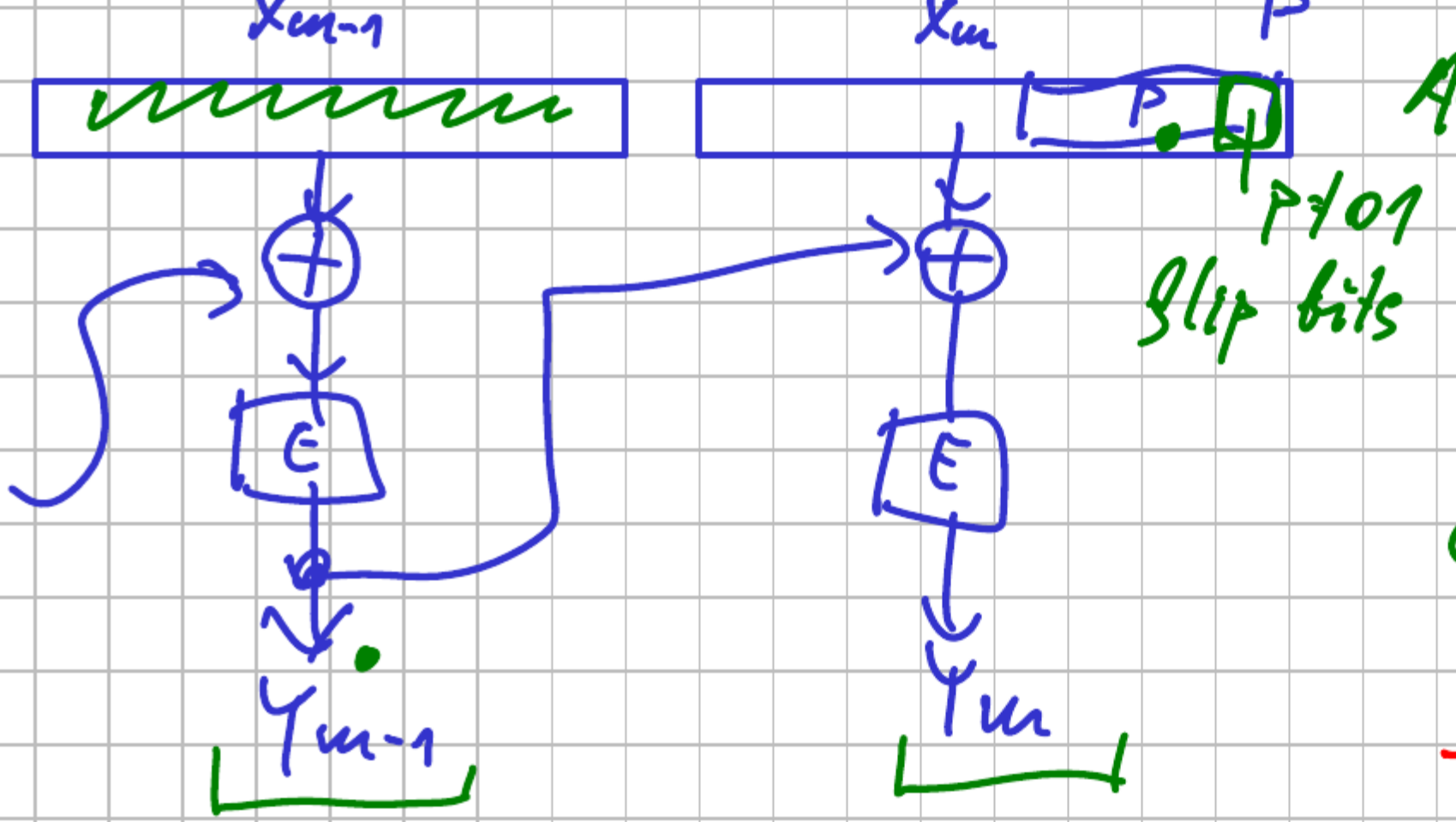
Assume padding : data | P ... ... P

P



Assume P ≠ 01

P ≠ 01

flip bits

exactly one solution with correct padding

$P \oplus F = 01$

↳ recovered P

TLS (HTTPS)