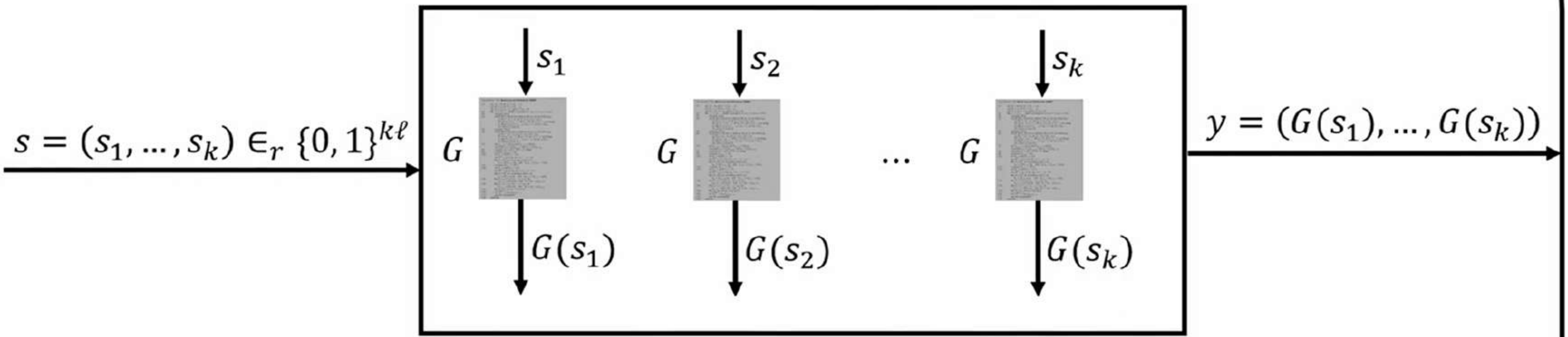
Composing PRGs

Composing PRGs

- Let $G: \{0,1\}^{\ell} \Rightarrow \{0,1\}^{L}$ be a secure PRG
- Goal: to construct a new secure PRG by composing G

- Parallel composition of G

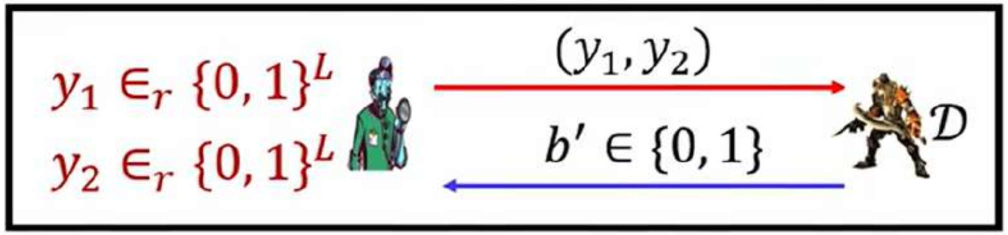


$G_{\text{new}}: \{0,1\}^{k\ell} \Rightarrow \{0,1\}^{kL}$

- If G is a secure PRG, then so is G_{new}, provided $k = \text{Poly}(n)$

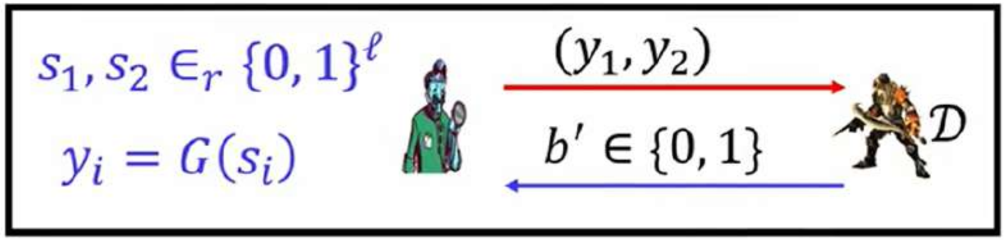
Parallel Composition of PRGs

- If $G: \{0,1\}^{\ell} \Rightarrow \{0,1\}^{L}$ is a secure PRG, then so is $G_{\text{new}}: \{0,1\}^{k\ell} \Rightarrow \{0,1\}^{kL}$, provided k =Poly(n)
  - Proof via hybrid argument --- for demonstration, assume that the repetition factor $k = 2$
- Goal: no distinguisher can distinguish apart a randomly generated sample of G_{new} from a random bit string of length $2L$ bits, with a significant probability



Experiment H_0

$\overset{c}{\approx}$

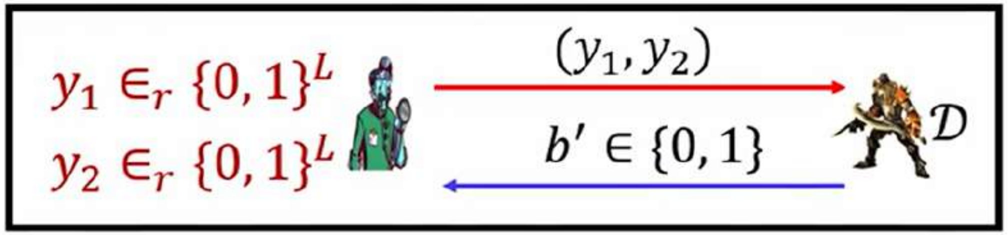


Experiment H_1

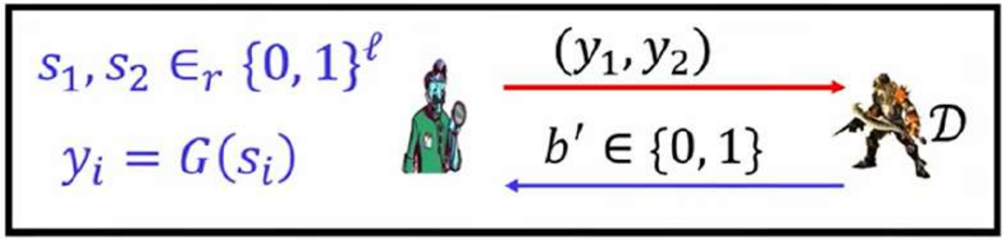
| Pr[$\mathcal{D}$ outputs b'=1 in H_0] $-$ Pr[$\mathcal{D}$ outputs b'=1 in H_1] | $\leq$ negl(n)

Parallel Composition of PRGs

- If $G: \{0,1\}^{\ell} \Rightarrow \{0,1\}^{L}$ is a secure PRG, then so is $G_{\text{new}} : \{0,1\}^{k\ell} \Rightarrow \{0,1\}^{kL}$, provided $k =$Poly(n)
    - ❖ Proof via hybrid argument --- for demonstration, assume that the repetition factor $k = 2$
- Goal: no distinguisher can distinguish apart a randomly generated sample of G_{new} from a random bit string of length $2L$ bits, with a significant probability



Experiment H_0

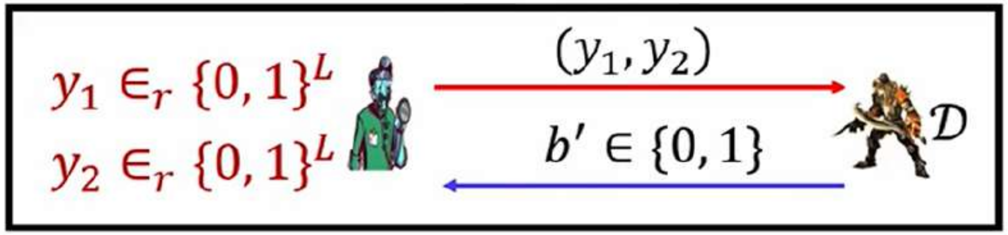


Experiment H_1

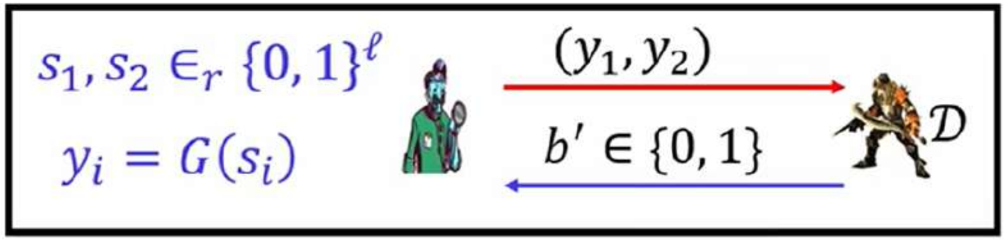
- To show that the experiments H_0 and H_1 are computationally indistinguishable for $\mathcal{D}$, we introduce an intermediate (hybrid) experiment H_{int}

Parallel Composition of PRGs

- If $G: \{0,1\}^{\ell} \Rightarrow \{0,1\}^{L}$ is a secure PRG, then so is $G_{\text{new}} : \{0,1\}^{k\ell} \Rightarrow \{0,1\}^{kL}$, provided k =Poly(n)
  - Proof via hybrid argument --- for demonstration, assume that the repetition factor $k = 2$
- Goal: no distinguisher can distinguish apart a randomly generated sample of G_{new} from a random bit string of length $2L$ bits, with a significant probability



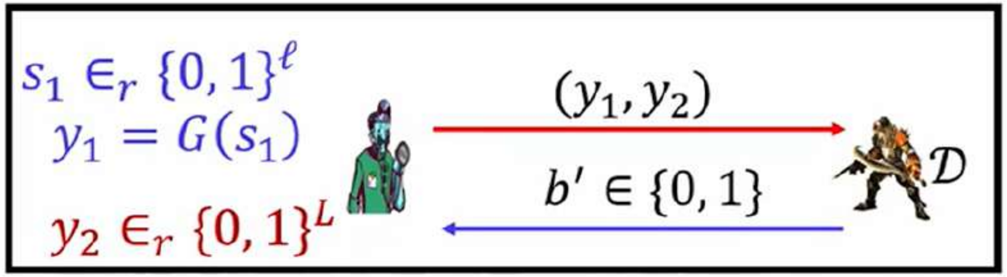
Experiment H_0



Experiment H_1

$\overset{c}{\approx}$ $\overset{c}{\approx}$

| Pr[$\mathcal{D}$ outputs b'=1 in H_0] − Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] | $\leq$ negl$_1(n)$

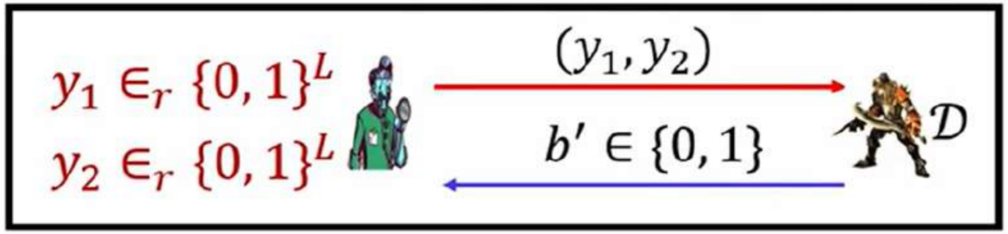


Experiment H_{int}

| Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] − Pr[$\mathcal{D}$ outputs b'=1 in H_1] | $\leq$ negl$_2(n)$

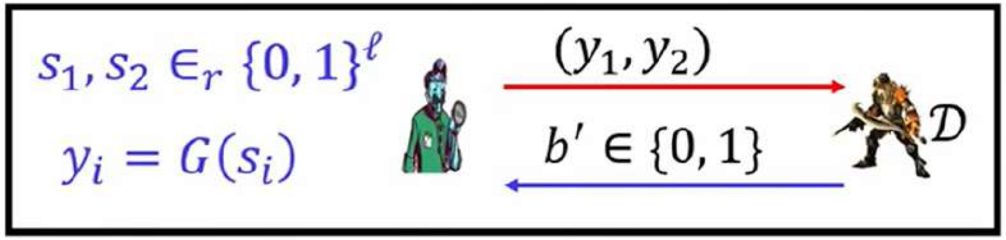
Parallel Composition of PRGs

- If $G: \{0,1\}^{\ell} \Rightarrow \{0,1\}^{L}$ is a secure PRG, then so is $G_{\text{new}}: \{0,1\}^{k\ell} \Rightarrow \{0,1\}^{kL}$, provided k =Poly(n)
  - Proof via hybrid argument --- for demonstration, assume that the repetition factor $k = 2$
- Goal: no distinguisher can distinguish apart a randomly generated sample of G_{new} from a random bit string of length $2L$ bits, with a significant probability



Experiment H_0

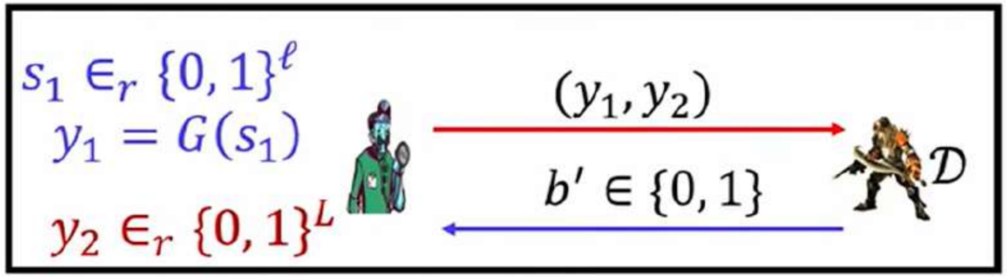
$\overset{c}{\approx}$



Experiment H_1

$|\Pr[\mathcal{D}$ outputs b'=1 in $H_0] - \Pr[\mathcal{D}$ outputs b'=1 in $H_1]| \leq \text{negl}_1(n) + \text{negl}_2(n)$

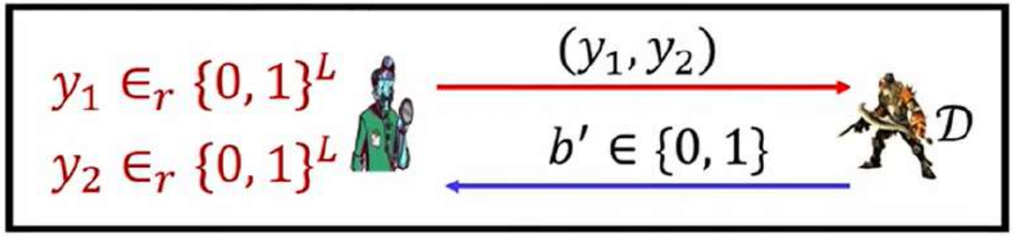
$|\Pr[\mathcal{D}$ outputs b'=1 in $H_0] - \Pr[\mathcal{D}$ outputs b'=1 in $H_{int}]| \leq \text{negl}_1(n)$



Experiment H_{int}

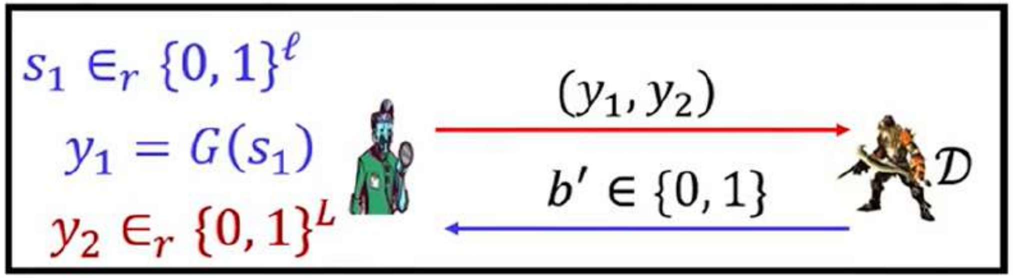
$|\Pr[\mathcal{D}$ outputs b'=1 in $H_{int}] - \Pr[\mathcal{D}$ outputs b'=1 in $H_1]| \leq \text{negl}_2(n)$

Parallel Composition of PRGs



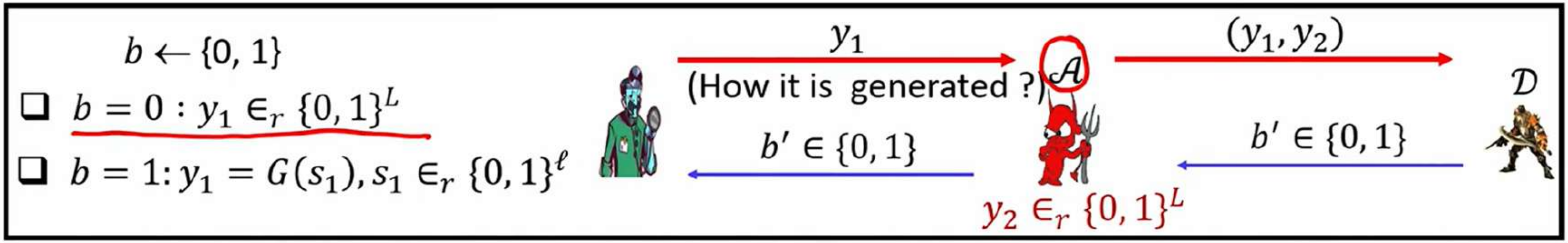
Experiment H_0

$\overset{c}{\approx}$



Experiment H_{int}

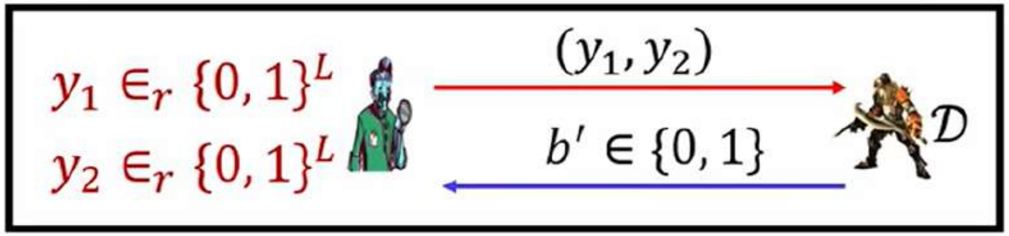
- If G is a PRG, then | Pr[$\mathcal{D}$ outputs b'=1 in H_0] − Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] | $\leq \text{negl}_1(n)$
  - If $\mathcal{D}$ can significantly distinguish between H_0 and H_{int}, then it can be used to significantly distinguish a random y_1 from a pseudorandom y_1



Pr[$\mathcal{A}$ outputs b'=1 | $b = 0$] = Pr[$\mathcal{D}$ outputs b'=1 in H_0]

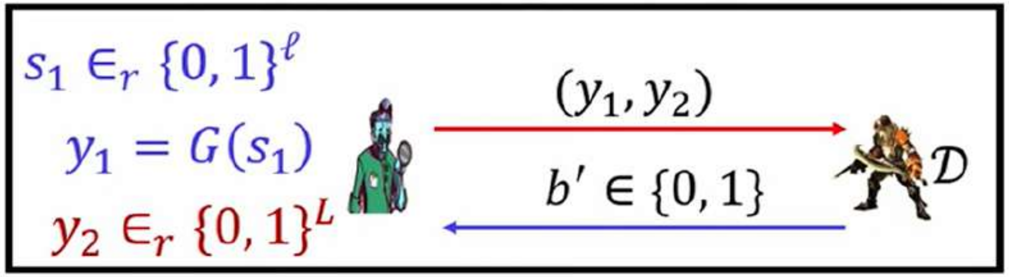
- If $b = 0$, then view of $\mathcal{D}$ is the same as in H_0

Parallel Composition of PRGs



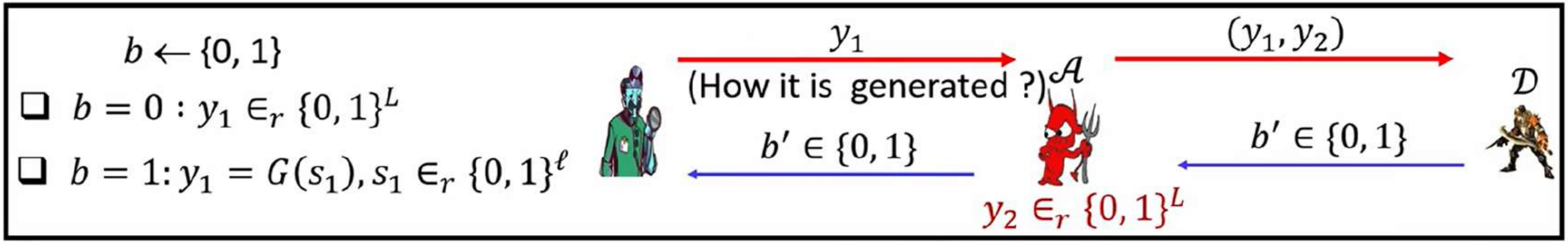
Experiment H_0

$\overset{c}{\approx}$



Experiment H_{int}

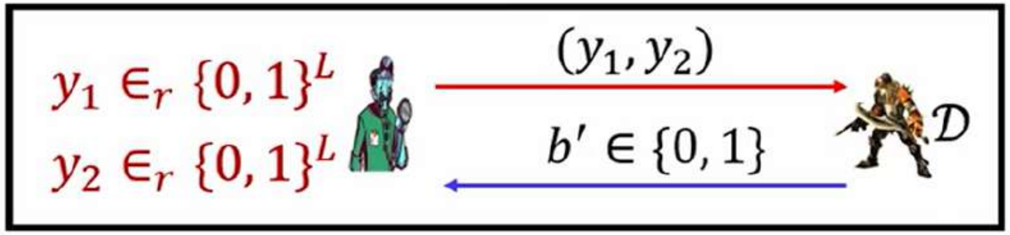
- If G is a PRG, then | Pr[$\mathcal{D}$ outputs b'=1 in H_0] − Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] | $\leq \text{negl}_1(n)$
  - If $\mathcal{D}$ can significantly distinguish between H_0 and H_{int}, then it can be used to significantly distinguish a random y_1 from a pseudorandom y_1



Pr[$\mathcal{A}$ outputs b'=1 | b = 1] = Pr[$\mathcal{D}$ outputs b'=1 in H_{int}]

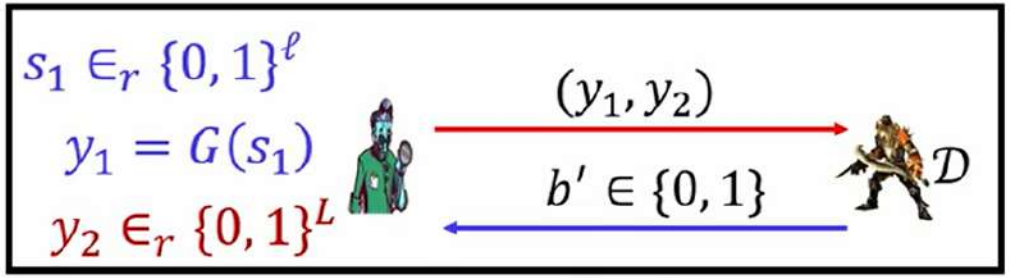
- If $b = 1$, then view of $\mathcal{D}$ is the same as in H_{int}

Parallel Composition of PRGs



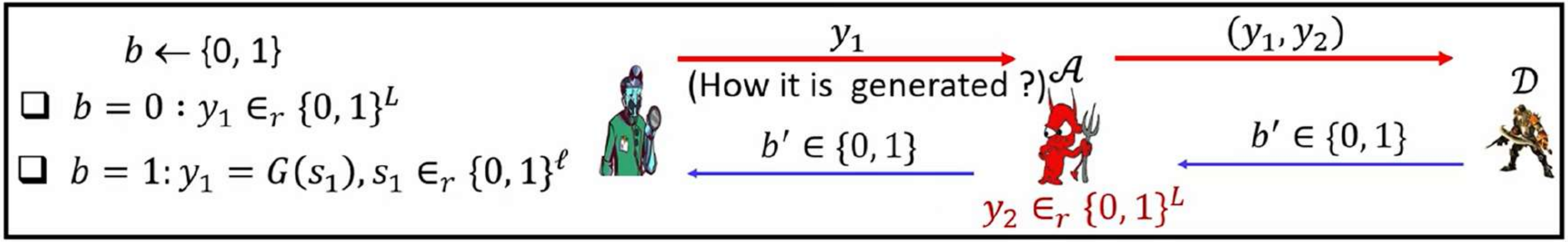
Experiment H_0

$\overset{c}{\approx}$



Experiment H_{int}

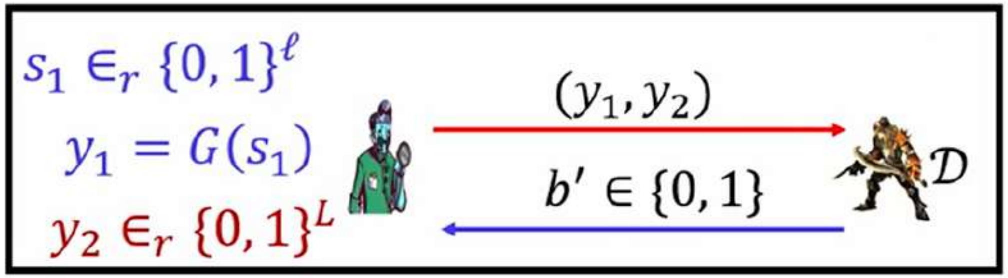
- If G is a PRG, then | Pr[$\mathcal{D}$ outputs b'=1 in H_0] − Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] | $\leq \mathsf{negl}_1(n)$
  - If $\mathcal{D}$ can significantly distinguish between H_0 and H_{int}, then it can be used to significantly distinguish a random y_1 from a pseudorandom y_1



| Pr[$\mathcal{A}$ outputs b'=1 | b = 0] − Pr[$\mathcal{A}$ outputs b'=1 | b = 1] |

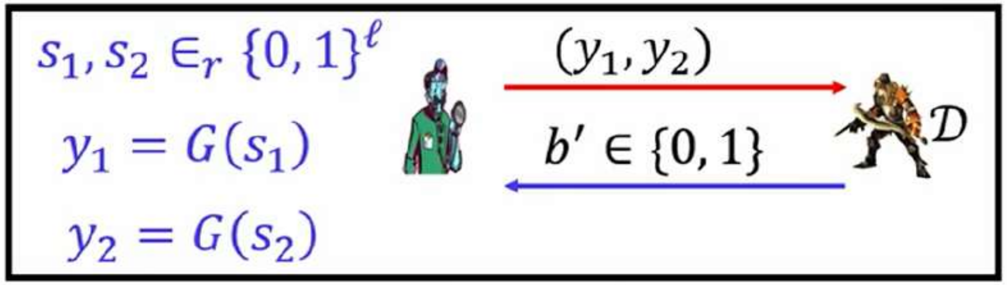
= | Pr[$\mathcal{D}$ outputs b'=1 in H_0] − Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] |

Parallel Composition of PRGs



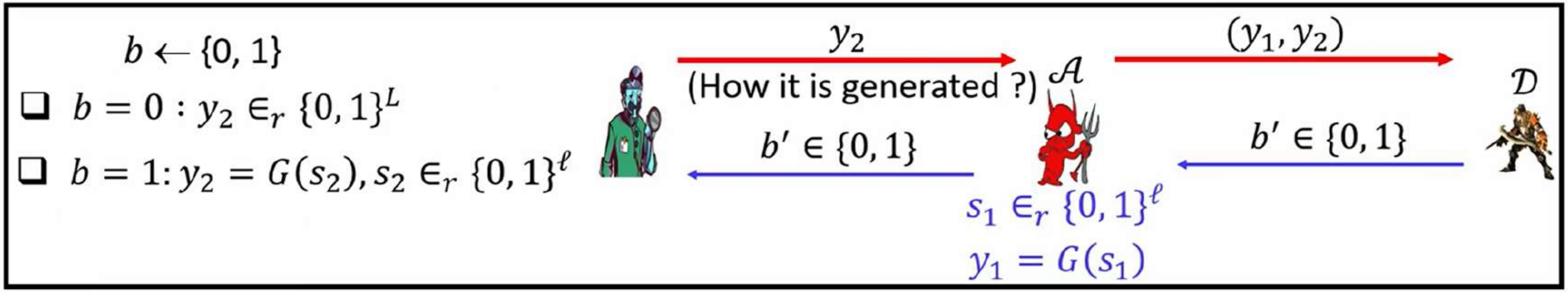
Experiment H_{int}

$\overset{c}{\approx}$



Experiment H_1

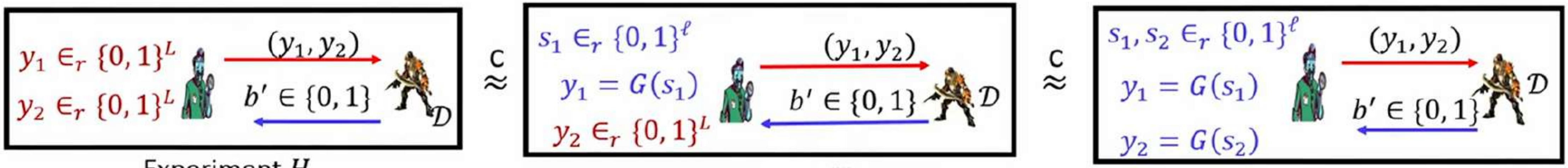
- If G is a PRG, then | Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] $-$ Pr[$\mathcal{D}$ outputs b'=1 in H_1] | $\leq \text{negl}_2(n)$



| Pr[$\mathcal{A}$ outputs b'=1 | $b = 0$] $-$ Pr[$\mathcal{A}$ outputs b'=1 | $b = 1$] |

$=$ | Pr[$\mathcal{D}$ outputs b'=1 in H_{int}] $-$ Pr[$\mathcal{D}$ outputs b'=1 in H_1] |

Parallel Composition of PRGs



Experiment H_0 | Experiment H_{int} | Experiment H_1

- If G is a PRG, then experiments H_0 and H_{int} are computationally indistinguishable

$$| \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_0] - \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_{int}] | \leq \text{negl}_1(n)$$

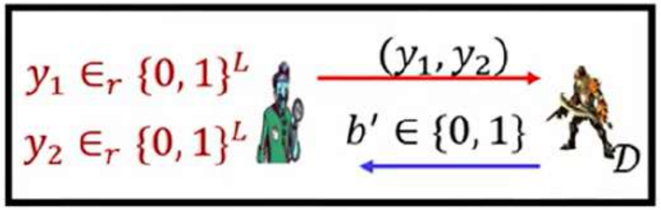
- If G is a PRG, then experiments H_{int} and H_0 are computationally indistinguishable

$$| \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_{int}] - \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_1] | \leq \text{negl}_2(n)$$

- It follows that

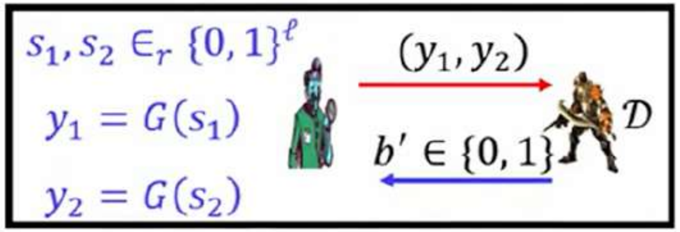
$$| \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_0] - \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_1] | \leq \text{negl}_1(n) + \text{negl}_2(n)$$

Parallel Composition of PRGs



Experiment H_0

$\overset{c}{\approx}$



Experiment H_1

- If G is a PRG, then experiments H_0 and H_{int} are computationally indistinguishable

$$| \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_0] - \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_{int}] | \le \text{negl}_1(n)$$

- If G is a PRG, then experiments H_{int} and H_0 are computationally indistinguishable

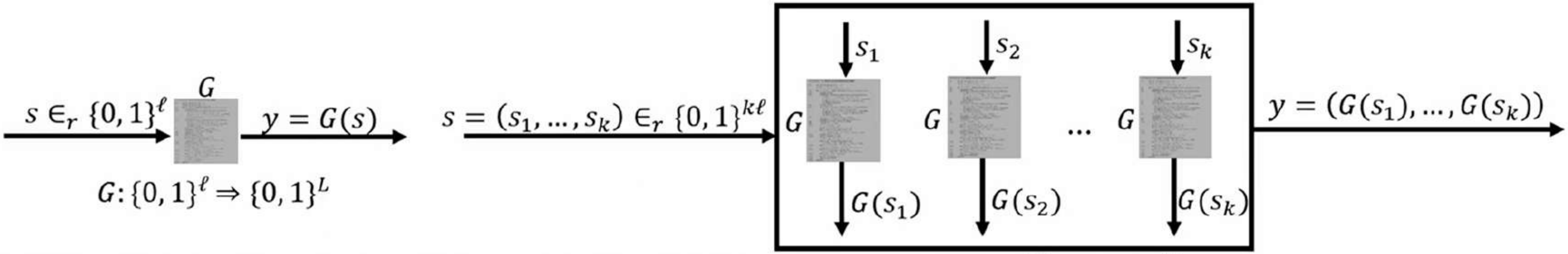
$$| \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_{int}] - \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_1] | \le \text{negl}_2(n)$$

- It follows that

$$| \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_0] - \Pr[\mathcal{D} \text{ outputs } b'=1 \text{ in } H_1] | \le \text{negl}_1(n) + \text{negl}_2(n) \le \text{negl}(n)$$

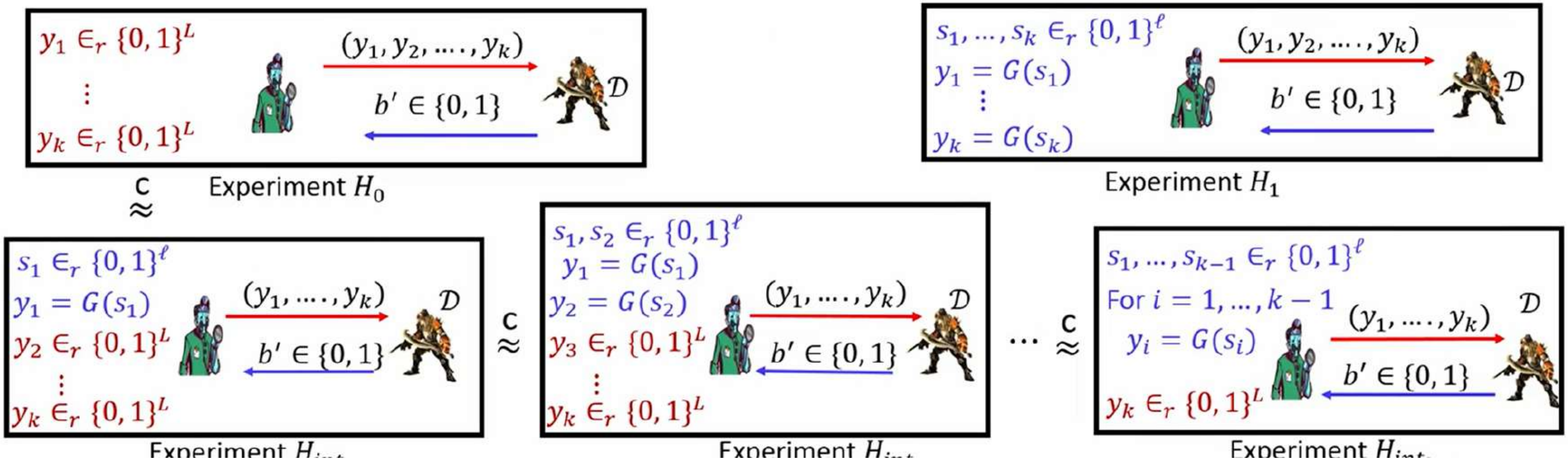
- Algorithm $G_{\text{new}}: \{0,1\}^{2\ell} \Rightarrow \{0,1\}^{2L}$ is a PRG

Parallel Composition of PRGs : General Case

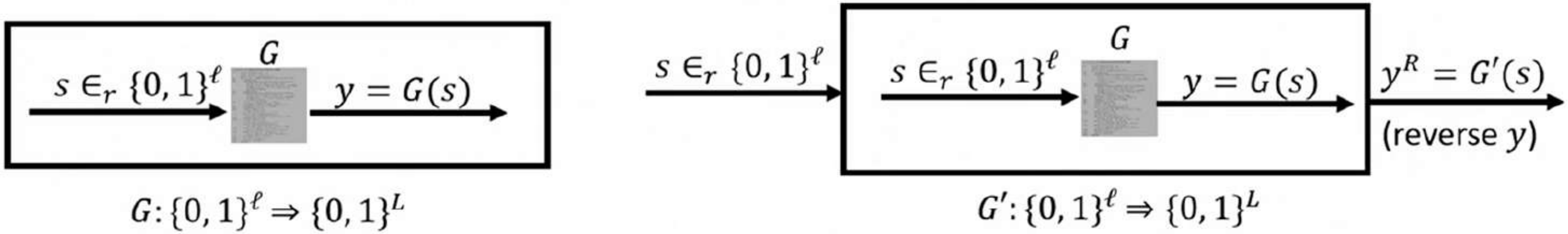


- If G is a PRG then G_{new} is also a PRG, provided $k = \text{Poly}(n)$

$G_{\text{new}}: \{0,1\}^{k\ell} \Rightarrow \{0,1\}^{kL}$



PRG : An Example



- If G is a secure PRG then G' is also a secure PRG
  - An adversary who can significantly distinguish apart reverse$(G(s))$ from a random string, can significantly distinguish apart $G(s)$ from a random string

- $b \leftarrow \{0,1\}$
- $b = 0 : y \in_r \{0,1\}^L$
- $b = 1$: $y = G(s)$, where $s \in_r \{0,1\}^\ell$

$y \in \{0,1\}^L$ →

← $b' = B$

$\mathcal{D}_G$

$Y = y^R \in \{0,1\}^L$ →

← $B = 0$ (TRG) / $B = 1$ (G')

$\mathcal{D}_{G'}$

- $\Pr[\mathcal{D}_G$ outputs $b' = 1 \mid b = 1] = \Pr[\mathcal{D}_{G'}$ outputs $B = 1 \mid Y$ is the output of $G']$
  - If y is the output of G then Y is the output of G'