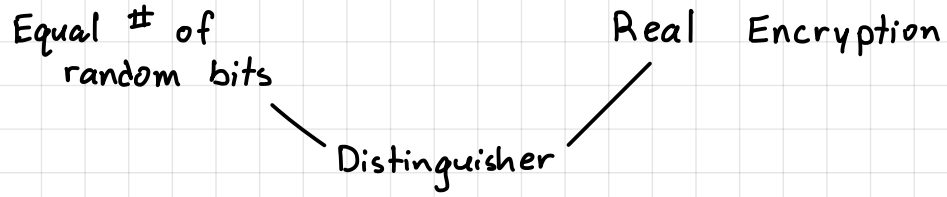
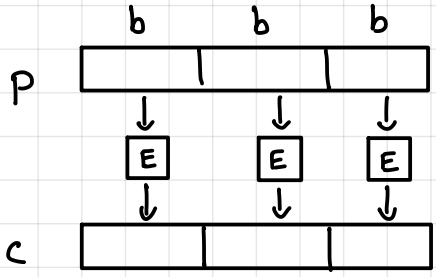
Formally encryption security model: Indistinguishible from random.



Let $E: \{0,1\}^b \to \{0,1\}^b$ be a random permutation

ECB (electronic codebook)



World 1
on f(x)
return ECB(x)

World 2
on f(x)
return |x| random bits

idea 1: if $f(\langle 0 \rangle_b) = f(\langle 0 \rangle_b)$
output real
else
output random

Same thing twice = ECB

Advantage $= 1 - \frac{1}{2^b} \approx 1$

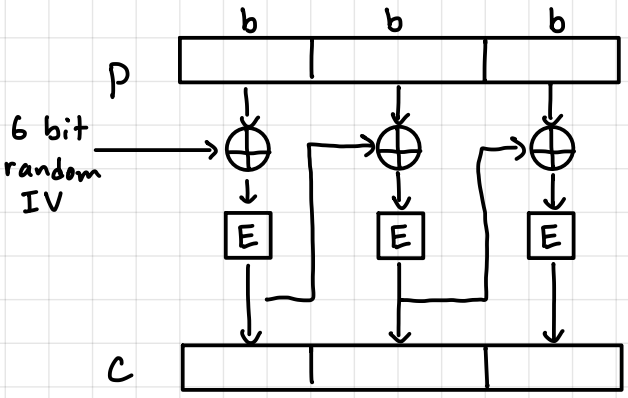
idea 2: $x = f(\langle 0 \rangle_{2b})$

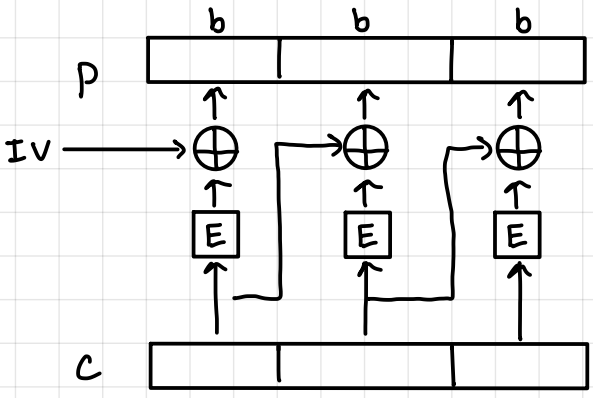
$x_0 || x_1 = x$ // split in half

if $x_0 = x_1$
output real

else
output random

CBC (cipher block chaining)





parallelizable

Send: (IV, C)

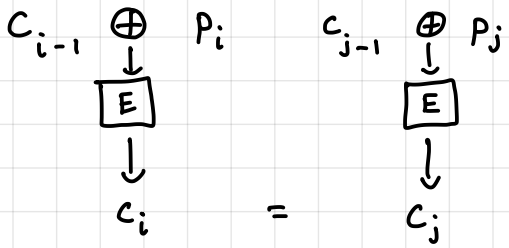
ciphertext expansion by 6 bits

not parallelizable

- sends both the IV and ciphertext on the wire

→ use this to decrypt ciphertext

observe that: if $c_i = c_j$



then $c_{i-1} \oplus P_i = c_{j-1} \oplus P_j$

$$\boxed{P_i \oplus P_j = c_{i-1} \oplus c_{j-1}}$$

Distinguisher:

for $i = 1, 2, \ldots, q$

IV_i = random b bits

P_i = random b bits

$C_i = f(iv_i, P_i)$

if $(C_i = C_j)$ for any $j < i$

if $iv_i \oplus iv_j = P_i \oplus P_j$

output real CBC

else

output random

Adv ≈ 1 when a repeat occurs

Probability of repeat $\approx \frac{q^2}{2^b}$ (binary bound)

Thus, Adv $\approx \frac{q^2}{2^b}$ ⇐ good if q is small or b is large

For example: AES $b = 128$

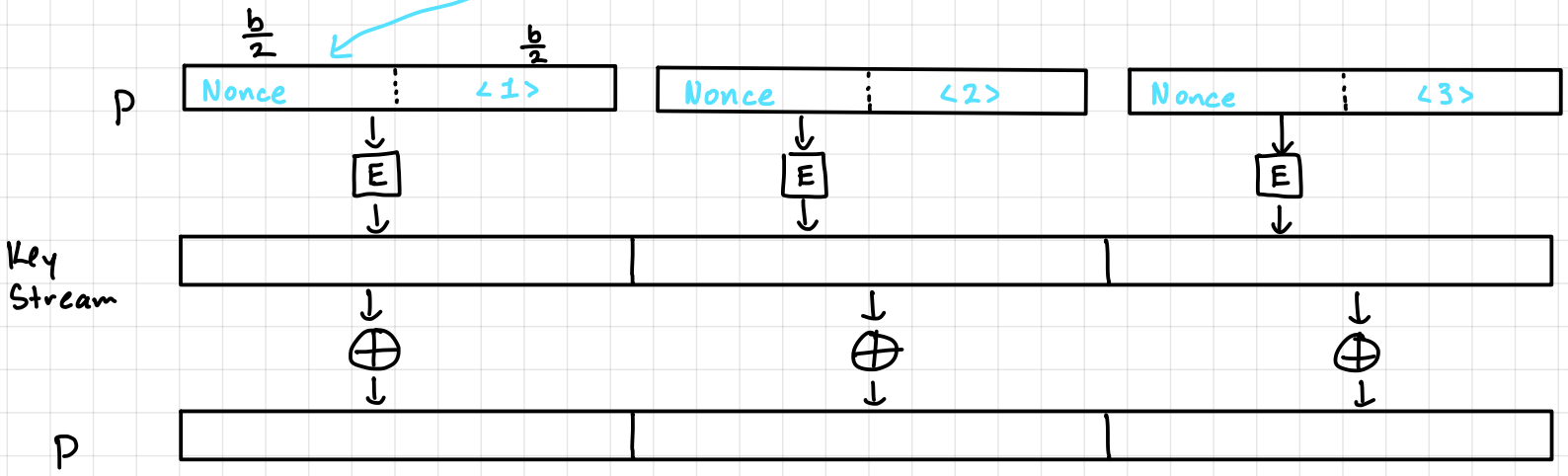
$$\frac{q^2}{2^{128}} < 2^{-32}$$

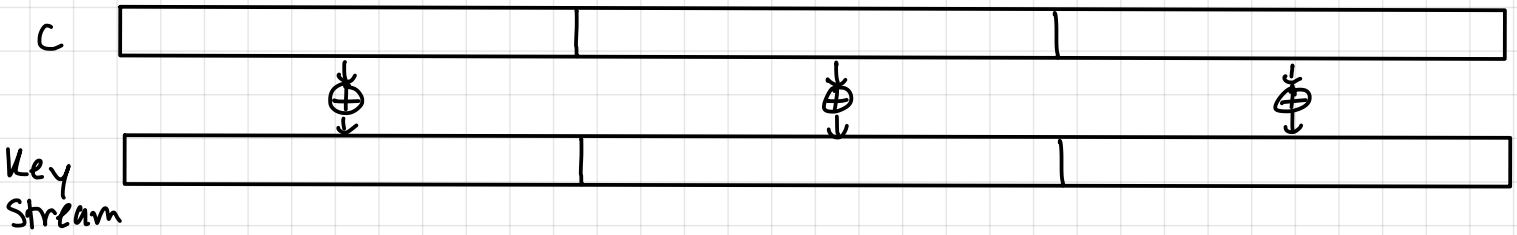
$$q^2 < 2^{96}$$

$$q < 2^{48}$$

CTR (Counter)

Nonce: number used once
(doesn't have to be random)





- No inverse E^{-1} needed

send (nonce, c)

- No separate decryption

OFB (Output Feedback)