Chosen Plaintext Attack (CPA)

Una breve introducción con ejemplos prácticos

Emanuel Nicolás Herrador

Facultad de Matemática, Astronomía, Física y Computación

Septiembre 2025

Índice

Motivación

Encriptación donde un tercero (*atacante*) tiene acceso al oráculo de encriptación. I.e., puede dar múltiples mensajes y obtener sus correspondientes cifrados.

Ejemplo 1

Ana usando un servidor encriptando varios archivos con una misma key corta.

Ejemplo 2

Comunicación no sincronizada entre Ana y Bob compartiendo una sola key en una red insegura.

Idea I

Tipo de cifrado

Si el cifrado es determinístico $\Rightarrow$ Es inseguro para este uso.

Si es determinístico, entonces leakea información sobre el contenido porque se puede ver fácilmente si dos mensajes son iguales. Además, deja abierto muchos ataques para obtener la key en base a los diferentes mensajes cifrados de los plaintexts enviados por el atacante explotando alguna vulnerabilidad del cifrado en sí o su implementación.

Idea II

¿Qué usaremos?

Si queremos un cifrado que no sea vulnerable en este escenario, necesitaremos hacer uso de *cifrados probabilísticos*.

De modo que diferentes encriptaciones de un mismo mensaje bajo la misma key (generalmente) producen diferentes ciphertexts.

Seguridad

La seguridad buscada en este escenario es *semantic security against chosen plaintext attack*, o también conocida como *CPA-security*.

Índice

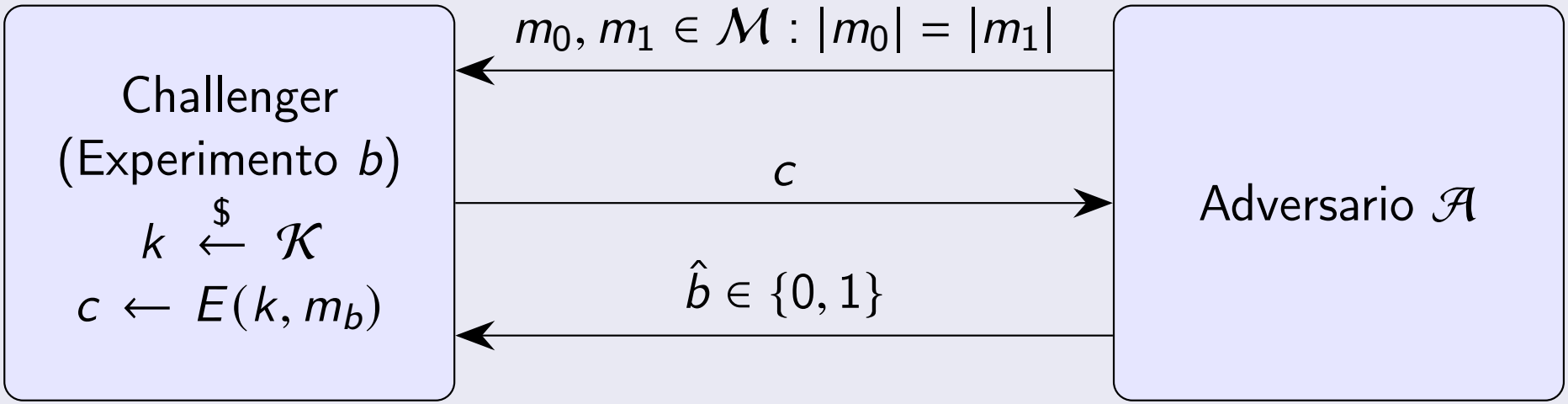
Contenido

Se hará un repaso de temas anteriores del libro: **semantic security** y **PRF**.
Se presentarán, de forma general, los conceptos de **multi-key semantic security** y **CPA-security**; junto con **construcciones de cifrados** CPA-secure (construcción genérica, randomized counter mode, CBC) junto con sus versiones **nonce-based**.
En cuanto a ejemplos, se verán **vulnerabilidades en cifrados determinísticos** (AES ECB mode) y **mal uso del nonce** (AES CTR mode).

Índice

Definición 3 (Semantic security game)

Dados cifrado $\mathcal{E} = (E, D)$ definido sobre $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ y adversario $\mathcal{A}$, definimos dos experimentos $(b = 0, 1)$ como:



Sea W_b el evento donde $\mathcal{A}$ envía $\hat{b} = 1$ en el Experimento b, la ventaja de $\mathcal{A}$ sobre semantic security respecto a $\mathcal{E}$ es:

$$\mathrm{SSadv}[\mathcal{A}, \mathcal{E}] := |\Pr[W_0] - \Pr[W_1]|$$

Repaso II

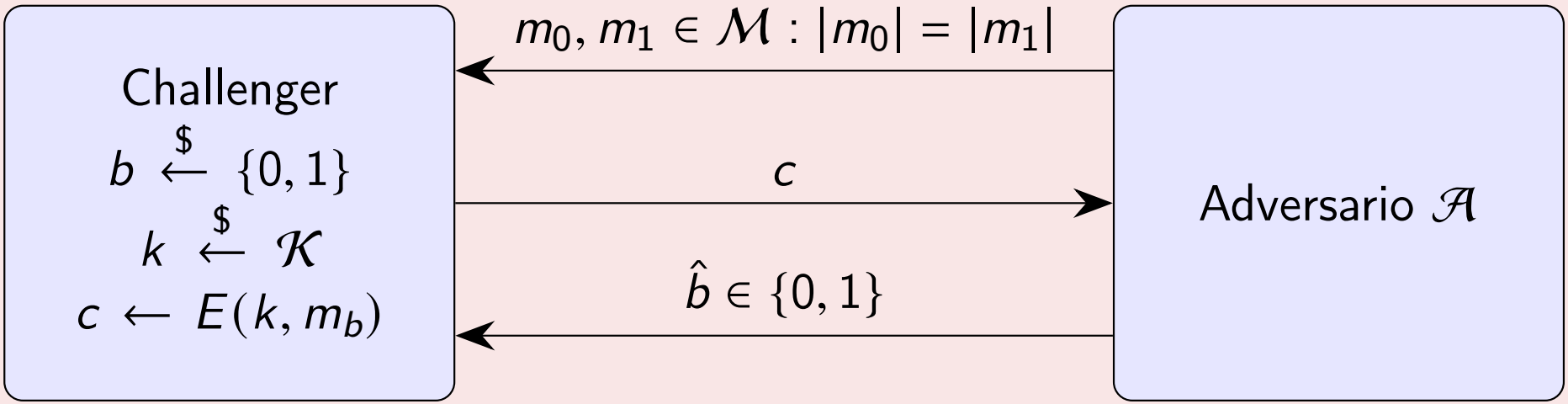
Definición 4 (Semantic security)

$\mathcal{E}$ es semánticamente seguro si para todo adversario $\mathcal{A}$ eficiente, $\mathrm{SSadv}[\mathcal{A}, \mathcal{E}]$ es despreciable.

Repaso III

Versión bit-guessing

Se considera el siguiente juego donde $\mathcal{A}$ gana si $\hat{b} = b$.



Donde si el evento W es cuando $\mathcal{A}$ gana, la ventaja es:

$$\mathsf{SSadv}^*[\mathcal{A}, \mathcal{E}] = \left| \Pr[W] - \frac{1}{2} \right|$$

Se cumple que $\mathsf{SSadv}[\mathcal{A}, \mathcal{E}] = 2 \cdot \mathsf{SSadv}^*[\mathcal{A}, \mathcal{E}]$.

Repaso IV

Idea sobre PRF

Sean $\mathcal{K}, \mathcal{X}, \mathcal{Y}$ conjuntos finitos y $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$, se pretende que F sea un algoritmo determinista eficiente y tal que $F(k, \cdot)$ *luzca* como una función random $\mathcal{X} \to \mathcal{Y}$.
Es decir, que $F(k, \cdot)$ parezca elegida uniformemente del conjunto $\text{Funs}[\mathcal{X}, \mathcal{Y}]$ de todas las funciones $f : \mathcal{X} \to \mathcal{Y}$.

Idea sobre seguridad de PRF

Sigue el mismo esquema que el anterior solo que los adversarios tienen Q queries antes de tener que adivinar el tipo de experimento (si viene de F o de $\text{Funs}[\mathcal{X}, \mathcal{Y}]$).
La ventaja se define de la misma forma, al igual que los PRFs seguros y su versión bit-guessing.

Índice

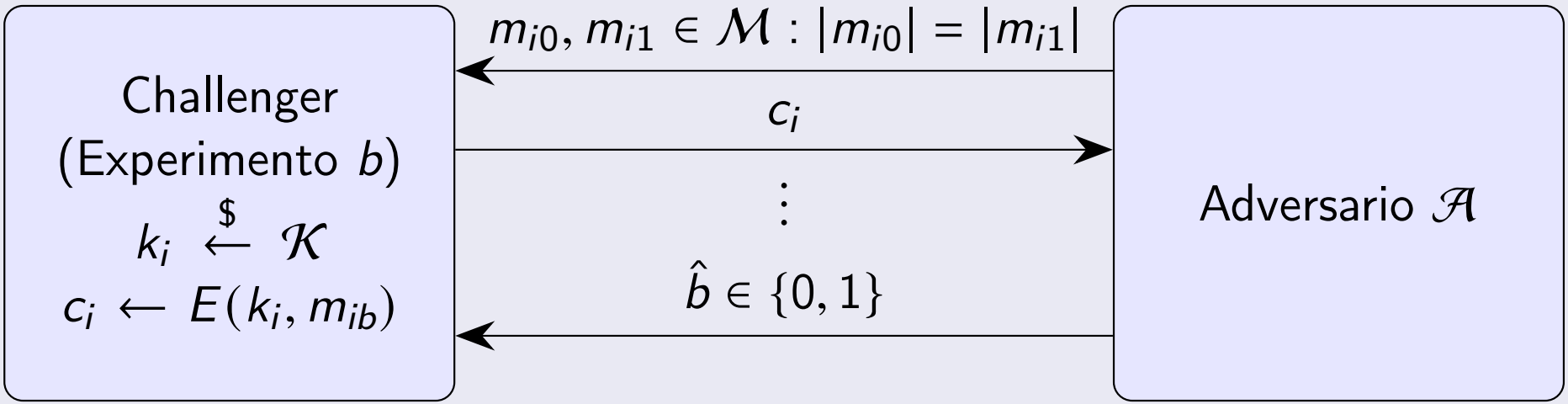
Multi-key attacks I

Dado un cifrado semánticamente seguro, ¿puedo usarlo para cifrar más de un mensaje tomando claves diferentes para cada uno?

Multi-key attacks II

Definición 5 (Multi-key semantic security)

Dado cifrado $\mathcal{E} = (E, D)$ definido sobre $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ y adversario $\mathcal{A}$, definimos los experimentos $b = 0, 1$ (con q queries) como:



La ventaja es

$$\mathrm{MSSadv}[\mathcal{A}, \mathcal{E}] := |\Pr[W_0] - \Pr[W_1]|$$

y $\mathcal{E}$ es semánticamente seguro para múltiples claves si para todo adversario $\mathcal{A}$ la ventaja es despreciable.

Multi-key attacks III

Teorema 6

Si $\mathcal{E}$ es semánticamente seguro, entonces es también semánticamente seguro para múltiples claves.
I.e., semantic security $\Rightarrow$ multi-key semantic security.

Demostración.

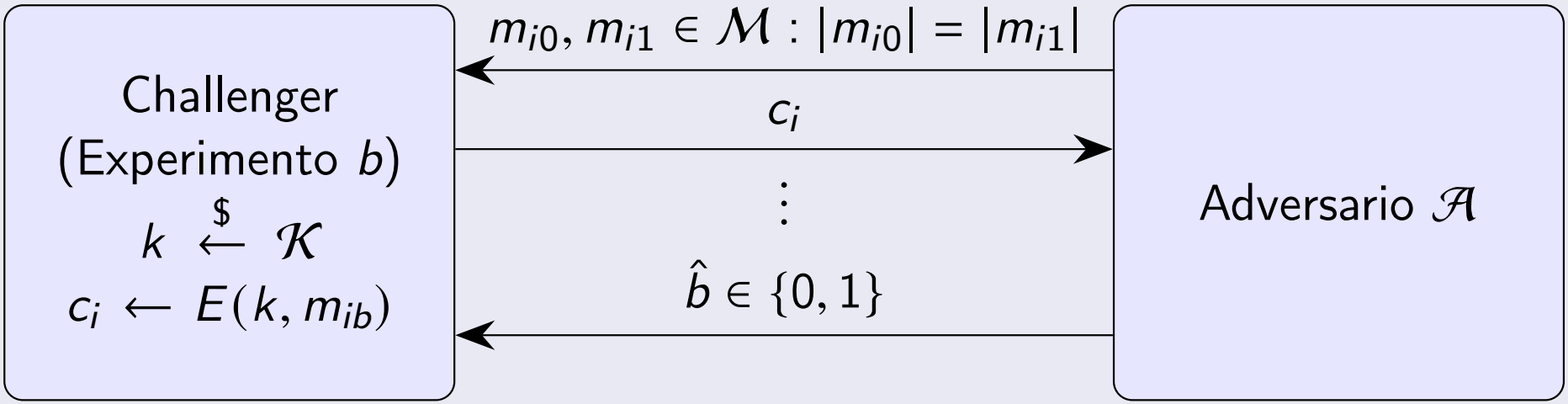
Supongamos el juego visto antes para multi-key security. Como $\mathcal{E}$ es semánticamente seguro, entonces si para $i \xleftarrow{\$} \{1, \ldots, k\}$ modifico el Challenger para que encripte $m_{i\bar{b}}$ en vez de m_{ib} (donde $\bar{b}$ es el complemento de b en $\{0, 1\}$), entonces $\mathcal{A}$ no puede notar la diferencia. Siguiendo el argumento para las Q queries, cambiamos todo el experimento completo. Luego, $\mathcal{A}$ no puede distinguir tampoco el juego multi-key. $\square$

Índice

CPA security I

Definición 7 (CPA security)

Dados $\mathcal{E} = (E, D)$ definido sobre $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ y adversario $\mathcal{A}$, definimos los experimentos $b = 0, 1$ con queries como:



Donde la ventaja es:

$$\mathrm{CPAadv}[\mathcal{A}, \mathcal{E}] := |\Pr[W_0] - \Pr[W_1]|$$

Y $\mathcal{E}$ es *CPA secure* si $\forall \mathcal{A}$ adversario eficiente, su ventaja es despreciable.

CPA security II

Nota

El juego es el mismo que para multi-key semantic security solo que se usa una sola key k.

Tiene la variante bit-guessing donde $\mathsf{CPAadv}^*[\mathcal{A}, \mathcal{E}] := \left|\Pr[\hat{b} = b] - \frac{1}{2}\right|$ y $\mathsf{CPAadv}^*[\mathcal{A}, \mathcal{E}] = 2 \cdot \mathsf{CPAadv}^*[\mathcal{A}, \mathcal{E}]$.

Se suele llamar también como **IND-CPA** (indistinguishable against chosen plaintexts attacks) porque el juego sobre el que se define este concepto de seguridad se basa en no poder distinguir de qué mensaje viene el ciphertext. Es decir, que parezca uniformemente distribuido en $\mathcal{C}$.

Índice

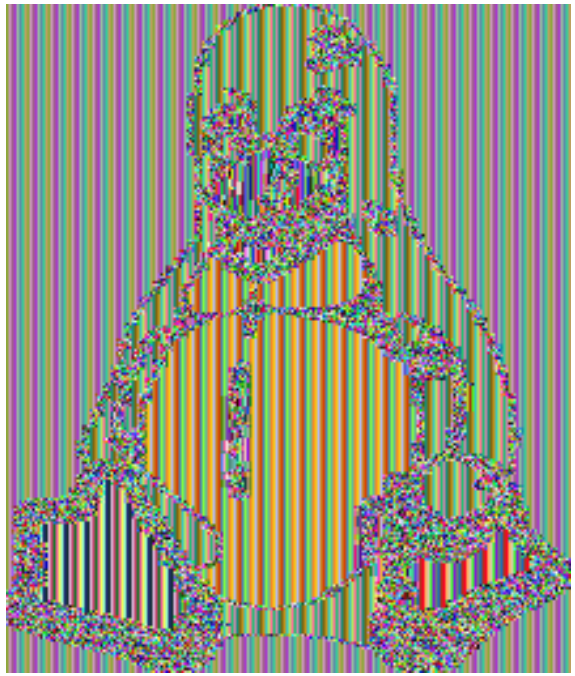
Casos sencillos

Algunos ejemplos de cifrados vulnerables ante CPA son *caesar cipher*, *Vignère* o *XOR simple* con misma key.
Uno más complejo es *RC4* cuando se reutiliza la misma clave k para varios mensajes (debido a que se repite el keystream), dado que se puede recuperar todo el keystream. Sin embargo, el caso donde no se repite sigue siendo inseguro porque $\mathcal{A}$ puede enviar varios plaintexts y observar los correspondientes ciphertexts para recuperar parcialmente la key debido a que los primeros bytes del keystream generado están sesgados (no son del todo aleatorios).

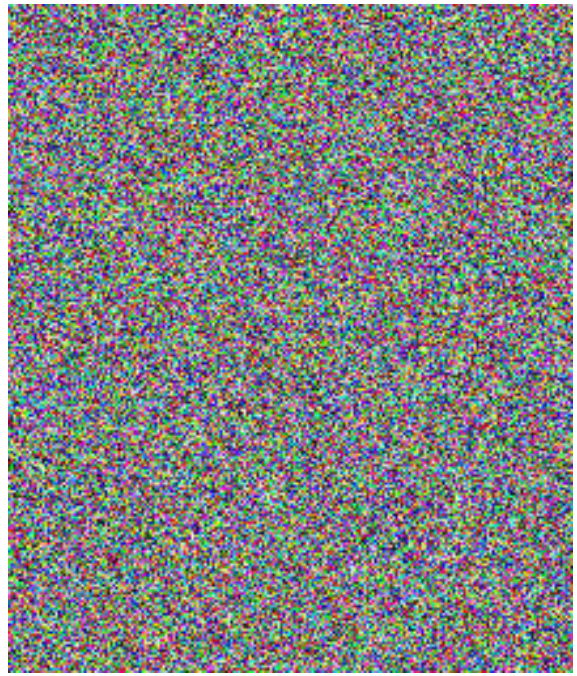
ECB vs. CBC I

Considerando el cifrado por bloques AES, el modo ECB es determinístico mientras que CBC probabilístico. Podemos ver el leakage de ECB en el ejemplo de encriptar una imagen:

(a) Imagen original



(b) Modo ECB



(c) Modo CBC

ECB vs. CBC II

¿Cómo obtener estas imágenes?

El código es análogo tanto para ECB como para CBC:

```
magick Tux.svg Tux.ppm
head -n 3 Tux.ppm > header.txt
tail -n +4 Tux.ppm > body.bin
openssl enc -aes-128-ecb -nosalt -pass pass:"password" -in
  ↪  body.bin -out body.ecb.bin
cat header.txt body.enc.bin > Tux.ecb.ppm
magick Tux.ecb.ppm Tux-ecb.svg
```

Ejemplo 8

Demo CTF challenge de CryptoHack: ECB Oracle.

Índice

Construcción genérica I

Veremos cómo convertir cualquier cifrado semánticamente seguro $\mathcal{E} = (E, D)$ en un cifrado $\mathcal{E}'$ CPA secure usando una PRF F adecuada.

Construcción

Sea $\mathcal{E} = (E, D)$ definido sobre $(\mathcal{K}, \mathcal{M}, \mathcal{C})$ y F una PRF definida sobre $(\mathcal{K}', \mathcal{X}, \mathcal{K})$, definimos $\mathcal{E}' = (E', D')$ definido sobre $(\mathcal{K}', \mathcal{M}, \mathcal{X} \times \mathcal{C})$ como:

Algoritmo 1: $E'(k', m)$

Input: $k' \in \mathcal{K}', \ m \in \mathcal{M}$
Output: $(x, c) \in \mathcal{X} \times \mathcal{C}$
$x \xleftarrow{\$} \mathcal{X}$
$k \leftarrow F(k', x)$
$c \leftarrow E(k, m)$
return (x, c)

Algoritmo 2: $D'(k', c')$

Input: $k' \in \mathcal{K}, c' = (x, c) \in \mathcal{X} \times \mathcal{C}$
Output: $m \in \mathcal{M}$
$k \leftarrow F(k', x)$
$m \leftarrow D(k, c)$
return m

Construcción genérica II

Teorema 9

Si F es una PRF segura, $\mathcal{E}$ un cifrado semánticamente seguro y $N := |\mathcal{X}|$ super-poly (i.e., tal que $\frac{1}{N}$ es despreciable), entonces el cifrado $\mathcal{E}'$ definido anteriormente es CPA seguro.
Además, sea $\mathcal{A}$ el adversario que ataca a $\mathcal{E}'$, su ventaja cumple que:

$$CPAadv[\mathcal{A}, \mathcal{E}'] \leq \frac{Q^2}{N} + 2 \cdot PRFadv[\mathcal{B}_F, F] + Q \cdot SSadv[\mathcal{B}_\mathcal{E}, \mathcal{E}]$$

donde se considera el juego de CPA-security con Q queries, y tal que existen los adversarios $\mathcal{B}_F$ que ataca al juego de PRF security, y $\mathcal{B}_\mathcal{E}$ para el de semantic security. $\mathcal{B}_F, \mathcal{B}_\mathcal{E}$ son elementos del adversario $\mathcal{A}$.

Construcción genérica III

Nota

Se pide que $\frac{1}{N}$ sea despreciable para que la probabilidad de que F genere el mismo valor x dos veces sea despreciable.

Idea de la demostración.

Como F es una PRF segura, entonces podemos reemplazar F como una verdadera función random. Usando la suposición de que N es super-poly, entonces la probabilidad de que dos valores $x \in \mathcal{X}$ generados sean el mismo, es despreciable. Luego, en este escenario eso significa que las claves del challenger son todas generadas de forma independiente. Finalmente, el juego se reduce al de multi-key security. Por ello, por teorema como $\mathcal{E}$ es semánticamente seguro, también es semánticamente seguro para claves múltiples. Esto se puede extender a $\mathcal{E}'$. □

Randomized counter mode I

Construcción

Sea $F : \mathcal{K} \times \mathcal{X} \to \mathcal{Y}$ una PRF con $\mathcal{X} = \{0, \ldots, N-1\}$, $\mathcal{Y} = \{0,1\}^n$. Para cualquier $\ell \geq 1$ acotado polinómicamente, definimos el cifrado $\mathcal{E} = (E, D)$ sobre $(\mathcal{K}, \mathcal{Y}^{\leq \ell}, \mathcal{X} \times \mathcal{Y}^{\leq \ell})$ como:

Algoritmo 3: $E(k, m)$

Input: $k \in \mathcal{K}, m \in \mathcal{Y}^{\leq \ell} : v := |m|$
Output: $(x, c) \in \mathcal{X} \times \mathcal{Y}^v$
$x \xleftarrow{\$} \mathcal{X}$
for $j \leftarrow 0$ ***to*** $v - 1$ **do**
  $c[j] \leftarrow F(k, x + j \mod N) \oplus m[j]$
return (x, c)

Algoritmo 4: $D(k, c')$

Input: $k \in \mathcal{K}, c' = (x, c) \in \mathcal{X} \times \mathcal{Y}^{\leq \ell}$:
  $v := |c|$
Output: $m \in \mathcal{Y}^v$
for $j \leftarrow 0$ ***to*** $v - 1$ **do**
  $m[j] \leftarrow F(k, x + j \mod N) \oplus c[j]$
return m

La componente x del ciphertext es llamada típicamente como *valor inicial* o **IV**.

Randomized counter mode II

Teorema 10

Si F es una PRF segura y N super-poly, entonces para cualquier $\ell \geq 1$ acotado polinómicamente, el cifrado $\mathcal{E}$ definido anteriormente es CPA seguro.
Además, sea $\mathcal{A}$ el adversario que ataca a $\mathcal{E}'$ en el juego de CPA-security con Q queries, su ventaja cumple que:

$$CPAadv[\mathcal{A}, \mathcal{E}] \leq \frac{2Q^2\ell}{N} + 2 \cdot PRFadv[\mathcal{B}, F]$$

donde $\mathcal{B}$ es el adversario que ataca a F en el juego de PRF security y es un elemento de $\mathcal{A}$.

Randomized counter mode III

Idea de la demostración.

Como F es PRF segura, podemos reemplazarla por una función random f. Como N es super-poly y cada IV es elegido random, entonces el challenger nunca evalúa f en el mismo punto dos veces, excepto con probabilidad despreciable. En este escenario, significa que la encriptación de cada mensaje es un OTP independiente. Luego, la ventaja de $\mathcal{A}$ en CPA-security game es despreciable. □

Modo CBC I

Como ejemplo de un cifrado por bloques CPA seguro:

Construcción

Dados $\mathcal{E} = (E, D)$ un cifrado por bloques definido sobre $(\mathcal{K}, \mathcal{X})$ donde $\mathcal{X} = \{0,1\}^n$; $N := |\mathcal{X}| = 2^n$ y $\ell \geq 1$ acotado polinómicamente, entonces definimos el cifrado $\mathcal{E}' = (E', D')$ sobre $(\mathcal{K}, \mathcal{X}^{\leq \ell}, \mathcal{X}^{\leq \ell+1} \setminus \mathcal{X}^0)$ como:

Algoritmo 5: $E'(k, m)$

Input: $k \in \mathcal{K}, m \in \mathcal{X}^{\leq \ell} : v := |m|$
Output: $c \in \mathcal{X}^{\leq \ell+1} \setminus \mathcal{X}^0$
$c[0] \xleftarrow{\$} \mathcal{X}$
for $j \leftarrow 0$ ***to*** $v - 1$ **do**
  $c[j+1] \leftarrow E(k, c[j] \oplus m[j])$
return c

Algoritmo 6: $D'(k, c)$

Input: $k \in \mathcal{K}, c \in \mathcal{X}^{\leq \ell+1 \setminus \mathcal{X}^0} : v := |c| - 1$
Output: $m \in \mathcal{X}^v$
for $j \leftarrow 0$ ***to*** $v - 1$ **do**
  $m[j] \leftarrow D(k, c[j+1]) \oplus c[j]$
return m

Aquí, la primer componente $c[0]$ es el IV.

Modo CBC II

Teorema 11

Si $\mathcal{E} = (E, D)$ es un cifrado seguro por bloques definido sobre $(\mathcal{K}, \mathcal{X})$ y $N := |\mathcal{X}|$ es super-poly, entonces para cualquier $\ell \geq 1$ acotado polinómicamente, el cifrado $\mathcal{E}'$ definido anteriormente es CPA seguro. Sea $\mathcal{A}$ el adversario para CPA de $\mathcal{E}'$ con Q queries, su ventaja cumple:

$$CPAadv[\mathcal{A}, \mathcal{E}'] \leq \frac{2Q^2\ell^2}{N} + 2 \cdot BCadv[\mathcal{B}, \mathcal{E}]$$

donde $\mathcal{B}$ es el adversario que ataca a $\mathcal{E}$ en el juego de seguridad de cifrados por bloques, y que forma parte de $\mathcal{A}$.

Modo CBC III

Demostración.

La prueba es análoga a la anterior porque por corolario de **PRF Switching Lemma**, $\mathcal{E} = (E, D)$ cifrado por bloques definido sobre $(\mathcal{K}, \mathcal{X})$ con $N := |\mathcal{X}|$ super-poly es un cifrado por bloques seguro si y solo si E es una PRF segura. □

Nota

No agrego PRF Switching Lemma como contenido de repaso o adicional porque requiere agregar también las nociones de concepto de cifrado por bloques y su seguridad.

Índice

Encriptación nonce-based I

Todos los esquemas de cifrado vistos sufren de *expansión del ciphertext*, es decir, los mensajes cifrados son más largos que los originales. Para ello, la idea es agregar un input más $\mathcal{N}$ a los algoritmos de encriptación y decriptación; convirtiendo a estos ahora en determinísticos.
La intención es que un mensaje encriptado con un nonce debe ser desencriptado con el mismo nonce.

Correctitud

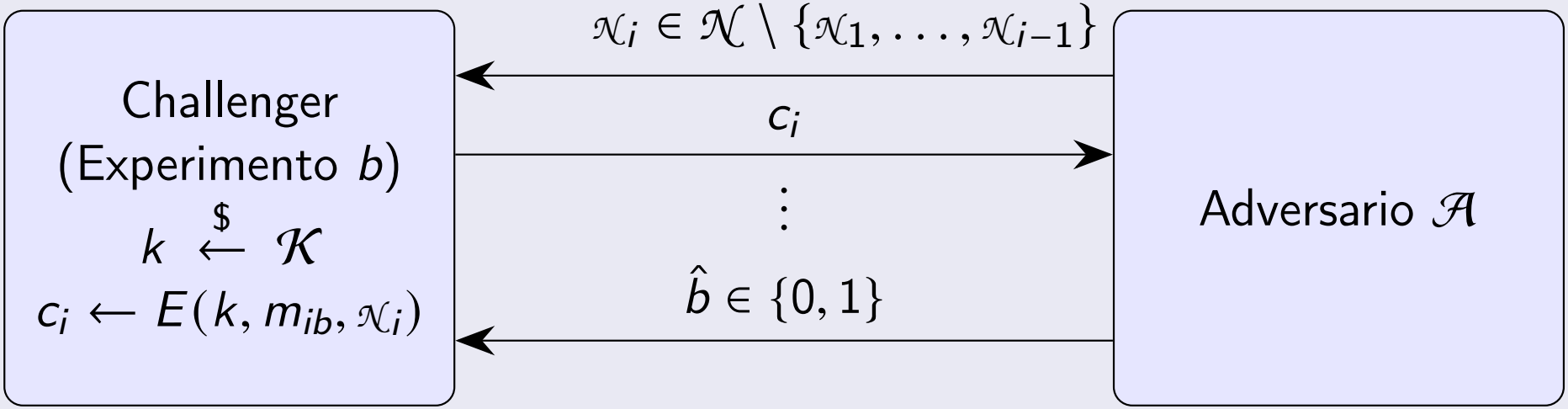
$\forall k \in \mathcal{K}, m \in \mathcal{M}, \mathcal{N} \in \mathcal{N}, \ D(k, E(k, m, \mathcal{N}), \mathcal{N}) = m.$

Encriptación nonce-based II

Definición 12 (nonce-based CPA security)

Dados cifrado $\mathcal{E} = (E, D)$ definido sobre $(\mathcal{K}, \mathcal{M}, \mathcal{C}, \mathcal{N})$, y adversario $\mathcal{A}$, se definen los experimentos $b = 0, 1$ como:

$$m_{i0}, m_{i1} \in \mathcal{M} : |m_{i0}| = |m_{i1}|$$



La ventaja se define como:

$$\text{nCPAadv}[\mathcal{A}, \mathcal{E}] := |\Pr[W_0] - \Pr[W_1]|$$

Encriptación nonce-based III

Nota

La ventaja se define asumiendo que ningún nonce es usado más de una vez en el proceso de encriptación.
También se define su versión bit-guessing con

$$\mathsf{nCPAadv}[\mathcal{A}, \mathcal{E}] = 2 \cdot \mathsf{nCPAadv}^*[\mathcal{A}, \mathcal{E}]$$

donde $\mathsf{nCPAadv}^*[\mathcal{A}, \mathcal{E}] := \left|\Pr[\hat{b} = b] - \frac{1}{2}\right|$

Definición 13 (nonce-based CPA security)

Un cifrado $\mathcal{E}$ nonce-based es CPA seguro si para todo adversario eficiente $\mathcal{A}$, la ventaja $\mathsf{nCPAadv}[\mathcal{A}, \mathcal{E}]$ es despreciable.

Modificaciones a ciphers CPA-secure para ser nonce-based I

Cifrado genérico nonce-based

Se debe tratar el valor $x \in \mathcal{X}$ como un nonce.

Nonce-based counter mode

Asumiendo que $\ell | N$ (en la práctica son potencias de 2), $\mathcal{N} = \{0, \ldots, \frac{N}{\ell} - 1\}$ y el input a la PRF F debe ser $x := \mathcal{N}\ell$. De este modo, $\mathcal{N}_1 \neq \mathcal{N}_2 \in \mathcal{N} \Rightarrow \{x_1, \ldots, x_1 + \ell - 1\} \cap \{x_2, \ldots, x_2 + \ell - 1\} = \emptyset$ para $x_1 := \mathcal{N}_1\ell,\ x_2 := \mathcal{N}_2\ell$.

Nonce-based CBC mode

La idea es mapear nonce a pseudorandom IV usando una PRF sobre $(\mathcal{K}', \mathcal{N}, \mathcal{X})$ con $\mathcal{K}', \mathcal{N}$ arbitrarios. De este modo, sea $\mathcal{E}'$ este cifrado, el espacio de claves es $\mathcal{K} \times \mathcal{K}'$ y el IV se computa como $c[0] := F(k', \mathcal{N})$.

Modificaciones a ciphers CPA-secure para ser nonce-based II

CPA-security

Todos son CPA seguros bajo condición de que sus elementos (PRFs, cifrado por bloques) también sean seguros, así como también se mantienen las variables acotadas polinómicamente y los super-poly.

Vulnerabilidades ante mal uso de nonces

Ejemplo 14

Demo CTF challenge de la Hacker Class COMPFEST16: *Reduce, Reuse, Recycle*

¡Gracias!