Pseudorandom Generators

HW2 due next Wed
HW1 median/avg = 29/40

In OTP, key must be uniformly chosen

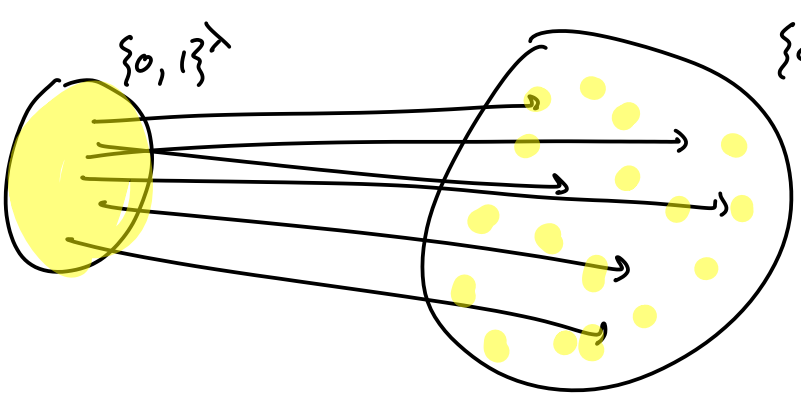
If we settle for computational security (poly-time Adv libs that can be negligibly diff)
maybe it's ok if key/mask only "looks uniform"

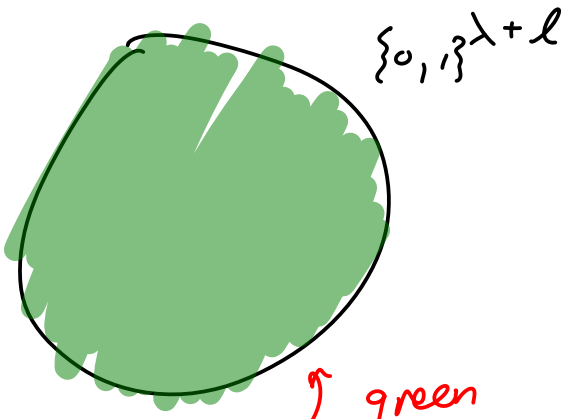
Pseudorandom Generator (PRG):

idea: take a short, uniform "seed", "expand" it to something longer that "looks uniform"

Def: $G: \{0,1\}^\lambda \longrightarrow \{0,1\}^{\lambda+\ell}$ deterministic function

ℓ = "stretch" of G





Security Def:

↑ yellow distribution

↑ green

```
QUERY():
    s ← {0,1}^λ
    return G(s)
```

$\approx$

```
QUERY():
    z ← {0,1}^(λ+ℓ)
    return z
```

Application of PRG:

encrypt long m with short k via

$$c = G(k) \oplus m$$

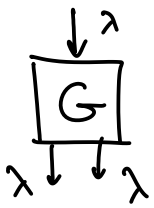
[slides]

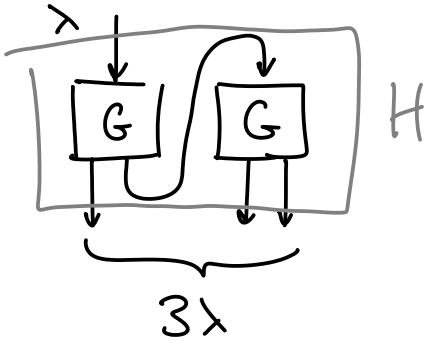
Extending a PRG:

Suppose $G: \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ (length-doubling)

Construct $H: \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ (length-tripling)

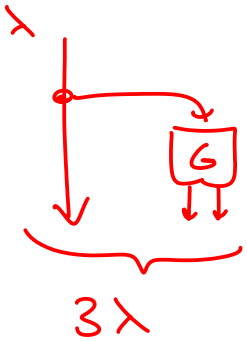
idea:





[security proof on slides]

Note: on HW



construction is INSECURE