IIC3253: Criptografía y Seguridad Computacional - Tarea #2

Raimundo Herrera - rjherrera@uc.cl

16 de abril de 2018

Problema 1

Determine si las siguientes funciones G' son generadores pseudo-aleatorios.

1. $\boldsymbol{G' : \{0,1\}^{2\lambda} \to \{0,1\}^n, G'(x = x_1 x_2 ... x_{2\lambda}) = G(x_1 x_2 ... x_\lambda)}$

   G' si es PRG. Para demostrarlo, lo haré por reducción. Asumamos que G' no es pseudo-aleatorio, si esto es así, entonces existe un distinguidor D' tal que

   $$\Pr[D'(G'(U_{2\lambda})) = 1] - \Pr[D'(U_{2\lambda}) = 1] > \text{negl}(2\lambda)$$

   Se puede construir un distinguidor $D(z)$ para G de la siguiente forma

   - $b \leftarrow D'(z)$
   - output b

   Como ambos distinguidores G y G' reciben como input elementos de n bits, su funcionamiento es análogo. Basta demostrar entonces que efectivamente son equivalentes, esto es, que este último distinguidor especificado distingue G.

   Evidentemente sabemos que

   $$\Pr[D'(U_\lambda) = 1] = \Pr[D(U_\lambda) = 1]$$

   Por otro lado, notemos que el input de G' viene de $U_{2\lambda}$, y que el de G viene de U_λ. Como son ambas distribuciones uniformes, se puede mirar el input de G' como $K||K'$. De este modo, independiente del valor de K' se tiene, por construcción de G' que

   $$G'(K||K') = G(K)$$

   Así, es inmediato que

   $$\Pr_{K,K' \sim U_\lambda}[D'(G'(K||K')) = 1] = \Pr_{K \sim U_\lambda}[D(G(K)) = 1]$$

Ya que los distinguidores son equivalentes y $G'(K||K') = G(K)$.

De este modo, como ambas probabilideades son iguales, se tiene que

$$\Pr[D'(U_{2\lambda}) = 1] - \Pr[D'(U_{2\lambda}) = 1] = \Pr[D(U_\lambda) = 1] - \Pr[D(U_\lambda) = 1]$$

Y como el lado de la izquierda por lo que asumimos en un principio es no negligible, entonces el lado derecho también. De este modo, se concluye que si G' no es PRG entonces G tampoco lo es, lo que contradice lo enunciado inicialmente. De este modo, por contrapositivo se demuestra que G' si es PRG.

■

2. $\boldsymbol{G' : \{0,1\}^\lambda \to \{0,1\}^{2n}, G'(x) = G(x)||G(x+1)}$

G' no es PRG. Para mostrarlo, construiré G de forma que, siendo G efectivamente PRG, se pueda generar un distinguidor D' para G', que muestre que no es PRG.

Sea $G'' : \{0,1\}^{\lambda-1} \to \{0,1\}^{n-1}$ un PRG, definamos G de la siguiente manera

$$G : \{0,1\}^\lambda \to \{0,1\}^n, G(x_1x_2...x_\lambda) = G''(x_1x_2...x_{\lambda-1})||x_\lambda$$

Es fácil ver que el G propuesto es pseudo-aleatorio ya que los primeros $n-1$ bits son generados por G'' que es PRG y el último bit x_λ es independiente de los primeros. Realizando reducción y por contrapositivo se puede demostrar, de este modo, demostraré que, si G no es pseudo-aleatorio entonces G'' tampoco lo es.

Si G no es pseudo-aleatorio, entonces existe D^* tal que distingue G.

Construyamos $D^{**}(z = z_1...z_{\lambda-1})$ tal que

- $u \sim U_1$
- $x = z||u$
- $b \leftarrow D^*(x)$
- output b

Ese distinguidor toma su input z, le agrega un bit aleatorio como último elemento y este nuevo string lo utiliza en el distinguidor que asumimos existía para G, luego entregando el output que este de. De este modo, si existe un distinguidor para G, entonces existe un distinguidor para G'', de modo que, G'' no podría ser PRG. Y como lo es, entonces por el argumento expuesto, G tiene que serlo.

Continuando con el contraejemplo, recapitulemos. Tenemos el siguiente $G(x) = G''(x_1x_2...x_{\lambda-1})||x_\lambda$ que es pseudo-aleatorio. Lo que sigue es mostrar que usando ese G en la definición de G', este último pasa a ser distinguible.

Tomemos G' en términos del nuevo G, y sea $y = x + 1$

$$G'(x) = G(x)||G(y)$$
$$G'(x) = G''(x_1x_2...x_{\lambda-1})||x_\lambda||G''(y_1y_2...y_{\lambda-1})||y_\lambda$$

Sabemos que x es un string binario, y en caso de que el número que represente sea par, al sumarle 1, el resultado, es decir y, solo difiere en el último bit, pasando de 0 a 1. De este modo basta construir un distinguidor que verifique que los $n-1$ primeros bits son iguales a los $n-1$ bits de la segunda mitad (ya que G'' habría recibido el mismo input de $\lambda - 1$ bits para cada uno, por lo tanto entrega el mismo output) y que el enésimo bit sea 0 y el último 1. Así, sea $D'(z)$ el siguiente distinguidor

- $a = z_1...z_{n-1}$
- $b = z_{n+1}...z_{2n-1}$
- si $a = b$ y $z_n = 0$ y $z_{2n} = 1$ output 1
- en otro caso output 0

Este distinguidor compara los primeros dígitos de cada mitad del output de G', de modo de poder comprobar la igualdad. Ahora, con este distinguidor el análisis de probabilidades para el caso en que efectivamente proviene de un generador es el siguiente:

$$\begin{aligned}
\Pr[D(G'(U_\lambda)) = 1] &= \Pr[D(G'(U_\lambda)) = 1 \mid U_\lambda \text{ par}] \cdot \Pr[U_\lambda \text{ par}] \\
&+ \Pr[D(G'(U_\lambda)) = 1 \mid U_\lambda \text{ impar}] \cdot \Pr[U_\lambda \text{ impar}] \\
&= \Pr[D(G'(U_\lambda)) = 1 \mid U_\lambda \text{ par}] \cdot 1/2 \\
&+ \Pr[D(G'(U_\lambda)) = 1 \mid U_\lambda \text{ impar}] \cdot 1/2 \\
&= 1 \cdot 1/2 + 0 \cdot 1/2 \\
&= 1/2
\end{aligned}$$

Ahora, la segunda probabilidad, es decir, si el input proviene de un string aleatorio:

$$\Pr[D(U_\lambda) = 1] = 2^{-(n+1)}$$

Esto porque, del universo de todos los strings binarios de largo $2n$, un cuarto de ellos tienen el dígito de al medio igual a 0 y el del final igual a 1. Además, la cantidad de strings cuyos bits de la primera mitad son iguales a los de la segunda (sin considerar el de al medio y el final), corresponden a 2^{n+1}. Así la cantidad de strings que cumplen ambas condiciones son 2^{n-1}. Por lo que, de un universo de 2^{2n} strings, se obtiene la probabilidad explicitada.

Finalmente, restando ambas probabilidades se tiene:

$$\Pr[D(G'(U_\lambda)) = 1] - \Pr[D(U_\lambda) = 1] = 1/2 - 2^{-(n+1)}$$

Lo que evidentemente es no negligible. Demostrandose que con dicho distinguidor, se puede distinguir con una probabilidad no neglibible, por lo que G' no es PRG.

3. $\boldsymbol{G' : \{0,1\}^\lambda \to \{0,1\}^{n+1}, G'(x) = G(x)||x_1}$

   G' no es PRG. Con un procedimiento similar, sea $G'' : \{0,1\}^{\lambda-1} \to \{0,1\}^{n-1}$ un PRG, definamos G de la siguiente manera

   $$G : \{0,1\}^\lambda \to \{0,1\}^n, G(x_1x_2...x_\lambda) = x_1||G''(x_2x_3...x_\lambda)$$

   Evidentemente G es un PRG. La demostración por contrapositivo de que efectivamente es pseudo-aleatorio es idéntica a la de (1.2), solo que concatenando el bit aleatorio al principio del string, es decir, en el distinguidor hay que especificar $x = u||z$.

   De este modo, hay que mostrar que al usar este G que es PRG, se puede fabricar un distinguidor que quiebra G'. Tomemos entonces G' en términos del nuevo G recién definido:

   $$G'(x) = G(x)||x_1$$
   $$G'(x) = x_1||G''(x_2x_3...x_\lambda)||x_1$$

   De este modo, sea $D'(z)$ el siguiente distinguidor

   - si $z_1 = z_n$ output 1
   - en otro caso output 0

   Con este distinguidor el análisis de probabilidades se vuelve trivial.

   $$\Pr[D(G'(U_\lambda)) = 1] = 1$$

   Ya que siempre que venga del generador tendrá los bits inicial y final iguales. Por otro lado, si tomamos la otra probabilidad tenemos

   $$\Pr[D(U_\lambda) = 1] = 1/2$$

   Ya que la probabilidad de que un string binario tenga los bits inicial y final iguales es de 1/2 (0-0 y 1-1). Teniendo finalmente que

   $$\begin{aligned}\Pr[D(G'(U_\lambda)) = 1] - \Pr[D(U_\lambda) = 1] &= 1 - 1/2 \\ &= 1/2\end{aligned}$$

   Lo que no es neglibible, teniendo entonces que G' no es PRG.

Problema 2

Determine si las siguientes funciones F' son también funciones pseudo-aleatorios.

1. $\boldsymbol{F' : \{0,1\}^{\lambda} \times \{0,1\}^{\lambda-1} \to \{0,1\}^{2\lambda}, F'(k,x) = F(k,0||x)||F(k,1||x)}$

   F' sí es PRF. Por propiedades de las funciones pseudo-aleatorias, sea f una de ellas, para $i \neq j$, $f(i)$ es independiente de $f(j)$. En este caso se puede tener en cuenta que $0||x$ y $1||x$ nunca serán iguales, y de este modo, para x_1 y x_2 distintos, $0||x_1$, $1||x_1$, $0||x_2$, $1||x_2$ son todos distintos.

   Así, los outputs de F para cada caso serán independientes, por lo tanto no podré fabricar nunca un distinguidor que gane con probabilidad mayor a negligible, ya que nunca podrá igualar partes de los resultados de F_k con una certeza mayor que si viniera de una distribución aleatoria.

   La demostración formal es por contrapositivo y se desprende inmediatamente de construir el oráculo, pero no alcancé a incluirla.

2. $\boldsymbol{F' : \{0,1\}^{\lambda} \times \{0,1\}^{\lambda-1} \to \{0,1\}^{2\lambda}, F'(k,x) = F(k,0||x)||F(k,x||1)}$

   F' no es PRF. Para mostrarlo construiré un distinguidor que sea capaz de distinguir a F' de una función aleatoria en tiempo polinomial. Sea $D'_F(1^{1-\lambda}$ con acceso al oráculo $\mathcal{O}$ construido de la siguiente forma

   - $a = \mathcal{O}(0^{\lambda-1})$
   - $b = \mathcal{O}(0^{\lambda-2}||1)$
   - si $a_{\lambda+1}...a2\lambda = b_1...b\lambda$ output 1
   - en otro caso output 0

   Con este distinguidor, intuitivamente se ve que se puede lograr distinguir cuando la segunda mitad de la primera llamada al oráculo, es igual a la primera mitad de la segunda llamada al oráculo.

   Haciendo el análisis de probabilidades, se tiene que para cualquier k con el distinguidor anterior, la condición expresada se va a cumplir, ya que sucederá que la segunda mitad de a será $F_k(0^{\lambda-1}||1)$ y la primera mitad de b será $F_k(0^{\lambda-1}||1)$, también, por lo que la probabilidad es

   $$\Pr_{k \sim U_\lambda}[D_F^{F_k}(1^{\lambda-1}) = 1] = 1$$

   Por otro lado, la probabilidad cuando se tiene un f cualquiera como oráculo, corresponde a la probabilidad de que las dos mitades sean iguales, y el análisis es el mismo que para una distribución uniforme de largo λ, por lo que

   $$\Pr_{f \sim \mathcal{F}_\lambda}[D_F^{f}(1_\lambda) = 1] = 1/2^{\lambda}$$

De este modo la probabilidad siguiente se vuelve no negligible, de modo que no es PRF.

$$\Pr_{k\sim U_\lambda}[D_F^{F_k}(1^{\lambda-1})=1] - \Pr_{f\sim \mathcal{F}_\lambda}[D_F^{f}(1^{\lambda})=1] = 1-1/2^\lambda$$
$$> \text{negl}(\lambda-1)$$

3. $\boldsymbol{F' : \{0,1\}^\lambda \times \{0,1\}^\lambda \to \{0,1\}^\lambda, F'(k,x) = F(x,k)}$

   F' no es PRF. Para mostrarlo consideraré un F que si es PRF para el cual, utilizandolo en F' se puede construir un distinguidor.

   Sea F'' una PRF, se define F de la siguiente forma:

$$F = \begin{cases} F''(k,x) & \text{si } k \neq 0^\lambda \\ 0^\lambda & \text{si } k = 0^\lambda \end{cases}$$

   Es posible demostrar por contrapositivo que si F'' es PRF entonces F también lo es. Es sencillo, sin embargo, notar que F es PRF puesto que solo difiere en un elemento, 0^λ. Desde el punto de vista de las probabilidades, como ese elemento es solamente 1 de un universo de 2^λ, es negligible la probabilidad de distinguir, ya que el caso se presenta una cantidad negligible de veces.

   Volviendo al análisis, usando este F propuesto para F', se puede construir el siguiente distinguidor D_F con acceso al oráculo $\mathcal{O}$.

   - $a = \mathcal{O}(0^\lambda)$
   - si $a = 0^\lambda$ output 1
   - en otro caso output 0

   Haciendo el análisis de probabilidades, se tiene que, para el caso en que $\mathcal{O}$ se comporta como F', como le damos el mensaje 0^λ, este será la llave para nuestro F, entonces, el output será siempre el mismo 0^λ, por lo que

$$\Pr_{k\sim U_\lambda}[D_F^{F'_k}(1^{\lambda})=1] = 1$$

   Por el otro lado, si el oráculo se comporta como f, es decir, se comportaría como una distribución uniforme, la probabilidad de que el oráculo arroje 0^λ es 1 caso de entre el total de casos posibles 2^λ, esto es

$$\Pr_{f\sim \mathcal{F}_\lambda}[D_F^{f}(1^{\lambda})=1] = 1/2^\lambda$$

   Finalmente, con esto, se tiene que

$$\Pr_{k\sim U_\lambda}[D_F^{F'_k}(1^{\lambda})=1] - \Pr_{f\sim \mathcal{F}_\lambda}[D_F^{f}(1^{\lambda})=1] = 1-1/2^\lambda$$
$$> \text{negl}(\lambda)$$

Problema 3

PRFs $\implies$ PRGs

Similarmente al argumento utilizado siempre, demostrar lo pedido equivale a, por contrapositivo, demostrar que si el G propuesto no es PRG, entonces F no es PRF.

Pero antes de realizar la demostración para la pseudo-aleatoriedad, cabe señalar que la expansión $\lambda \cdot \ell$ es inmediata. Como F_k es una función cuyo output es de largo λ para todo input, y en la construcción de G, se concatena ℓ veces F_k, entonces trivialmente la expansión de G es $\lambda \cdot \ell$

Volviendo, si G no es pseudo-aleatorio, entonces existe un D_G tal que

$$\Pr[D_G(G(U_\lambda)) = 1] - \Pr[D_G(U_\lambda) = 1] > \text{negl}(\lambda)$$

Lo que se busca es poder crear un distinguidor D_F para F tal que

$$\Pr_{k \sim U_\lambda}[D_F^{F_k}(1^\lambda) = 1] - \Pr_{f \sim \mathcal{F}_\lambda}[D_F^{f}(1^\lambda) = 1] > \text{negl}(\lambda)$$

Donde tanto k como f son elegidos uniformemente de sus respectivos conjuntos. Para construir D_F, se tiene el oráculo $\mathcal{O}$ que responde en tiempo constante cuando se le solicita un input.

Para el distinguidor, como puede consultar cuantas veces quiera al oráculo, sea

$$y_i = \mathcal{O}(i) \ \forall i \in \{0, ..., \ell\}$$

Armando entonces la siguiente expresión para y:

$$y = y_1 || y_2 || ... || y_\ell$$

Ahora, el distinguidor tras tener construido y, llama al distinguidor que ya sabemos que existe, D_G, de modo que su procedimiento es

- $b \leftarrow D_G(y)$
- output b

El análisis es el siguiente, si el oráculo es $F_k(\cdot)$, entonces por construcción de G, se tiene que es exactamente equivalente a y, por lo que el distinguidor gana con probabilidad no negligible. En caso contrario, esto es, el oráculo es $f(\cdot)$, entonces gana con probabilidad negligible.

Desde el punto de vista de las probabilidades, se tiene que, como y es justamente la construcción de G,

$$\Pr_{k \sim U_\lambda}[D_F^{F_k}(1^\lambda) = 1] = \Pr[D_G(G(U_\lambda)) = 1]$$

Por otro lado, las funciones aleatorias f elegidas, son independientes entre si, esto es $f(i)$ es elegida independientemente de $f(j)$ para todo par $i \neq j$. De este modo, y

corresponde a escoger aleatoriamente un número de uns distribución uniforme, ya que cada función se comporta como tal. De esto se tiene que

$$\Pr_{f\sim\mathcal{F}_\lambda}[D_F^f(1^\lambda)=1]=\Pr[D_G(U_\lambda)=1]$$

Entonces, finalmente se tiene que

$$\Pr[D_G(G(U_\lambda))=1]-\Pr[D_G(U_\lambda)=1]=\Pr_{k\sim U_\lambda}[D_F^{F_k}(1^\lambda)=1]-\Pr_{f\sim\mathcal{F}_\lambda}[D_F^f(1^\lambda)=1]>\text{negl}(\lambda)$$

Como el distinguidor para F se reduce a utilizar el distinguidor para G con los mismos resultados de este último, entonces se concluye que existe un D_F construido como se explicitó, tal que F no es una PRF si G no es PRG.

Por lo tanto, por contrapositivo, G ha de ser PRG, ya que F efectivamente es PRF.

■