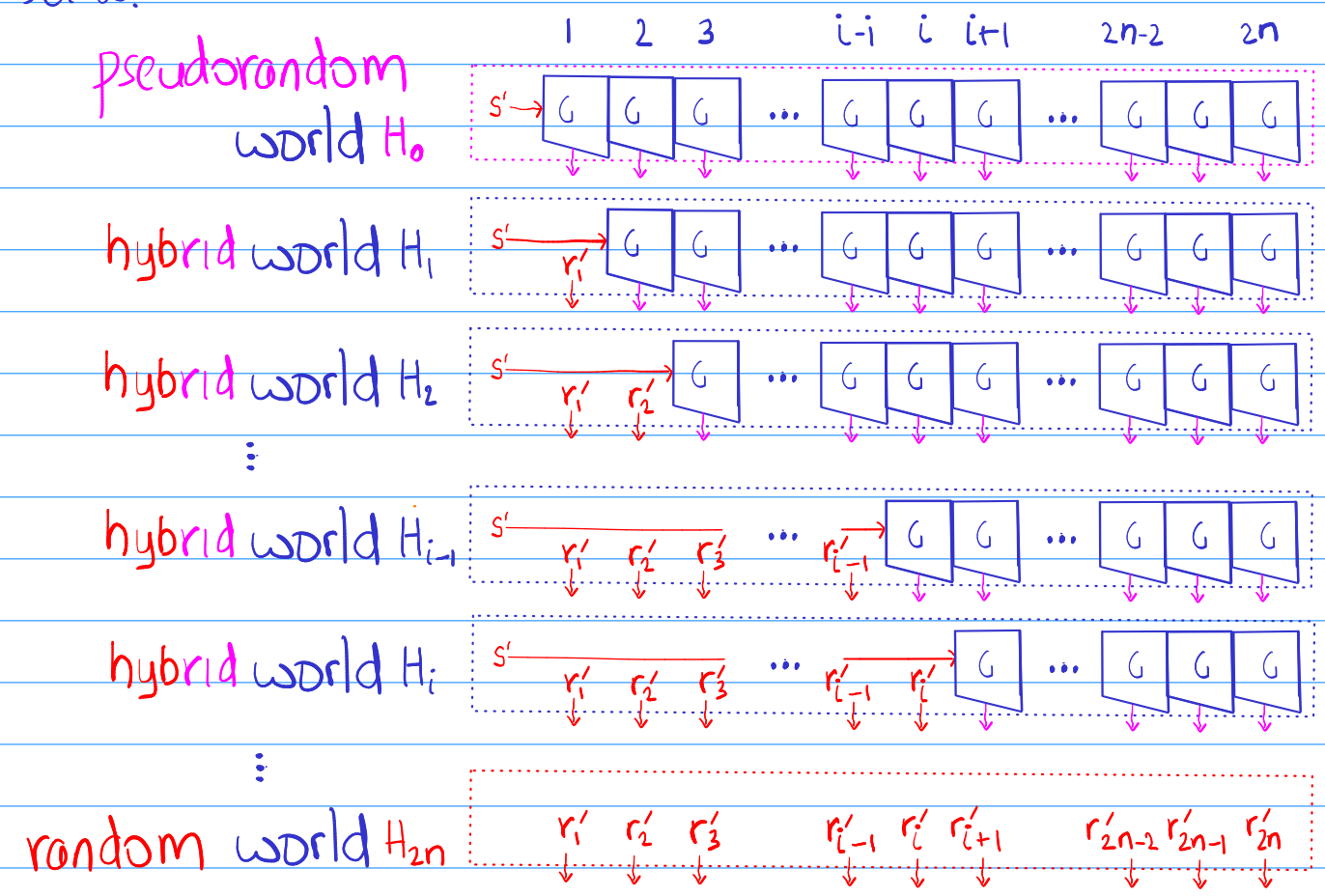
CS409m: Introduction to Cryptography (Aut' 25)

Lecture 06 — Instructor: Chethan Kamath

1) **Theorem 2** If G is a PRG, then so is G'.

Proof. Recall from the lecture that we proceed by a hybrid argument consisting of $2n+1$ worlds $H_0, H_1, \ldots H_{2n-1}, H_{2n}$ illustrated below.



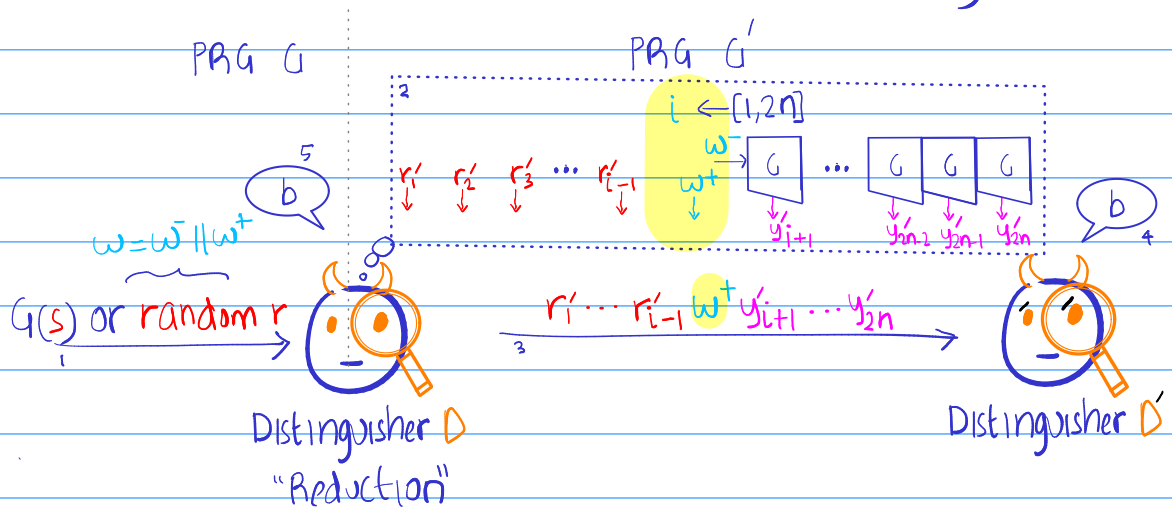
More formally, the hybrid world H_i, $i \in [0, 2n]$ is defined as follows:

$H_i(1^n)$:
- Sample $r_1', \ldots, r_i' \leftarrow \{0,1\}$
- Sample $s' \leftarrow \{0,1\}^n$, and set $y_i^- := s'$
- For $j \in [i+1, 2n]$:
  - (compute $y_{j+1}^- \| y_{j+1}^+ = G(y_j^-)$
  - Set $y_{j+1}' = y_{j+1}^+$
- output $r_1', \ldots r_i'\ y_{i+1}' \ldots y_{2n}'$

Recall that for a $(n+1)$-bit string x, x^- denotes its n-bit prefix, while x^+ denotes its last bit.

Recall also that we showed in Claim 1 (using an averaging argument) that if D' can distinguish H_0 from H_{2n} with some probability δ, then there exist two intermediate worlds H_i and H_{i+1}, for some $i \in [0, 2n-1]$, that D' distinguishes with probability at least $\delta/2n$. This distinguishing advantage can, in turn, be exploited to distinguish PRG G's two worlds as stated in Claim 2. Let's turn this informal argument into a proof.

Assume for contradiction that there exists a distinguisher D' that distinguishes the two worlds of G'. We construct a distinguisher D for the two worlds of G. Recall the reduction from Slide 6. The analysis follows.



Since D' is assumed to distinguish the two worlds of G' with non-negligible probability, there exists a polynomial p, such that for infinely many ns,

$$\left| \Pr_{s' \leftarrow \{0,1\}^n} [D'(G'(s')) = 0] - \Pr_{r' \leftarrow \{0,1\}^{2n}} [D'(r') = 0] \right| \geq 1/p(n) \quad (1)$$

By definition of the hybrid worlds, (1) implies that for infinitely-many ns

$$\left|\Pr\left[D'(H_0(1^n))=0\right] - \Pr\left[D'(H_{2n}(1^n)=0\right]\right| \geq 1/p(n), \quad (11)$$

where the probabilities are over the random coins used in the respective worlds.

Now, let's analyse the distinguisher D. Since D mimics D''s output, D outputs 0 only if D' does. It follows that

$$\left|\Pr_{s\leftarrow\{0,1\}^n}\left[D(G(s))=0\right] - \Pr_{r\leftarrow\{0,1\}^{n+1}}\left[D(r)=0\right]\right|$$

$$= \left| \Pr_{\substack{i\leftarrow[1,2n] \\ r'_1,\dots r'_{i-1}\leftarrow\{0,1\} \\ s\leftarrow\{0,1\}^n}} \left[D'(r'_1,\dots r'_{i-1}, \underbrace{y^+}_{y^-y^+:=G(s)}, y'_{i+1}\cdots y'_{2n})=0\right] - \right.$$

$$\left. \Pr_{\substack{i\leftarrow[1,2n] \\ r'_1,\dots r'_{i-1}\leftarrow\{0,1\} \\ r^-r^+\leftarrow\{0,1\}^{n+1}}} \left[D'(r'_1,\dots r'_{i-1}, r^+, y'_{i+1}\cdots y'_{2n})=0\right] \right| \quad (111)$$

(Hybrid world H_{i-1} / Hybrid world H_i)

Note that for a fixed i, the distribution of $(r'_1,\dots r'_{i-1}, y^+, y'_{i+1}\cdots y'_{2n})$ in the top part of (111) is identical to the hybrid H_{i-1}; similarly the distribution of $(r'_1,\dots r'_{i-1}, r^+, y'_{i+1}\cdots y'_{2n})$ in its bottom part is identical to H_i. Therefore

$$(111) = \left|\Pr_{i\leftarrow[1,2n]}\left[D'(H_{i-1})=0\right] - \Pr_{i\leftarrow[1,2n)}\left[D'(H_i)=0\right]\right|$$

$$= \frac{1}{2n} \left| \sum_{i=1}^{2n} \left(\Pr[D'(H_{i-1}) = 0] - \Pr[D'(H_i) = 0] \right) \right| \quad (*)$$

$$= \frac{1}{2n} \left| \Pr[D'(H_0) = 0] - \Pr[D'(H_{2n}) = 0] \right| \overset{(1)}{\geq} \frac{1}{2n} \cdot \frac{1}{p(n)}$$

Thus, putting everything together, we get that for infinitely many n's,

"security loss"

$$\left| \Pr_{s \leftarrow \{0,1\}^n} [D(G(s)) = 0] - \Pr_{r \leftarrow \{0,1\}^{n+1}} [D(r) = 0] \right| \geq 1/2np(n).$$

However, this contradicts G's pseudorandomness. ⚡ ∎