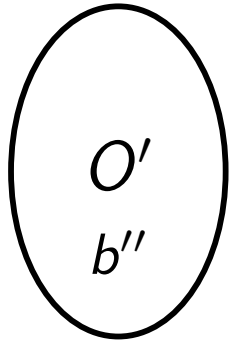
What does the adversary look like?



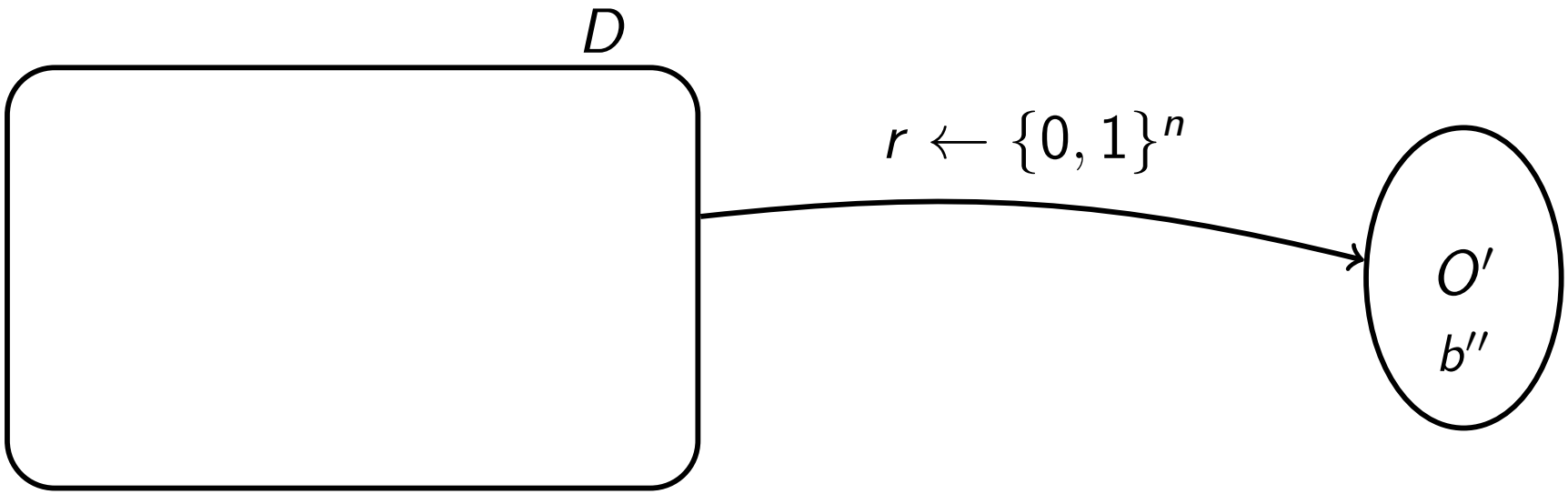
By assumption, $\Pr[b = b'] = \frac{1}{2} + \eta(n)$, with η non-negligible.

What distinguisher must we build?



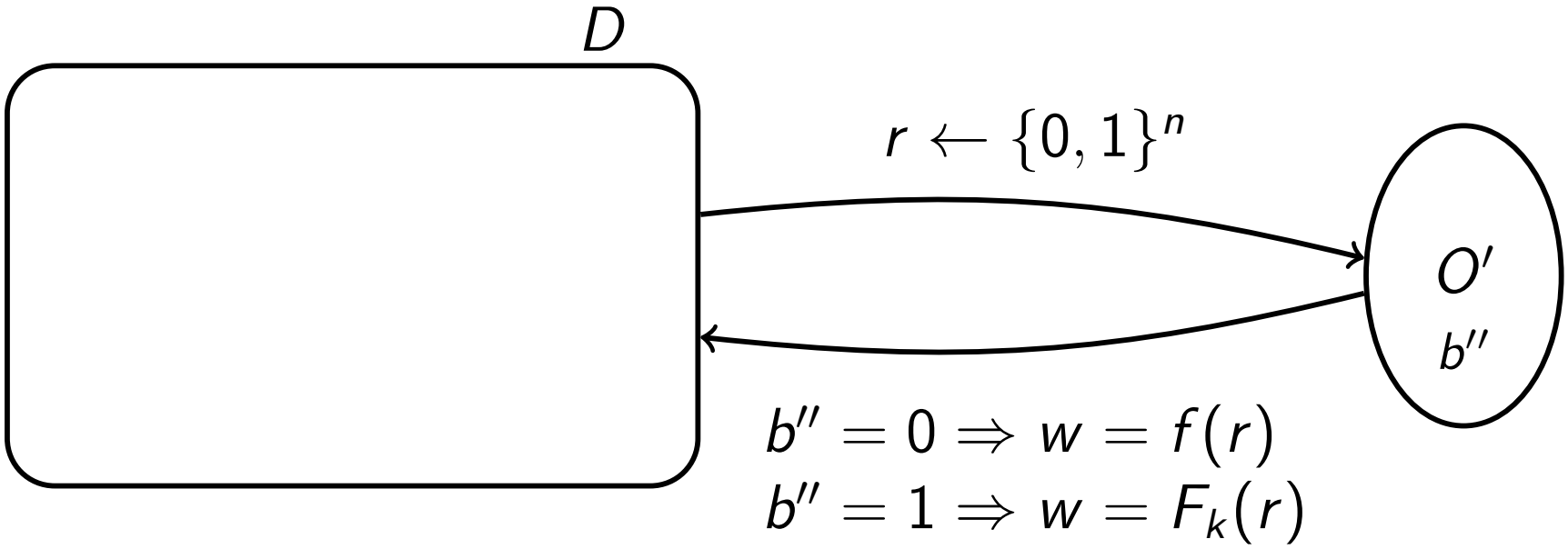


What distinguisher must we build?



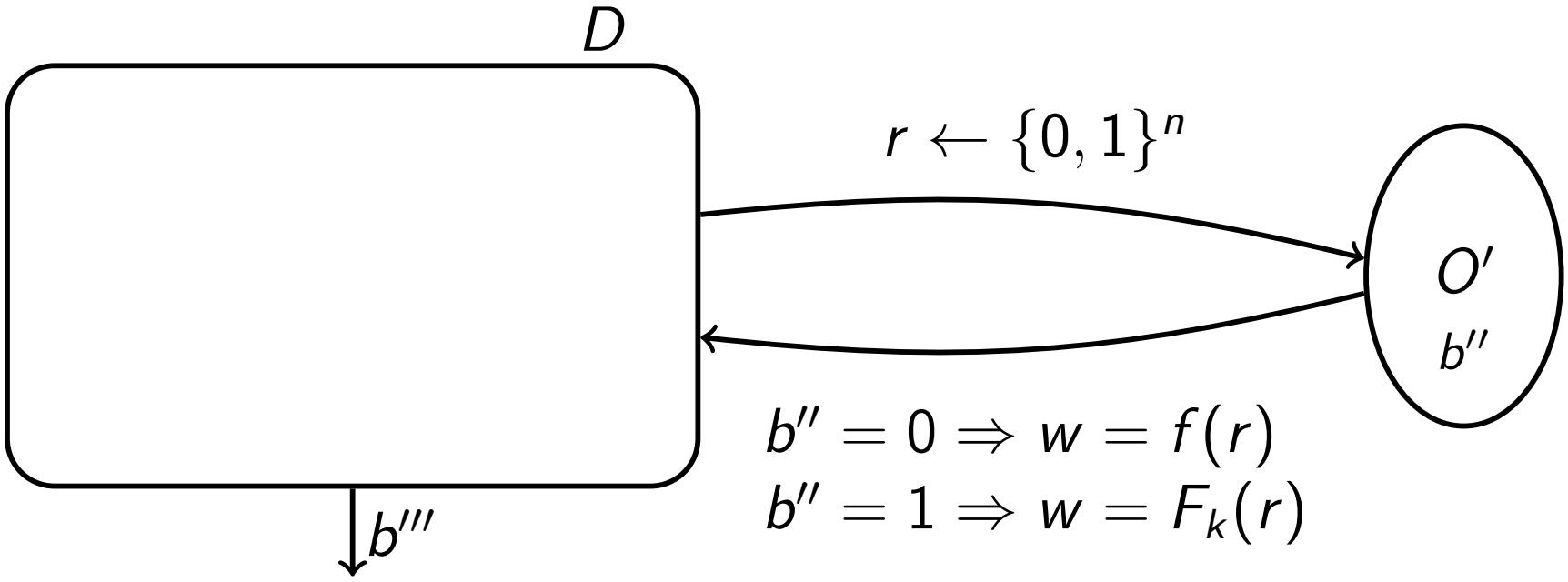
Query phase

What distinguisher must we build?



Query phase

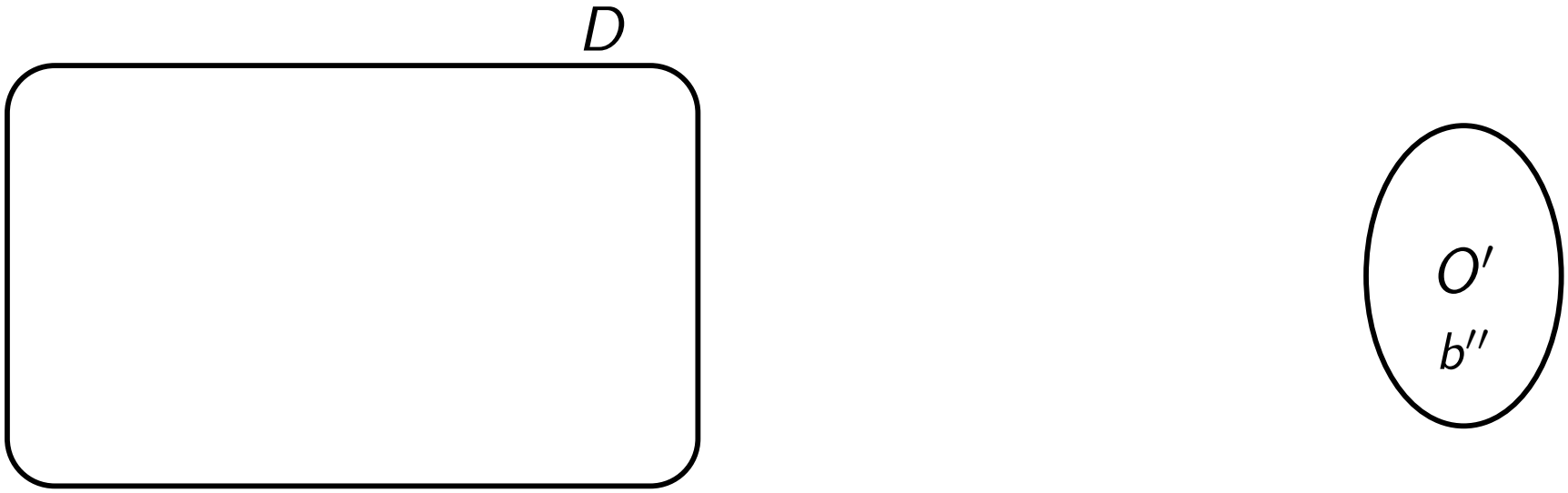
What distinguisher must we build?



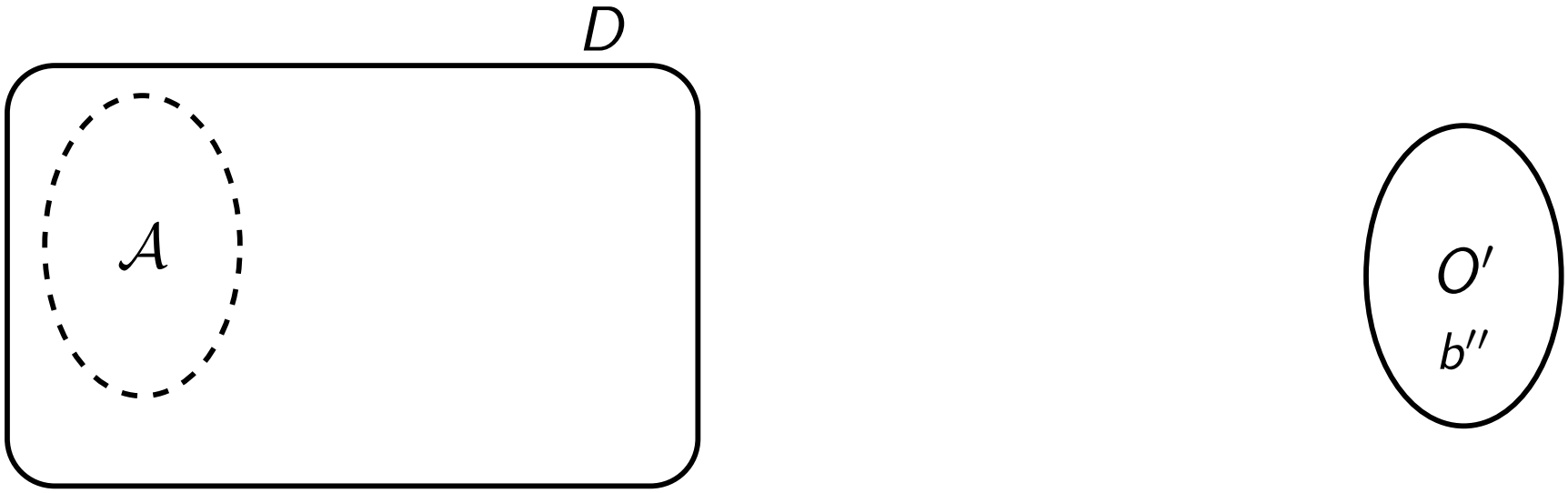
Query phase

Answer phase

Reduction

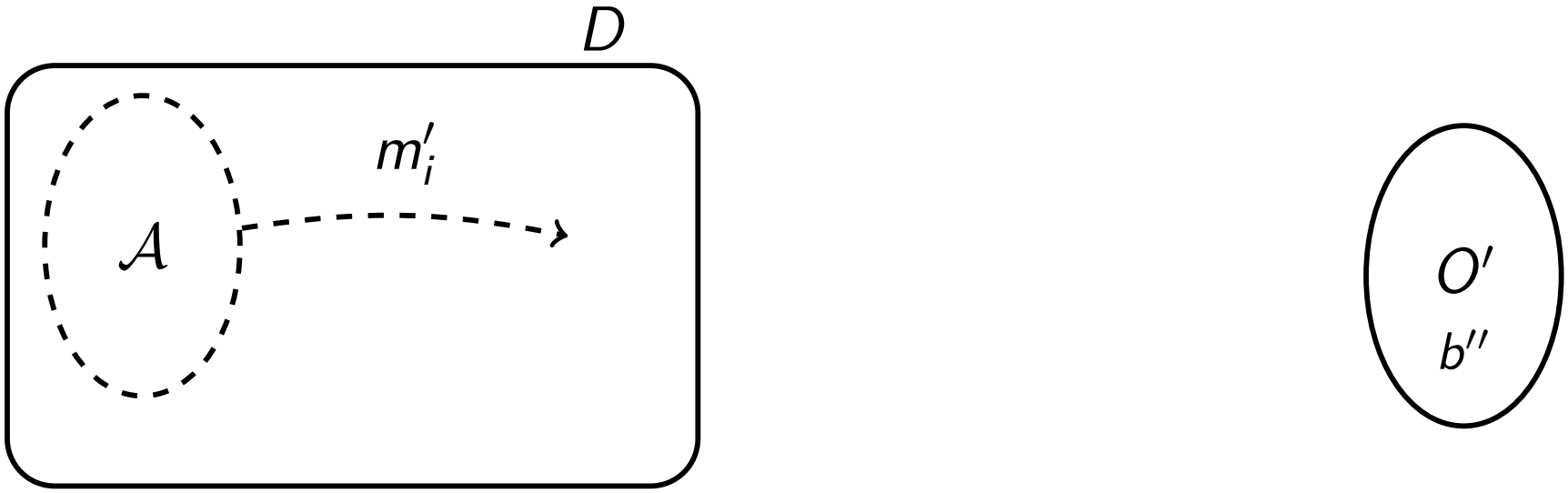


Reduction



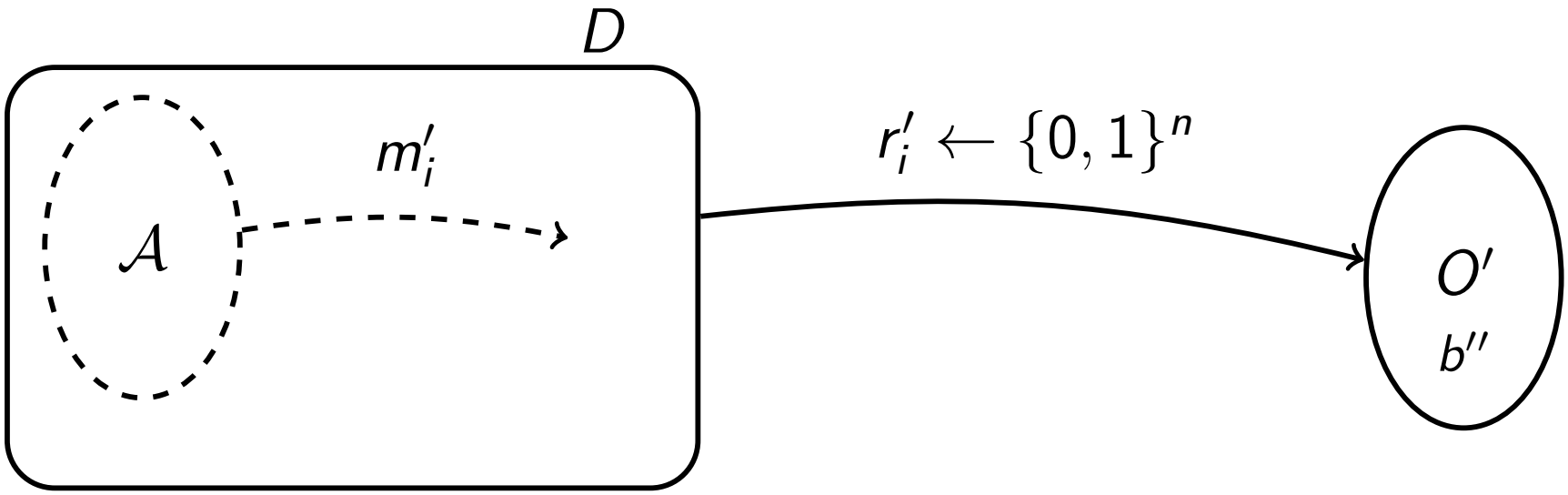
Reduction

Query phase 1



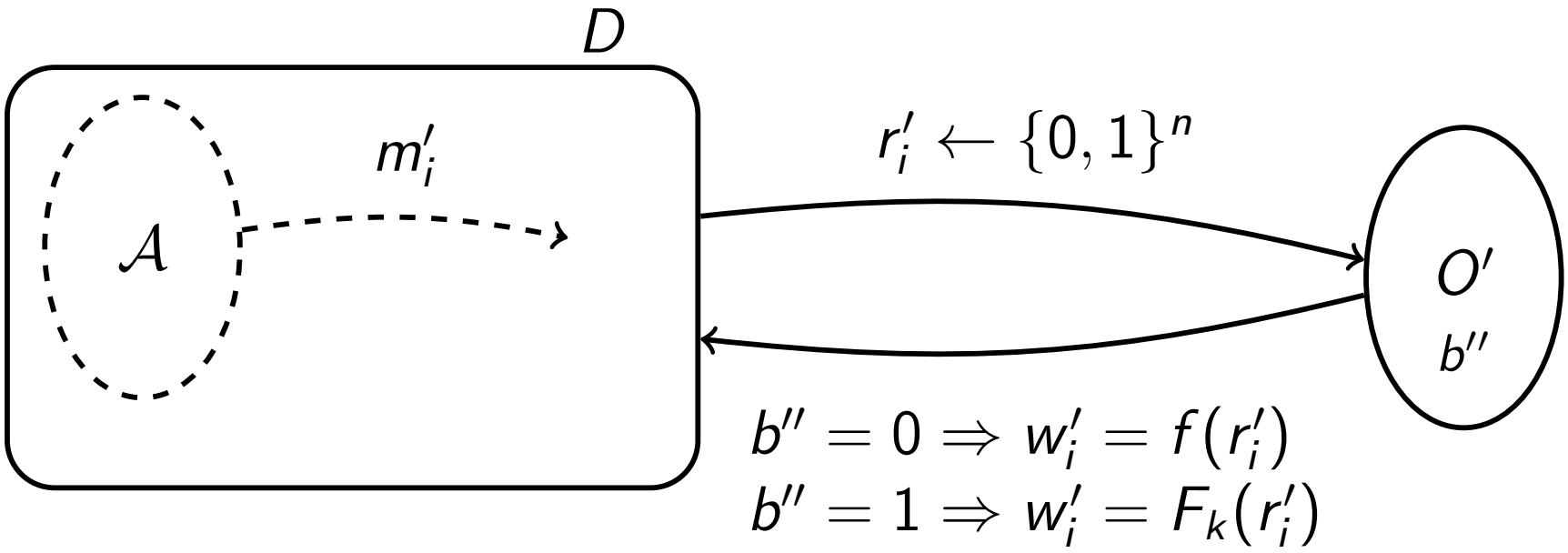
Reduction

Query phase 1



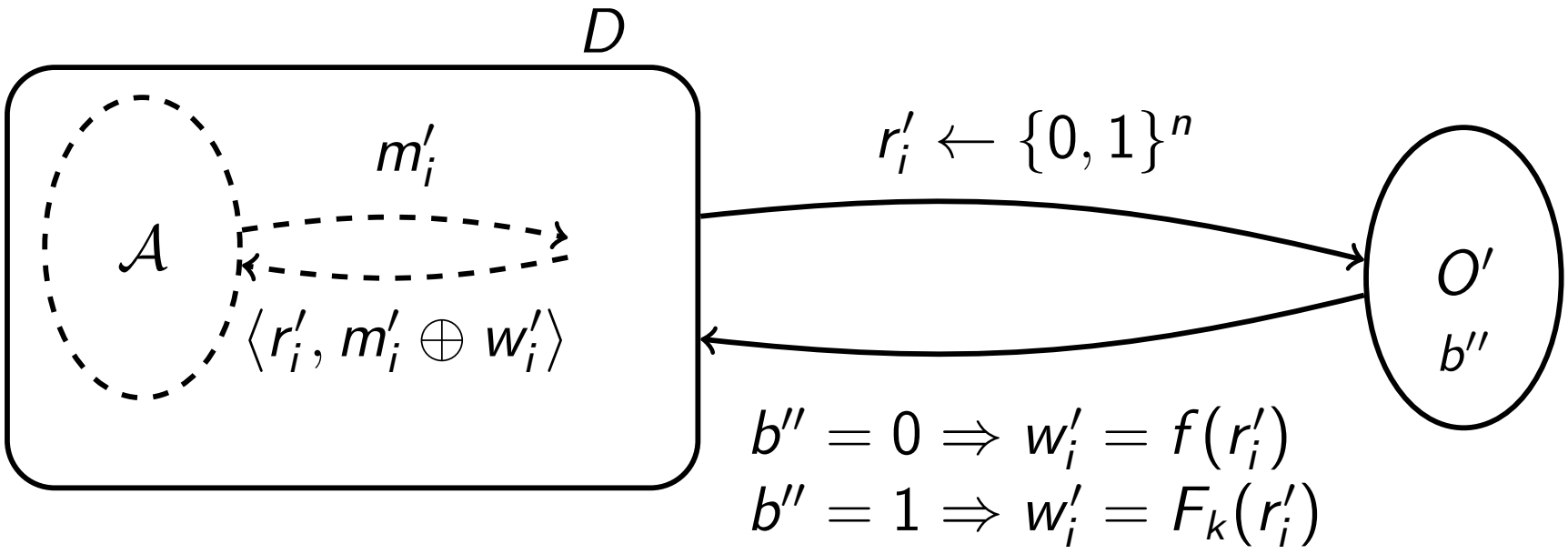
Reduction

Query phase 1



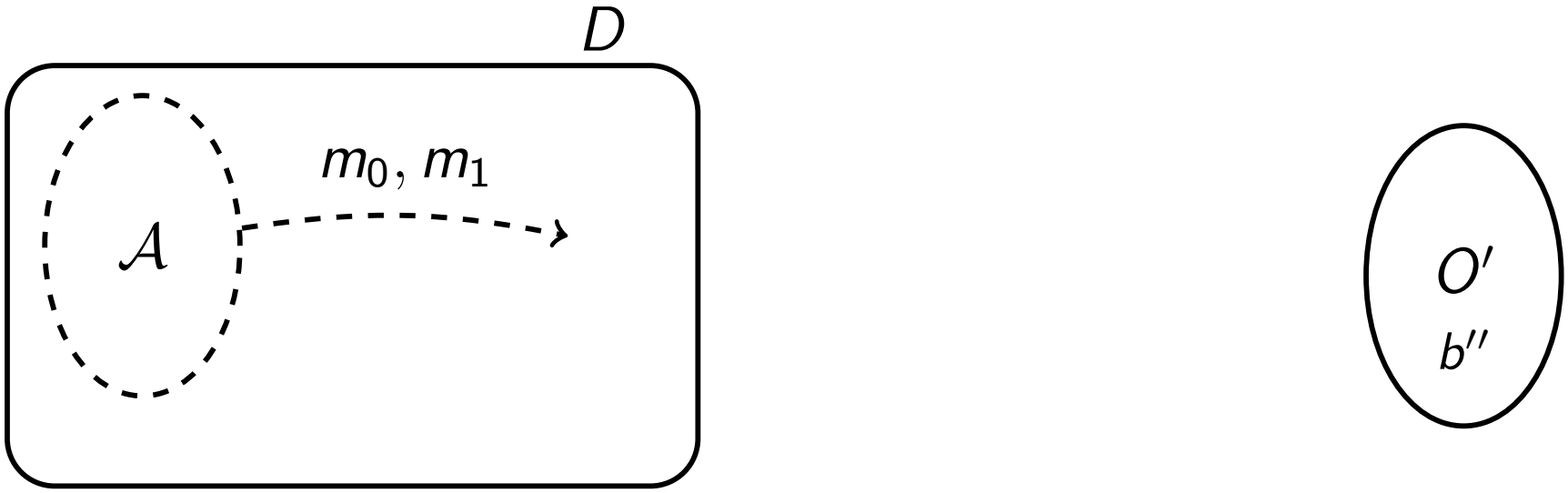
Reduction

Query phase 1



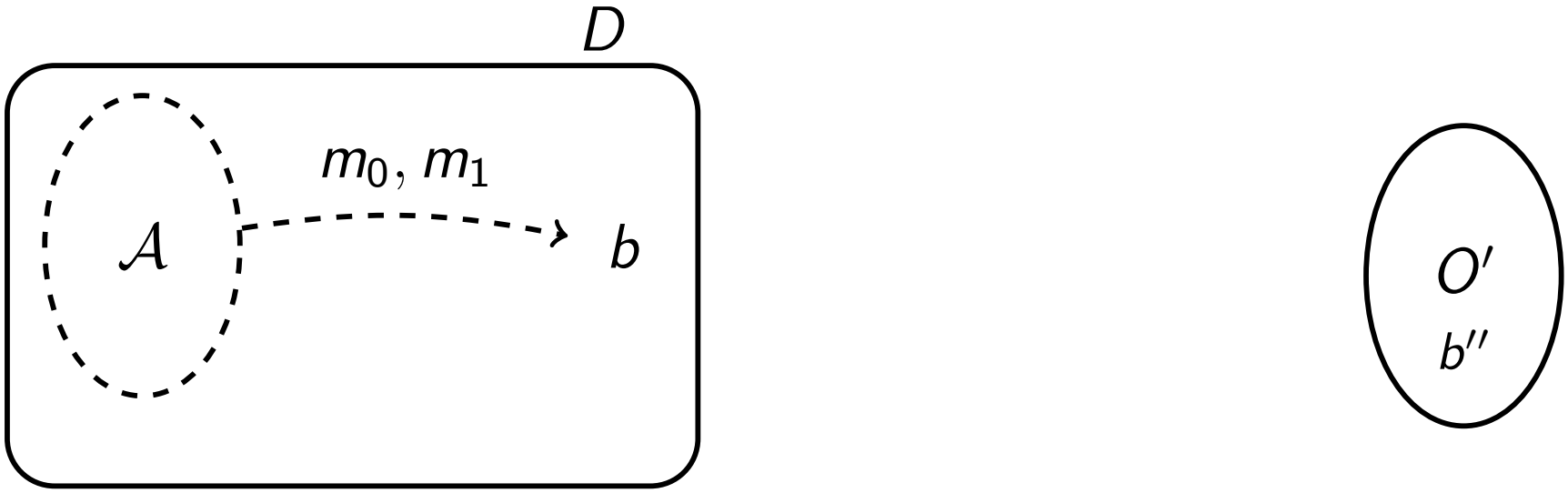
Reduction

Challenge phase



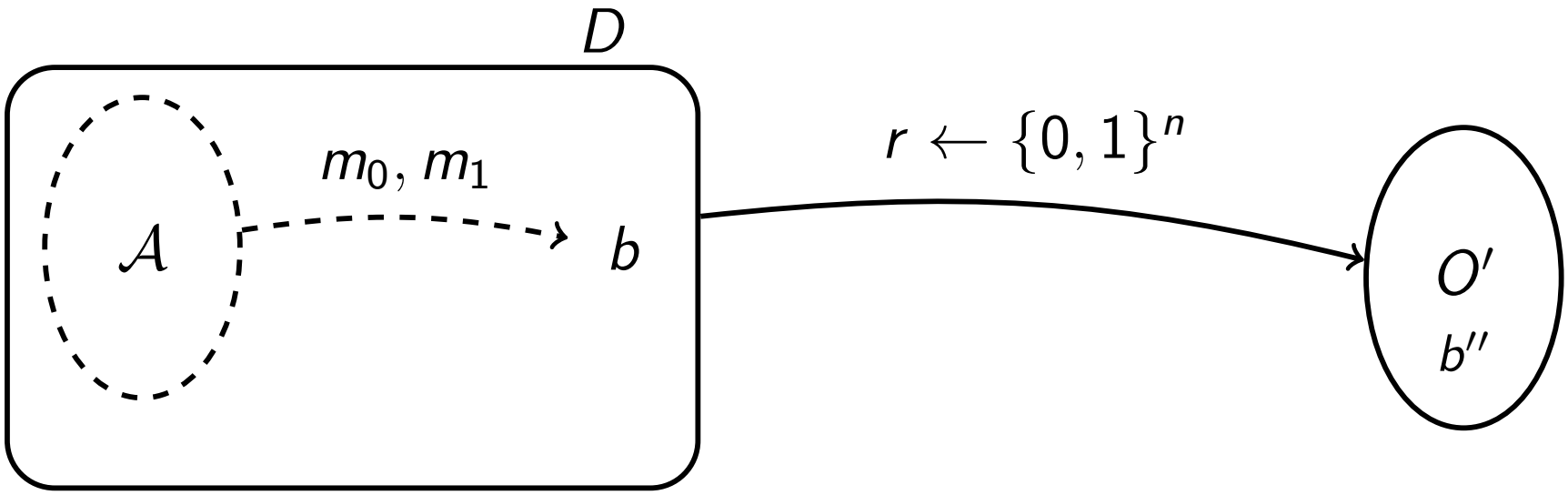
Reduction

Challenge phase



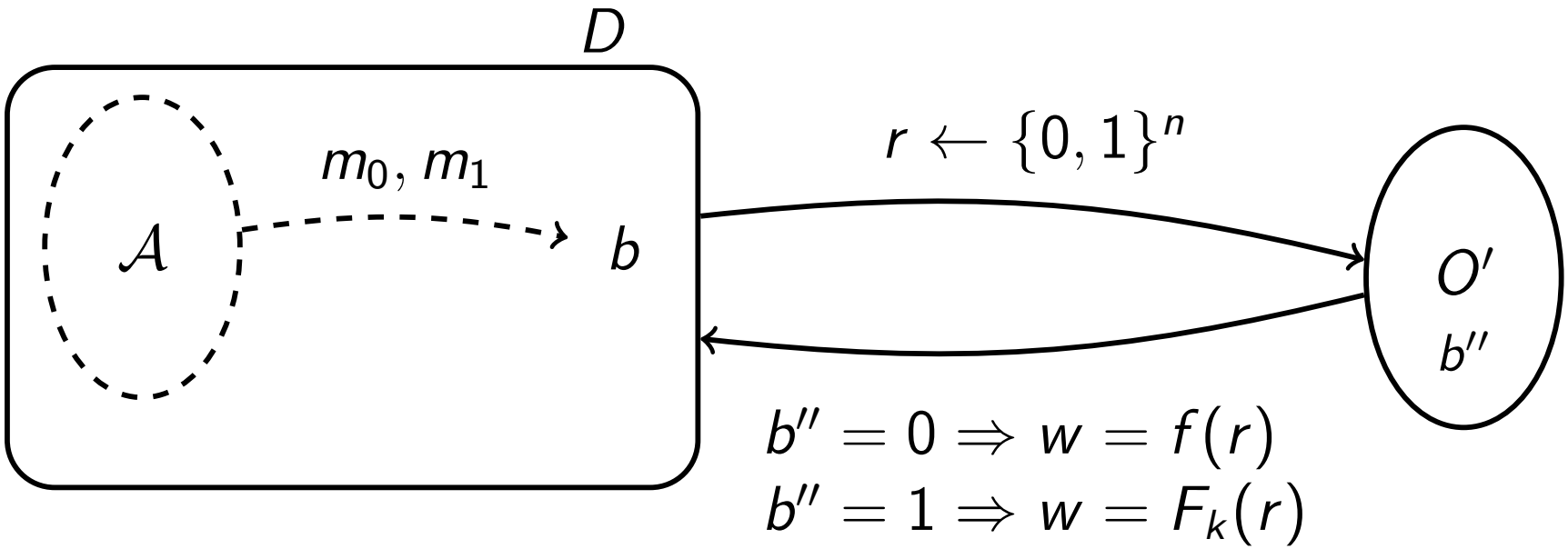
Reduction

Challenge phase



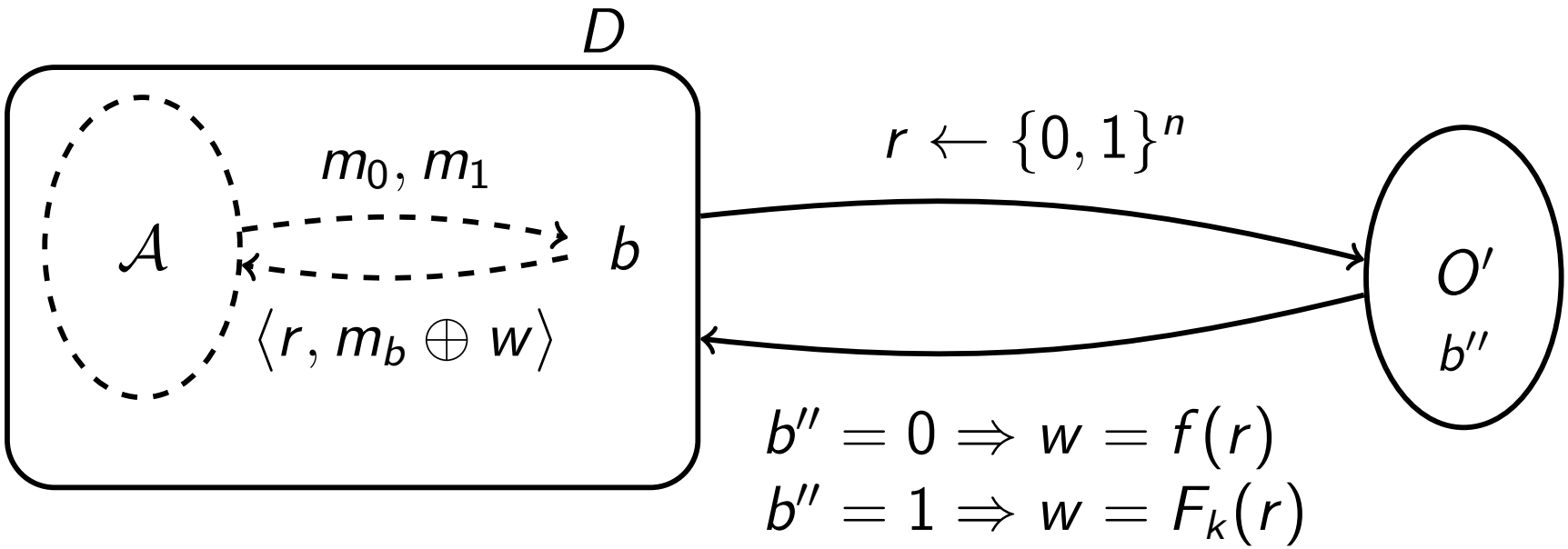
Reduction

Challenge phase

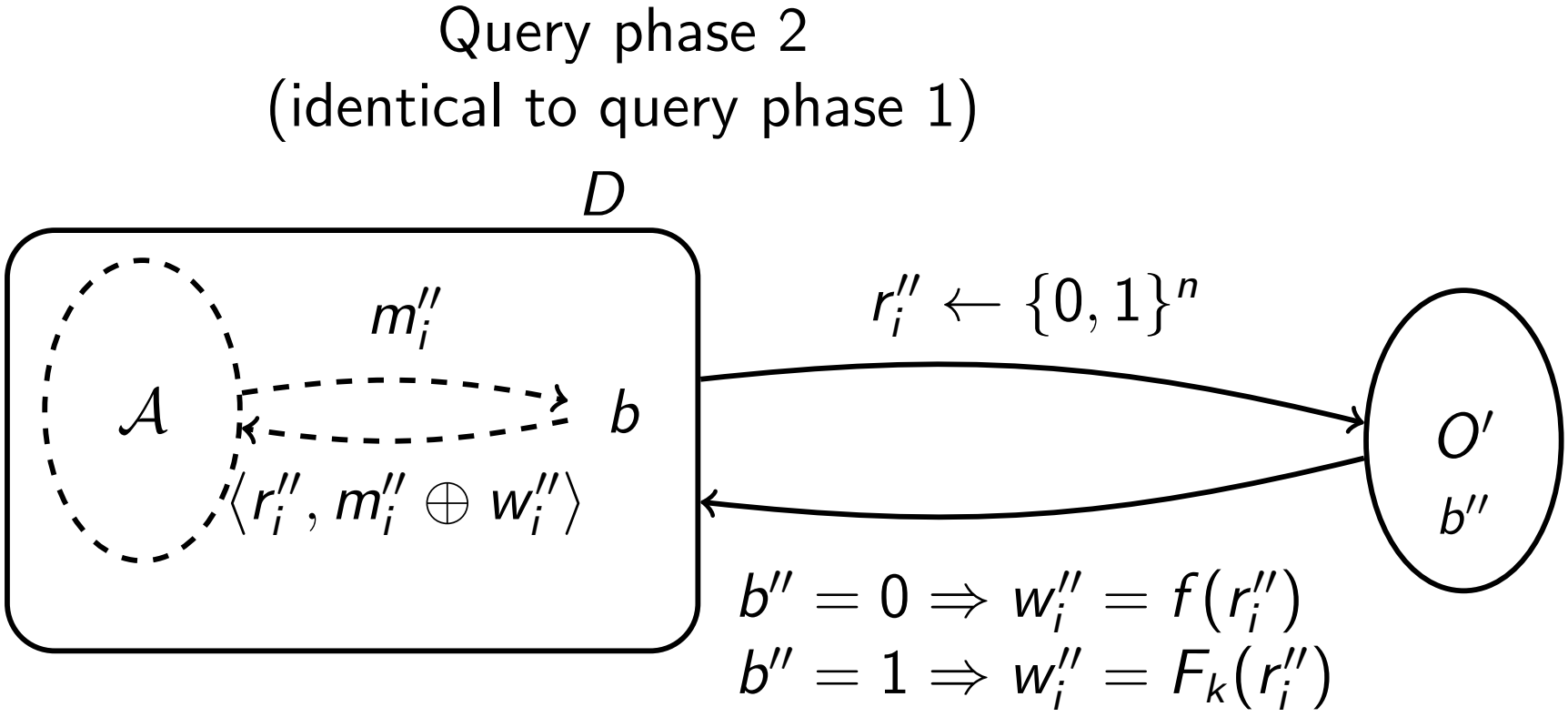


Reduction

Challenge phase

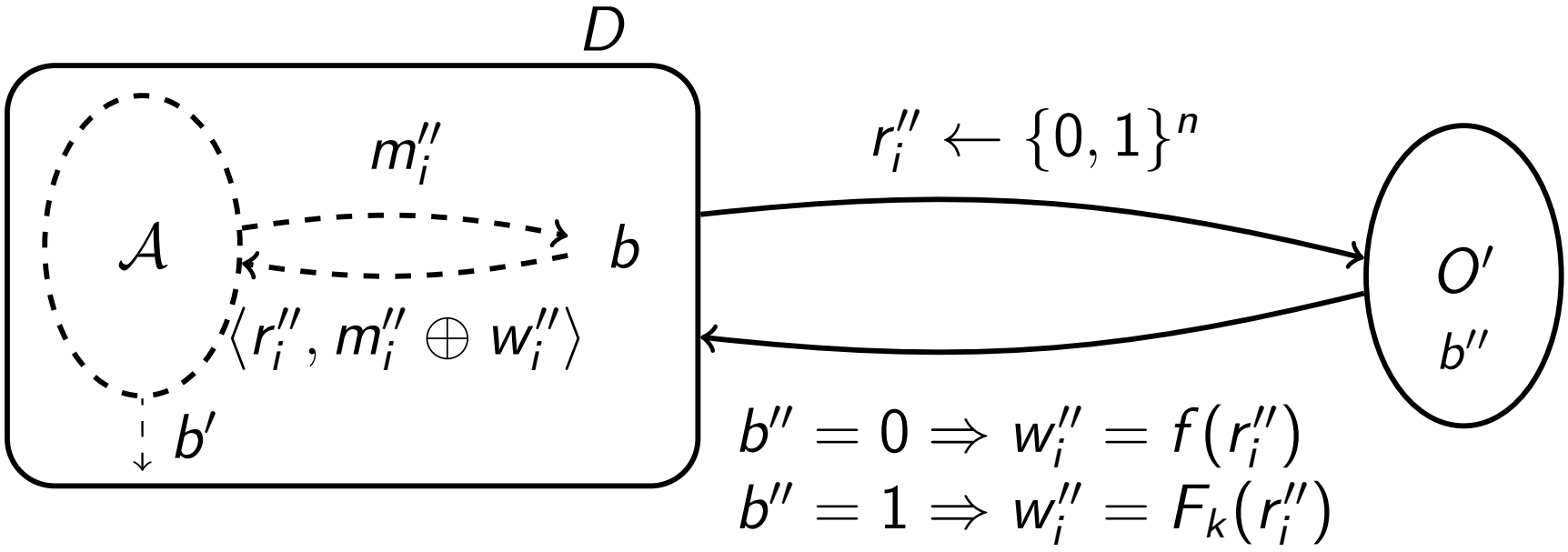


Reduction


Query phase 2
(identical to query phase 1)
D
$\mathcal{A}$
m_i''
b
$\langle r_i'', m_i'' \oplus w_i'' \rangle$
$r_i'' \leftarrow \{0,1\}^n$
O'
b''
$b'' = 0 \Rightarrow w_i'' = f(r_i'')$
$b'' = 1 \Rightarrow w_i'' = F_k(r_i'')$

Reduction

Answer phase



Reduction

Answer phase