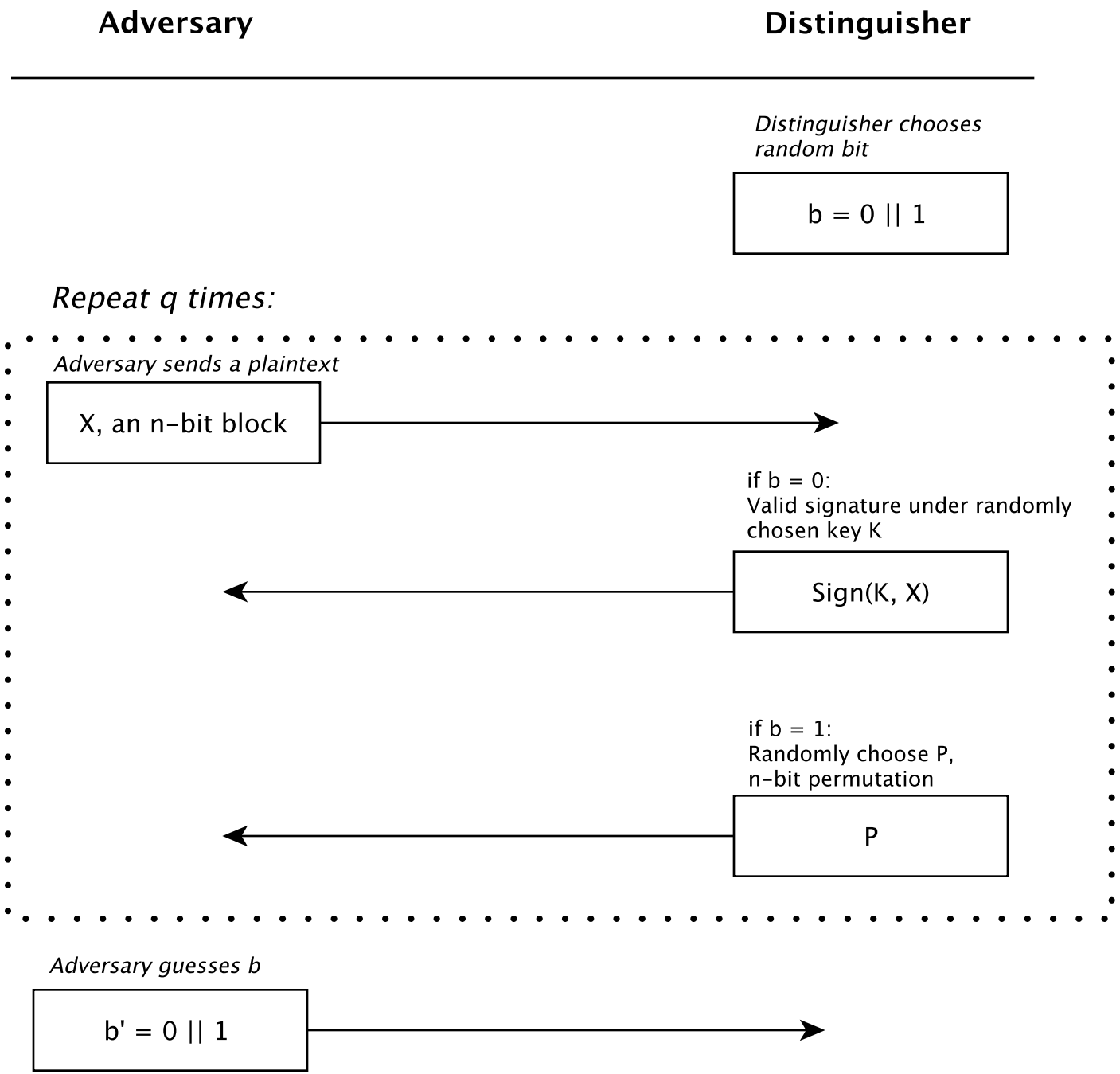
Adversary
Distinguisher
Distinguisher chooses random bit
b = 0 || 1
Repeat q times:
Adversary sends a plaintext
X, an n-bit block
if b = 0:
Valid signature under randomly chosen key K
Sign(K, X)
if b = 1:
Randomly choose P, n-bit permutation
P
Adversary guesses b
b' = 0 || 1