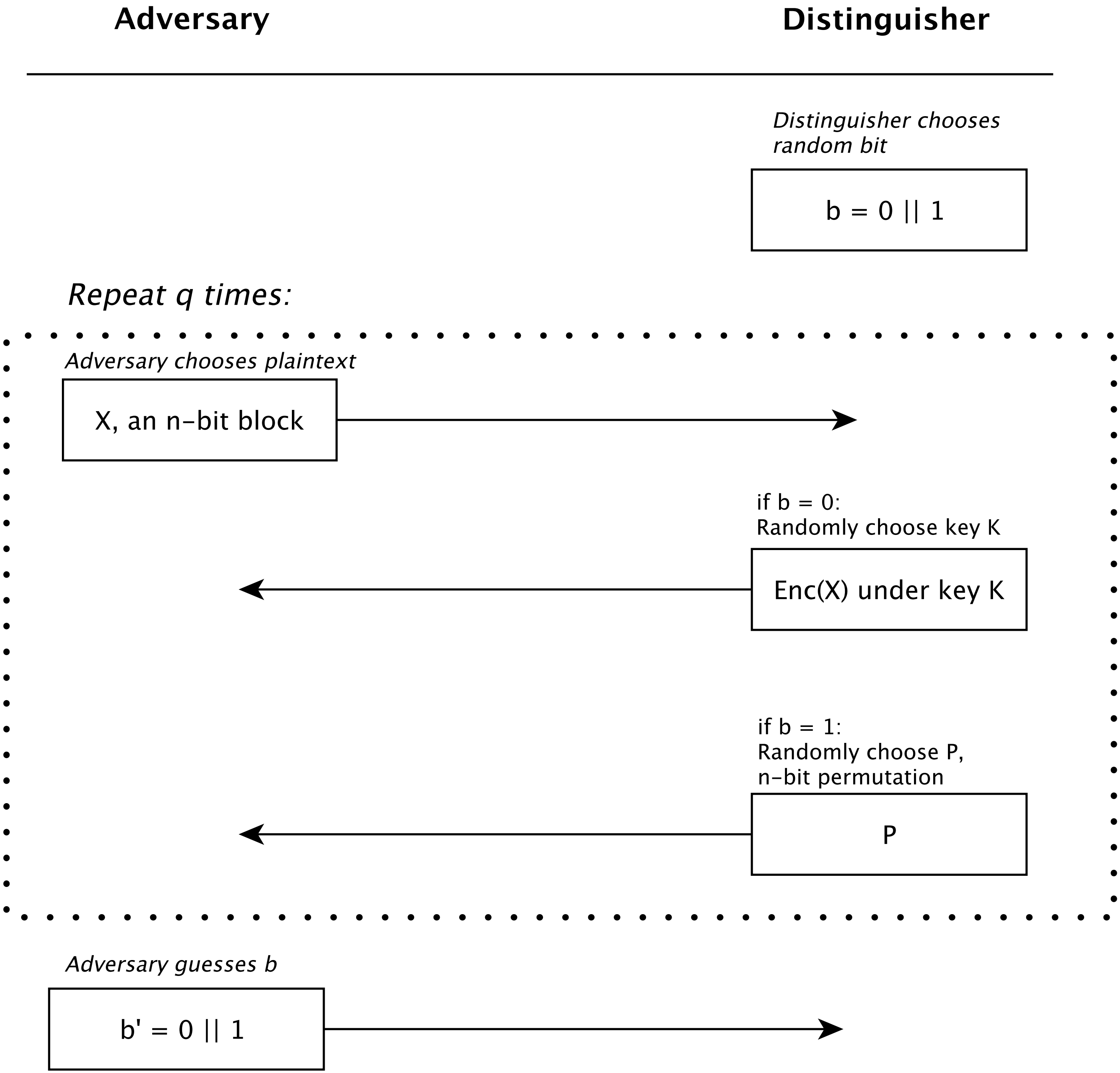
Adversary
Distinguisher
Distinguisher chooses random bit
b = 0 || 1
Repeat q times:
Adversary chooses plaintext
X, an n-bit block
if b = 0:
Randomly choose key K
Enc(X) under key K
if b = 1:
Randomly choose P,
n-bit permutation
P
Adversary guesses b
b' = 0 || 1