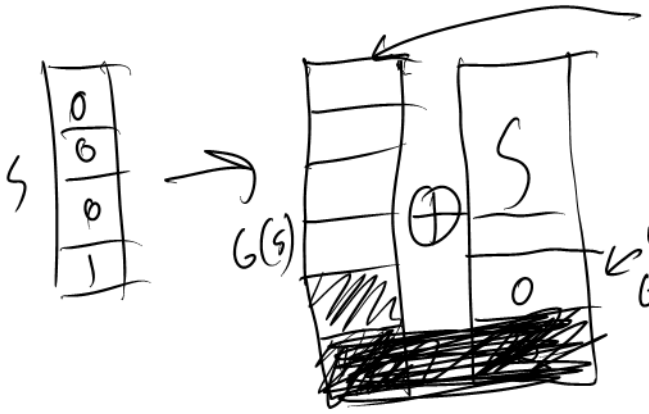


last $\ell(n)-n$ bits of $G(s)$ are the same as $G'(s)$

$\frac{1}{2^{\ell(n)-n}}$ $G(s)\oplus$ $\frac{1}{2}$

Uniform: 0 exactly the same

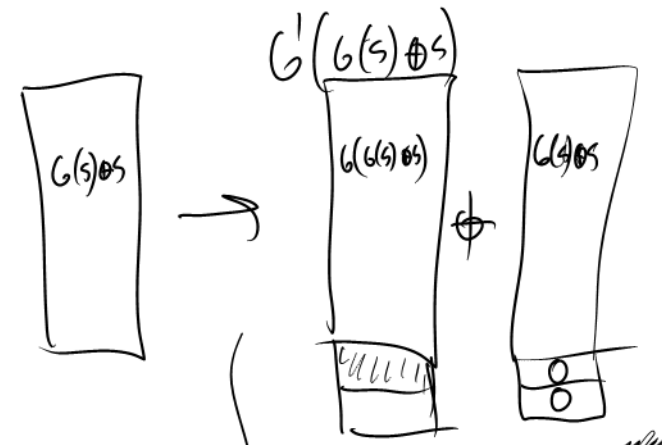
$G(s)\oplus G'(s) = G(s)\oplus G(s)\oplus s$

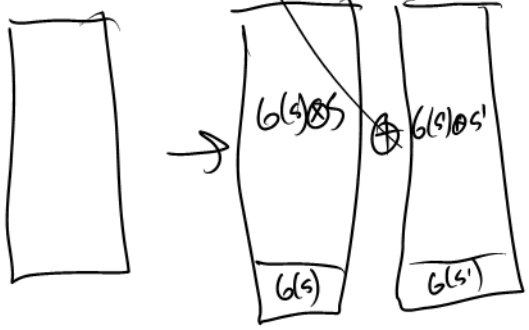
Suppose $s' = G(s)\oplus s$

select $s \in \{0,1\}^n$

select two random outputs $G(s)$ and $G'(s)$ with probability 2^{-n} $G(s)\oplus G'(s)$ will have its last $\ell(n)-n$ bits set to 0

Suppose $\bigoplus_{i=1}^{\ell(n)}(G(s)\oplus s) = 1$





Suppose $G(s) = G(s')$ in the last bit

There is a 2^{-n} chance they are the same with G, but $2^{-\ell(n)}$ chance they are the same with U_ℓ

For each $G(s)$,

For each s, $G(s)\oplus s$ can take on any value with probability 2^{-n}. Similarly,