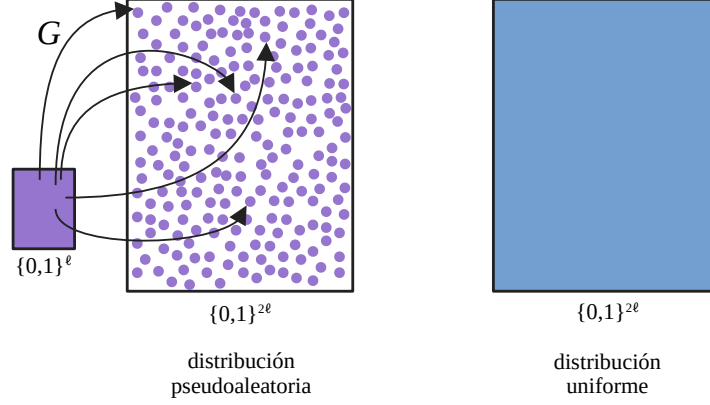


Clase 4: Bit security y OTP computacional

Fernando Virdia, versión: 0.1, mayo 2025

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



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!

Definición 8 ((ε, t) -atacante). Sean $\varepsilon \in [0, 1]$, $t \geq 1$. Dado una experimento de seguridad Exp , un (ε, t) -Exp-atacante contra Exp es un algoritmo (posiblemente aleatorio) $\mathcal{A}$ que corre en tiempo $\leq t$ con ventaja $\text{Adv}(\text{Exp}, \mathcal{A}) \geq \varepsilon$.

Definición 9 ((ε, t) -seguridad). Sea Π una primitiva criptográfica, y sea “X” una noción de seguridad con experimento Exp^X . Decimos que Π otorga (ε, t) -X-seguridad si no existe ningún (ε, t) - Exp^X -atacante contra Π .

En otras palabras, cualquier algoritmo $\mathcal{A}$ que juegue Exp^X ,

- o si corre en tiempo $\leq t$ pero obtiene solamente ventaja $< \varepsilon$,
- o corre en tiempo $> t$ para obtener ventaja $\geq \varepsilon$.

Comentario 15. Contra un sistema (ε, t) -seguro pueden existir atacantes “triviales”. Estos sugieren un máximo nivel de seguridad que un tipo de primitiva puede obtener.

- Por ejemplo, si $G: \{0, 1\}^\ell \rightarrow \{0, 1\}^m$ con $m = 2\ell$ es una función aleatoria en $\text{Func}(\{0, 1\}^\ell, \{0, 1\}^m)$, el siguiente atacante corre en tiempo $\approx 2^\ell$ y gana con ventaja $\approx 1 - 2^{-\ell}$:

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

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

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

Su ventaja es $\text{Adv}(\text{Exp}^{\text{PRG}}, \mathcal{A}) = \left| \Pr[\text{Exp}^{\text{PRG}}(\mathcal{A}, 0) \Rightarrow 1] - \Pr[\text{Exp}^{\text{PRG}}(\mathcal{A}, 1) \Rightarrow 1] \right|$, con $\Pr[\text{Exp}^{\text{PRG}}(\mathcal{A}, 0) \Rightarrow 1] = 0$ (si $b = 0$, entonces $y \in L$ y $\mathcal{A}$ adivina $b' = 0$ siempre correctamente), y con $\Pr[\text{Exp}^{\text{PRG}}(\mathcal{A}, 1) \Rightarrow 1] = \Pr[y \notin L]$, 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 $G: \{0, 1\}^\ell \rightarrow \{0, 1\}^{2\ell}$ 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: $z \leftarrow G(00 \dots 0)$
2: if $y = z$ return 0 ($b' = 0$, “PRG”)
3: else return 1 ($b' = 1$, “random”).

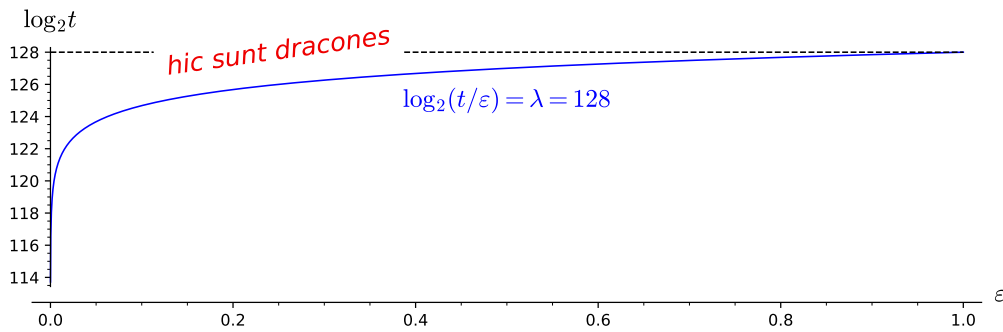
EJERCICIO: Demuestren que $\mathcal{A}$ es un $(\varepsilon \approx 2^{-\ell}, t \approx 1)$ -atacante. (Idea: el espacio $G(\{0, 1\}^\ell)$ es mas chico de $\{0, 1\}^{2\ell}$.)

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

Definición 10 (λ -bits de seguridad). Sea Π una primitiva criptografica, y sea “ X ” una nocion de seguridad con experimento Exp^X . Supongamos que existe $\lambda \in \mathbb{Z}_{>0}$ tal que para cualquier $\varepsilon \in [0, 1]$, Π otorga (ε, t) - X -seguridad con $t \geq 2^\lambda \cdot \varepsilon$. Entonces decimos que Π otorga λ bits de X -seguridad.

Comentario 16. Si una primitiva otorga λ -bits de seguridad, esto quiere decir que

- es necesario trabajar un tiempo $\geq 2^\lambda$ para obtener ventaja ≈ 1 ,
- trabajando un tiempo $t \approx 1$ solamente se puede obtener ventaja $\approx 2^{-\lambda}$,
- trabajando un tiempo $t \approx \sqrt{2^\lambda}$ se puede obtener una ventaja $\approx 1/\sqrt{2^\lambda}$.



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 k ($= m$).

Definición 11 (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 $G: \{0, 1\}^\ell \mapsto \{0, 1\}^m$ un PRG. $\Pi = (\text{Gen}, \text{Enc}, \text{Dec})$ es un one-time pad pseudoaleatorio (PR-OTP, “pseudorandom OTP”), si

$\text{Gen}()$	$\text{Enc}(k, m)$	$\text{Dec}(k, c)$
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 17. 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 $G: \{0, 1\}^5 \rightarrow \{0, 1\}^{10}$, 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 $\Pr[G(k) = c \oplus m_1] = 0$.

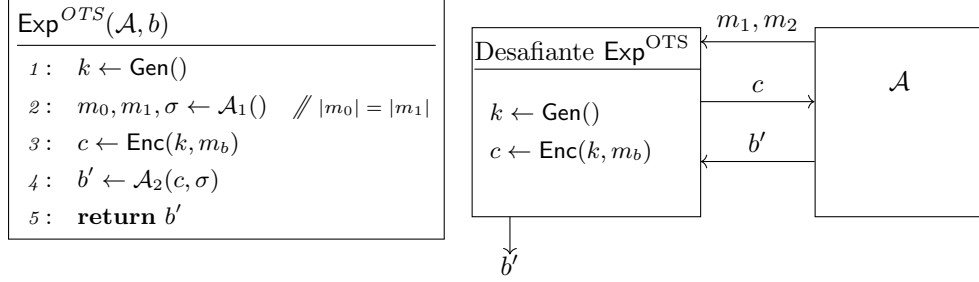
PREGUNTA: Alguien tiene alguna idea de que podemos intentar demostrar?

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



Decimos que Π otorga one-time (ε, t) -secrecy³ 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

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

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

“para cualquier $\mathcal{A}$ en tiempo $\leq t \dots |\Pr - \Pr| \leq \varepsilon$ ”.

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].