Clase 4: definiciones de seguridad "bit-guessing"

Fernando Virdia, versión: 0.0.1, junio 2024

Comentario 12 *Este tipo de definición dice que $\mathcal{A}$ no logra distinguir el experimento "$b = 0$" del experimento "$b = 1$", si $\varepsilon \approx 0$.*

Esta intuición puede ser formalizada usando la equivalente definición de "bit-guessing": bajo las condiciones de Definition 7, G es un (ε, t)-PRG si dado el experimento $\overline{\mathsf{Exp}^{\mathrm{PRG}}}$,

$\overline{\mathsf{Exp}^{\mathrm{PRG}}}(\mathcal{A})$

1 : $b \xleftarrow{\$} \{0,1\}$

2 : $b' \leftarrow \mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, b)$

3 : **return** $[\![b = b']\!]$

$$\mathsf{Adv}(\overline{\mathsf{Exp}^{\mathrm{PRG}}}, \mathcal{A}) \coloneqq \left| \Pr[\overline{\mathsf{Exp}^{\mathrm{PRG}}}(\mathcal{A}) \Rightarrow 1] - \frac{1}{2} \right| \leq \frac{\varepsilon}{2}.$$

Lemma 3 *Bajo las condiciones de Definition 7,*

$$\mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{A}) = 2 \cdot \mathsf{Adv}(\overline{\mathsf{Exp}^{\mathrm{PRG}}}, \mathcal{A}).$$

Demostración. Usando el teorema de la probabilidad total,

$$\begin{aligned}
\Pr[\overline{\mathsf{Exp}^{\mathrm{PRG}}}(\mathcal{A}) \Rightarrow 1] &= \Pr[b' = b] \\
&= \Pr[b' = b \mid b = 0]\cancelto{1/2}{\Pr[b = 0]} + \Pr[b' = b \mid b = 1]\cancelto{1/2}{\Pr[b = 1]}.
\end{aligned}$$

Ahora notamos que por definición de $\mathsf{Exp}^{\mathrm{PRG}}$,

$$\begin{aligned}
&\Pr[b' = b \mid b = 0] = \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 0] = 1 - \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1], \\
&\text{y} \quad \Pr[b' = b \mid b = 1] = \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1].
\end{aligned}$$

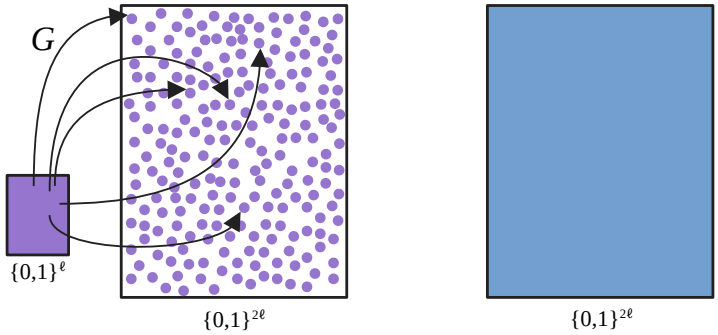
De consecuencia,

$$\begin{aligned}
\mathsf{Adv}(\overline{\mathsf{Exp}^{\mathrm{PRG}}}, \mathcal{A}) &= \left| \Pr[b' = b] - \frac{1}{2} \right| \\
&= \left| \frac{1}{2} \left(\Pr[b' = b \mid b = 0] + \Pr[b' = b \mid b = 1] \right) - \frac{1}{2} \right| \\
&= \left| \frac{1}{2} \left(1 - \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1] + \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1] \right) - \frac{1}{2} \right| \\
&= \frac{1}{2} \left| \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1] \right| \\
&= \frac{1}{2} \mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{A}).
\end{aligned}$$

□

Comentario 13 *Este misma equivalencia vale para la mayor parte de los experimentos que consideramos en criptografía.*

Comentario 14 *Que quieren decir exactamente (ε, t)?*



El output de $G(\cdot) \in \{0,1\}^m$ *es muy lejano de ser uniforme en* $\{0,1\}^m$, **si uno puede ver "de una" la distribución**.

La definición de (ε, t)*-PRG* no dice *que* $G(s \xleftarrow{\$} \{0,1\}^\ell) \sim U(\{0,1\}^m)$ *si no que* un adversario $\mathcal{A}$ que corre en tiempo $\leq t$ *no puede distinguirlas!*

En otras palabras, si un "(ε, t)*-atacante" es un adversario que termina en tiempo* $\leq t$ *con ventaja* $> \varepsilon$*, un sistema* (ε, t)*-seguro es un sistema para el cual no existen* (ε, t)*-atacantes: un atacante requiere correr por tiempo* $> t$ *para obtener ventaja* $> \varepsilon$*, o si corre en tiempo* $\leq t$ *obtiene solamente ventaja* $\leq \varepsilon$.

Contra un sistema (ε, t)*-seguro pueden existir atacantes "triviales".*

- *Por ejemplo, si* $G\colon \{0,1\}^\ell \to \{0,1\}^m$ *con* $m = 2\ell$ *es un* (ε, t)*-PRG, el siguiente atacante corre en tiempo* $\approx 2^\ell$ *y gana con ventaja* $\approx 1 - 2^\ell$*:*

$\mathcal{A}(y \in \{0,1\}^m)$	
1 :	$L = \{\}$
2 :	**for** $x \in \{0,1\}^\ell$:
3 :	$\quad L \leftarrow L \cup \{G(x)\}$
4 :	**if** $y \in L$ **return** "PRG" $(b' = 0)$
5 :	**else return** "random" $(b' = 1)$.

Claramente, $\mathcal{A}$ *corre en tiempo* $\approx 2^\ell$.

EJERCICIO: *Demuestren que* $\mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{A}) \approx 1 - 2^{-\ell}$

Su ventaja es $\mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{A}) = \left|\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1]\right|$*, con* $\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1] = 0$ *(si* $b = 0$*, entonces* $y \in L$ *y* $\mathcal{A}$ *adivina* $b' = 0$ *siempre correctamente), y con* $\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1] = \Pr[y \notin L]$*, que dado* $b = 1 \Leftrightarrow y \notin L$ *pasa con probabilidad* $\approx (1 - 2^{-m})^{2^\ell} \approx 1 - 2^\ell \cdot 2^{-m} = 1 - 2^{-\ell}$.

Esto quiere decir que contra un PRG $G\colon \{0,1\}^\ell \to \{0,1\}^{2\ell}$ *siempre existe un* $(\varepsilon \approx 1 - 2^{-\ell}, t \approx 2^\ell)$*-atacante.*

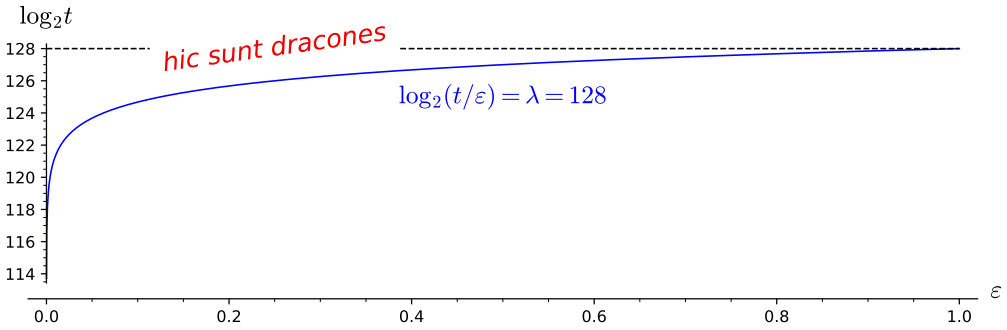
- *En el otro extremo, se considere el siguiente atacante:*

$\mathcal{A}(y \in \{0,1\}^m)$	
1 :	$z \leftarrow G(00\ldots0)$
2 :	**if** $y = z$ **return** "PRG" $(b' = 0)$
3 :	**else return** "random" $(b' = 1)$.

EJERCICIO: *Demuestren que* $\mathcal{A}$ *es un* $(\varepsilon \approx 2^{-\ell}, t \approx 1)$*-atacante. (Idea: el espacio* $G(\{0,1\}^\ell)$ *es mas chico de* $\{0,1\}^{2\ell}$*.)*

Aquí $\mathcal{A}$ *corre en tiempo* $t \approx 1$*, pero con pésima ventaja:* $\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 0) \Rightarrow 1] = \Pr[G(s \xleftarrow{\$} \{0,1\}^\ell) \neq G(0\ldots0)] \approx 1 - 2^{-\ell}$*, mientras* $\Pr[\mathsf{Exp}^{\mathrm{PRG}}(\mathcal{A}, 1) \Rightarrow 1] = \Pr[y \neq G(0\ldots0)] \approx 1 - 2^{-2\ell}$*, que implica* $\mathsf{Adv}(\mathsf{Exp}^{\mathrm{PRG}}, \mathcal{A}) \approx 2^{-\ell} - 2^{-2\ell} \approx 2^{-\ell}$*. Por lo cual existe un* $(\varepsilon \approx 2^{-\ell}, t \approx 1)$*-atacante.*

Comentario 15 *Generalmente, si un sistema ofrece algún tipo* (ε, t)*-"X-security", decimos que ofrece* $\log_2(t/\varepsilon)$ *"bits de seguridad X". Dado* $\lambda = \log_2(t/\varepsilon)$*, obtenemos* $\varepsilon = 2^{-\lambda} \cdot t$*, indicando que con* λ *bits de seguridad, es necesario trabajar* $\approx 2^\lambda$ *tiempo para tener ventaja* ≈ 1*.*



Regresemos al problema del OTP: para cifrar mensajes $m \in \{0,1\}^m$ precisamos transmitir de manera segura una clave $k \sim U(\{0,1\}^m)$.
PREGUNTA: Como podemos usar un PRG?

Idea: Podemos remplazar la clave aleatoria $k \xleftarrow{\$} \{0,1\}^m$ con una clave pseudoaleatoria $k \leftarrow G(s)$, donde $s \xleftarrow{\$} \{0,1\}^\ell$ es mas corta que m.

Definición 8 (PR-OTP) *Sean* $\ell, m \in \mathbb{Z}_{>0}$ *con* $\ell < m$*,* $\mathcal{K} = \{0,1\}^\ell$*,* $\mathcal{M} = \mathcal{C} = \{0,1\}^m$*. Sea* $G\colon \{0,1\}^\ell \mapsto \{0,1\}^m$ *un PRG.* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *es un* one-time pad pseudoaleatorio *(PR-OTP, "pseudorandom OTP"), si*

$\mathsf{Gen}()$	$\mathsf{Enc}(k, m)$	$\mathsf{Dec}(k, c)$
1 : $k \xleftarrow{\$} \mathcal{K}$	1 : $c \leftarrow m \oplus G(k)$	1 : $m' \leftarrow c \oplus G(k)$
2 : **return** k	2 : **return** c	2 : **return** m'

Comentario 16 *El nuevo cifrado* no otorga secreto perfecto. *En la demostración del OTP, el pasaje clave era*

$$\Pr[k = c \oplus m_0] = \Pr[k = c \oplus m_1] \quad \forall m_0, m_1, c$$

Dado $G\colon \{0,1\}^5 \to \{0,1\}^{10}$*, no todo valor en* $\{0,1\}^{10}$ *tiene una "pre-imagen" en* $\{0,1\}^5$*. Es posible que* $\exists m_0, m_1, c$ *tales que* $\Pr[G(k) = c \oplus m_0] > 0$ *y* $\Pr[G(k) = c \oplus m_1] = 0$*.*

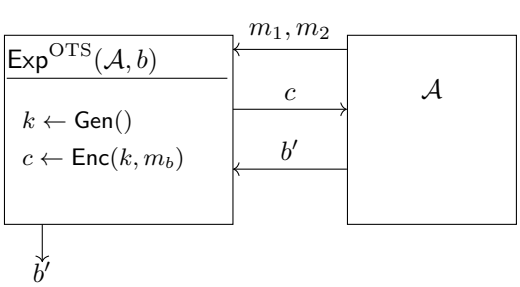
PREGUNTA: Alguien tiene alguna idea de que podemos intentar demostrar?
Idea: Podríamos intentar demostrar OT ε-secrecy?

Como vimos, dándole suficiente tiempo al adversario, todo PRG es inseguro. Las demostraciones en criptografía son del tipo "si $\exists$ un ataque en el esquema $\Rightarrow \exists$ un ataque en el componente", y solo tienen sentido si creemos que $\nexists$ un ataque en el componente.

Necesitamos una definición de seguridad que considere un adversario con tiempo limitado.

Definición 9 (One-time (ε, t)**-secrecy)** *Sea* $\Pi = (\mathsf{Gen}, \mathsf{Enc}, \mathsf{Dec})$ *un SKES. Dado un adversario* $\mathcal{A} = (\mathcal{A}_1, \mathcal{A}_2)$ *y un bit* $b \in \{0,1\}$*, definimos el experimento* $\mathsf{Exp}^{OTS}(\mathcal{A}, b)$*,*

$\mathsf{Exp}^{OTS}(\mathcal{A}, b)$
1 : $k \leftarrow \mathsf{Gen}()$
2 : $m_0, m_1, \sigma \leftarrow \mathcal{A}_1()$
3 : $c \leftarrow \mathsf{Enc}(k, m_b)$
4 : $b' \leftarrow \mathcal{A}_2(c, \sigma)$
5 : **return** b'



Decimos que Π *otorga* one-time (ε, t)-secrecy[3] *si para cualquier adversario* $\mathcal{A}$ *que corre en tiempo* $\leq t$ *y produce mensajes de igual de largo* $|m_0| = |m_1|$, *su* ventaja *("advantage") en distinguir* $b = 0$ *de* 1 *es*

$$\left|\Pr[\mathsf{Exp}^{OTS}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\mathsf{Exp}^{OTS}(\mathcal{A}, 1) \Rightarrow 1]\right| \leq \varepsilon.$$

Hasta ahora habíamos visto definiciones de seguridad "information-theoretical" (secreto perfecto; "para cualquier $\mathcal{A} \ldots \Pr = \Pr$"), y "estadistica" ($\varepsilon$-secrecy, "para cualquier $\mathcal{A} \ldots | \Pr - \Pr | \leq \varepsilon$"). Finalmente llegamos a una definición de seguridad "computacional":

"para cualquier $\mathcal{A}$ **en tiempo** $\leq t \ldots | \Pr - \Pr | \leq \varepsilon$".

Es esta relajación de requisitos que nos permite de obtener la mayor parte de las garantías criptográficas.

[3] "EAV-security" en [KL20], "semantic security" en [BS23].