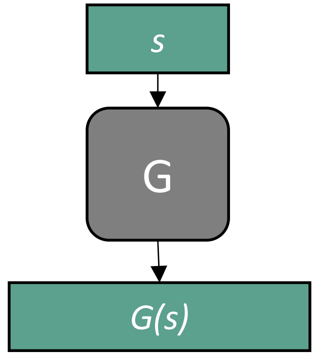
Pseudo-Random Generator (PRG)

G **deterministic** is *PRG* if for all *seed* with $|seed| = n$:

1. $l(n) = |G(s)| > |s| = n$ *(expansion)*
2. $\forall \mathcal{D}$ PPT, $\exists\ \varepsilon(n)$ negligible such that

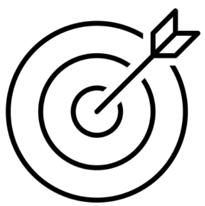
$$Adv^{PRG}_{\mathcal{D},G}(n) = |\Pr[\mathcal{D}(r) = 1] - \Pr[\mathcal{D}(G(s)) = 1]| \le \varepsilon(n)$$

where $r \leftarrow^{R} \{0,1\}^{l(n)}$ and $s \leftarrow^{R} \{0,1\}^{n}$ *(pseudo-randomness)*



$\mathcal{D}$: distinguisher
$\mathcal{D}()$ output: 0 = not random, 1 = random
PPT: Probabilistic Polynomial in Time
$r \leftarrow^{R} \{0,1\}^{l(n)}$: r is random on $l(n)$ bits
$s \leftarrow^{R} \{0,1\}^{n}$: s is random on n bits

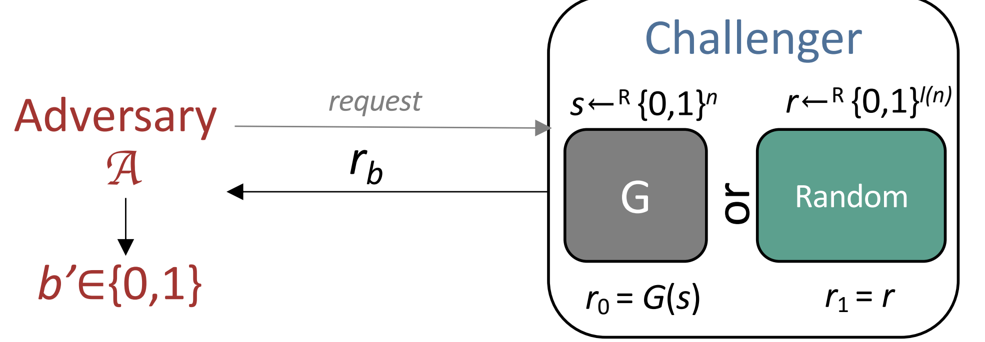
A **unpredictable** PRG is secure *(Theorem Yao'82)*
A **predictable** PRG is insecure!



Indistinguishability from random

$Dist^{PRG}_{\mathcal{A},G}(n) = 1$ if $b = b'$ and 0 otherwise

$b \in \{0,1\}$ *(fixed if more req.)*



G is PRG (cryptographically strong) if $\forall \mathcal{A}$ PPT, $\exists\ \varepsilon(n)$ negligible such that:

$$\Pr[Dist^{PRG}_{\mathcal{A},G}(n) = 1] \le \tfrac{1}{2} + \varepsilon(n)$$