**Criptografía y Seguridad Computacional** **2017-01**

# El Argumento Híbrido

## El argumento híbrido

El argumento híbrido es una técnica que permite demostrar que dos distribuciones son computacionalmente indistinguibles. La técnica funciona de la siguiente manera:

Sean $H_0$ y $H_n$ dos distribuciones aparentemente lejanas (o para las cuales la reducción a quebrar la primitiva criptográfica parece compleja). Para demostrar que son $H_0, H_n$ computacionalmente indistinguibles vía el argumento, primero creamos distribuciones intermedias (híbridos) $H_1, \dots H_{n-1}$ tales que los pares consecutivos $H_i$ y $H_{i-1}$ sean muy similares. Luego demostramos que para todo $i \in \{1 \dots n\}$ $H_i$ es computacionalmente indistinguible de $H_{i-1}$. Finalmente deducimos que $H_0$ es computacionalmente indistinguible de $H_n$.

El razonamiento es el siguiente: Si $H_i$ es comp. ind. de $H_{i-1}$, entonces $|\Pr[D(h_{i-1}) = 1] - \Pr[D(h_i) = 1]| = \mathsf{negl}_i(\lambda)$ para una función negligible $\mathsf{negl}_i$. Cómo esto se cumple para todo $i$, entonces existe una función negligible $\mathsf{negl}$ tal que

$$\begin{aligned} n \cdot \mathsf{negl}(\lambda) &= \sum_{i=1}^{n} |\Pr_{h_{i-1} \sim H_{i-1}}[D(h_{i-1}) = 1] - \Pr_{h_i \sim H_i}[D(h_i) = 1]| \\ &\geq |\sum_{i=1}^{n} \Pr_{h_{i-1} \sim H_{i-1}}[D(h_{i-1}) = 1] - \Pr_{h_i \sim H_i}[D(h_i) = 1]| \\ &= |\Pr_{h_0 \sim H_0}[D(h_0) = 1] - \Pr_{h_n \sim H_n}[D(h_n) = 1]| \end{aligned}$$

Concluimos que mientras $n$ sea polinomial en $\lambda$, entonces $H_0$ y $H_n$ son computacionalmente indistinguibles.

## Ejemplo: Extensión de PRG

Vimos en clases que si tenemos un generador pseudo-aleatorio de $\lambda + 1$ bits de output, entonces podemos generar una cantidad arbitraria (pero

polinomial) de bits pseudo-aleatorios.

La construcción es la siguiente: Dada PRG $G : \{0,1\}^\lambda \to \{0,1\}^{\lambda+1}$, construímos PRG $G^{(n)}$ como:

1. Con input $X \in \{0,1\}^\lambda$, $X^0 \leftarrow X$.
2. Para $i$ desde 1 hasta $n$:
   a) $W^i \leftarrow G(X^{i-1})$
   b) $X^i = W^i_{1\ldots\lambda}$, # primeros lambda bits
   c) $y_i = sW^i_\lambda$ # últimos lambda bits
3. Output $Y = y_1||y_2||\ldots||Y_n$

Para demostrar que $G^{(n)}$ es una PRG utilizamos el argumento híbrido con $H_0 = G(X)$ para $X$ uniforme en $\{0,1\}^\lambda$ y $H_n = U_n$ (uniforme de $n$ bits). Las distribuciones híbridas $H_i$ son tales que los primeros $i$ bits son uniformes y los últimos $n-i$ son generados por $G^{(n-i)}$.

Ahora demostramos vía una reducción a distinguir entre la distribución $G(U)$ y a distribución uniforme que, para todo $i$, $H_i$ es computacionalmente indistinguible de $H_{i-1}$. Informalmente, la reducción funciona de la siguiente forma: dado el input $Z$, generamos un valor $h^*$ tal que si $Z$ es uniforme, entonces la distribución inducida por $h^*$ es igual a $H_i$. Pero si $Z$ es $G(u)$ para $u \sim U_\lambda$, entonces $h^*$ corresponde a $H_{i-1}$.

Reducción $D(Z)$:

1. Generamos $i-1$ bits uniformes $h^*_1 \ldots h^*_{i-1}$. (Ambas distribuciones son iguales en los primeros $i-1$ bits.
2. $h^*_i = Z_{\lambda+1}$, $X = Z_{1\ldots\lambda}$
3. Computamos $h^*_i, \ldots, h^*_n \leftarrow G^{(n-i)}(X)$
4. $b \leftarrow D^{(i)}(h^*)$ (Ejecutamos el distinguidor $D^{(i)}$ que distingue entre $H_{i-1}$ y $H_i$)
5. Output $b$.

Análisis: Si $Z$ es uniforme entonces $h^*$ esta idénticamente distribuido con $H_i$ pués $h^* = U_i||G^{(n-i)}(X)$ en donde $X$ es uniforme. En cambio, si $Z$ es $G(u)$ para $u \sum U_\lambda$, entonces $h^*$ esta idénticamente distribuido con $H_{i-1}$: Los primeros $i-1$ son uniformes. El $i$-ésimo bit es el último bit del output de $G(u)$ (o más

bien el primer bit del output de $G^{(n-i+1)}(u)$) al igual que en $H_{i-1}$. Los últimos $n-i$ bits son generados como $G^{(n-i)}(X) = G^{(n-i)}(G(u)_{1\ldots\lambda}) = G^{n-i+1}(u)$. Por lo tanto, la variable $h^*$ esta idénticamente distribuida con $H_{i-1}$. Concluimos que si $G$ es PRF, entonces $D$ no puede distinguir con probabilidad no negligible y por lo tanto $H_i$ es computacionalmente indistinguible de $H_{i-1}$.