CENTRO DE INVESTIGACIÓN Y DE ESTUDIOS AVANZADOS
DEL INSTITUTO POLITÉCNICO NACIONAL

Unidad Zacatenco

Departamento de Computación

”Seguridad Demostrable para Códigos de Autenticación de Mensajes”

Tesis que presenta

Víctor Alberto Espinosa Valladolid

para obtener el Grado de

Maestro en Ciencias

en Computación

Director de Tesis

Dr. Juan Carlos Ku Cauich

Ciudad de México Agosto, 2024

Dedicado a mi familia
por todo su apoyo y amor incondicional

II

Resumen

Esta tesis se centra en el estudio riguroso de la seguridad demostrable en criptografía, con un enfoque particular en los códigos de autenticación de mensajes (MAC). La tesis se erige sobre una base sólida de conceptos teóricos provenientes de la probabilidad, la teoría de la información y la criptografía simétrica. Estos fundamentos proporcionan el marco necesario para abordar los temas centrales de la investigación.

Asimismo, se realiza un estudio exhaustivo de los cifradores por bloques entonables, que son considerados la piedra angular de muchos sistemas criptográficos modernos. Se introduce el concepto de oráculo como una herramienta teórica para modelar la interacción entre un adversario y un sistema criptográfico.

Se define formalmente el concepto de familia de funciones, que es fundamental para las funciones pseudoaleatorias y las estrategias que pueden emplear los adversarios para distinguirlas de funciones verdaderamente aleatorias. Se presta especial interés en el concepto de seguridad incondicional, que se basa en la teoría de la información y no depende de supuestos computacionales.

Adicionalmente, se explica con alto grado de detalle la técnica de los coeficientes H, una herramienta poderosa para demostrar la seguridad de construcciones criptográficas. Se ofrecen demostraciones rigurosas de los teoremas principales y se generaliza la definición de transcrito bueno, proporcionando así una medida de seguridad para cualquier sistema probabilístico.

Por último, se muestra la aplicación de la técnica H al análisis del esquema ZMAC, un MAC basado en cifradores por bloques entonables. Se identifican las propiedades de seguridad de ZMAC y se demuestra su resistencia a diversos tipos de ataques. Además, se proponen mejoras para optimizar la eficiencia computacional de ZMAC sin comprometer su seguridad.

Abstract

This dissertation delves into a rigorous examination of provable security in cryptography, with a particular focus on Message Authentication Codes (MAC). The thesis is grounded in a solid foundation of theoretical concepts drawn from probability theory, information theory, and symmetric cryptography. These underpinnings provide the necessary framework to address the core research topics.

Furthermore, a comprehensive study of block ciphers, which are widely regarded as the cornerstone of many modern cryptographic systems, is undertaken. The concept of an oracle is introduced as a theoretical tool to model the interaction between an adversary and a cryptographic system.

The concept of a function family is formally defined, which is fundamental to understanding pseudorandom functions and the strategies adversaries may employ to distinguish them from truly random functions. Particular attention is paid to the notion of unconditional security, which is grounded in information theory and independent of computational assumptions.

Furthermore, the thesis provides a highly detailed explanation of the H-coefficient technique, a powerful tool for proving the security of cryptographic constructions. Rigorous proofs of the main theorems are presented, and the definition of a good transcript is generalized, providing a security measure for any probabilistic system.

Finally, the application of the H-coefficient technique to the analysis of the ZMAC scheme, a MAC based on block ciphers, is demonstrated. The security properties of ZMAC are identified, and its resistance to various attacks is proven. Additionally, improvements are proposed to optimize the computational efficiency of ZMAC without compromising its security.

Agradecimientos

Primeramente, a mis padres, Sonia y Víctor, por apoyarme en mis metas y brindarme la educación necesaria para cumplir mis objetivos. De manera muy especial, a mi hermano Erick por asistirme en todos los aspectos ilustrativos de mi disertación. Además, agradezco:

Al Departamento de Computación del CINVESTAV, por la oportunidad y la formación adquirida.

A todos los profesores que me impartieron clases por sus enseñanzas. Sobre todo al Doctor Cuauhtémoc y la Doctora Sonia por apoyarme con todos los problemas relacionados con mi cambio de programa.

A mis compañeros de computación, que más que compañeros son mis amigos.

Y por último, le doy gracias al CONAHCYT por la beca otorgada para realizar mis estudios de maestría.

Índice general

Índice de algoritmos

Índice de figuras

Índice de tablas

Capítulo 1

Introducción

1.1. Antecedentes

La criptografía moderna es la piedra angular de las comunicaciones y la seguridad informática, con productos finales que son inmensamente prácticos. En el esquema básico se presentan tres entidades: el remitente, el receptor y el adversario. El remitente y el receptor desean comunicarse entre sí, pero no existen canales ideales que conecten a las partes. El problema principal de la criptografía es garantizar la seguridad de la comunicación a través de un medio inseguro, considerando distintas características como la integridad, la discreción, la privacidad, el no repudio y la autenticidad de un mensaje (Bellare & Rogaway, 2005).

Los códigos de autenticación de mensajes (MAC, por sus siglas en inglés) son uno de los aspectos más importantes de la criptografía. En pocas palabras, los MAC son una versión de la firma digital de clave secreta para autenticar mensajes. Los MAC están diseñados para proveer integridad al mensaje y autenticidad del emisor. Esto se logra al detectar cuándo un adversario inserta o modifica la información transmitida. De esta manera, sólo el emisor está en posibilidad de enviar mensajes que serán considerados como auténticos por parte del receptor. Esto significa que una pareja (M, S) siempre satisface $\mathcal{V}_k(M, S) = 1$ si y sólo si esta fue enviada por el emisor. Note que en este caso el adversario trata de falsificar la pareja (M, S). La ventaja que se tiene para falsificar la pareja es mayor a la ventaja que se tiene en recuperar la llave secreta. Así, la falsificación es más importante que la recuperación de la llave.

En la criptografía moderna, los esquemas criptográficos deben contar con una demostración matemática rigurosa que garantice la seguridad del esquema. El objetivo de cualquier esquema de clave secreta es lograr una especie de "indistinguibilidad" entre el sistema real (una instancia de una familia de funciones) y un sistema ideal (usualmente, una función aleatoria). Si un adversario no es capaz de distinguir el sistema real del ideal, podemos garantizar las propiedades criptográficas de la familia, por lo tanto, deseable a ser utilizado como un cifrado por bloques. Para esto, se considera un adversario, el cual cuenta con un oráculo que responde a sus preguntas, obteniendo así un conjunto de pares de textos en claro y textos cifrados. Dependiendo de estas parejas, se puede tener la distinción de encontrarse en el mundo de la familia específica o

de la familia de las funciones aleatorias, denotando estos mundos como mundo 1 y mundo 0, respectivamente.

Mundo 0: La función $\mathbb{O}$ es un oráculo ideal elegido uniformemente al azar de una distribución D.

Mundo 1: La función $\mathbb{O}$ es una función criptográfica, es decir, una instancia de la familia F dada por una clave k.

Para probar la seguridad utilizando el enfoque de secuencia de juegos, se construye una serie de experimentos en pseudocódigo, donde el adversario se encuentra en un mundo $\flat \in \{0, 1\}$. La técnica de los juegos de distinción desarrollada por Bellare y Rogaway (2005) comienza con el adversario $\mathcal{A}$ interactuando con un retador por medio de preguntas y respuestas iterativas. Este experimento puede entenderse de manera más sencilla, considerándolo como un algoritmo (oráculo) $\mathbb{O}$ que retorna una secuencia de pares entrada-salida. Después de esta interacción, $\mathcal{A}$ obtiene una muestra del comportamiento de $\mathbb{O}$ que puede estudiar para tomar una decisión sobre el valor de $\flat$ y terminar el juego.

El acto de decidir en cuál mundo se localiza se formaliza con la idea de un "distinguidor", *i.e.* un algoritmo con acceso a una función $\mathbb{O}$ que intenta decidir en cuál de ambos mundos se encuentra. Generalmente, el objeto es identificar si $\mathbb{O}$ es un objeto idealizado o una función criptográfica. De este modo, la ventaja del distinguidor se calcula de la diferencia en el evento $\flat = 1$ entre ambos mundos.

$$\mathbf{Adv}_{\mathbb{O}}^{\text{Exp}}(A) := \Pr\left[\texttt{Mundo 1} : \flat = 1\right] - Pr[\texttt{Mundo 0} : \flat = 1] \tag{1.1}$$

Con base en cada juego, se realiza un análisis probabilístico para acotar la ventaja del distinguidor o la ecuación (1.1). Esta es la técnica contemporánea desarrollada por Bellare y Rogaway (2006), donde los juegos se representan como un pseudocódigo con variables y banderas que representa la decisión del adversario. Por ello, el paradigma actual para diseñar MAC iterativas de clave simétrica es la construcción de PRFs basadas en cifradores por bloques como CBC-MAC, PMAC, OMAC y LightMAC (Iwata & Kurosawa, 2003). Algunas de las construcciones más comunes proveen seguridad de hasta $2^{n/2}$ consultas de un adversario, en donde n es el tamaño del bloque del cifrador. No obstante, estas construcciones sólo aseguran alcanzar el límite de seguridad conocido como "La cota de cumpleaños" (*Birthday Bound*).

En los últimos años, se ha utilizado una herramienta más robusta introducida por Patarin (2009) en el SAC 2008 (aunque ya utilizada en trabajos anteriores) denominada "La técnica de Coeficientes H". En resumen, la técnica H consiste en un adversario y un oráculo interactuando, a través de secuencias llamadas transcritos. La técnica establece que la ventaja para distinguir el oráculo real del ideal está limitada por la probabilidad de encontrar cierto transcrito en el comportamiento del oráculo real. A diferencia de la técnica de juego, la técnica de Coeficientes H no asume distribuciones de probabilidad implícitas en los oráculos y requiere cálculos explícitos de probabilidad en ambos casos para limitar la relación entre ellos.

1.1.1. Motivación

En la era digital actual, la comunicación segura se ha vuelto esencial en diversos ámbitos, desde las transacciones bancarias hasta las comunicaciones gubernamentales. La integridad y autenticidad de los mensajes son aspectos fundamentales para garantizar la confianza en las comunicaciones electrónicas. Los códigos de autenticación de mensajes desempeñan un papel crucial en este contexto, proporcionando un mecanismo para verificar la integridad y autenticidad de los datos transmitidos.

Sin embargo, a medida que aumentan las sofisticadas amenazas cibernéticas, es cada vez más importante contar con garantías formales sobre la seguridad de los esquemas criptográficos. La seguridad demostrable ofrece un marco riguroso para analizar y evaluar la resistencia de los sistemas criptográficos ante nuevos ataques.

Para garantizar esto, mostraremos que la indistinguibilidad de una función pseudoaleatoria es una de las mayores medidas de seguridad que nos protege contra cualquier clase de ataque que busque recuperar la llave, o hasta falsificar firmas digitales. Si bien el objetivo principal de un MAC es la inalterabilidad del mensaje y la verificación del emisor, la indistinguibilidad de bits aleatorios puede ser una meta de reemplazo valiosa para evaluar la seguridad. Si las etiquetas son indistinguibles de valores aleatorios, es difícil predecir el valor de la firma que un MAC pueda generar (Moch & List, 2019).

En un alto nivel, muchas de las construcciones MAC siguen el paradigma de diseño Hash-then-PRF (HtPRF): el mensaje M se mapea primero en una secuencia de bloques que garantice que cada bloque tenga la misma longitud (éste se logra gracias a una operación de *padding*). Enseguida, se obtiene un hash corto de toda la secuencia de bloques, a través de una función hash universal. Por último, este hash se cifra a través de una PRF de longitud de entrada fija para obtener una firma corta correspondiente a todo el mensaje. Este método es simple (en particular es determinista y sin estado); sin embargo, tiene límites de seguridad dados por la cota del cumpleaños en la ecuación (1.2). Cualquier colisión, en la salida de la función hash, se traduce en una posibilidad de falsificar las etiqueta que entrega el MAC. Esto suele ser suficiente para romper la seguridad del esquema:

$$\mathbf{Adv}^{\text{FORGE}}_{\text{UHF}}(\mathcal{A}) \;\leq\; \frac{q(q-1)}{2^{n+1}} \;\leq\; \frac{q^2}{2^n} \tag{1.2}$$

La cota de cumpleaños es el límite que invalida la garantía de privacidad cuando ocurre una colisión interna, con probabilidad dada por (1.2), después de procesar $2^{n/2}$ bloques con la misma clave. El ataque ocurre en una construcción MAC que toma valores con longitud de n bits y requiere no más de $O(q^2/2^n)$ consultas de un adversario inteligente, lo que significa que es posible realizar una falsificación de la firma (*forgery*). Éste es un problema severo para los cifradores ligeros (64 bits) derivados del Triple-DES y, en menor medida, para los cifradores de 128 bits como GCM u OCB3 (Yasuda, 2011).

En particular, es de nuestro interés emplear cifradores por bloques para generar códigos de autenticación de mensajes con seguridad más allá de la cota de cumpleaños (*Beyond-Birthday-Bound*). Este límite es un problema intrínseco al uso de familias de permutaciones pseudo-

aleatorias (Bhattacharjee et al., 2020). No obstante, en los últimos 10 años los investigadores han lanzado propuestas novedosas que logran superar este límite a través de distintas técnicas, como los cifradores entonables o el uso de bloque con doble HASH. La importancia de este trabajo radica en estudiar dichas construcciones, analizarlas y entender sus propiedades, puesto que la búsqueda de nuevos códigos de autenticación o el diseño de modos de operación eficientes (computacionalmente) son uno de los asuntos de actualidad más importantes que varios miembros de la comunidad criptográfica investigan.

1.2. Objetivos de la Tesis

Objetivo General

- Encontrar las propiedades necesarias en esquemas basados en cifradores por bloques para garantizar códigos de autenticación de mensajes seguros más allá de la cota de cumpleaños.

Objetivos específicos

1. Entender las distintas técnicas de demostración de seguridad incondicional.
2. Analizar la construcción de las funciones pseudoaleatorias.
3. Definir un nuevo marco de trabajo para los sistemas probabilísticos,
4. Estudiar el esquema de autenticación ZMAC.
5. Realizar la demostración de seguridad de ZMAC.
6. Elaborar un documento sobre los resultados obtenidos.

1.2.1. Estructura de la Tesis

El cuerpo de este documento está dividido por los siguientes capítulos con sus respectivas secciones, de la siguiente manera:

1. **Introducción:** se presenta el contexto, los objetivos y las contribuciones. Además, presentamos brevemente el contendido de cada capítulo y añadimos una sección sobre conocimientos básicos de probabilidad.

2. **Cifradores por bloques entonables:** explicamos el funcionamiento de una de las primitivas criptográficas más populares, los esquemas simétricos. Explicamos brevemente algunos conceptos sobre seguridad y problemas que pueden presentarse en su construcción

3. **Oráculos y familias de funciones:** definimos de manera rigurosa las bases para desarrollar sistemas criptográficos desde la perspectiva de las familias de funciones y el comportamiento de sistemas probabilísticos.

4. **Adversarios y pseudo-aleatoriedad:** introducimos el concepto de función pseudoaleatoria, así como las estrategias y ataques que puede realizar un adversario para poder distinguirla de una función aleatoria.

5. **Seguridad incondicional:** desarrollamos con profundidad los distintos conceptos de seguridad, enfocándonos en el análisis bajo teoría de la información. Adicionalmente, señalamos algunas propiedades importantes como la seguridad perfecta, la indistingubilidad derecha-izquierda y la privacidad de los esquemas simétricos.

6. **Códigos de autenticación de mensajes:** introducimos los conceptos y propiedades más importantes para los esquemas de autenticación, así como algunos resultados importantes sobre los MAC. Demostramos de manera rigurosa los teoremas sobre ”La paradoja de cumpleaños”, la construcción MAC como PRF y el Lema PRF-PRP.

7. **Técnica de los coeficientes H:** estudiamos de forma detallada los teoremas principales descritos por Patarin (2009). Ofrecemos demostraciones más extendidas de cada resultado y describimos algunas equivalencias entre las distintas maneras de emplear la técnica H dadas por Jha y Nandi (2022), Hoang y Tessaro (2016). Generalizamos la definición de transcrito bueno para ser consistente con el estudio del comportamiento descrito por Polderman y Willems (1997).

8. **ZMAC:** por último, desarrollamos un estudio de caso con ZMAC para demostrar cómo aplicar la técnica H con mucho detalle y detenimiento en cada propiedad. Como conclusión de nuestro análisis, entregamos algunas propuestas de mejora para implementar ZMAC con mayor eficiencia computacional.

1.3. Contribuciones

Entregamos un documento que recopila los resultados principales de varios artículos, principalmente los expuestos por Jha y Nandi (2022) y Patarin (2009). Asimismo, ampliamos la teoría sobre seguridad demostrable, homogeneizando los conceptos de Bellare y Rogaway (2005) y Katz y Lindell (2014), con la formalización del comportamiento introducida por Polderman y Willems (1997).

Ofrecemos pruebas rigurosas sobre cómo estudiar la seguridad de cualquier esquema criptográfico a partir de su comportamiento entrada-salida (observable). Originalmente, el propósito de introducir este marco de trabajo era generalizar los resultados de los coeficientes H para sistemas más complejos como autómatas celulares, redes neuronales u osciladores caóticos. Esto con el fin de introducir los sistemas dinámicos en el paradigma moderno de la criptografía.

Hoy por hoy, la teoría de sistemas dinámicos para diseñar generadores de números pseudoaleatorios y funciones pseudoaleatorias se basa principalmente en pruebas experimentales y carecen de las propiedades de los cifradores por bloques tales como la *indistinguibilidad derecha-izquierda* o su cota de *seguridad incondicional*.

Por este motivo, exponemos con gran detalle los resultados de la técnica H y entregamos una definición de transcrito bueno al comportamiento de cualquier sistema probabilístico.

Por último, exponemos un estudio de caso sobre ZMAC para demostrar cómo los teoremas expuestos en este documento nos permiten garantizar la seguridad de un código de autenticación de mensajes más allá de la cota de cumpleaños. A su vez, mientras examinamos el esquema de autenticación, encontramos varias observaciones que agrupamos como una propuesta de mejora de ZMAC.

1.4. Preliminares

1.4.1. Notación

Escribimos $\{0,1\}^\ell$ a las cadenas con longitud de ℓ-bits cuya cardinalidad es $\left|\{0,1\}^\ell\right| = 2^\ell$. Usualmente, usamos las letras $i, j, k, m, n, \ell \in \mathbb{N}$ para denotar índices. Asimismo, la sucesión estrictamente creciente de todos los índices menores que m la denotamos como $\mathfrak{I}_m = \{1, 2, \ldots, m\}$.

Para un elemento $\mathbf{X} \in \{0,1\}^n$ de una cadena de n-bits, escribimos $\mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_\ell$ como cada uno de los bits en la cadena $\mathbf{X}$. También, denotamos $|\mathbf{X}|$ como la longitud en bits de una cadena y $\mathbf{X}[i]$ como el i-ésimo elemento de la cadena. En este caso, $|\mathbf{X}| = n$ y $\mathbf{X}[i] = \mathbf{x}_i$.

Dado $\ell \leq n$, denotamos $\lceil\!\lceil \mathbf{X} \rceil\!\rceil^\ell = \mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_\ell$ como la operación de tomar los primeros ℓ bits en orden lexicográfico. De manera similar, $\lfloor\!\lfloor \mathbf{X} \rfloor\!\rfloor_{n-\ell} = \mathbf{x}_\ell\mathbf{x}_{\ell+1}\ldots\mathbf{x}_n$ representa la operación de tomar los últimos $n-\ell$ bits en orden lexicográfico. Sean $\mathbf{Y}, \mathbf{Z} \in \{0,1\}^*$. Entonces, escribimos $\mathbf{X}\|\mathbf{Y}\|\mathbf{Z}$ como la concatenación de las tres cadenas.

Para un conjunto X, escribimos $X^{(q)}$ como el conjunto de todas las tuplas de q elementos (o q-uplas) y denotamos simplemente $x^q = (x_1, x_2, \ldots, x_q) \in X^{(q)}$ como una q-upla. Además, decimos que una secuencia $x_1, \ldots, x_q$ es **distinta por pares** si $x_i \neq x_j$ para todo $j > i$.

Habitualmente, dado un valor fijo $a \in A$ y una función $f : A \times B \to Z$ con múltiples entradas, escribimos $f_a(b) = f(a, b)$ para todo valor $b \in B$.

1.4.2. Probabilidad

Introducimos algunos conceptos fundamentales de probabilidad para preparar al lector con el rigor que emplearemos a lo largo de este documento.

Definición 1.4.1. *Un **espacio de probabilidad** es una tripleta $(\Omega, \mathbb{S}, \mu)$ conformada por un conjunto distinto del vacío Ω, denominado el **espacio muestral**, y una colección de subconjuntos $\mathbb{S} \subseteq 2^{\Omega}$ del espacio muestral, tal que*

1. *El total está incluido:*
$$\Omega \in \mathbb{S}$$
2. *Es cerrado bajo complementos:*
$$S \in \mathbb{S} \Rightarrow S^{\complement} \in \mathbb{S}$$
3. *Es cerrado bajo uniones numerables:*
$$S_1, S_2 \ldots, S_m \in \mathbb{S} \Rightarrow \bigcup_{n \in \mathbb{N}} S_n \in \mathbb{S}$$

*donde cada $S \in \mathbb{S}$ es llamado **evento** o suceso. También, está definida una métrica μ sobre el espacio Ω con imagen en el intervalo $[0, 1]$, denominada **función de probabilidad**.*

1. *La medida del vacío es cero:*
$$\mu(\varnothing) = 0$$
2. *La medida del total es uno:*
$$\mu(\Omega) = 1$$
3. *La aditividad satisface:*
$$\mu\left(\bigcup_{n \in \mathbb{N}} S_n\right) = \sum_{n \in \mathbb{N}} \mu(S_n)$$

Definición 1.4.2. *El **soporte** de una función f sobre un conjunto Ω es el conjunto de todos los elementos cuya imagen es distinta de la nulidad,*

$$\mathbf{Sop}\, f := \left\{ w \in \Omega \mid f(w) \neq 0 \right\}$$

Definición 1.4.3. *Una **variable aleatoria** $X : \Omega \longrightarrow \mathbb{R}$ es una función real definida sobre un espacio muestral, tal que para todo $[a, b] \in \mathbb{R}$ se tiene quE $X^{-1}\left([a, b]\right) \in \mathbb{S}$ es un evento. Se denota*

$$\Pr\left[\, X = x \,\right] := \mu\left(\left\{ w \in \mathbb{S} \mid X(w) = x \right\}\right)$$

como la probabilidad de los eventos tales que X es igual a x.

x_1	x_2	$\cdots$	x_i
$P(x_1)$	$P(x_2)$	$\cdots$	$P(x_i)$

Tabla 1.1: Distribución de la variable aleatoria X

Si la imagen de la variable aleatoria $X(\Omega) = \{x_1, x_2, \ldots, x_n\}$ es finita, entonces $X(\Omega)$ define un espacio de probabilidad tal que $P(x_i) := \Pr[X = x_i]$ es la probabilidad de cada $x_i \in X(w)$.

Definición 1.4.4. *La función de probabilidad P relacionada con una variable aleatoria $X \sim P$ se conoce como la **distribución de** X y se puede expresar como la tabla 1.1.*

Considerando la distribución anterior, entonces:

Definición 1.4.5. *Las variables aleatorias $X_1, X_2, \ldots, X_n$ son llamadas **mutuamente independientes** o independientes si*

$$P(X_1, X_2, \ldots, X_n) = P(X_1) \cdot P(X_2) \cdots P(X_n)$$

*Deje que X sea una variable aleatoria. Entonces se define la **esperanza** o el valor esperado como*

$$\mathrm{Ex}\left[X\right] := \sum_{i=0}^{n} x_i \cdot P(x_i)$$

para toda $x_i \in X(\Omega)$. Advierta cómo la esperanza es una función lineal.

Definición 1.4.6. *Sean dos funciones de probabilidad P_1 y P_2 sobre Ω. Entonces, la **distancia estadística** entre P_1 y P_2 se define como*

$$\| P_1 - P_2 \| := \frac{1}{2} \sum_{w \in \Omega} | P_1(w) - P_2(w) |$$

Si en lugar de dos funciones de probabilidad se tienen dos variables aleatorias X, Y sobre Ω,

$$\langle X, Y \rangle := \| X(\Omega) - Y(\Omega) \|$$

Las siguientes propiedades de la distancia estadística aseguran que la variación total sobre un conjunto de distribuciones es una métrica acotada.

Lema 1.4.7. *Para cualquier función de probabilidad P_i indexada por i se cumple*

1. *La no negatividad:*
$$\| P_1 - P_2 \| \geq 0$$
2. *La simetría:*
$$\| P_1 - P_2 \| = \| P_1 - P_2 \|$$

3. *La identificación:*

$$\| P_1 - P_2 \| = 0 \Leftrightarrow P_1 = P_2$$

4. *La desigualdad triangular:*

$$\| P_1 - P_n \| \leq \sum_{i=1}^{n-1} \| P_i - P_{i+1} \|$$

5. *El supremo es 1 si y sólo si los soportes son disjuntos:*

$$\| P_1 - P_2 \| \leq 1 \Leftrightarrow \mathbf{Sop}\, P_1 \cap \mathbf{Sop}\, P_2 = \varnothing$$

Es evidente que la distancia estadística cumple con este lema, puesto que por definición, estas propiedades se heredan del valor absoluto y la distribución.

Lema 1.4.8. *Dadas las distribuciones de probabilidad P_1 y P_2 sobre Ω, entonces*

$$\max_S [\, P_1(S) - P_2(S) \,] = \sum_{w \in \Omega} \max\{0, P_1(w) - P_2(w)\} = \| P_1 - P_2 \|$$

El máximo es alcanzado con un conjunto S si y sólo si $\Omega_> \subseteq S \subseteq \Omega_\geq$, donde

$$\Omega_> := \{ w \in \Omega \mid P_1(w) > P_2(w) \}$$
$$\Omega_\geq := \{ w \in \Omega \mid P_1(w) \geq P_2(w) \}$$

Demostración. Para cualquier $w \notin \Omega_\geq$ se tiene que la diferencia $P_1(w) - P_2(w) < 0$. Luego, por hipótesis,

$$\begin{aligned} \sum_{w \in \Omega} \max\{\, 0, P_1(w) - P_2(w) \,\} &= \sum_{w \in \Omega_\geq} \max\{\, 0, P_1(w) - P_2(w) \,\} + \sum_{w \notin \Omega_\geq} \max\{\, 0, P_1(w) - P_2(w) \,\} \\ &= \sum_{w \in \Omega_\geq} | \, P_1(w) - P_2(w) \, | = \max_S [\, P_1(S) - P_2(S) \,] \end{aligned}$$

Esta igualdad se satisface debido a que S es superconjunto de $\Omega_>$. Para la otra parte de la ecuación, primero se parte el espacio en dos clases $\Omega = \Omega_> \cup \Omega_>^\complement$. Así, por simetría del valor absoluto se sigue que

$$\begin{aligned} \sum_{w \in \Omega} | \, P_1(w) - P_2(w) \, | &= \sum_{w \in \Omega_>} | \, P_1(w) - P_2(w) \, | + \sum_{w \notin \Omega_>} | \, P_2(w) - P_1(w) \, | \\ &= P_1(\Omega_>) - P_2(\Omega_>) + P_2(\Omega_>^c) - P_1(\Omega_>^c) \\ &= P_1(\Omega_>) - P_2(\Omega_>) + P_1(\Omega_>) - P_2(\Omega_>) \\ &= 2 \cdot \max_S [\, P_1(S) - P_2(S) \,] \end{aligned}$$

Por la Definición 1.4.6, se concluyen ambas partes de la ecuación. □

Corolario 1.4.9. *Sean $P_2 \sim X_2$ y $P_1 \sim X_1$ variables aleatorias con sus respectivas distribuciones sobre Ω. Para toda w en el soporte de P_1 deje que*

$$\epsilon_{opt}(w) = \text{máx}\left\{ 0, 1 - \frac{P_2(w)}{P_1(w)} \right\}$$

Entonces, la distancia estadística entre las distribuciones es

$$\| P_1 - P_2 \| = \text{Ex}\left[\epsilon_{opt}\left(X_1\right)\right]$$

Demostración.

$$\begin{aligned}
\text{Ex}\left[\epsilon_{opt}\left(X_1\right)\right] &= \sum_{w \in \mathbf{Sop}\, P_1} \epsilon_{opt(w)} \cdot P_1(w) + \sum_{w \notin \mathbf{Sop}\, P_1} \epsilon_{opt(w)} \cdot P_1(w) \\
&= \sum_{w \in \mathbf{Sop}\, P_1} \text{máx}\{\, 0, 1 - \frac{P_2(w)}{P_1(w)} \,\} \cdot P_1(w) \\
&= \sum_{w \in \mathbf{Sop}\, P_1} \text{máx}\{\, 0, P_1(w) - P_2(w) \,\} \; + \sum_{w \notin \mathbf{Sop}\, P_1} \text{máx}\{\, 0, P_1(w) - P_2(w) \,\} \\
&= \sum_{w \in \Omega} \text{máx}\{\, 0, P_1(w) - P_2(w) \,\} \\
&= \| P_1 - P_2 \|
\end{aligned}$$

Observe que $\text{máx}\{\, 0, P_1(w) - P_2(w) \,\} = 0$ si $w \notin \mathbf{Sop}\, P_1$.

□

Capítulo 2

Cifradores por bloques

Los cifradores por bloques (BC por sus siglas en inglés) son herramientas fundamentales en la criptografía de clave privada (simétrica), la principal tecnología disponible para este tipo de criptografía. Este capítulo explora estas herramientas y describe el estado actual de su desarrollo.

Es importante destacar que los cifrados por bloques son únicamente ingredientes crudos para construir soluciones más útiles, primitivas criptográficas empleadas en la construcción de distintos esquemas criptográficos. Como en cualquier herramienta poderosa, hay que aprender a usarlos correctamente. Incluso, un cifrado por bloques mal empleado podría generar vulnerabilidades en un esquema perfectamente seguro.

Definición 2.0.1. *Un* **cifradores por bloques***, denotado* $\mathcal{E} : \{0,1\}^k \times \{0,1\}^n \longrightarrow \{0,1\}^n$*, es una permutación indexada al conjunto de claves* $\{0,1\}^k$*. Esto significa que para cada clave* $\mathbf{K}$ *se tiene una permutación del conjunto* $\{0,1\}^n$*, representada por la función* $\mathcal{E}_{\mathbf{K}}$*. Las entradas de* $\mathcal{E}_{\mathbf{K}}$ *se denominan* ***Textos planos*** *y las salidas,* ***Textos cifrados****.*

Un BC sólo puede cifrar mensajes que corresponden a su tamaño de bloque. En la práctica, la longitud m de un mensaje a cifrar es un múltiplo positivo del tamaño n del bloque. De lo contrario, se puede realizar un proceso para rellenar (*padding*) apropiadamente el mensaje hasta conseguir una longitud divisible por el tamaño del bloque, $n|m$. Generalmente, un BC es un algoritmo público bien especificado y más adelante se hablará de estas permutaciones indexadas, vistas además como una familia de funciones.

Dados un texto cifrado $\mathbf{C} \in \{0,1\}^n$, un texto plano $\mathbf{M} \in \{0,1\}^n$ y una clave $\mathbf{K} \in \{0,1\}^k$, calcular $\mathcal{E}_{\mathbf{K}}(\mathbf{M})$ y $\mathcal{E}_{\mathbf{K}}^{-1}(\mathbf{C})$ es relativamente rápido. Por el principio de Kerckhoff, definido por Shannon (1949), la seguridad del cifrador depende únicamente de la elección de la clave secreta $\mathbf{K}$. Por este motivo, el cifrador por bloques debe estar diseñado para que esta tarea sea computacionalmente difícil de lograr.

En consecuencia, como primera aproximación, podríamos pensar que el objetivo del adversario es recuperar la clave $\mathbf{K}$, dados algunos ejemplos de entrada-salida del cifrador. Posteriormente, refinaremos la idea de seguridad en el Capitulo 5, mostrando que la seguridad contra la

recuperación de la clave secreta es una condición necesaria pero no suficiente para la seguridad de un BC.

2.1. Ataques en cifradores por bloques

Históricamente, el estudio de ataques a las primitivas criptográficas es conocido como criptoanálisis. El criptoanálisis de un BC empieza considerando el siguiente problema:

Sea $q \geq 0$ un parámetro entero y sea $\mathbf{T}$ una clave secreta de k bits elegida al azar. Permita que el adversario tenga una secuencia de q ejemplos de entrada-salida del cifrador, digamos: $(\mathbf{M}_1, \mathbf{C}_1), \ldots, (\mathbf{M}_q, \mathbf{C}_q)$ tales que $\mathbf{C}_i = \mathcal{E}_{\mathbf{T}}(\mathbf{M}_i)$ para cada $i \leq q$. Así, el objetivo del adversario es encontrar la clave aleatoria $\mathbf{T}$.

La estrategia más obvia que puede emplear un adversario es la búsqueda exhaustiva de claves. El ataque consiste en recorrer todas las claves posibles $\mathbf{K} \in \{0,1\}^k$ hasta encontrar una que explique los pares de entrada-salida. Cabe mencionar que nunca consideramos un adversario que realice consultas redundantes, por lo que la secuencia de textos planos es distinta por pares, formalmente, $M_i \neq M_j$ para todo $j > i$.

A continuación, considere un atacante con un ejemplo único de entrada-salida del cifrador, esto es $q = 1$. Para cada iteración $i \in \{1, ..., 2^k\}$, sea $\mathbf{T}'_i$ la i-ésima cadena de k bits en orden lexicográfico.

```
ALGORITMO A^NR ( M_1, C_1 ):
    for i = 1, ..., 2^k haz
        si E_{T'_i}(M_1 = C_1) entonces regresa T'_i
```

Algoritmo 2.1.1: Búsqueda ingenua de clave secreta

Por lo tanto, $\mathbf{T}'_i$ es la supuesta clave secreta que buscamos. Cabe mencionar que este ataque siempre devuelve una clave consistente con el ejemplo de entrada-salida $(\mathbf{M}_1, \mathbf{C}_1)$. Sin embargo, que la clave devuelta sea correcta, $\mathbf{T}'_i = \mathbf{T}$, depende del cifrador por bloques. Esta manera de atacar un cifrador es bastante ingenua, pero nos ayuda a entender un par de conceptos importantes sobre la seguridad computacional.

Ejemplo 2.1.1. Supongamos que se cifra por bloques la palabra **FELINO** (un bloque por letra) y se obtiene el cifrado $ONILEF$ con la clave T_0. Entonces, dado el par entrada-salida (F, O) el algoritmo puede arrojar los resultados de la Tabla 2.1.

Note cómo existen varias claves consistentes (precisamente 120) para la muestra (F, O), que pueden ser obtenidas con el ataque representado por el Algoritmo 2.1.1.

Si asumimos un BC con un comportamiento uniformemente aleatorio, entonces la longitud de la clave k y la longitud del bloque n son parámetros relevantes para evaluar si el ataque será

T_0	T_1	T_2	T_3	T_4	T_5	T_6	T_7
F	O	O	O	O	O	O	O
E	N	E	L	I	F	N	N
L	E	L	F	F	N	F	F
I	F	I	I	N	E	E	I
N	I	F	N	E	L	L	L
O	L	N	E	L	I	I	E

Tabla 2.1: Posibles textos cifrados obtenidos por $\mathcal{A}^{\text{NR}}$

exitoso. La probabilidad de que un ataque devuelva la clave secreta puede aumentar evaluando más muestras de pares entrada-salida.

ALGORITMO $A^{\text{KR}}(\,(\mathbf{M}_1, \mathbf{C}_1), \ldots, (\mathbf{M}_q, \mathbf{C}_q)\,)$:
  for $i = 1, \ldots, 2^k$ **haz**
    si $\mathcal{E}_{\mathbf{T}_i}(\mathbf{M}_1) = \mathbf{C}_1 \wedge \cdots \wedge \mathcal{E}_{\mathbf{T}_i}(\mathbf{M}_q) = \mathbf{C}_q$ **entonces regresa** $\mathbf{T}_i$

Algoritmo 2.1.2: Recuperación exhaustiva de clave secreta

Un valor bastante pequeño, digamos $q = k/n$, es suficiente para que este ataque devuelva la clave correcta. Para una permutación pseudoaleatoria como DES (Bellare & Rogaway, 2005), $q = 2$ muestras son suficientes. Por lo tanto, ningún BC es perfectamente seguro, ya que un atacante siempre puede recuperar una clave consistente con suficiente tiempo. A pesar de ello, un buen cifrador por bloques está diseñado para que esta tarea sea computacionalmente prohibitiva.

Supongamos una cantidad de muestras q lo suficientemente pequeña e ignoremos el costo computacional de $\mathcal{A}^{\text{KR}}$. En el peor de los casos, el ataque podría utilizar 2^k cálculos del cifrador por bloques. No obstante, podrían ser menos; si tuviéramos suerte y la clave secreta se encontrará en la primera mitad del espacio de búsqueda, entonces sólo harían falta $2^{(k-1)}$ cálculos. Por lo tanto, una mejor medida de seguridad considera el costo promedio de cualquier ataque:

$$\mathrm{Ex}\left[\mathcal{A}^{\text{KR}}\right] = \sum_{i=1}^{2^k} i \cdot \Pr\left[\,\mathbf{T}_i = \mathbf{T}\,\right] = \sum_{i=1}^{2^k} \frac{i}{2^k} = \frac{1}{2^k} \cdot \sum_{i=1}^{2^k} i = \frac{1}{2^k} \cdot \frac{2^k(2^k+1)}{2} \approx 2^{k-1}$$

Esta aproximación nos indica un resultado bastante evidente. Una clave secreta $\mathbf{T}$, elegida uniformemente al azar, tiene una probabilidad de $1/2^k$ de ser igual a la clave que devuelve nuestro algoritmo.

Ahora, tomando en cuenta el costo computacional, observe que $\mathcal{A}^{\text{KR}}$ realiza i cálculos del cifrador $\mathcal{E}$ para encontrarla. Por lo tanto, el costo de la recuperación de la clave mediante búsqueda exhaustiva es proporcional al tamaño de la clave. Por esto, el parámetro k está relacionado con la seguridad del cifrador.

2.2. Limitaciones en la recuperación de clave secreta

La seguridad de los BC ha sido tradicionalmente evaluada en términos de la dificultad para recuperar la clave secreta. Este enfoque se ejemplifica con el Algoritmo 2.1.2. Sin embargo, la seguridad contra la recuperación de claves es limitada como concepto, ya que no garantiza la seguridad en todos los usos prácticos en los que se emplean cifradores por bloques.

Considere el cifrador por bloques $\mathcal{E} : \{0,1\}^{128} \times \{0,1\}^{256} \longrightarrow \{0,1\}^{256}$ y defina el texto cifrado como $\mathbf{C} = (\!|\mathcal{E}_{\mathbf{K}}(\mathbf{X}_l)\|\mathbf{X}_r|\!)$ donde el bloque izquierdo $\mathbf{X}_l = \lceil\!|\mathbf{M}|\!\rceil^{128}$ son los primeros 128 bits del texto plano y el bloque derecho $\mathbf{X}_r = \lfloor\!|\mathbf{M}|\!\rfloor_{128}$ son los últimos 128 bits. La recuperación de claves es tan difícil como el experimento anterior, pero el texto cifrado revela la segunda mitad del texto plano.

Esto podría parecer artificial, puesto que revelar la mitad del texto no es una condición para un buen cifrado. Es más, podríamos enumerar todas las propiedades deseadas para un buen cifrador (incluido no revelar ningún bit del texto plano). Sin embargo, únicamente terminaríamos con una larga lista de condiciones insuficientes, sin ninguna pista sobre cómo diseñar cifradores para todo uso práctico.

Esto es uno de los problemas del enfoque clásico: construcciones improvisadas, sin análisis y con soluciones *ad hoc*. A lo largo de esta tesis veremos cómo el paradigma moderno explorado por los pioneros Bellare y Rogaway (2005) y Katz y Lindell (2014) consiste en definiciones generales, teoremas sólidos y demostraciones rigurosas, que nos otorgan garantías sobre todas las propiedades que deseamos en nuestras aplicaciones criptográficas.

Capítulo 3

Familias de funciones

Una manera de analizar la seguridad de los cifradores por bloque es por medio de las funciones pseudoaleatorias. La indistinguibilidad entre una función aleatoria y una función pseudoaleatoria es lo que nos permite medir la seguridad de nuestras construcciones criptográficas. Antes de estudiar las funciones pseudoaleatorias, es importante definir algunos conceptos que nos ayudaran a entender de manera más intuitiva el propósito de las demostraciones de seguridad y la importancia de dichas funciones.

En este capítulo se introducen las definiciones de función aleatoria, permutación aleatoria, sistemas aleatorios, entre otras. Estas son herramientas esenciales para el diseño de primitivas criptográficas, como los cifradores de bloques y otras aplicaciones útiles como códigos de autenticación de mensajes, que abordaremos en los siguientes capítulos.

Todos estos objetos criptográficos pueden ser entendidos como familias, debido a lo cual, primero introduciremos lo que significa una familia de funciones, antes de modelar estos sistemas criptográficos.

Definición 3.0.1. *Una **familia de funciones** es un mapa $F : K \times X \longrightarrow Y$, donde K, X, Y son conjuntos finitos distintos del vacío. De modo alterno, se visualiza como una colección de funciones indexadas*

$$\left\{ F_k : X \to Y \mid k \in K \right\}$$

Se denota Y^X a la familia de todas las funciones con dominio X (espacio de entradas) y rango Y (espacio de salidas). También, es posible expresar como $Dom(F)$ al espacio de entradas, $Ran(F)$ al espacio de salidas y $Key(F)$ al espacio de claves de la familia.

En criptografía, los sistemas criptográficos como un BC o un MAC se modelan a partir de una familia de funciones con buenas propiedades criptográficas. Esto implica estudiar varias familias de funciones distintas.

En particular, la familia de todas las funciones con dominio $\{0,1\}^n$ y rango $\{0,1\}^m$ es denotada $\mathrm{Func}\,(n,m)$. Observe que la cantidad de todas las funciones $F_k : \{0,1\}^n \to \{0,1\}^m$ indexadas por k y, por tanto, la cantidad de sus claves es

$$|Key(F)| = |\mathrm{Func}\,(n,m)\,| = 2^{m2^n}$$

Por añadidura, podemos construir un espacio de claves asociado al conjunto $\mathrm{Func}\,(n, m)$ para modelarlo como una familia de funciones. Para definir este espacio, debemos considerar el conjunto de todas las sucesiones de longitud 2^n generadas por todas las posibles entradas de $\{0,1\}^m$, formalmente descritas como

$$Key\left(\mathrm{Func}\,(n,m)\right) = \left\{(\mathbf{Y}_1, \mathbf{Y}_2, \ldots, \mathbf{Y}_{2^n}) \mid \mathbf{Y}_i \in \{0,1\}^m,\, i \in \mathfrak{I}_{2^m}\right\}$$

Ejemplo 3.0.1. Considere la familia $\mathrm{Func}\,(3,2)$. Observe que para una instancia $F_{\mathbf{k}}$ de la familia, se puede representar su comportamiento entrada-salida con la siguiente tabla:

$\mathbf{X}$	000	001	010	011	100	101	110	111
$F_{\mathbf{k}}(\mathbf{X})$	11	01	00	00	10	11	01	11

En este caso, la clave específica para esta función es

$$\mathbf{k} = (11, 01, 00, 00, 10, 11, 01, 11)$$

Se puede apreciar la correspondencia de las imágenes de F_k con las $\mathbf{Y}_i$. Así, el espacio de claves de $\mathrm{Func}\,(3,2)$ corresponde con el conjunto de todas las 8-tuplas cuyos componentes son cadenas de 2-bit. Exactamente, existen

$$2^{2\cdot 2^3} = 2^{16} = 65,536$$

tuplas dentro del espacio de claves.

3.1. Funciones aleatorias

Una función aleatoria es muy distinta de una función, puesto que dada una entrada x, la función siempre retorna una salida específica r. No obstante, una función aleatoria no es determinista, *i.e.*, dada una entrada x, el resultado de una función aleatoria es incierto y lo único que podemos saber es que y ocurre con cierta probabilidad.

El comportamiento de una función aleatoria no es predecible, pero puede ser modelado e incluso mejor comprendido a través de una función probabilística.

Definición 3.1.1. *Una **función probabilística** $f : X \xrightarrow{\text{⚅}} Y$ es una variable aleatoria cuyos valores son funciones $X \to Y$. Se puede modelar una función probabilística como una familia $f : ⚅ \times X \to Y$ indexada por un conjunto finito ⚅, denominado el **espacio de monedas**.*

Dada una entrada $x \in X$ y una moneda $\mathrm{R} \in ⚅$, se define la variable aleatoria $f(x)$ para toda salida $y \in Y$ como

$$\Pr_{\mathrm{R} \leftarrow ⚅}\left[f(x) = y\right] := \Pr\left[\, f(\mathrm{R}, x) = y \,\middle|\, \mathrm{R} \xleftarrow{\$} ⚅ \,\right] = \sum_{\substack{\hat{r} \in ⚅ : \\ f(\hat{r}, x) = y}} \Pr\left[\, \mathrm{R} = \hat{r} \,\right]$$

Cabe mencionar que usualmente no especificaremos la naturaleza del espacio de monedas ⚅, de tal modo que emplearemos la notación de la izquierda, en vez de la notación de Jha y Nandi (2022).

Supongamos que el espacio de monedas ⚅ es un espacio degenerado, *i.e.*, un *singleton*. Entonces la función probabilística es simplemente una función $X \to Y$. Por otro lado,

Definición 3.1.2. *Si la cantidad de monedas es* $|⚅| = |Y^X|$ *y la distribución de* f *es uniforme, entonces la función probabilística* $f : X \xrightarrow{⚅} Y$ *denota una* ***función aleatoria*** $f \xleftarrow{\$} Y^X$.

El término función aleatoria puede ser engañoso, ya que podría dar la impresión de que algunas funciones son intrínsecamente "aleatorias" y otras no; sin embargo, esto es incorrecto. La aleatoriedad de una función se refiere a cómo fue seleccionada, no a una característica inherente de la función en sí.

Por ejemplo, al elegir una función al azar entre todas las funciones, siempre es posible obtener la función constante que devuelve 0 para cualquier elemento del dominio. En resumen, la aleatoriedad de una función individual carece de sentido; una función aleatoria simplemente significa una función seleccionada al azar de la familia total de funciones.

A continuación, discutiremos una serie de afirmaciones sobre las funciones aleatorias, que son de suma importancia recordarlas para capítulos posteriores. Ahora, considere una función aleatoria $f \xleftarrow{\$} Y^X$ con cardinalidad $|Y| = M$ y $|X| = N$ para las siguientes proposiciones:

Proposición 3.1.3. *Sean* $x \in X$ *y* $y \in Y$ *fijos. Entonces*

$$\Pr[\, f(x) = y \,] = \frac{1}{M}$$

Demostración. Dada una función $\hat{f}$, la probabilidad de que ésta coincida con otro elemento del espacio Y^X es $1/M^N$. Además, sí $\hat{f}(x) = y$, entonces cualquier función que cumpla esta condición no puede enviar x a otra imagen. Así,

$$\left\{ X \setminus \{x_1\} \xrightarrow{\hat{f}} Y \;\middle|\; \hat{f}(x_1) = y \right\}$$

es el conjunto de todos los eventos favorables.

$$\therefore \quad \Pr[\, f(x) = y \,] = \sum_{\hat{f} : x \mapsto y} \Pr\left[f = \hat{f} \right] = \sum_{\hat{f} : x \mapsto y} \frac{1}{M^N} = \frac{M^{N-1}}{M^N} = \frac{1}{M}$$

□

Dado el procedimiento y el resultado, se observa que la probabilidad no depende del dominio, así como tampoco depende de los valores x o y.

Proposición 3.1.4. *Sean $x_1, x_2 \in X$ y sea $y \in Y$. Entonces,*

$$\Pr\left[\, f(x_1) = y,\ f(x_2) = y \,\right] = \begin{cases} M^{-1} & x_1 = x_2 \\ M^{-2} & x_1 \neq x_2 \end{cases}$$

Demostración. Si $x_1 = x_2$, la justificación del primer caso es idéntica a la Proposición 3.1.3.

En caso contrario, la cantidad de eventos en el espacio de distribución es la cardinalidad del conjunto de todas las funciones con dominio $X \setminus \{x_1, x_2\}$ y rango Y.

$$\begin{aligned} \therefore \quad \Pr\left[\, f(x_1) = y,\ f(x_2) = y \,\right] &= \sum_{\hat{f}: x_1 \mapsto y,\, x_2 \mapsto y} \Pr\left[\, f = \hat{f} \,\right] \\ &= \sum_{\hat{f}: x_1 \mapsto y,\, x_2 \mapsto y} \frac{1}{M^N} \\ &= \frac{M^{N-2}}{M^N} \ = \ \frac{1}{M^2} \end{aligned}$$

□

Advierta que en la proposición anterior se obtiene el mismo resultado, incluso si se consideran imágenes $y_1 \neq y_2$ distintas para $x_1 \neq x_2$ distintos.

Proposición 3.1.5. *Considere $x_1, x_2 \in X$ y $y_1, y_2 \in Y$ fijos, tal que $x_1 \neq x_2$. Entonces*

$$\Pr\left[\, f(x_1) = y_1 \;\middle|\; f(x_2) = y_2 \,\right] = \frac{1}{M}$$

Demostración. De la Proposición 3.1.4 y por definición de la probabilidad condicional, se tiene que

$$\begin{aligned} \Pr\left[\, f(x_1) = y_1 \;\middle|\; f(x_2) = y_2 \,\right] &= \frac{\Pr\left[\, f(x_1) = y_1,\ f(x_2) = y_2 \,\right]}{\Pr\left[\, f(x_2) = y_2 \,\right]} \\ &= \frac{\frac{1}{M^2}}{\frac{1}{M}} \ = \ \frac{1}{M} \end{aligned}$$

□

De la proposición anterior, observamos la independencia entre las parejas de entradas y salidas de una función aleatoria.

Proposición 3.1.6. *Sea $x_1, x_2 \in X$ y $y \in Y$ fijos. Luego,*

$$\Pr\left[\, f(x_1) \oplus f(x_2) = y \,\right] = \begin{cases} 1 & \text{SI } x_1 = x_2, \quad y = 0 \\ 0 & \text{SI } x_1 = x_2, \quad y \neq 0 \\ M^{-1} & \text{SI } x_1 \neq x_2 \end{cases}$$

Demostración. Sea $x_1 = x_2$. Entonces, $f(x_1) = f(x_2) \Leftrightarrow \hat{y} = f(x_1) \oplus f(x_2) = 0$. Esto implica que la probabilidad es nula para cualquier $\hat{y} \neq 0$, y es uno en caso contrario.

Ahora, suponga $x_1 \neq x_2$ y tome en cuenta todas las posibles parejas de imágenes en y. Entonces, se escribe el siguiente sistema de ecuaciones

$$\begin{cases} f(x_2) = & y \oplus y' \\ f(x_1) = & y' \end{cases}$$

Luego, la probabilidad deseada es la probabilidad de elegir una función f aleatoriamente que satisfaga una de las posibles parejas (y, y') . Por consiguiente,

$$\begin{aligned} \Pr\left[\, f(x_1) \oplus f(x_2) = y \,\right] &= \sum_{y' \in Y} \Pr\big[f(x_1) = y', f(x_2) = \underbrace{y' \oplus y}_{\delta} \,\big] \\ &= \sum_{y' \in Y} \Pr\left[\, f(x_2) = \delta \;\middle|\; f(x_1) = y' \,\right] \cdot \Pr\left[\, f(x_1) = y' \,\right] \\ &= \sum_{y' \in Y} \frac{1}{M} \frac{1}{M} \;=\; \frac{M}{M} \end{aligned}$$

Por cerradura de la operación $\delta \in Y$ se puede aplicar la Proposición 3.1.5.

□

En particular, este teorema será de importancia para los resultados probabilísticos con la operación XOR o para cualquier resultado definido sobre el campo de Galois $\mathrm{GF}(2^n)$.

Proposición 3.1.7. *Sea $g : Y \longrightarrow Z$ una función de partición que envía los elementos de su dominio de manera uniforme a su rango, con $|\, Z \,| = L \leq |Y|$. Dados $x_1, x_2 \in X$ distintos con $y \in Y$ y $z \in Z$ fijos, se tiene que*

$$\Pr\left[\, g(f(x_2)) = z \;\middle|\; f(x_1) = y \,\right] = \frac{1}{L}$$

Demostración. Primero, analizamos la composición $X \xrightarrow{\hat{f}} Y \xrightarrow{g} Z$. Ya que $|Z| \leq |Y|$, entonces la probabilidad para $g(\hat{f}(x_2)) = z$ es mayor o igual que antes. Debido a que g es una función uniforme que particiona el dominio Y en M/L partes, para cada imagen en Z se deduce que

$$\Pr\left[\, g\big(f(x_2)\big) = z \;\middle|\; f(x_1) = y \,\right] = \sum_{\hat{y} \in Y/Z} \Pr\left[\, f(x_2) = \hat{y} \;\middle|\; f(x_1) = y \,\right] = \frac{M/L}{M} = \frac{1}{L}$$

□

La proposición anterior afirma que, si se particiona el rango de una función aleatoria de manera uniforme, se obtiene una composición con una distribución uniforme pero con un menor rango. Para mayor claridad sobre g, vea el siguiente ejemplo:

Ejemplo 3.1.1. Sea $g : \{0,1\}^4 \longrightarrow \{0,1\}^2$ una función que toma sólo los últimos 2 bits de cada cadena, entonces se tiene la Tabla 3.1.

$\mathbf{Y}$	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
$g(\mathbf{Y})$	**00**	01	10	11	**00**	01	10	11	**00**	01	10	11	**00**	01	10	11

Tabla 3.1: Truncamiento de los 2 bits menos significativos

Advierta cómo g mapea la misma cantidad de elementos a **00** del mismo modo que a cualquier otro elemento de $\{0,1\}^2$, generando así una partición del conjunto $\{0,1\}^4$ dividida por los 2 bits más significativos. En específico, $g(\mathbf{Y})$ es la función $\lceil\mathbf{Y}\rceil^2$.

3.2. Permutaciones aleatorias

Como se había mencionado, los BC pueden ser considerados familias de permutaciones, un caso específico de las familias de funciones. Con el fin de entender una permutación como una función, imagine un mazo de naipes con 52 cartas ordenadas de la manera usual. Al barajar el mazo de naipes, hemos mezclado las 52 cartas sin eliminar ni agregar ninguna al mazo. Esto conserva la cantidad de elementos en el mazo, pero el proceso ha cambiado completamente el orden de las cartas. Tenemos, entonces, una regla de asociación entre el orden original y el nuevo.

Una familia de permutaciones busca modelar este principio, mezclar los mismos elementos dentro de un conjunto. Dentro de las familias de permutaciones existen familias que son de mayor interés para la criptografía, conocida como permutaciones aleatorias, las cuales se formalizarán en esta sección.

Definición 3.2.1. *Una **permutación** π es una función biyectiva con el mismo dominio y rango. Por lo tanto, una familia*

$$P := \left\{ P_k : Y \to Y \mid k \in K \right\}$$

*es una **familia de permutaciones** si cada instancia de P_k es una permutación. Del mismo modo, la familia de todas las permutaciones sobre Y es denotada $Y^\dagger$.*

Observe cómo una familia de permutaciones P tiene rango $Dom(P) = Ran(P)$. Se denota $\mathrm{Perm}\,(m)$ al conjunto de todas las permutaciones de $\{0,1\}^m$ tal que $|\mathrm{Perm}\,(m)| = 2^m!$.

En general, la cantidad de permutaciones de N elementos tomados r a la vez satisface

$$(N)_r := N(N-1)(N-2)\cdots(N-r-1)$$

A continuación, se ilustra con más detalle algunas características de las permutaciones indexadas y las permutaciones aleatorias. En $\mathrm{Perm}\,(m)$, el espacio de claves se puede interpretar como el conjunto de todas las sucesiones de longitud 2^m, en donde todas las entradas de cada sucesión son distintas y son elementos de $\{0,1\}^m$.

$$Key\left(\mathrm{Perm}\,(m)\right) = \left\{(Y_1, Y_2, \ldots, Y_{2^m}) \mid Y_i \in \{0,1\}^m \textit{ distintas por pares}, i \in \mathfrak{I}_{2^m}\right\}$$

Así, podemos considerar al conjunto de todas las permutaciones de la cadena $\{0,1\}^m$ como una familia de permutaciones, ya que podemos hablar de sus permutaciones indexadas.

Ejemplo 3.2.1. Considere la familia $\mathrm{Perm}\,(3)$ cuyos valores están en el conjunto $\{0,1\}^3$. Advierta que dada una instancia $P_{\mathbf{k}}$ de la familia se puede representar su comportamiento entrada-salida con la siguiente tabla:

$\mathbf{Y}$	000	001	010	011	100	101	110	111
$P_{\mathbf{k}}(\mathbf{Y})$	111	001	100	101	100	011	000	110

En este caso, la clave específica para esta función es

$$\mathbf{k} = (111, 001, 100, 101, 100, 011, 000, 110)$$

Se puede observar que el espacio de claves de $\mathrm{Perm}\,(3)$ consta de las 8-tuplas que corresponde con la secuencia de todas las cadenas de 3-bit sin repeticiones, con algún orden dado. Exactamente, existen

$$2^3! = 8! = 40,320$$

tuplas dentro del espacio de claves.

A continuación, una serie de resultados probabilísticos de las permutaciones. Para las siguientes proposiciones se utilizará una permutación aleatoria $p \xleftarrow{\$} Y^\dagger$ con rango Y de cardinalidad M.

Proposición 3.2.2. *Sean $x, y \in Y$ elementos fijos. Entonces,*

$$\Pr\left[\,p(x) = y\,\right] = \frac{1}{M}$$

Demostración. El análisis es similar a elegir p aleatoriamente de Y^Y.

$$\Pr\left[\,p(x) = y\,\right] = \sum_{\hat{p}: x \mapsto y} \Pr\left[\,p = \hat{p}\,\right] = \frac{(M-1)!}{M!} = \frac{1}{M}$$

□

El resultado coincide con las familias de funciones en general, no obstante, las similitudes se desvanecen cuando se tienen más de dos elementos en el rango.

Proposición 3.2.3. *Dados los elementos fijos $x_1, x_2, y \in Y$, se tiene*

$$\Pr\left[\, p(x_1) = y,\, p(x_2) = y \,\right] = \begin{cases} 0 & \Leftarrow \quad x_1 \neq x_2 \\ M^{-1} & \quad\;\; x_1 = x_2 \end{cases}$$

Demostración. Se sabe que $x_1 \neq x_2$ si y sólo si la permutación $\hat{p}$ tiene imágenes distintas. Por lo tanto, dado $y = p(x_1) = p(x_2)$, la probabilidad es cero. Por el contrario, dado $x_1 = x_2$ la demostración se reduce a la Proposición 3.2.2. □

Proposición 3.2.4. *Sean los elementos fijos $x_1, x_2, y_1, y_2 \in Y$ con $x_1 \neq x_2, y_1 \neq y_2$. Se tiene que*

$$\Pr\left[\, p(x_1) = y_1,\, p(x_2) = y_2 \,\right] = \frac{1}{M(M-1)}$$

Demostración. Sea $\hat{p}$ tal que $\hat{p}(x_1) = y_1$ y $\hat{p}(x_2) = y_2$. Observe que $y_1 \neq y_2$, así la cantidad de variaciones de $\hat{p}$ son todas las permutaciones sobre el conjunto $(Y \setminus \{x_1, x_2\})^\dagger$. Entonces,

$$\begin{aligned} \Pr\left[\, p(x_1) = y_1,\, p(x_2) = y_2 \,\right] &= \sum_{\hat{p}: x_1 \mapsto y_1,\, x_2 \mapsto y_2} \Pr\left[\, p = \hat{p} \,\right] \\ &= \sum_{(Y \setminus \{x_1, x_2\})^\dagger} \frac{1}{M!} \\ &= \frac{(M-2)!}{M!} \;=\; \frac{1}{M(M-1)} \end{aligned}$$

□

Proposición 3.2.5. *Considere $x_1, x_2, y_1, y_2 \in Y$ elementos fijos, $x_1 \neq x_2$. Entonces*

$$\Pr\left[\, p(x_1) = y_1 \;\middle|\; p(x_2) = y_2 \,\right] = \begin{cases} 0 & \Leftarrow \quad y_1 = y_2 \\ \frac{1}{M-1} & \quad\;\; y_1 \neq y_2 \end{cases}$$

Demostración. Se sabe que $x_1 \neq x_2$ si y sólo si $\hat{p}(x_1) \neq \hat{p}(x_2)$. Por lo tanto, no es posible que ocurra $p(x_1) = y_1 = y_2 = p(x_2)$. Por el contrario, dado $y_1 \neq y_2$ se tiene que

$$\begin{aligned} \Pr\left[\, p(x_1) = y_1 \;\middle|\; p(x_2) = y_2 \,\right] &= \frac{\Pr\left[\, p(x_1) = y_1,\, p(x_2) = y_2 \,\right]}{\Pr\left[\, p(x_2) = y_2 \,\right]} \\ &= \frac{\frac{1}{M(M-1)}}{\frac{1}{M}} \;=\; \frac{1}{M-1} \end{aligned}$$

gracias a la Proposición 3.2.4.

□

Proposición 3.2.6. *Sean $x_1, x_2 \in X$ elementos fijos y $y \in Y$. Luego*

$$\Pr\left[\, p(x_1) + p(x_2) = y \,\right] = \begin{cases} 1 & x_1 = x_2, \quad y = 0 \\ 0 & x_1 = x_2, \quad y \neq 0 \\ 0 & x_1 \neq x_2, \quad y = 0 \\ M^{-1} & x_1 \neq x_2, \quad y \neq 0 \end{cases}$$

Demostración. Ya que p es una permutación, se deduce que $p(x_1) \oplus p(x_2) = 0$ si y sólo si $x_1 = x_2$. Dado $x_1 = x_2$, la probabilidad es nula para $y \neq 0$ y uno de otro modo. Asimismo, si $x_1 \neq x_2$, entonces no es posible que $p(x_1) + p(x_2) = 0$.

En consecuencia, dadas entradas $x_1 \neq x_2$ con salida no nula $y \neq 0$ se sigue

$$\begin{aligned} \Pr\left[\, p(x_1) = y_1 \;\middle|\; p(x_2) = y_2 \,\right] &= \sum_{y' \in Y \setminus \{0\}} \Pr\left[p(x_1) = y', p(x_2) = \underbrace{y' \oplus y}_{\delta} \right] \\ &= \sum_{y' \in Y \setminus \{0\}} \Pr\left[\, p(x_2) = \delta \;\middle|\; p(x_1) = y' \,\right] \Pr\left[\, p(x_1) = y' \,\right] \\ &= \sum_{y' \in Y \setminus \{0\}} \frac{1}{M-1} \frac{1}{M-1} \\ &= \frac{M-1}{(M-1)^2} \;=\; \frac{1}{M-1} \end{aligned}$$

Gracias a la cerradura de la operación $\delta \in Y$, y la igualdad se satisface acorde a la Proposición 3.2.5.

□

Proposición 3.2.7. *Sea $Y \xrightarrow{g} Z$ una función que particiona el dominio y mapea sus elementos de manera uniforme a su rango, con $|\, Z \,| = L \leq M$. Dados $x_1, x_2 \in Y$ distintos con $y \in Y$ y $z \in Z$ fijos, se tiene que*

$$\Pr\left[\, g(p(x_2)) = z \;\middle|\; p(x_1) = y \,\right] = \begin{cases} \frac{M}{L(M-1)} & \Leftarrow \quad z \neq g(y) \\ \frac{M/L - 1}{M-1} & \quad\;\; z = g(y) \end{cases}$$

Demostración. Aunque p es una permutación, se puede apreciar que g no lo es necesariamente. A pesar de ello, sabemos que g particiona al conjunto Y y por consiguiente, tenemos la equivalencia:

$$Y \xrightarrow{p} Y \xrightarrow{g} Z \;\Leftrightarrow\; Y \xrightarrow{p} Y/Z$$

tal que Y/Z es el conjunto de elementos que cumplen $g(\hat{p}(x_2)) = z$.

Cuando $\hat{y} \neq y$, existen a lo mucho $|\, Y/Z \,| = M/L$ elementos que cumplen con la condición. Por el contrario, si $\hat{y} = y$, entonces no es posible que la imagen de $g(\hat{p}(x_2))$ coincida con z, por

lo que tenemos $M/L - 1$ eventos favorables.

$$\begin{aligned}\therefore \quad \Pr\left[\, g\big(p(x_2)\big) = z \;\middle|\; p(x_1) = y \,\right] &= \frac{\Pr\left[\, g\big(p(x_2)\big) = z,\, p(x_1) = y \,\right]}{\Pr\left[\, p(x_1) = y \,\right]} \\ &= \sum_{\hat{y} \in Y/Z} \frac{\Pr\left[\, p(x_2) = \hat{y},\, p(x_1) = y \,\right]}{\Pr\left[\, p(x_1) = y \,\right]} \\ &= \sum_{\hat{y} \in Y/Z} \frac{1}{M-1} \;=\; \frac{M/L - 1}{M-1}\end{aligned}$$

Esto se concluye de la Proposición 3.2.4 y 3.2.5.

□

3.2.1. Permutaciones entonables

Recientemente, se han publicado nuevos diseños de esquemas criptográficos basados en una nueva primitiva descubierta por Rogaway (2004), conocida como cifradores por bloques entonables o TBC (*Tweakable Block Cipher*). Esta propuesta es lo suficientemente flexible para varias funcionalidades criptográficas, y a su vez, brinda una mayor resistencia a las colisiones que los cifradores BC tradicionales. Un TBC consiste en una familia de permutaciones con dos espacios de entrada: uno para textos planos y otro para seleccionar configuraciones, denominadas tonos. De esta manera, se comprime más información por bloque y se añade mayor variabilidad al texto cifrado.

Este espacio de tonos permite configurar de manera dinámica la relación entre el espacio de claves y las permutaciones posibles de un cifrador por bloques. A continuación, mostramos como modelar un TBC a partir de una familia de funciones, tal como hemos estado modelando otros objetos criptográficos a lo largo de este capítulo.

Definición 3.2.8. *Una **permutación entonable** es una permutación criptográfica, extendida por el espacio adjunto T, tal que*

$$\overline{P} := \left\{ P_k^t \mid (k,t) \in K \times T \right\}$$

donde T se denomina espacio de tonos. Se denota P_k^t a la instancia $\overline{P}(k,t)$ y espacio de tonos $Twk(\overline{P})$.

El propósito de una permutación entonable es añadir mayor variabilidad a la cantidad de permutaciones que pueden ser instanciadas por una familia de permutaciones.

Ejemplo 3.2.2. Sea $\overline{P}$ una permutación entonable con rango Y $= Ran(\overline{P}) = \{0,1\}^3$ y espacio de tonos T. Dada una clave $\mathbf{K} \xleftarrow{\$} Key(\overline{P})$, observe los resultados de la Tabla 3.2:

$\mathbf{T}$	$\mathbf{T}_0$				$\mathbf{T}_1$			
$\mathbf{Y}$	000	001	010	011	100	101	110	111
$P_{\mathbf{K}}^{\mathbf{T}}(Y)$	001	010	110	100	001	010	100	110

Tabla 3.2: Permutación $P_{\mathbf{K}}^{\mathbf{T}}$ para los tonos $\mathbf{T}_0$ y $\mathbf{T}_1$

Advierta que al añadir un espacio adjunto extra, se pueden seleccionar dos permutaciones distintas $P_{\mathbf{K}}^{\mathbf{T}_0}$ y $P_{\mathbf{K}}^{\mathbf{T}_1}$ para dos tonos $\mathbf{T}_0 \neq \mathbf{T}_1$.

De esta manera, el comportamiento de la familia $\overline{P}(\mathbf{T})$ puede mapear el par $(\mathbf{T}, \mathbf{Y})$ a imágenes repetidas de 3 bits, asemejando el comportamiento de una familia de funciones. Esto será de suma importancia para los siguientes capítulos, donde hablaremos de seguridad e indistinguibilidad de funciones pseudoaleatorias.

3.3. Sistemas de respuesta

Un sistema probabilístico es un modelo matemático para estudiar el comportamiento de un algoritmo probabilístico interactivo como caja negra. Un algoritmo interactivo (probabilístico) es usualmente modelado como un autómata (probabilística). El concepto de sistema latente de Polderman y Willems (1997), que se describe en este documento, busca generalizar la interacción que existe entre el oráculo y el adversario para capturar el comportamiento de estos algoritmos. De manera análoga a las propuestas de Maurer et al. (2006), buscamos estudiar la integración de varios sistemas complejos con fines útiles para la criptografía.

Definición 3.3.1. *Un modelo matemático es una tripleta $(\Omega, \mathfrak{B}, E)$ conformada por un espacio muestral Ω, un espacio finito E y un subconjunto del universo $\mathfrak{B} \subseteq \Omega$ denominado el **comportamiento** tal que*

$$\mathfrak{B} := \{\omega \in \Omega \mid f_1(\omega) = f_2(\omega)\}$$

donde $f_1, f_2 : \Omega \to E$ son funciones que mapean una muestra ω a un elemento de E.

Cabe mencionar que el comportamiento está conformado por tuplas $\omega = (x, y) \in \Omega$ o muestras de entrada-salida obtenidas por los algoritmos que deseamos modelar. Usualmente, $f_1(\omega) = f_2(\omega)$ es una condición de equilibrio para un sistema dinámico, pero en este caso la empleamos como cualquier ecuación de interés dada por nuestro análisis de seguridad.

De esta manera, el comportamiento nos permite formalizar el estudio de los algoritmos como cajas negras, y nos da un enfoque para analizar los algoritmos interactivos de la siguiente manera:

Definición 3.3.2. *Un **sistema latente** o autómata es una tupla $(T, \Omega, L, \mathfrak{B})$ conformada por un conjunto de índices T, un espacio muestral Ω, un espacio de variables latentes L y un comportamiento interno $\mathfrak{B} \subseteq (\Omega \times L)^T$.*

Un autómata está asociado a un modelo matemático $(\Omega, \mathfrak{B}_{i/o})$ *cuyo comportamiento (observable) es*

$$\mathfrak{B}_{i/o} := \left\{ \omega : T \to \Omega \mid \exists \ell : T \to \mathbb{L} \ \textit{tal que} \ (\omega, \ell) \in \mathfrak{B} \right\}$$

Advierta cómo $\mathfrak{B}$ representa un mapa

$$t \ \mapsto \ (\omega_1, \ell_1), (\omega_2, \ell_2), \ldots, (\omega_t, \ell)$$

que describe la totalidad del funcionamiento de un sistema o algoritmo, mientras que el comportamiento $\mathfrak{B}$ (observable) es la generalización del sistema visto como una caja negra. De este modo, $\mathfrak{B}$ está conformado por todas las tuplas $\omega^q \sim \ell^q$ relacionadas con una variable latente. Rememore que una tupla $w^q \in \Omega$ se escribe $w^q = w_1, \, w_2, \, \ldots, \, w_q \, \forall q \geq 1$.

Es relevante destacar, que las variables latentes ℓ_i representan la incertidumbre implícita y directamente inobservable de una caja negra. Adicionalmente, es posible clasificar dos tipos de sistemas de acuerdo a su naturaleza:

- Un **sistema determinista**: es un modelo matemático muy útil para describir distintos algoritmos iterativos. El autómata descrito por Maurer (2002) puede ser modelado como un sistema de $(\mathbb{Z}^+, \Omega, S, \Sigma)$ indexado por $q \in \mathbb{Z}^+$ con un espacio muestral $\Omega = X \times Y$ y espacio de variables latentes S. El comportamiento (observable) de un autómata se define como

  $$\Sigma_{i/o} = \left\{ (x_1, y_1), \ldots, (x_q, y_q) \;\middle|\; \exists s : (x_i, y_i, s_i) \in \hat{\Sigma} \right\}$$

  y su comportamiento latente,

  $$\Sigma = \left\{ (x_1, y_1, s_1), \ldots, (x_q, y_q, s_q) \mid (y_i, s_i) = f(x_i, s_{i-1}) \right\}$$

  con estado inicial s_0 fijo. Observe cómo el comportamiento describe una secuencia de funciones indexadas mediante tuplas (x_i, y_i) funcionalmente compatibles.

- Un **sistema probabilístico**: es análogo a un autómata probabilístico cuyo sistema $(T, \Omega, \boxdot, \mathfrak{P})$ está relacionado con un espacio de probabilidad $(\Omega, \mathfrak{P}, \Pr[\,\cdot\,])$. Usualmente, se denota

  $$\mathbb{P}(\mathfrak{B}_{i/o}) = \Pr\left[\, \omega^q \in \mathfrak{B}_{i/o} \, \right]$$

  como el comportamiento de un sistema probabilístico o como variable aleatoria. En un sistema determinista, las variables latentes representan los estados internos que no son observables. En cambio, en un sistema probabilístico, el espacio de monedas $\boxdot$ representa la incertidumbre que tenemos del sistema en cuestión.

Visto lo anterior, se define de la siguiente manera los oráculos sobre la base del comportamiento.

Definición 3.3.3. *Un **oráculo** $\mathbb{O}$ o sistema de respuesta es un sistema probabilístico indexado por $i \in \mathfrak{I}_q$ consultas, cuyo comportamiento es una función probabilística $F : X \xrightarrow{\$} Y$ tal que para todo $(x_i, y_i) \in \Omega$*

$$\mathbb{P}^{\mathbb{O}}_{x^q}(y^q) \;:=\; \Pr\left[\, \mathbb{O}(x^q) = y^q \,\right] \;=\; \prod_{i=1}^{q} \Pr\left[\, F(x_i) = y_i \middle| \, F(x_j) = y_j \;\forall j < i \,\right]$$

Así, un sistema de respuesta se entiende como un sistema cuyo comportamiento es una secuencia de variables aleatorias dependientes entre si.

3.3.1. Oráculos deterministas

En ciencias de la computación, un oráculo es el concepto formal para modelar una caja negra (una máquina hipotética). Para ser específico, un oráculo es un sistema que responde de manera unívoca cada consulta que se le realice. La naturaleza del oráculo no es importante, lo esencial es que el comportamiento del oráculo puede variar dependiendo de las necesidades de nuestras pruebas o experimentos a estudiar.

El comportamiento de un oráculo puede estar asociado a un experimento $\mathbf{Exp}$. En particular, para un experimento de distinción, el comportamiento de un oráculo puede variar dependiendo del mundo en el que se encuentre. No obstante, antes de hablar más sobre los experimentos, es importante explicar algunos ejemplos de sistemas de respuesta.

Sean $(x_1, y_1), \ldots, (x_q, y_q) \in \Omega$ una secuencia de muestras entrada-salida y sea K el espacio de claves. Entonces:

Definición 3.3.4. *Un oráculo $\mathbb{F}$ puede comportarse como una familia $\left\{ F_k : X^{(q)} \to Y^{(q)} \mid k \in K \right\}$, denominada **función criptográfica**, de tal manera que para una clave $k \in K$,*

$$\mathbb{F}(k, x^q) = (F_k(x_1), F_k(x_2), \ldots, F_k(x_q)) \quad \forall x^q \in X^{(q)}$$

Cabe mencionar que $X^{(q)}$ representa el conjunto de tuplas x^q.

Definición 3.3.5. *Un oráculo $\mathbb{P}$ puede comportarse como una familia $\left\{ P_k : Y^{(q)} \to Y^{(q)} \mid k \in K \right\}$. En este escenario, es necesario definir la siguiente función criptográfica:*

$$P_k^{\pm} : \{1, -1\} \times Y^{(q)} \longrightarrow Y^{(q)}$$

de tal manera que $(1, x^q)$ mapea a la función $P_k(x^q)$ mientras que $(-1, x^q)$ mapea a la función inversa $P_k^{-1}(x^q)$.

Se define $P_k(\pm 1, x^q) := P_k^{\pm}(x^q)$ para el sistema de respuesta $\mathbb{P}^{\pm}$, mientras que la familia $\left\{ P_k^{\pm} \mid k \in K \right\}$ asociada al sistema se denomina **permutación fuertemente criptográfica**.

Es posible interpretar el comportamiento de un oráculo cuando actúa como permutación criptográfica o cuando actúa como su inversa, a través de un concepto introducido por Jha y Nandi (2022) conocido como representación unidireccional.

Definición 3.3.6. *Una **representación unidireccional** (α^q, x^q, y^q) es una tripleta asociada a una tripleta de tuplas $(\alpha^q, x^q, y^q) \in \{1, -1\} \times Y^{2q}$ dada, tal que para cada $i \in \mathfrak{I}_q$*

$$(a_i, b_i) := \begin{cases} (x_i, y_i), & \alpha_i = 1 \\ (y_i, x_i), & \alpha_i = -1 \end{cases}$$

La representación unidireccional es una forma equivalente de la forma original, puesto que la tripleta original se puede reconstruir de forma única a partir de la definición.

3.3.2. Oráculos aleatorios

El modelo de oráculo aleatorio apareció en primer lugar en el contexto de la teoría de la complejidad que permite estudiar algoritmos elaborados a través de esta abstracción (Bennett & Gill, 1981). Gracias a Bellare y Rogaway (1993), los oráculos fueron empleados en las demostraciones de seguridad para facilitar las pruebas mediante reducción.

En estas pruebas de reducción se evalúa cómo las construcciones reales pueden asemejar el comportamiento de los objetos ideales con cierto error acotado. Deje que X, Y y T sean conjuntos finitos con $|Y| = N$. Entonces:

Proposición 3.3.7. *Un oráculo p es una función aleatoria uniforme(URF) si su comportamiento es una función aleatoria $\rho \xleftarrow{\$} Y^X$ tal que para todo $y^q \in Y^{(q)}$ y $x^q \in X^{(q)}$*

$$\Pr\left[\, \mathsf{p}(x^q) = y^q \,\right] = \frac{1}{N^d}$$

donde d es la cantidad de x_i distintos por pares dentro de x^q. Para cualquier otro x^q o y^q la probabilidad es cero.

Antes de introducir la demostración primero consideré el siguiente ejemplo:

Ejemplo 3.3.1. Consideremos un oráculo y una función aleatoria $\rho \xleftarrow{\$} Y^X$ con $Y = \{0, 1\}^2$. Luego, para visualizar las posibilidades de 7 consultas, supongamos la siguiente respuesta del oráculo $(10, 11, 00, 10, 01, 11, 10) \in Y^{(7)}$.

$X^{(q)}$	x_1	x_2	x_3	x_4	x_5	x_6	x_7
$\mathsf{p}(x^q)$	10	11	00	10	01	11	10

Tabla 3.3: Comportamiento del oráculo como función aleatoria uniforme

Luego, para calcular la probabilidad de la primera entrada tenemos que

$$\Pr\left[\, \rho(x_1) = 10 \,\right] = \frac{1}{2^2} = \frac{1}{4}$$

De hecho, la probabilidad para cada entrada es exactamente igual debido a la naturaleza de ρ, ver 3.1.3. Enseguida, observe la Tabla 3.3 y considere la Proposición 3.1.4.

$$\therefore \quad \Pr\left[\, \rho(x^7) = (10, 11, 00, 10, 01, 11, 10) \,\right] = \frac{1}{4^7} = \frac{1}{16\,384}$$

Demostración. Por la Definición 3.3.3 de un sistema de respuesta, para cualquier cantidad $q < |X|$ de consultas y una cardinalidad $|X| = N$, es evidente que se tendrá una probabilidad de $1/N^q$. Además, tenga en cuenta que para cualquier $z^q \notin Y(q)$ el evento $\rho(x^q) = z^q$ no puede ocurrir.

□

Proposición 3.3.8. *Un oráculo π es una permutación aleatoria uniforme(URP) si su comportamiento es una permutación aleatoria $Y \xleftarrow{\$} Y$ tal que para todo $a^q, b^q \in Y^q$*

$$\Pr\left[\, \pi(a^q) = b^q \,\right] = \frac{1}{(N)_d}$$

donde d es la cantidad de x_i distintos por pares dentro de x^q. En cualquier otro caso la probabilidad es cero.

Ejemplo 3.3.2. Consideremos un oráculo y una permutación aleatoria $\pi \xleftarrow{\$} Y^\dagger$ con $Y = \{0,1\}^3$. Luego, para visualizar las posibilidades de 7 consultas, supongamos la siguiente respuesta del oráculo $(100, 000, 101, 001, 011, 010, 110) \in Y^{(7)}$.

$Y^{(q)}$	y_1	y_2	y_3	y_4	y_5	y_6	y_7
$\pi(x^q)$	100	000	101	001	011	010	110

Tabla 3.4: Comportamiento del oráculo como permutación aleatoria uniforme

Así, la probabilidad de la primera entrada tenemos que

$$\Pr\left[\, \pi(y_1) = 100 \,\right] = \frac{1}{2^3} = \frac{1}{8}$$

Como es de esperar, de acuerdo a la naturaleza de π (Proposición 3.2.2). A continuación, vea la Tabla 3.4 y recuerde las Proposiciones 3.2.4 y 3.2.5.

$$\therefore \quad \Pr\left[\, \pi(y^7) = (100, 000, 101, 001, 011, 010, 110) \,\right] = \frac{1}{(8)_7} = \frac{1}{40\,320}$$

Demostración. Por la Definición 3.2.3, vea que para cualquier cantidad $q < |Y|$ de consultas y una cardinalidad $|Y| = N$, se tendrá una probabilidad $1/(N)_q$.

□

En general, sea (γ^q, a^q, b^q) una representación unidireccional de (x^q, y^q). Entonces, para cualquier URP su probabilidad como permutación aleatoria fuerte es:

$$\Pr\left[\,\pi^{\pm}(\gamma^q, x^q) = y^q\,\right] := \frac{1}{(N)_d}$$

tal que d es la cantidad de a_i distintos de a^q, los cuales son el mismo número de b_i distintos de b^q. Por último, para una permutación entonable tenemos que:

Proposición 3.3.9. *Un oráculo $\overline{\pi}$ es una permutación entonable aleatoria uniforme(TURP) si su comportamiento es una permutación entonable aleatoria $\overline{\pi} \xleftarrow{\$} T \times Y^{\dagger}$, tal que para toda $a^q, b^q \in Y^{(q)}$,*

$$\Pr\left[\,\overline{\pi}(t^q, a^q) = b^q\,\right] = \prod_{i=1}^{q} \frac{1}{N - \alpha_i}$$

donde cada α_i es la cantidad de índices $j < i$ tales que $x_i \neq x_j$ para cada $t_i = t_j$.

Ejemplo 3.3.3. Consideremos un oráculo y una permutación entonable aleatoria $\overline{\pi} \xleftarrow{\$} T \times Y^{\dagger}$ con $T \times Y = \{0,1\} \times \{0,1\}^3$. Luego, para visualizar las posibilidades de 7 consultas, se supone la siguiente respuesta del oráculo $(100, 000, 101, 001, 011, 010, 110) \in Y^{(7)}$. Enseguida, para entender el proceso del cálculo:

$Y^{(7)}$	y_1	y_2	y_3	y_4	y_5	y_6	y_7
$T^{(7)}$	0	0	1	1	0	1	0
$\overline{\pi}(t^7, x^7)$	100	000	101	001	011	010	110

Tabla 3.5: Comportamiento del oráculo como permutación aleatoria uniforme

Para calcular la probabilidad de una permutación entonable, por la Proposición 3.2.3, se sabe que dos pares $(t_i, y_i) = (t_j, y_j)$ no pueden tener imágenes distintas. Por lo tanto, podemos ordenar las probabilidades juntando los tonos idénticos $t_i = t_j$ de la Tabla 3.5, así

$$\Pr\left[\begin{array}{c} \overline{\pi}(t^7, y^7) = (100, 000, 101, \\ 001, 011, 010, 110) \end{array}\right] = \Pr\left[\begin{array}{ll} \overline{\pi}(0^4, a^4) & = (100, 000, 011, 110), \\ \overline{\pi}(1^3, b^3) & = (101, 001, 010) \end{array}\right]$$

Es posible realizar esto porque las instancias π^0 y π^1 son independientes. Note cómo existen 4 índices correspondientes al tono 0 y 3 índices para el tono 1, tales que las tuplas $a^4 = y_1y_2y_5y_7$ y $b^3 = y_3y_4y_6$ corresponden a las entradas de cada sistema, respectivamente.

$$\therefore \quad \Pr\left[\begin{array}{ll} \overline{\pi}(0^4, a^4) & = (100, 000, 011, 110), \\ \overline{\pi}(1^3, b^3) & = (101, 001, 010) \end{array}\right] = \frac{1}{(2^3)_4} \cdot \frac{1}{(2^3)_3} = \frac{1}{564\,480}$$

Demostración. En general, para un sistema $\overline{\mathbb{P}}$ cuyo comportamiento es una permutación entonable, es posible desacoplarlo en sistemas independientes $\mathbb{P}^t$ cuyo comportamiento es una permutación, tal que

$$\Pr\left[\,\overline{\mathbb{P}}(t^q, x^q) = y^q\,\right] = \prod_{t=0}^{\lambda} \Pr\left[\,\mathbb{P}^t(a^k) = b^k\,\right]$$

donde λ es la cantidad de tonos t_i en t^q distintos por pares y (a^k, b^k) es el par de tuplas correspondientes al comportamiento de $\mathbb{P}^t$ para cada tono fijo t. Por definición de sistema de respuesta, se concluye la prueba.

□

Con esta última conclusión, hemos introducido todos los conceptos de probabilidad fundamentales para estudiar cualquier primitiva criptográfica. Enseguida abordaremos en los siguientes capítulos, algunos fundamentos para diseñar aplicaciones reales tales como esquemas criptográficos.

Capítulo 4

Pseudoaleatoriedad y adversarios

Las funciones aleatorias son los objetos ideales para fines criptográficos. Debido a su naturaleza, es imposible predecir con precisión algún valor concreto de ésta, incluso para el adversario más poderoso e inteligente que imaginemos. Éste es el motivo que impulsa a estudiar las funciones pseudoaleatorias para sus aplicaciones en esquemas de cifrados con seguridad incondicional.

Antes de definir una función pseudoaleatoria, es importante entender otros conceptos. En particular, qué es un adversario, qué es un distinguidor y cuáles son sus objetivos. A continuación, describimos al antagonista principal de nuestros esquemas de cifrado.

4.1. Adversarios

En criptografía y en ciencias de la computación, el hablar de un adversario $\mathcal{A}$ se refiere a un algoritmo iterativo capaz de ejecutar otro algoritmo B como subrutina, denotado $\mathcal{A}^B$. De tal manera que el adversario interactúa con B hasta obtener la respuesta deseada. Podríamos considerar al adversario como un sistema de respuesta, cuyo comportamiento interno está relacionado con la estrategia que emplea para solucionar un algoritmo. Éste, generalmente, es un sistema criptográfico y dependiendo del objetivo del adversario, pudiera contestar con un modelo de la primitiva, una clave secreta, un texto plano o simplemente con un bit.

Un adversario puede comportarse de distintas maneras, por lo que es importante tener en cuenta las siguientes estrategias:

Ataque de texto plano conocido (KPA): un adversario posee una cantidad fija de muestras de texto plano y cifrado recolectadas del sistema criptográfico.

Ataque de texto plano elegido (CPA): se considera un adversario con mayor poder, puesto que se le permite tener acceso al cifrador como caja negra, y obtener los textos cifrados correspondientes de cualquier texto plano de su elección.

Ataque de texto cifrado elegido (CCA): se le permite al adversario no solamente obtener textos cifrados de la caja negra, sino también consultar textos cifrados y observar sus textos

planos correspondientes.

Para cualquiera de estos ataques, podemos considerar un comportamiento adaptativo o no adaptativo. Un adversario **no adaptativo** selecciona a priori todas las consultas que desea realizar a la caja negra, después espera la respuesta de la caja negra y por último evalúa todas las muestra que tiene a su disposición.

Un adversario **adaptativo** es capaz de realizar una consulta a la vez, evaluando cada respuesta de manera iterativa para seleccionar mejores consultas cada vez. Esto a veces es denominado como un ataque de texto bien elegido.

Definición 4.1.1. *Un **adversario** $\mathcal{A}$ es un sistema probabilístico cuyo comportamiento es compatible con una función probabilística $Y \xrightarrow{⚅} X$. Un adversario es llamado:*

- **No adaptativo**: si $\mathcal{A}(y^q)$ es independiente de cualquier entrada y^q. Es decir, el comportamiento del adversario depende únicamente del espacio de monedas ⚅.
- **Determinista**: si el espacio de monedas ⚅ es degenerado. En este caso, el adversario se comporta como un autómata.

Definición 4.1.2. *Una **función de decisión** $\flat : \mathcal{A}(Y^{(q)}) \longrightarrow \{0,1\}$ es una función binaria que toma la imagen de un adversario y devuelve un bit. Al adversario $\mathcal{A} \sim \flat$, relacionado con una función de decisión, se le denomina **distinguidor**.*

La clase de los distintos ataques posibles que puede ejecutar un distinguidor se denota

$$ATK := \{KPA, CPA, CCA\}$$

y escribimos $\mathcal{A} \in ATK$ como un adversario bajo alguna clase de ataque.

4.2. Función pseudoaleatoria

Una función pseudoaleatoria (PRF) es una función indexada tal que una instancia elegida aleatoriamente es computacionalmente indistinguible de cualquier función aleatoria. Esto significa que observar el comportamiento de entradas y salidas de una función no es suficiente para decidir si la función pertenece a una familia dada. Para poder verificar que una familia de funciones cumple con los criterios de ser una función pseudoaleatoria se tiene el siguiente experimento.

Imagine que usted tiene acceso a una función g como caja negra, *i.e.*, no posee ningún modelo ni conocimiento sobre los estados internos de la función. Lo único que puede realizar es estudiar el comportamiento entrada-salida de la caja g al ingresar entradas válidas y observar las respuestas. Suponga que el comportamiento de la caja varía de dos maneras posibles, dependiendo del mundo en que se encuentre. Estos mundos posibles se definen de la siguiente manera:

- **Mundo 0:** el oráculo $\mathbb{O}$ es tomado uniformemente al azar de la familia de todas las funciones $X \to Y$, es decir, el sistema de respuesta es una URF $\rho \xleftarrow{\$} Y^X$.
- **Mundo 1:** el oráculo $\mathbb{O}$ es un sistema determinista que se comporta como una instancia de la familia F generada por una clave $k \xleftarrow{\$} Key(F)$ tomada al azar.

El propósito de este experimento es medir la probabilidad de que una persona o entidad (formalmente un distinguidor) sea capaz de resolver si se encuentra interactuando con la caja en el mundo 0 o el mundo 1. Intuitivamente, este experimento es análogo a una *prueba de Turing* para funciones pseudoaleatorias.

Un distinguidor puede realizar cualquier número de preguntas a la caja y terminar el experimento cuando esté seguro sobre el mundo en que se encuentra. Este proceso está basado en los juegos de indistinguibilidad propuestos por Shoup (2004), y nos permite definir la calidad de F como función pseudoaleatoria, a partir de la dificultad que encuentra un distinguidor en este experimento. Formalmente, se define la indistinguibilidad computacional con el siguiente algoritmo:

Definición 4.2.1. *Sea $F : K \times X \to Y$ una familia y $\mathcal{A}^{\mathbb{O}}$ un distinguidor con acceso a un oráculo. Se definen los siguientes experimentos:*

EXPERIMENTO $\mathbf{Exp}_0^{\text{PRF}}(\mathcal{A}; \rho)$:
- $\rho \xleftarrow{\$} Y^X$
- $\mathbb{O} \leftarrow \rho$
- $\flat \leftarrow \mathcal{A}^{\rho}$
- **regresa** $\flat$

EXPERIMENTO $\mathbf{Exp}_1^{\text{PRF}}(\mathcal{A}; F)$:
- $k \xleftarrow{\$} \mathcal{K}$
- $\mathbb{O} \leftarrow F_k$
- $\flat \leftarrow \mathcal{A}^{F_k}$
- **regresa** $\flat$

Algoritmo 4.2.1: Experimento PRF: Mundo 0 y Mundo 1

La probabilidad de éxito de un distinguidor se define como

$$\mathbf{Adv}_F^{\text{PRF}}(\mathcal{A}) := \Pr\left[\,\mathbf{Exp}_1^{\text{PRF}}(\mathcal{A}; F) \;\Rightarrow\; 1\,\right] - \Pr\left[\,\mathbf{Exp}_0^{\text{PRF}}(\mathcal{A}; \rho) \;\Rightarrow\; 1\,\right]$$

Este experimento formaliza el concepto de mundo, que hablamos anteriormente, al introducir dos oráculos totalmente independientes. Se denota $\mathcal{A}^{\rho}$ como un distinguidor que ejecuta al oráculo ideal como subrutina y $\mathcal{A}^{F_k}$ cuando ejecuta al oráculo real. De esta manera, el Mundo 0 corresponde al experimento que estudia el comportamiento del oráculo (objeto) ideal, mientras que el Mundo 1, estudia el comportamiento del oráculo (objeto) real. Reflexione, cómo la idea detrás de estos experimentos es análoga a un examen de Turing.

Es importante resaltar que un distinguidor inteligente $\mathcal{A}$ interactuando con el oráculo real, en el Mundo 1, tendrá una probabilidad muy alta de retornar 1. Mientras tanto, el mismo distinguidor, en el Mundo 0, tendrá una probabilidad muy baja de hacerlo. Por lo tanto, es posible

calcular la diferencia entre ambos experimentos mediante el estudio del comportamiento de ambos oráculos.

Un punto importante de esta definición es que el adversario $\mathcal{A}$ no tiene conocimiento sobre la clave $k \in Key(F)$. No tiene sentido experimentar con una función pseudoaleatoria si k es conocida, a priori, por un adversario. De lo contrario, el distinguidor puede diferenciar el objeto real del ideal de manera trivial sin necesidad de estudiar sus comportamientos.

Cada tipo de adversario tendrá diferentes probabilidades de éxito, principalmente por dos motivos. Un adversario muy inteligente puede consultar menos preguntas, pero consiguiendo mayor información. Mientras que un adversario con más recurso realizará tantas consultas como sea posible hasta eventualmente obtener la respuesta deseada de su oráculo. En general, esperamos que a medida que un adversario obtenga más muestras de entrada-salida, su capacidad para determinar en qué mundo se encuentra aumentará.

En criptografía, una función pseudoaleatoria puede no ser segura para aplicaciones criptográficas, ya que el experimento por sí solo no garantiza que la ventaja de un distinguidor cualquiera esté limitada por ciertos recursos informáticos específicos. En los siguientes capítulos estudiaremos a más detalle la relación entre los adversarios y la seguridad de un esquema criptográfico.

4.3. Permutación pseudoaleatoria

Una familia de funciones $E : K \times Y \to Y$ es una permutación pseudoaleatoria si el comportamiento de entrada-salida de una instancia aleatoria de la familia es "computacionalmente indistinguible" de una permutación aleatoria de Y.

En este contexto, hay dos tipos de experimentos que se pueden considerar. El primero, como antes, consiste en un adversario con acceso a un oráculo para estudiar el comportamiento de la familia que está siendo probada. Sin embargo, cuando E es una familia de permutaciones, también se puede considerar el caso en que el adversario recibe, además, un oráculo para E^{-1}. Consideramos estas configuraciones en orden. La primera es la configuración de ataques de texto en claro elegido, mientras que la segunda es la configuración de ataques de texto cifrado elegido.

Considere el siguiente experimento, tome una familia de funciones F sin exigir que F sea una familia de permutaciones. Luego, se definen los mundos de la siguiente manera:

- **Mundo 0:** El oráculo $\mathbb{O}$ es tomado uniformemente al azar de la familia de todas las permutaciones $Y \to Y$, *i.e.*, su comportamiento es una permutación aleatoria $g \xleftarrow{\$} Y^X$.
- **Mundo 1:** El oráculo $\mathbb{O}$ es un sistema determinista que se comporta como una instancia de la familia $F : \{F_k \mid k \in \mathcal{K}\}$ generada por una clave tomada al azar $k \xleftarrow{\$} \mathcal{K}$.

Observe que el Mundo 1 es idéntico al mundo (oráculo) real para una PRF. Igual que antes, se considera un distinguidor que estudia el comportamiento de dos objetos para determinar con cuál está interactuando. Este experimento se formaliza de la siguiente manera:

Definición 4.3.1. *Sea $F : K \times Y \to Y$ una familia de funciones, y $\mathcal{A}$ un distinguidor con acceso a un oráculo $\mathbb{O}$ para realizar consultas hasta retornar un bit $\flat$. Se definen los siguientes experimentos:*

EXPERIMENTO $\mathbf{Exp}_0^{\text{PRP}}(\mathcal{A}, F)$:
- $\pi \xleftarrow{\$} Y^{\dagger}$
- $\mathbb{O} \leftarrow \pi$
- $\flat \leftarrow \mathcal{A}^{\pi}$
- **regresa** $\flat$

EXPERIMENTO $\mathbf{Exp}_1^{\text{PRP}}(\mathcal{A}, F)$:
- $k \xleftarrow{\$} \mathcal{K}$
- $\mathbb{O} \leftarrow F_k$
- $\flat \leftarrow \mathcal{A}^{F_k}$
- **regresa** $\flat$

Algoritmo 4.3.1: Experimento PRP: Mundo 0 y Mundo 1

La probabilidad de éxito de un distinguidor bajo CPA se define como

$$\mathbf{Adv}_F^{\text{PRP}}(\mathcal{A}) := \Pr\left[\,\mathbf{Exp}_1^{\text{PRP}}(\mathcal{A}; F) \to 1\,\right] - \Pr\left[\,\mathbf{Exp}_0^{\text{PRP}}(\mathcal{A}; \pi) \to 1\,\right]$$

De esta manera el experimento es análogo a la Definición 4.2.1. La diferencia principal es que el oráculo ideal con el que se compara F, ya no es una función aleatoria, sino una permutación aleatoria. Sin embargo, esta definición puede no ser suficiente para definir una permutación pseudoaleatoria criptográficamente segura, puesto que un adversario más inteligente podría hacer uso de una estrategia no trivial que consiste en consultar la inversa de la permutación aleatoria.

Como una familia de funciones no está obligada a tener una función inversa, esta evaluación no es posible bajo la manera en que está definido el experimento. Por ello, una familia de funciones que sea indistinguible de una permutación aleatoria bajo este experimento es conocida como una permutación pseudoaleatoria bajo ataque de texto plano elegido (CPA por sus siglas en inglés).

4.3.1. Permutación pseudoaleatoria fuerte

Como se mencionó, el experimento PRP bajo CPA está limitado a considerar un adversario que estrictamente consulta pares de texto plano y cifrado, conforme interroga a un oráculo. Un adversario más astuto puede seleccionar textos cifrados para encontrar sus respectivos textos planos asociados y de esta manera obtener un par de texto cifrado-plano congruente que le permita decidir si está interactuando con el oráculo real o el ideal.

Lo anterior, se obtiene al emplear familias de permutaciones (como los BC) en lugar de una familia de funciones usual. Esto permite que un adversario en el mundo 1, ahora pueda consultar la función inversa de la permutación. De lo contrario, no se puede garantizar que la función dada por la familia posea una inversa, ocasionando problemas por la manera en que está diseñado el experimento. Formalmente, se define el experimento de la siguiente manera:

Definición 4.3.2. *Sea $P : K \times Y \to Y$ una familia de permutaciones y sea $\mathcal{A}^{\mathbb{O}}$ un distinguidor con acceso a un oráculo $\mathbb{O}$, para realizar consultas hasta retorna un bit $\flat$. Se definen los siguientes experimentos:*

EXPERIMENTO $\mathbf{Exp}_0^{\text{SPRP}}(\mathcal{A}, P)$:
- $\pi \xleftarrow{\$} Y^{\dagger}$
- $\mathbb{O} \leftarrow \pi$
- $\flat \leftarrow \mathcal{A}^{\pi, \pi^{-1}}$
- **regresa** $\flat$

EXPERIMENTO $\mathbf{Exp}_1^{\text{SPRP}}(\mathcal{A}, P)$:
- $k \xleftarrow{\$} \mathcal{K}$
- $\mathbb{O} \leftarrow P_k$
- $\flat \leftarrow \mathcal{A}^{P_k, P_k^{-1}}$
- **regresa** $\flat$

Algoritmo 4.3.2: Experimento SPRP: Mundo 0 y Mundo 1

La probabilidad de éxito del distinguidor bajo CCA se define como

$$\mathbf{Adv}_P^{\text{SPRP}} := \Pr\left[\,\mathbf{Exp}_0^{\text{SPRP}}(\mathcal{A}; \pi) \to 1\,\right] - \Pr\left[\,\mathbf{Exp}_1^{\text{SPRP}}(\mathcal{A}; P) \to 1\,\right]$$

Observe que en el mundo 0, el oráculo ideal se comporta del mismo modo que en el Experimento 4.3.1. Sin embargo, ahora sí requerimos que P sea una familia de permutaciones para que el adversario puede consultar la función inversa P_k^{-1}, si así lo desea. Este experimento se conoce como permutación pseudoaleatoria bajo ataque de texto cifrado elegido o de permutación pseudoaleatoriamente fuerte.

4.3.2. Relación entre el experimento PRP y SPRP

Debido a que un adversario bajo CCA puede decidir no realizar ninguna consulta a la inversa de su oráculo, en ese caso, parece evidente que el adversario está prácticamente realizando un ataque CPA. Para evaluar este concepto consideré la siguiente proposición:

Proposición 4.3.3. *Sea $P : \left\{P_k \mid k \in K\right\}$ una familia de permutaciones y sea $\mathcal{A}^{\mathbb{O}}$ un distinguidor bajo el experimento $\mathbf{Exp}^{\text{PRP}}$ que realiza a lo más q consultas. Entonces, existe un adversario $\mathcal{B}$ bajo el experimento $\mathbf{Exp}^{\text{PRP}}$ realizando la misma cantidad q de consultas de textos planos, sin consultar P_k^{-1}, tal que*

$$\mathbf{Adv}_P^{\text{SPRP}}(\mathcal{B}) \geq \mathbf{Adv}_P^{\text{PRP}}(\mathcal{A})$$

Demostración.
Si un adversario $\mathcal{A}$ bajo CCA no realiza ninguna consulta de texto cifrado, entonces $\mathcal{A}$ tendrá la misma ventaja bajo CPA.

$$\mathbf{Adv}^{\text{PRP}}(\mathcal{A}) = \mathbf{Adv}^{\text{SPRP}}(\mathcal{A})$$

Se asume que $\mathcal{B}$ es un adversario bajo CCA que tiene la misma inteligencia que $\mathcal{A}$, pero realiza al menos una consulta de texto cifrado. Debido a que la ventaja de los adversarios también depende de la cantidad de consultas que realicen:

$$\therefore \quad \mathbf{Adv}^{\text{PRP}}(\mathcal{A}) \; = \mathbf{Adv}^{\text{SPRP}}(\mathcal{A}) \; \leq \mathbf{Adv}^{\text{SPRP}}(\mathcal{B})$$

□

Este resultado implica que el conjunto de adversarios bajo CPA está incluido en el conjunto de adversarios bajo CCA. Por ello, la Definición 3.3.5 (referente a una permutación) es bastante general para hablar de cualquier permutación pseudoaleatoria.

Con todo lo dicho, en el siguiente capítulo estudiaremos el enfoque moderno referente a la seguridad de los esquemas de cifrado simétrico. Es importante recordar las propiedades de una función pseudoaleatoria, puesto que más adelante veremos como se emplean para la construcción de un MAC.

Capítulo 5

Seguridad e Indistinguibilidad

En los capítulos anteriores se mencionaron varios objetos importantes en la criptografía, por ejemplo, funciones pseudoaleatorias, permutaciones pseudoaleatorias y el modelo de oráculo aleatorio. El propósito del modelo de Bellare y Rogaway (2005) es estudiar los objetos criptográficos a partir de las propiedades de ciertos objetos perfectos. Además, se planteó la idea de medir la ventaja de un adversario como su probabilidad de éxito en un experimento bien definido. Cada experimento específico tiene sus propias condiciones de éxito para un adversario dado y el éxito del adversario crece de acuerdo a la capacidad de cómputo que posea: tiempo de ejecución, espacio de memoria y cantidad de consultas.

Para los esquemas simétricos se utiliza un concepto de indistinguibilidad más general basado en la teoría de la información conocido como **seguridad incondicional**. La seguridad incondicional o de complejidad teórica de información se basa informalmente en considerar un adversario con capacidad de cómputo infinita. Lo que significa que se ignoran los parámetros del tiempo de ejecución y el espacio de memoria en nuestro análisis, para enfocarnos sólo en la cantidad de consultas q y su tamaño μ. Este enfoque precisa acotar la información pertinente que puede obtener un adversario con cada consulta, para adivinar con qué objeto se encuentra interactuando. Antes de entrar en más detalle sobre el significado de seguridad incondicional, es esencial repasar las definiciones fundamentales.

5.1. Esquema de cifrado

En el esquema clásico tenemos a un grupo conformado por un emisor y un receptor que se comunican a través de un canal inseguro, en donde se encuentra a un "hombre en el medio" conocido como el adversario. La solución es emplear una clave secreta, la cual permite ocultar sus mensajes a través del canal inseguro, de esta manera pueden establecer un protocolo de comunicación privado entre los dos. Debido a que tanto el emisor como el receptor deben tener el mismo conocimiento (comparten la misma clave) estos esquemas son denominados simétricos.

El esquema simétrico especifica un algoritmo de cifrado que indica al emisor cómo procesar el texto plano utilizando la clave, produciendo así el texto cifrado que se transmite realmente. Un

esquema de cifrado también especifica un algoritmo de descifrado que indica al receptor cómo recuperar el texto plano original de la transmisión, posiblemente realizando también alguna verificación. Finalmente, hay un algoritmo de generación de claves, la cual produce una clave que las partes necesitan compartir. La descripción formal se enuncia a continuación.

Definición 5.1.1. *Un esquema de cifrado simétrico es una tripleta* $(\mathcal{K}, \mathcal{E}, \mathcal{D})$ *que consta de tres algoritmos eficientes:*

1. ***Generación de claves aleatorias***: *el algoritmo* $\mathcal{K}$ *genera una clave secreta tomada al azar* $k \xleftarrow{\$} \mathrm{K}_\Sigma$.

2. ***Cifrado de mensaje***: *dado un mensaje* $m \in \mathrm{M}_\Sigma$ *y una clave secreta* k*, el algoritmo* $\mathcal{E}$ *genera un texto cifrado* $c \leftarrow \mathcal{E}_k(m)$

3. ***Descifrado determinista***: *dado un texto cifrado* $c \in \mathrm{C}_\Sigma$ *y una clave secreta* k*, el algoritmo* $\mathcal{D}$ *regresa un mensaje* $m = \mathcal{D}_k(c)$.

De manera análoga a una familia de funciones, un esquema de cifrado está asociado a un espacio de claves K_Σ, un espacio de mensajes M_Σ y un espacio de cifrados C_Σ. Estos algoritmos están definidos sobre los espacios antes nombrados, pero puede existir el caso de que tomemos un mensaje $m \notin \mathrm{M}_\Sigma$ o un texto cifrado $c \notin \mathrm{C}_\Sigma$ inválido. Por lo tanto, denotamos $\perp$ como el resultado para un valor indefinido en un esquema.

Cabe destacar que $\mathcal{E}$ puede ser un algoritmo probabilístico (con estado o sin estado) que genera un texto cifrado $c \leftarrow \mathcal{E}_k(m)$, mientras que $\mathcal{D}$ está obligado a ser un algoritmo determinista que siempre devuelve $\mathcal{D}_k(c) = m$. Estos algoritmos pueden estar basados en cifradores por bloques o permutaciones públicas. De esta manera, un equipo conformado por un emisor y receptor pueden establecer la comunicación en un canal inseguro.

Diseñar estos algoritmos a través de un enfoque informal sólo genera varios problemas (discutidos en el capítulo acerca de cifradores por bloques) al diseñar esquemas complejos y hablar de su seguridad. Ésta es la filosofía con la que se han creado los sistemas más antiguos como "El cifrado Vigenere" hasta la construcción de la máquina enigma (Shimeall & Spring, 2014).

No obstante, lo que la historia ha mostrado es que todos estos esquemas han sido rotos y a pesar de proponer soluciones para repararlos, estas soluciones se confían de tener la ventaja tecnológica. Creer que un sistema siempre va a estar al borde de la vanguardia y que el adversario es incapaz de superarnos en inteligencia o poder de cómputo es una aproximación muy ingenua para garantizar la seguridad de un esquema. La criptografía moderna actualmente está fundamentada sobre definiciones, hipótesis y pruebas matemáticas sólidas. Este enfoque riguroso constituye la diferencia entre la filosofía clásica, basada en propuestas Ad hoc, y el formalismo moderno (Goldwasser & Micali, 1984; Savage, 2013; Shannon, 1949).

5.2. Seguridad perfecta

Imaginemos un adversario que conoce la distribución de probabilidad sobre M, así como el esquema de cifrado empleado por un grupo conformado de un emisor y de un receptor. Si el emisor manda al receptor un mensaje cifrado, el adversario puede interceptar el mensaje y observarlo. Esto se denomina un ataque bajo texto cifrado único, y es el esquema de seguridad clásico de la criptografía (Bellare & Rogaway, 2005; Shannon, 1949).

Asumimos un esquema clásico en donde un emisor envía mensajes ocultos a un receptor a través de un canal inseguro, y un adversario se encuentra en medio, interfiriendo en los mensajes que se envían. Para que este esquema de seguridad sea perfectamente seguro, un adversario en posesión de un texto cifrado c no puede ganar algún conocimiento sobre la distribución de los mensajes en M.

Definición 5.2.1. *Sea $k \in \mathrm{K}_\Sigma$ una llave secreta y sean $m, m' \in \mathrm{M}_\Sigma$ dos mensajes distintos. Entonces, Σ es un esquema **perfectamente seguro** si la probabilidad para todo texto cifrado $c \in \mathrm{C}_\Sigma$ es*

$$\Pr\left[\mathcal{E}_k(m) = c\right] = \Pr\left[\mathcal{E}_k(m') = c\right] \tag{5.1}$$

Repare en cómo esta definición de seguridad exige que la distribución $\mathcal{E}_k(\mathbf{M})$ sea precisamente la distribución uniforme. El concepto de seguridad perfecta es muy poderoso. Debido a que un adversario, sin conocimiento de la clave secreta, tiene la misma ventaja escuchando un texto cifrado que escuchando todos. Estos conceptos de indistinguibilidad entre textos, ventaja de un adversario y distribución uniforme serán muy importante para encontrar una condición de suficiencia para la seguridad de cualquier esquema criptográfico.

Viendo este teorema desde la teoría de la información, la conclusión es bastante evidente, puesto que Shannon (1949) pide que la entropía de un esquema sea máxima para garantizar que su seguridad. Un adversario al obtener un texto cifrado c no es capaz de conocer algo sobre cualquier otro texto cifrado $c' = \mathcal{E}_k(m')$. Es pertinente resaltar que esto es muy problemático, ya que el adversario podría buscar todos los mensajes en el espacio M_Σ. y aun así no tener alguna pista sobre qué mensaje m fue cifrado para obtener c. Para asimilar mejor este resultado, se analiza el esquema de Un-sólo-uso (*One-time-pad*).

5.2.1. One-Time-Pad

El esquema de cifrado de Un-sólo-uso (*One-time-pad*) es un esquema de cifrado determinista, cuyo algoritmo de generación de claves $\mathcal{K}$ devuelve una cadena aleatoria de $\mathbf{K} \in \{0,1\}^k$. El algoritmo de cifrado mantiene un contador estático ctr que inicialmente es cero. Entonces, los algoritmos de cifrado y descifrado operan de la siguiente manera:

ALGORITMO $\mathcal{E}(\mathbf{M}, \mathbf{K})$
- $ctr \leftarrow 0$ ◁ *valor estático*
- $m \leftarrow |\mathbf{M}|$
- **si** $ctr + m > |\mathbf{K}|$ **entonces**
  - **regresa** $\perp$
- $\mathcal{C} \leftarrow \mathbf{M} \oplus \mathbf{k}_{ctr+1} \,[\!]\, \ldots \,[\!]\, \mathbf{k}_{ctr+m}$
- $ctr \leftarrow ctr + m$
- **regresa** $ctr - m, \mathcal{C}$

ALGORITMO $\mathcal{D}(\mathcal{C}', \mathbf{K}, ctr)$
- $m \leftarrow |\mathcal{C}'|$
- **si** $ctr + m > |\mathbf{K}|$ **entonces**
  - **regresa** $\perp$
- $\mathbf{M} \leftarrow \mathcal{C}' \oplus \mathbf{k}_{ctr+1} \,[\!]\, \ldots \,[\!]\, \mathbf{k}_{ctr+m}$
- **regresa** $\mathbf{M}$

Algoritmo 5.2.1: Esquema de cifrado *One-time-pad*

En este caso, cada $\mathbf{K}|_i$ representa el i-ésimo bit dentro de la clave secreta $\mathbf{K}$. El contador ctr consiste en un parámetro que permite variar y seleccionar la cantidad de bits que se usarán como una máscara para el mensaje $\mathbf{M}$. Después, el cifrador realiza una operación XOR bit por bit $\mathbf{K}|_i \oplus \mathbf{M}|_i$ entre la llave y el mensaje. Para un bit del cifrado $\mathcal{C}_i$ sólo existen dos posibles resultados: 1 o 0, por lo que la probabilidad de adivinar la llave correcta es $1/2$. Por lo tanto, para cualquier índice entre $ctr + 1$ y $ctr + m$, se tiene que

$$\Pr\left[\, \mathcal{E}_{\mathbf{K}}(\mathbf{M}) = \mathcal{C} \,\right] = \prod_{i=1}^{m} \frac{1}{2^i} = \frac{1}{2^m}$$

Como la llave $\mathbf{K}$ es tomada al azar de las cadenas de $\{0,1\}^k$ distribuidas de manera uniforme, es posible que el mensaje sea más grande que la clave. Por ello, el algoritmo siempre verifica el tamaño de la clave $\mathbf{K}$, el contador ctr y el mensaje m para asegurar que el cifrado sea posible $|\mathbf{K} + ctr| = |\mathbf{M}|$. La seguridad de este esquema se hace evidente al notar que la operación XOR preserva la uniformidad en la distribución de los bits de llave tomada al azar.

$$\therefore \quad \Pr\left[\, \mathcal{E}_{\mathbf{K}}(\mathbf{M}) = \mathcal{C}' \,\right] = \frac{1}{2^m}$$

Observe cómo el esquema *One-time-pad* cumple con la Definición 5,2,1. Antes de concluir, advierta que la naturaleza de este algoritmo implica la necesidad de poseer una clave de la misma longitud (incluso mayor) que el mensaje a cifrar para garantizar seguridad perfecta. No obstante, este problema no es exclusivo del esquema *One-time-pad*. El Teorema 2.10 de Katz y Lindell (2014), demuestra que todo esquema Σ perfectamente seguro requiere un espacio de claves $|\mathrm{K}_\Sigma| \geq |\mathrm{M}_\Sigma|$. Esta clase de resultados, nos revela la naturaleza entre la seguridad informática y los recursos computacionales.

5.3. Seguridad computacional

Como se discutió, es posible obtener un esquema con un enorme nivel de seguridad, pero a un costo muy alto, que es factible sólo para algunas agencias gubernamentales o multinacionales.

Sin embargo, para cualquier uso práctico de la criptografía, ¿es necesario tal nivel de seguridad? Es obvio que la Definición 5.2.1 es una condición suficiente, pero quizás no necesaria.

El ideal de seguridad perfecta es la meta a alcanzar para cualquier criptógrafo, pero en ciencias de la computación se busca un compromiso entre los objetivos y el costo. Esto es de suma importancia para aplicaciones de bajos recursos: el área de salud, el hogar, el campo, para mejorar la eficiencia energética o combatir el cambio climático.

A continuación, se estudia un concepto de seguridad, posiblemente más débil que el propuesto por Shannon aunque más general, que nos permite contemplar todo tipo de adversarios siempre y cuando especifiquemos la cantidad de recursos a los que se tiene acceso.

5.3.1. Enfoque asintótico

La seguridad computacional se basa en el enfoque de la teoría de complejidad algorítmica. Introducimos una variable n que parametriza la seguridad de un esquema de cifrado Σ, así como los recursos del equipo emisor-receptor. Cuando un equipo ejecuta el esquema de cifrado, se asume que ellos asignan un valor para n (generalmente el tamaño de la llave) y este valor es conocido por el adversario.

Recordemos que un adversario es un algoritmo, por lo tanto podemos definir un adversario eficiente como un algoritmo que rompe un esquema en tiempo polinómico (dado por el parámetro de seguridad n, es decir, $p(n)$). En teoría de la complejidad, se sabe que un problema fácil es un problema que es resuelto en tiempo polinómico, mientras que un problema difícil se resuelve en tiempo no polinómico. Por ello se define:

Definición 5.3.1. *Una **función negligible** es una función $\xi : \mathbb{N} \to [0, \infty)$ tal que para toda función polinómica positiva $p \in \mathbb{R}[n]$ existe un n_0 tal que*

$$\forall n > n_0 : \ f(n) < \frac{1}{p(n)}$$

De este modo, se puede hacer uso de la notación de complejidad para medir los recursos de cualquier adversario. Es importante mencionar que cualquier esquema de cifrado práctico requiere emplear algoritmos que se ejecuten en tiempo polinómico. Así, la teoría de la complejidad es una manera de estudiar los esquemas de cifrado para su implementación real.

Se retomarán las funciones negligibles durante el siguiente capítulo. Por el momento, enunciamos lo siguiente: 2^{-n}, $2^{-\sqrt{n}}$ y $n^{-\log n}$ son ejemplos de funciones negligibles y la combinación lineal de funciones negligibles sigue siendo negligible.

5.3.2. Ataque de recuperación de llave

Uno de los ataques más simples es la recuperación de la clave en un esquema de cifrado. Como estudiamos en el capítulo de cifradores por bloques, la recuperación de clave es un experimento básico, pero no es suficiente garantía para la seguridad de un esquema simétrico.

Ahora, empleando el enfoque asintótico, se definirá un experimento más general (por lo tanto más fuerte) para estudiar la seguridad de un esquema contra cualquier adversario. Es oportuno señalar, que podemos clasificar la seguridad de este experimento como condicional o incondicional.

Un experimento (prueba) de **seguridad condicional** toma en cuenta los recursos computacionales de un adversario, por ejemplo: tiempo de ejecución t, memoria de almacenamiento ϑ, cantidad de consultas q de una subrutina y la longitud ℓ de las cadenas de bits empleadas en cada consulta.

La **seguridad incondicional**, por el contrario, asume adversarios con capacidad de computación ilimitada. Este tipo de pruebas no busca delimitar los recursos computacionales que posee un adversario, sino cuantificar sus recursos informáticos, principalmente la cantidad de consultas q que requiere de un oráculo. Debido a que un adversario con infinita capacidad de cómputo es más peligroso, concentraremos nuestros esfuerzos únicamente en la seguridad incondicional.

Definición 5.3.2. *Sea $F : K \times X \to Y$ una familia de funciones y sea $\mathcal{B}$ un adversario que interactúa con un oráculo $\hat{F} : X \to Y$ hasta adivinar una clave k' secreta. Entonces, considere el siguiente experimento:*

EXPERIMENTO $\mathbf{Exp}^{\text{KR}}(\mathcal{B}, F)$:
  $k \xleftarrow{\$} K$
  $k' \leftarrow \mathcal{B}^{F_k}$
  si $k = k'$ **entonces regresa** 1
  si no regresa 0

Algoritmo 5.3.1: Experimento de recuperación de clave secreta

La ventaja del adversario $\mathcal{B}$ para la recuperación de la clave secreta es

$$\mathbf{Adv}_F^{\text{KR}}(\mathcal{B}) := \Pr\left[\,\mathbf{Exp}^{\text{KR}}(\mathcal{B}, F) = 1\,\right]$$

Esta definición es lo suficientemente general como para considerar todo tipo de ataque. Cualquiera de los ataques clásicos contra esquemas como búsqueda exhaustiva, criptoanálisis diferencial, criptoanálisis lineal y cualquier método heurístico, corresponden a estrategias específicas que selecciona el adversario $\mathcal{B}$. En general, el adversario puede considerar cualquier algoritmo de búsqueda para encontrar la clave secreta k y emplear muestras del comportamiento de la instancia F_k.

Además, este experimento logra capturar de manera parcial el concepto de seguridad perfecta. Un adversario con probabilidad negligible de éxito, en este experimento, garantiza seguridad perfecta si y sólo si la distribución de la familia de funciones F está uniformemente distribuida. Debido a que el enfoque asintótico no garantiza uniformidad, no se puede concluir nada más al respecto.

Por el contrario, un esquema perfectamente seguro puede ser roto si un adversario consigue las suficientes muestras de entrada-salida como para deducir unicamente una clave posible.

Debido a la naturaleza del esquema *One-time-pad* (Algoritmo 5.2.1), es trivial deducir la clave correcta a partir de un mensaje y su correspondiente texto cifrado. Como se menciona en el segundo capítulo, se requieren sólo dos muestras para garantizar la recuperación de la clave secreta en el AES y el DES.

Para entender mejor el experimento de recuperación de clave, consideremos el siguiente ejemplo:

Ejemplo 5.3.1. Sea $F : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^m$ una función indexada tal que $k = m \cdot n$ y considere una clave $\mathbf{K}$ de k-bits que forma una matriz de m renglones por n columnas. Sea $\mathbf{X} = \mathbf{x}_1 \cdots \mathbf{x}_m$ una secuencia de n-bits de entrada, y defina $F(\mathbf{K}, \mathbf{X})$:

$$F_{\mathbf{K}}(\mathbf{X}) = \begin{pmatrix} \mathbf{k}_{11} & \mathbf{k}_{12} & \dots & \mathbf{k}_{1n} \\ \mathbf{k}_{21} & \mathbf{k}_{22} & \dots & \mathbf{k}_{2n} \\ \vdots & & \ddots & \vdots \\ \mathbf{k}_{m1} & \mathbf{k}_{m2} & \dots & \mathbf{k}_{mn} \end{pmatrix} \cdot \begin{pmatrix} \mathbf{x}_1 \\ \mathbf{x}_2 \\ \vdots \\ \mathbf{x}_n \end{pmatrix} = \begin{pmatrix} \mathbf{y}_1 \\ \mathbf{y}_2 \\ \vdots \\ \mathbf{y}_m \end{pmatrix}$$

es decir,

$$\begin{array}{rcccccc} \mathbf{y}_1 & = & \mathbf{k}_{11} \cdot \mathbf{x}_1 & \oplus & \mathbf{k}_{12} \cdot \mathbf{x}_2 & \oplus \cdots \oplus & \mathbf{k}_{1m} \cdot \mathbf{x}_n \\ \mathbf{y}_2 & = & \mathbf{k}_{21} \cdot \mathbf{x}_1 & \oplus & \mathbf{k}_{22} \cdot \mathbf{x}_2 & \oplus \cdots \oplus & \mathbf{k}_{2n} \cdot \mathbf{x}_n \\ \vdots & & & \vdots & & \ddots & \\ \mathbf{y}_m & = & \mathbf{k}_{m1} \cdot \mathbf{x}_1 & \oplus & \mathbf{k}_{m2} \cdot \mathbf{x}_2 & \oplus \cdots \oplus & \mathbf{k}_{mn} \cdot \mathbf{x}_n \end{array}$$

Donde la clave $\mathbf{K}$ es el conjunto de todos los bits k_{ij} en la matriz y la aritmética de la operación se realiza módulo dos.

Sea $\mathcal{B}$ un adversario que ejecuta el siguiente ataque para recuperar la clave:

ALGORITMO $\mathcal{B}(\ F\ )$:
- $\mathbf{K} \leftarrow \varepsilon$
- **para cada** $i \in \mathfrak{I}_n$ **haz**
  - $\mathbf{X} \leftarrow 0^n,\ \mathbf{X}|_i \leftarrow 1$
  - $\mathbf{Y} \leftarrow F(\mathbf{X})$
  - $\hat{\mathbf{K}} \leftarrow [\![\hat{\mathbf{K}}\mathbf{Y}]\!]$
- **regresa** $\hat{\mathbf{K}}$

Al inicio del algoritmo, K es una cadena vacía. En este ataque, el adversario $\mathcal{B}$ genera una cadena $\mathbf{X}$ y la inicializa en ceros, excepto en la i-ésima posición en donde se la asigna $\mathbf{X}|_i = 1$. De esta manera, con cada iteración se obtiene una columna de la matriz $\mathbf{K}$ al consultar la imagen $F(\mathbf{X})$. Note cómo

$$F(0^{i-1} \,[\![\, 1 \,[\![\, 0^{n-i+2}) = \mathbf{k}_{1i} \,[\![\, \mathbf{k}_{2i} \,[\![\dots [\![\, \mathbf{k}_{mi}$$

Este ejemplo puede parecer trivial, sin embargo, no lo es. Es importante resaltar que la vulnerabilidad de F radica en su fuerte linealidad. Cualquier cifrado homomórfico es vulnerable a

este ataque, puesto que sus operaciones conservan un núcleo invariante (en este caso 0^n). Así, el adversario recupera la clave secreta con probabilidad de éxito.

$$\Pr\left[\,\mathbf{Exp}^{\text{KR}}(\mathcal{B}, F) = 1\,\right] = 1$$

No obstante, advierta que este algoritmo requiere al menos de n consultas al oráculo F. Esto significa que conforme el tamaño de la clave aumenta, la complejidad de encontrar la clave se torna lineal $O(q)$ con la cantidad de consultas q.

5.4. Privacidad

Suponga que se tiene un equipo conformado por un par de emisor y receptor. Ambos miembros son honestos y ejecutan un esquema de cifrado simétrico, de tal manera que ellos conocen una clave secreta tomada al azar. El adversario no conoce la clave secreta que selecciona el equipo, pero puede ver cualquier mensaje enviado entre ellos, ¿Cómo puede el adversario aprovecharse de esto?

Por ejemplo, es evidente que el adversario con suficientes pares de mensaje-cifrado, puede adivinar la clave secreta y descifrar cualquier otro texto cifrado futuro que se mande. Sin embargo, ¿existe alguna otra manera en que el adversario podría beneficiarse? De hecho, sí.

Supongamos que el equipo emisor-receptor decide ingenuamente usar un formato fijo, en donde el último bit corresponde con un voto a la opción 0 o a la opción 1. Luego, empleando el esquema *One-time-pad* empiezan a mandar sus respectivos votos cifrados. En este caso, nuestro adversario podría obtener información parcial del mensaje y violar el derecho al voto anónimo del equipo con alta probabilidad.

El problema aquí no es culpa realmente del equipo, puesto que un esquema criptográfico debe proteger la información del equipo independientemente del formato que elijan. Debido a que un único bit sólo puede ser adivinado con $1/2$ de probabilidad, tampoco es problema del Esquema 5.2.1, ya que éste es el máximo nivel de seguridad para un bit.

Como se ha mencionado varias en ocasiones, podríamos empezar a enlistar requerimientos como mezclar los bits del cifrado antes de ser enviado, usar máquinas de estados para variar los valores de cada bit, y demás propuestas, pero esto nunca es suficiente. La seguridad contra la recuperación de la clave e incluso la seguridad perfecta es una forma específica de lo que en criptografía se denomina seguridad semántica.

5.4.1. Seguridad Semántica

El concepto de privacidad, formalmente definido como seguridad semántica. La idea de Goldwasser y Micali (1984) mezcla la intuición de la seguridad perfecta con el enfoque asintótico. Originalmente, este enfoque fue introducido para la seguridad de esquemas asimétricos o de llave pública. Estas pruebas consisten en un análisis de seguridad condicional en donde se consideran adversarios con recursos computacionales finitos.

El experimento consiste en un adversario que escoge de manera iterativa una secuencia $M_1, M_2, \ldots, M_q$ de espacios de mensajes y al mismo tiempo se selecciona al azar una clave secreta $k \xleftarrow{\$} K$. Para cada espacio de mensajes M_i seleccionado por el adversario, se toman dos elementos al azar $\mathbf{X}_i, \mathbf{X}'_i \xleftarrow{\$} M_i$. Luego, existen dos casos posibles:

- **Mensaje Izquierdo:** Se le devuelve al adversario el texto cifrado $\mathbf{Y}_i$ correspondiente a $\mathbf{X}_i$.
- **Mensaje Derecho:** Se le devuelve al adversario el texto cifrado $\mathbf{Y}_i$ correspondiente a $\mathbf{X}'_i$.

El adversario desconoce cuál de los dos mensajes generó $\mathbf{Y}_i$. No obstante, puede seleccionar de manera cuidadosa un nuevo espacio M_{i+1} cada vez que obtiene un cifrado. Una vez que el adversario termina de analizar las muestras $(\mathbf{Y}_1, \ldots, \mathbf{Y}_q)$ toma una decisión de la siguiente manera: primero, el adversario selecciona un elemento $\mathbf{Z} \in \mathrm{C}_\Sigma$; luego, crea un sistema determinista $\mathbb{F}$ funcionalmente compatible con las muestras obtenidas, y por último, devuelve 1 si $\mathbb{F}(\mathbf{X}_1, \ldots, \mathbf{X}_q) = \mathbf{Z}$, de lo contrario, 0. Formalmente,

Definición 5.4.1. *Sea $\Sigma = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un esquema de cifrado y deje que $\mathcal{A}$ sea un adversario con acceso a un oráculo. Se considera el experimento:*

EXPERIMENTO $\mathbf{Exp}^{\text{SEC-L}}(\Sigma, \mathcal{A})$:
- $k \xleftarrow{\$} K,\ S \leftarrow \varnothing$
- **para cada** $i \in \mathfrak{I}_q$ **haz**
  - $(M_i, S) \leftarrow \mathcal{A}(S)$
  - $\mathbf{X}_i,\ \mathbf{X}'_i \xleftarrow{\$} M_i$
  - **si** $|\mathbf{X}_i| \neq |\mathbf{X}'_i|$ **entonces**
    - **regresa** $\mathbf{X}_i \leftarrow \mathbf{X}'_i \leftarrow \varepsilon$
  - $\mathbf{Y}_i \leftarrow \mathcal{E}_k(\mathbf{X}_i)$
  - $S \leftarrow S \cup \mathbf{Y}_i$
- $(\mathbb{F}, \mathbf{Z}) \leftarrow \mathcal{A}(S)$
- **regresa** $\mathbb{F}(\mathbf{X}_1, \ldots, \mathbf{X}_q) = \mathbf{Z}$

EXPERIMENTO $\mathbf{Exp}^{\text{SEC-R}}(\Sigma, \mathcal{A})$:
- $k \xleftarrow{\$} K,\ S \leftarrow \varnothing$
- **para cada** $i \in \mathfrak{I}_q$ **haz**
  - $(M_i, S) \leftarrow \mathcal{A}(S)$
  - $\mathbf{X}_i,\ \mathbf{X}'_i \xleftarrow{\$} M_i$
  - **si** $|\mathbf{X}_i| \neq |\mathbf{X}'_i|$ **entonces**
    - **regresa** $\mathbf{X}_i \leftarrow \mathbf{X}'_i \leftarrow \varepsilon$
  - $\mathbf{Y}_i \leftarrow \mathcal{E}_k(\mathbf{X}'_i)$
  - $S \leftarrow S \cup \mathbf{Y}_i$
- $(\mathbb{F}, \mathbf{Z}) \leftarrow \mathcal{A}(S)$
- **regresa** $\mathbb{F}(\mathbf{X}'_1, \ldots, \mathbf{X}'_q) = \mathbf{Z}$

Algoritmo 5.4.1: Experimento de seguridad semántica: Mensaje Izquierdo y Mensaje Derecho

*La **seguridad semántica** de Σ (la ventaja de $\mathcal{A} \in CPA$) se define*

$$\mathbf{Sec}^{\text{CPA}}_{\Sigma}(\mathcal{A}) := \Pr\left[\mathbf{Exp}^{\text{SEC-R}}_{\Sigma}(\mathcal{A}) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}^{\text{SEC-L}}_{\Sigma}(\mathcal{A}) \Rightarrow 1\right]$$

Como es habitual en estos experimentos, el primer algoritmo inicia el esquema al seleccionar una clave al azar del espacio de claves K_Σ y un espacio de estados S inicialmente vacío. Enseguida, se realiza un proceso iterativo para las q consultas. Observe cómo en cada iteración

se verifica que el tamaño de las cadenas $\mathbf{X}_i$ y $\mathbf{X}'_i$ sean iguales, de lo contrario, se borran las cadenas y las líneas consecutivas prácticamente no se ejecutan; mientras tanto, el estado S se actualiza en cada iteración. Así, podemos percatarnos de cómo este adversario es necesariamente adaptativo.

Al finalizar la iteración, el adversario calcula $\mathbb{F}$ y verifica que se cumpla la igualdad. El objetivo del adversario es seleccionar $\mathbf{Z}$ y $\mathbb{F}$ de tal manera que pueda diferenciar los mensajes izquierdos de los mensajes derechos. Advierta cómo este experimento es mucho más fácil de ganar para un adversario que el Experimento 5.3.1.

Es importante mencionar, que la seguridad semántica describe una noción de seguridad mucho más fuerte en términos computacionales. En este experimento, el adversario no requiere obtener información específica del esquema, sino que puede emplear cualquier tipo de información parcial a su conveniencia. De hecho, le otorgamos al adversario la habilidad de consultar adaptativamente los mensajes que crea conveniente y de diseñar el mejor modelo para predecir el texto cifrado que desee.

Las limitaciones de seguridad del esquema dependen de la capacidad de cómputo que se considere. Por ejemplo, el espacio de almacenamiento para todas la muestras obtenidas puede ser muy costoso, así como el tiempo de ejecución que se requiere para encontrar el modelo de predicción. Esta definición de seguridad es muy empleada en esquemas de llave pública que consideran problemas difíciles como la factorización de primos o la inversión del algoritmo discreto. Aun así, nuestra meta es alcanzar un nivel de seguridad incondicional para garantizar una seguridad casi perfecta en nuestros esquemas simétricos.

5.4.2. Experimento de Indistinguibilidad

Nuestro objetivo en esta sección es definir un experimento que garantice seguridad en un sentido tan fuerte como la seguridad semántica y que a su vez considere un adversario con capacidad de cómputo ilimitada como en el enfoque de seguridad incondicional. La propiedad fundamental que emplea este enfoque es conocido como indistinguibilidad.

La idea detrás de este experimento consiste en poner a prueba a un adversario, que no posee la clave secreta, a superar un desafío. Éste consiste en la selección de dos mensajes distintos de la misma longitud. Luego, a través de un oráculo, la obtención de un texto cifrado dependiendo de cada mundo:

- **Mundo 0:** El comportamiento del oráculo izquierdo es $\mathcal{E}_k\left(LR(*,*,0)\right)$. Siempre que el adversario haga una consulta (x_0, x_1), el oráculo calcula $y = \mathcal{E}_k(x_0)$, y devuelve y como la respuesta.

- **Mundo 1:** El comportamiento del oráculo derecho es $\mathcal{E}_k\left(LR(*,*,1)\right)$. Siempre que el adversario haga una consulta (x_0, x_1), el oráculo calcula $y \xleftarrow{\$} \mathcal{E}_k(x_1)$, y devuelve y como la respuesta.

El adversario consulta hasta q veces al oráculo, antes de tomar una decisión. El objetivo del oráculo es bastante simple, solamente tiene que adivinar en cuál de los dos mundos está, *i.e.*, tiene que decidir cuál de los dos mensajes fue cifrado: el derecho o el izquierdo. Antes de formalizar el experimento es necesario definir el oráculo con el que se interactúa.

Definición 5.4.2. *Sea un esquema de cifrado Σ, $\mathfrak{b} \in \{0,1\}$ un bit y deje que $x_0, x_1 \in M$ sean mensajes distintos. Entonces, se define el oráculo* ***Izquierdo-Derecho*** *como un sistema funcionalmente compatible con $LR : \mathrm{M}_\Sigma \times \mathrm{M}_\Sigma \times \{0,1\} \to M$ tal que*

$$LR(x_0, x_1, \mathfrak{b}) := \begin{cases} x_0 & \Leftarrow \ \mathfrak{b} = 0 \\ x_1 & \Leftarrow \ \mathfrak{b} = 1 \end{cases}$$

También llamamos al mundo (oráculo) "izquierdo", el mundo (oráculo) 0. Mientras que al mundo (oráculo) "derecho", lo denominamos el mundo (oráculo) 1. El problema para el adversario es interrogar a su oráculo de la manera más eficiente, para que de esta manera pueda decidir con cuál de los dos oráculos interactúa. Esto es análogo a la prueba de Turing, en donde una persona se encuentra interrogado a dos participantes (una persona y una máquina que finge ser una persona) sin conocimiento previo de quién es la persona y cuál es la máquina. Formalmente,

Definición 5.4.3. *Sea $\Sigma = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un esquema de cifrado simétrico y sea $\mathcal{A}$ sea un distinguidor con acceso a un oráculo. Considere el siguiente experimento:*

EXPERIMENTO $\mathbf{Exp}^{\text{CPA-0}}(\Sigma, \mathcal{A})$:
- $k \xleftarrow{\$} K$
- $\mathfrak{b} \leftarrow \mathcal{A}^{\mathcal{E}_k(LR(*,*,0))}$
- **regresa** $\mathfrak{b}$

EXPERIMENTO $\mathbf{Exp}^{\text{CPA-1}}(\Sigma, \mathcal{A})$:
- $k \xleftarrow{\$} K$
- $\mathfrak{b} \leftarrow \mathcal{A}^{\mathcal{E}_k(LR(*,*,1))}$
- **regresa** $\mathfrak{b}$

Algoritmo 5.4.2: Experimento de indistinguibilidad: Mensaje Izquierdo y Derecho

Por lo tanto, la indistinguibilidad del esquema Σ se define como

$$\mathbf{Ind}^{\text{CPA}}_\Sigma(\mathcal{A}) := \Pr\left[\mathbf{Exp}^{\text{CPA-1}}_\Sigma(\mathcal{A}) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}^{\text{CPA-0}}_\Sigma(\mathcal{A}) \Rightarrow 1\right]$$

Observe que este experimento es bastante general, así como lo deseamos. Debido a que nuestro adversario tiene acceso a un oráculo para interactuar con distintos textos cifrados, producidos por el sistema, se permite ignorar el costo computacional de cada respuesta del oráculo y el enfoque es únicamente en la información obtenida por cada consulta. De hecho, se puede reducir el experimento con el siguiente algoritmo equivalente:

Teorema 5.4.4. *Sea $\Sigma = (\mathcal{K}, \mathcal{E}, \mathcal{D})$ un esquema de cifrado simétrico y deje que $\mathcal{A}$ sea un distinguidor con acceso a un oráculo. Considere el siguiente experimento:*

EXPERIMENTO $\mathbf{Exp}^{\text{CPA-LR}}(\Sigma, \mathcal{A})$:
$k \xleftarrow{\$} K$, $\flat \xleftarrow{\$} \{0,1\}$
$\hat{\flat} \leftarrow \mathcal{A}^{\mathcal{E}_k(LR(*,*,\flat))}$
regresa $\flat = \hat{\flat}$

Algoritmo 5.4.3: Experimento de indistinguibilidad Izquierda-Derecha

Por lo tanto, la ventaja del distinguidor $\mathcal{A} \in CPA$ se resume en

$$\mathbf{Adv}^{\text{LR}}_{\Sigma} := 2 \cdot \Pr[\mathbf{Exp}^{\text{LR}}_{\Sigma}(\mathcal{A}) \Rightarrow 1] - 1$$

Demostración. Resolviendo, se tienen las siguientes desigualdades:

$$\begin{aligned}
\Pr[\mathbf{Exp}^{\text{LR}}_{\Sigma}(\mathcal{A}) \Rightarrow 1] &= \Pr\left[\flat = \hat{\flat}\right] \\
&= \Pr\left[\flat = \hat{\flat} \mid \flat = 1\right] \Pr[\flat = 1] + \Pr\left[\flat = \hat{\flat} \mid \flat = 0\right] \Pr[\flat = 0] \\
&= \Pr\left[\flat = \hat{\flat} \mid \flat = 1\right] \cdot \frac{1}{2} + \Pr\left[\flat = \hat{\flat} \mid \flat = 0\right] \cdot \frac{1}{2} \\
&= \Pr\left[\hat{\flat} = 1 \mid \flat = 1\right] \cdot \frac{1}{2} + \Pr\left[\hat{\flat} = 0 \mid \flat = 0\right] \cdot \frac{1}{2} \\
&= \frac{1}{2} \cdot \Pr\left[\hat{\flat} = 1 \mid \flat = 1\right] + \frac{1}{2} \cdot \left(1 - \Pr\left[\hat{\flat} = 1 \mid \flat = 0\right]\right) \\
&= \frac{1}{2} \cdot \Pr\left[\hat{\flat} = 1 \mid \flat = 1\right] + \frac{1}{2} - \frac{1}{2} \cdot \Pr\left[\hat{\flat} = 1 \mid \flat = 0\right] \\
&= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr\left[\hat{\flat} = 1 \mid \flat = 1\right] - \Pr\left[\hat{\flat} = 1 \mid \flat = 0\right]\right) \\
&= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr\left[\mathbf{Exp}^{\text{CPA-1}}_{\Sigma}\phi = 1\right] - \Pr\left[\mathbf{Exp}^{\text{CPA-0}}_{\Sigma}\phi = 1\right]\right) \\
&= \frac{1}{2} + \frac{1}{2} \cdot \left(\Pr\left[\mathbf{Exp}^{\text{CPA-1}}_{\Sigma}(\mathcal{A}) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}^{\text{CPA-0}}_{\Sigma}(\mathcal{A}) \Rightarrow 1\right]\right)
\end{aligned}$$

Aprecie cómo para un $\flat = 0$ fijo, la probabilidad se calcula sobre los mensajes izquierdos, mientras que para $\flat = 1$, la probabilidad se calcula sobre los mensajes derechos.

$$\therefore \quad \Pr[\mathbf{Exp}^{\text{LR}}_{\Sigma}(\mathcal{A}) \Rightarrow 1] = \frac{1}{2} + \frac{1}{2} \cdot \mathbf{Adv}^{\text{LR}}_{\Sigma}(\mathcal{A})$$

□

Esta conclusión no es difícil de seguir, puesto que al considerar adversarios bajo la teoría de la información, podríamos considerar una estrategia trivial en donde el adversario simplemente adivina el mundo de manera aleatoria, sin ni siquiera realizar una consulta al oráculo. Esta estrategia trivial, en promedio, tendría éxito el 50 % de las veces. De esta manera, el Teorema 5.4.4 es un algoritmo reducido del experimento anterior.

5.4.3. Indistinguibilidad implica Seguridad Semántica

Por último, para garantizar que la propiedad de indistinguibilidad Izquierda-Derecha sea la definición de seguridad que se busca, se necesita saber si es lo suficientemente general como la seguridad semántica.

Teorema 5.4.5. *Sea Σ un esquema simétrico y $\mathcal{A}$ un adversario bajo el experimento de seguridad semántica. Entonces, existe un distinguidor $\mathcal{B}$ bajo el experimento de indistinguibilidad Izquierda-Derecha, tal que*

$$\mathbf{Adv}^{\text{LR}}_{\Sigma}(\mathcal{B}) \geq \mathbf{Sec}^{\text{CPA}}_{\Sigma}(\mathcal{A})$$

Demostración. Considere un distinguidor $\mathcal{B}$ bajo el experimento de indistinguibilidad Izquierda-Derecha, cuya estrategia es

ALGORITMO $\mathcal{B}^{\Theta}(\,\Sigma\,)$:
- $S \leftarrow \varnothing$
- **para cada** $i \in \mathfrak{I}_q$ **haz**
  - $(M_i, S) \leftarrow \mathcal{A}(S)$
  - $\mathbf{X}_i,\, \mathbf{X}'_i \xleftarrow{\$} M_i$
  - **si** $|\,\mathbf{X}_i\,| \neq |\,\mathbf{X}'_i\,|$ **entonces**
    - **regresa** $\mathbf{X}_i \leftarrow \mathbf{X}'_i \leftarrow \varepsilon$
  - $\mathbf{Y}_i \leftarrow \Theta(\mathbf{X}'_i, \mathbf{X}_i)$
  - $S \leftarrow S \cup \mathbf{Y}_i$
- $(\mathbb{F}, \mathbf{Z}) \leftarrow \mathcal{A}(S)$
- **regresa** $\mathbb{F}(\mathbf{X}_1, \mathbf{X}_2, \ldots, \mathbf{X}_q) = \mathbf{Z}$

Algoritmo 5.4.4: Indistinguibilidad contra seguridad semántica

Suponga que $\mathcal{B}$ consulta al oráculo izquierdo. Entonces, $\mathcal{E}_k(LR(\mathbf{X}_i, \mathbf{X}'_i, 0)) = \mathcal{E}_k(\mathbf{X}_i) = \mathbf{Y}$. Por lo tanto, el Mundo 0 del Experimento 5.4.3 es igual al Mensaje Izquierdo del Experimento 5.4.1. Luego, para un adversario $\mathcal{A}$ en el experimento de seguridad semántica, se deduce que

$$\Pr\left[\,\mathbf{Exp}^{\text{CPA-0}}_{\Sigma}(\mathcal{B}) \;\Rightarrow\; 1\,\right] = \Pr\left[\,\mathbf{Exp}^{\text{SEC-L}}_{\Sigma}(\mathcal{A}) \;\Rightarrow\; 1\,\right]$$

Ahora deje que $\mathcal{B}$ consulte al oráculo derecho. Entonces $\mathcal{E}_k(LR(\mathbf{X}_i, \mathbf{X}'_i, 1)) = \mathcal{E}_k(\mathbf{X}'_i) = \mathbf{Y}$. De este modo, el Mundo 1 es igual al Mensaje Derecho del Experimento 5.4.1. Así,

$$\Pr\left[\,\mathbf{Exp}^{\text{CPA-1}}_{\Sigma}(\mathcal{B}) \;\Rightarrow\; 1\,\right] = \Pr\left[\,\mathbf{Exp}^{\text{SEC-R}}_{\Sigma}(\mathcal{A}) \;\Rightarrow\; 1\,\right]$$

Ya que el experimento de indistinguibilidad Izquierda-Derecha considera adversarios con infinita capacidad de cómputo, se concluye que $\mathcal{B}$ tiene mayor ventaja que $\mathcal{A}$.

□

Esto comprueba que la indistinguibilidad de un esquema es la condición de suficiencia que buscamos para estudiar la seguridad de los esquemas simétricos o de llave privada. Cabe mencionar, que podríamos considerar adversarios $\mathcal{A} \in CCA$ al considerar un oráculo que nos permita acceder tanto al cifrado $\mathcal{E}_k$ como al descifrado $\mathcal{D}_k$ mediante una representación unidireccional, recuerde la Definición 3.3.6. No obstante, aunque el análisis no es muy complejo, esto se sale de los alcances de la tesis referente a los MAC.

Capítulo 6

Códigos de autenticación de mensajes

Uno de los objetivos básicos en criptografía es permitir a dos entidades (emisor y receptor) comunicarse de forma segura utilizando un canal abierto. La privacidad es una meta muy importante en la criptografía, pero la autenticación de mensajes es incluso más importante. De este modo, es de suma importancia asegurar la integridad y autenticidad de un mensaje a través de un canal inseguro, de tal manera que cada entidad pueda validar que el mensaje ha sido enviado por la entidad que afirma haberlo hecho, además de verificar que el mensaje recibido no ha sido modificado.

Un código de autenticación de mensajes (MAC por sus siglas en inglés) es la versión de clave secreta de la firma digital. Un MAC puede ser visto como una función que comprime la información de un mensaje y genera una firma asociada a una clave secreta. Formalmente,

Definición 6.0.1. *Un MAC* $H : \{0,1\}^k \times \{0,1\}^* \longrightarrow \{0,1\}^n$ *es una función indexada por un espacio de llaves* $\{0,1\}^k$*, un espacio de mensajes* $\{0,1\}^*$ *de tamaño arbitrario y un espacio de firmas* $\{0,1\}^n$*. Cada instancia* $\mathcal{H}_k$ *de un código de autenticación de mensajes es una función de compresión que toma un* mensaje M *de tamaño arbitrario y (usualmente) genera una* firma T *de tamaño fijo.*

En la literatura, se suele hablar de un MAC no solamente como una función, sino además como la firma o el código generado por el MAC. En general, hablaremos de un MAC para cualquiera de estos casos, a excepción de que el contexto lo especifique.

La mayoría de los MAC se construyen a partir de una función *HASH*, la cual comprime el mensaje dividiéndolo en bloques y realizando operaciones entre ellos, usualmente operaciones XOR como PMAC (Yasuda, 2011). Los MAC pueden ser deterministas, con estado, aleatorizados, *pipelineables* (CBC-MAC y OMAC), entre otros (Bellare & Rogaway, 2005; Bellare et al., 1999; Iwata & Kurosawa, 2003).

Ineludiblemente, obtener aleatoriedad criptográficamente segura es muy costoso para varios escenarios. Por lo tanto, se suelen utilizar construcciones sin estado y basadas en *nonce*, donde el remitente es responsable de proporcionar un *nonce* único para cada mensaje a autenticar (Moch & List, 2019).

Antiguamente, los mensajes eran enviados en cartas o rollos de papiro sellados con cera, lacre o incluso tinta invisible, formando una figura o firma que permitiera identificar al remitente. Este sello protegía el mensaje de ser visto por terceros, ya que algún intruso que deseara ver su contenido tendría que romper el sello. Si el sello llega intacto, el receptor puede estar seguro de la integridad del mensaje y de la privacidad de la comunicación. A continuación, se describe el protocolo de autenticación moderno.

Definición 6.0.2. *Un esquema de autenticación Λ es una tripleta $(\mathcal{K}, \mathcal{H}, \mathcal{V})$ que consta de tres algoritmos eficientes:*

1. ***Generación de claves aleatorias*** : *el algoritmo $\mathcal{K}$ genera una clave secreta tomada al azar $k \xleftarrow{\$} K$.*

2. ***Algoritmo MAC***: *dado un mensaje $m \in M$ y una clave secreta k, el algoritmo $\mathcal{H}$ comprime el mensaje y genera una firma $t \leftarrow \mathcal{H}_k(m)$. Si el mensaje no puede ser procesado por el MAC, el algoritmo entrega un error de generación $\perp \leftarrow H$.*

3. ***Verificación determinista***: *dada una firma $t \in T$ y una clave secreta k, el algoritmo $\mathcal{V}$ entrega de manera determinista un bit. Se dice que el MAC ha sido autenticado si $\mathcal{V}_k(m, t) = 1$ y es rechazado en cualquier otro caso.*

De la definición anterior, se observa que un esquema de autenticación es similar a un esquema de cifrado simétrico. La función de validación tiene que ser determinista, mientras que la función MAC puede no serlo. Análogamente, se denota K_Λ como el espacio de claves del esquema, M_Λ como el espacio de mensaje y T_Λ como el espacio de firmas. Así mismo, un esquema de autenticación también se construye con base en primitivas criptográficas: cifradores por bloques, permutaciones públicas, funciones digesto (*HASH*) y cifradores por bloques entonables.

En los esquemas asimétricos basta con demostrar por reducción que falsificar la firma es tan difícil como romper la primitiva criptográfica del sistema. No obstante, cabe hacerse la pregunta, ¿existe una manera de falsificar esta firma sin necesidad de romper la primitiva? En el caso de los esquemas simétricos, la respuesta es clara, pero para entenderla es necesario explicar en primer lugar el significado de seguridad para un MAC.

6.1. Seguridad para MAC

En el capítulo anterior, se mencionó la definición de seguridad y cómo ésta garantiza la privacidad de las comunicaciones al no exponer nada de información parcial del esquema. No obstante, el objetivo de un MAC no es garantizar la privacidad de la comunicación *per se*, sino permitir autenticar los mensajes emitidos por un remitente. Para entender mejor la relación de seguridad entre las firmas MAC y la privacidad, empezaremos explicando el experimento de falsificación.

En este experimento, el objetivo del adversario es falsificar la firma MAC del emisor, pero la firma depende del mensaje enviado, el algoritmo MAC y la clave secreta. Para demostrar la seguridad de un esquema de autenticación, se asume que el mensaje está bajo control del adversario. Además el adversario conoce el algoritmo MAC, y peor aún, tiene acceso a un oráculo que permite interactuar con el MAC para obtener ejemplos de pares mensaje-firma.

Un adversario puede proponer mensajes falsos y consultar a su oráculo para obtener su firma respectiva. Si la respuesta del oráculo es una firma distinta a la firma original, el adversario propone un nuevo mensaje falso y vuelve a consultar al oráculo. Este proceso se repite hasta que el adversario logre encontrar una firma igual a la original. De esta manera, el receptor no puede distinguir el mensaje falso del real. Formalmente, definimos la seguridad como sigue:

Definición 6.1.1. *Sea un esquema de autenticación $\Lambda = (\mathcal{K}, \mathcal{H}, \mathcal{V})$ y sea $\mathcal{A}$ un adversario con acceso a un oráculo $\mathbb{O}$. Considere el siguiente experimento:*

EXPERIMENTO $\mathbf{Exp}^{\text{FORGE}}(\Lambda, \mathcal{A})$:
- $k \xleftarrow{\$} K,\ S \leftarrow \varnothing$
- **para cada** $i \in \mathfrak{I}_q$ **haz**
  - $(m_i, t_i) \leftarrow \mathcal{A}(S)$
  - $S \leftarrow S \cup (m_i, t_i)$
- $(m', t') \leftarrow \mathcal{A}(S)$
- **si** $(m', t') \notin S$ **entonces regresa** $\mathcal{V}_k(m', t') = 1$
- **si no regresa** 0

Algoritmo 6.1.1: Experimento de falsificación

La seguridad del esquema Λ se define como

$$\mathbf{Forge}^{\text{CPA}}_{\Lambda}(\mathcal{A}) = \Pr\left[\mathbf{Exp}^{\text{FORGE}}_{\Lambda}(\mathcal{A}) \Rightarrow 1\right]$$

En este experimento, se permite que un adversario consulte a un oráculo $\mathcal{H}_k$ para probar cualquier par de mensajes (m, t) hasta que el distinguidor $\mathcal{A}^{\mathcal{H}_k}$ devuelva 1. Cada mensaje consultado se guarda en un estado S que es retroalimentado al adversario para proponer nuevos mensajes.

Se dice que el MAC ha sido roto, si el adversario encuentra un par (m', t') tal que $\mathcal{V}_k(M', t') = 1$. Formalmente, pedimos que el par (m', t') no pertenezca al conjunto de mensajes consultados S, esto para evitar victorias triviales para el adversario. Fíjese cómo esta definición es lo suficientemente general para incluir cualquier ataque que involucre encontrar una imagen $F_k(m') = t'$.

En primer lugar, se le permite al adversario consultar mensaje de cualquier longitud. Esto no es trivial, puesto que un MAC que no genera una firma dependiente del tamaño del mensaje, se considera insegura.

En segundo lugar, el adversario no está obligado a consultar mensajes M' coherentes con ningún lenguaje, por lo que es más fácil encontrar falsificaciones en este experimento que en el uso práctico de un MAC.

Definición 6.1.2. *Dado un esquema de autenticación $\Lambda = (K, H, V)$. Se dice que un MAC H es **infalsificable** (o simplemente seguro), si la ventaja para cualquier adversario $\mathcal{A} \in CPA$ es negligible.*

$$\mathbf{Adv}_{H}^{\text{FORGE}}(\mathcal{A}) := \mathbf{Forge}_{\Lambda}^{\text{CPA}}(\mathcal{A}) \leq \epsilon(q)$$

Gracias al Experimento 6.1.1, se entiende la estrecha relación entre un esquema de autenticación y su correspondiente MAC. Esto es importante, debido a que no podemos hablar de la seguridad de H sin tomar en cuenta su algoritmo V correspondiente. Note cómo esta definición de seguridad es muy distinta a la indistinguibilidad Izquierda-Derecha que se escribió al final del capítulo anterior.

Para poder garantizar la seguridad de un MAC para todo uso práctico, no es suficiente con asegurar que cada firma sea indistinguible entre sí. Dado que un MAC puede tener un dominio mucho mayor que su rango, debemos considerar la facilidad con que se pueden encontrar firmas iguales para mensajes distintos, *i.e.*, su resistencia a las colisiones.

6.1.1. PRF como medida de seguridad

El motivo de haber estudiado tan minuciosamente la indistinguibilidad de una función pseudoaleatoria en los capítulos anteriores, se debe a que su naturaleza es muy útil para construir códigos de autenticación de mensajes. En principio, si un MAC genera una firma empleando una PRF, entonces falsificar la firma implica calcular una nueva entrada en la PRF tal que genere una salida idéntica a la firma. Debido a que una PRF es indistinguible de una función aleatoria, es difícil adivinar el comportamiento de una PRF más allá de simplemente conocer su distribución.

Para demostrar que la indistinguibilidad es una fuerte condición de seguridad, considere el siguiente resultado:

Teorema 6.1.3. *Sea F una función pseudoaleatoria asociada al esquema de autenticación Λ. Entonces, Λ es indistinguible bajo el experimento $\mathbf{Exp}^{\text{CPA-LR}}$ para cualquier adversario $\mathcal{A} \in CPA$.*

$$\mathbf{Adv}_{\Lambda}^{\text{LR}}(\mathcal{A}) \leq \mathbf{Adv}_{F}^{\text{PRF}}(\mathcal{B})$$

Demostración. Sea $F : K \times X \to Y$ una función pseudoaleatoria y deje que $\Lambda \sim F$ sea un esquema simétrico que emplea esta función como algoritmo de cifrado. Así,

$$\begin{aligned}\mathbf{Ind}_{\Lambda}^{\text{CPA}}(\mathcal{A}) &= \Pr\left[\mathbf{Exp}_{\Lambda}^{\text{CPA-1}}(\mathcal{A}) \Rightarrow 1\right] - \Pr\left[\mathbf{Exp}_{\Lambda}^{\text{CPA-0}}(\mathcal{A}) \Rightarrow 1\right] \\ &= \Pr\left[\mathcal{A}^{F_k(x_1)} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{F_k(x_0)} \Rightarrow 1\right]\end{aligned}$$

Sin perdida de generalidad, considere una función aleatoria $\rho \xleftarrow{\$} Y^X$ tal que

$$\Pr\left[\mathcal{A}^{F_k(x_0) \Rightarrow 1}\right] \geq \Pr\left[\mathcal{A}^{\rho(x_0)} \Rightarrow 1\right]$$

Podemos asumir esto, gracias a que F es también un sistema determinista. Dado un x fijo, un adversario $\mathcal{A}$ con suficientes recursos tendrá una ventaja mayor contra cualquier instancia F_k que para un ρ.

Suponga ahora un adversario $\mathcal{B}$ que pude seleccionar las entradas x_1, x_0.

$$\begin{aligned} \therefore \quad \mathbf{Ind}^{\text{CPA}}_{\Lambda}(\mathcal{A}) &\leq \Pr\left[\, \mathcal{A}^{F_k(x_1)} \Rightarrow 1 \,\right] - \Pr\left[\, \mathcal{A}^{\rho(x_0)} \Rightarrow 1 \,\right] \\ &\leq \Pr\left[\, \mathcal{B}^{F_k} \Rightarrow 1 \,\right] - \Pr\left[\, \mathcal{B}^{\rho} \Rightarrow 1 \,\right] \\ &\leq \mathbf{Adv}^{\text{PRF}}_{F}(\mathcal{B}) \end{aligned}$$

Aplicando el Teorema 5.4.4, se concluye la prueba. □

Es importante advertir de que en esta demostración, se ha llegado a la conclusión de que la seguridad del esquema Λ se reduce a la seguridad de la función F relacionada con al algoritmo de cifrado. Es necesario recordar esto, porque a partir de ahora se demostrará la seguridad de un esquema a través de pruebas por reducción. Además, esto nos permite apreciar la estrecha relación entre los esquemas de seguridad y sus primitivas.

Más aún, este resultado plantea una cuestión bastante interesante. Usualmente, asegurar la privacidad de la comunicación (seguridad semántica) parecía ser una de las metas más importantes y, sobre todo, difíciles de lograr para un criptógrafo. Sin embargo, aquí se argumenta que, de hecho, garantizar la autenticidad de un mensaje es una meta mucho más difícil de lograr.

La indistinguibilidad Izquierda-Derecha sólo garantiza que un adversario no pueda conocer algo de información parcial sobre algún mensaje, pero esto indica nada sobre la integridad de cada mensaje. No obstante, es evidente que asegurar la privacidad de las comunicaciones no implica que seamos capaces de verificar la autenticidad de éstas. Además, robar información no es la única manera en que un adversario puede hacer daño con nuestros mensajes.

6.1.2. Cota de cumpleaños

Recordemos que un adversario, en el experimento de falsificación, es capaz de interceptar los mensajes y reemplazarlos con mensajes manipulados. Ingenuamente, se podría pensar: un esquema de autenticación que no filtra nada de información parcial sobre el mensaje es suficiente para ser seguro; pero ¿acaso existe una manera de falsificar un mensaje sin necesidad de información alguna sobre el mensaje?

Imagine que se tiene un MAC basado en cifradores por bloques y un adversario que desea encontrar una colisión entre dos mensajes distintos. Además, deje que el adversario consulte a un oráculo en distintas entradas $x_1, x_2, \ldots, x_q$, tales que cada entrada es de la longitud máxima del BC. Debido a que un cifrador por bloques es una familia de permutaciones, se sabe que cualquiera de sus instancias siempre genera una secuencia $y_1, y_2, \ldots, y_q$ distinta por pares. Por el contrario, si el adversario estuviera interactuando con una función aleatoria, entonces existe la posibilidad de que ocurra alguna colisión $y_i = y_j$ dentro de la secuencia y^q.

En teoría de la probabilidad, existe una ley que describe la facilidad de encontrar una colisión, para un dominio dado, denominada "La paradoja del cumpleaños". Ésta puede entenderse

mejor al pensar sobre la cantidad de gente necesaria para encontrar dos personas con el mismo cumpleaños. Cabe señalar que es una paradoja contra-intuitiva, no verídica. La intuición sugiere que la probabilidad de encontrar esas personas crece linealmente, sin embargo, no es así. Antes de enunciar el teorema principal, se considera resolver una serie de resultados importantes:

Lema 6.1.4. *Sea* $0 \leq x \leq 1$. *Entonces*

$$\left(1 - \frac{1}{e}\right) \cdot x \leq 1 - e^{-x} \leq x$$

Demostración. Dado que e^x es una función continua, por el teorema del valor intermedio se deduce que

$$\frac{e^0 - e^{-x}}{0 - x} = \frac{1 - \frac{1}{e^x}}{-x} = \frac{1}{e^\alpha} \leq 1$$

para cualquier $\alpha \geq 0$. Ya que $e^x \leq e$ para toda $x \in [0, 1]$, entonces

$$x \geq 1 - \frac{1}{e^x} \geq x \cdot (1 - \frac{1}{e^x}) \geq x \cdot (1 - \frac{1}{e})$$

Simplificando, se obtiene el resultado deseado. □

El resultado anterior nos permite comprobar la cota de cumpleaños.

Lema 6.1.5. *Sea* $\mathcal{C}(N, q)$ *la probabilidad de que exista alguna colisión en una secuencia* $\omega^q = \omega_1, \ldots, \omega_q$ *de elementos de un conjunto* $|\Omega| = N$. *Entonces, la probabilidad de colisión está acotada asintóticamente por*

$$\mathcal{C}(N, q) = \Theta\left(\frac{q(q-1)}{N}\right)$$

para todo $q \leq \sqrt{2N}$.

Demostración.

($\leq$) Primero, considere $q = 2$. Dado ω_1 fijo, entonces la probabilidad de que ocurra al menos una colisión es

$$\mathcal{C}(N, 2) = \Pr\left[\, \omega_2 = \omega_1 \,\right] = \frac{1}{N}$$

Ahora, suponga que $\mathcal{C}(N, k) \leq k(k-1)/(2N)$ para todo $N > k$. Dados $\omega_1, \omega_2, \ldots, \omega_k$, entonces

$$\mathcal{C}(N, k+1) = \Pr\left[\, \exists j \leq k : \ \omega_{k+1} = \omega_j \,\right] \ \leq \sum_{j<i}^{k} \Pr\left[\, \omega_{i+1} \ = \omega_i \ \middle|\ \omega_i \neq \omega_j \,\right]$$

$$\leq \sum_{i=1}^{k} \frac{i}{N} \ = \frac{k(k-1)}{2N} + \frac{k}{N} \ = \mathcal{C}(N, k) + \frac{k}{N}$$

Por inducción, se verifica la cota superior.

$$\therefore \quad \mathcal{C}(N, q) \leq \frac{q(q-1)}{2N} \tag{6.1}$$

($\geq$) Para la cota inferior, considere la probabilidad de que la secuencia $\omega_1, \ldots, \omega_k$ sea distinta por pares, *i.e.*, el evento de que no exista ninguna colisión en una secuencia de k elementos. Sea $j < i$. Entonces,

$$\Pr\left[\, \omega_{i+1} \neq \omega_i \;\middle|\; \omega_i \neq \omega_j \,\right] \;= 1 - \mathcal{C}(N, i+1) \;= 1 - \frac{i}{N} \tag{6.2}$$

Observe cómo este evento es complemento del caso anterior. Luego, dados $\omega_1, \omega_2, \ldots, \omega_q$, se tiene que

$$\begin{aligned} 1 - \mathcal{C}(\Omega, k) &= \Pr\left[\, \omega_1, \ldots, \omega_k \text{ distinta por pares} \,\right] \\ &= \prod_{1 \leq j < i}^{k-1} \Pr\left[\, \omega_{i+1} \neq \omega_i \;\middle|\; \omega_i \neq \omega_j \,\right] \\ &= \prod_{i=1}^{k-1} \left(1 - \frac{i}{N}\right) \;= \prod_{i=1}^{k-1} \left(1 - (1 - e^{-\frac{i}{N}})\right) \\ &= \prod_{i=1}^{q-1} e^{-\sum_{i=1}^{q-1} i/N} \;= e^{-q(q-1)/2N} \end{aligned}$$

Ya que $i/N < 1$, se puede aplicar el Lema 6.1.4. También, sea $q < \sqrt{2N}$.

$$\therefore \quad \mathcal{C}(\Omega, k) \;= 1 - e^{-q(q-1)/2N} \;\geq \left(1 - \frac{1}{e}\right) \frac{q(q-1)}{2N} \tag{6.3}$$

En conclusión, de (6.3) y (6.1) se sigue la inclusión Θ.

□

Sorprendentemente, un adversario aplicando el principio de la cota de cumpleaños puede crear un ataque muy eficiente y barato, pues solamente tiene que consultar a su oráculo en diferentes entradas hasta encontrar una colisión. A continuación, se muestra el resultado principal en el ataque de la cota de cumpleaños.

Teorema 6.1.6. *Sea $\mathcal{E} : \left\{ E_k \mid k \in K \right\}$ una familia de permutaciones con $|Dom(\mathcal{E})| = |Ran(\mathcal{E})| = N$. Entonces, existe un adversario $\mathcal{A}$ realizando a lo más $q \leq \sqrt{2N}$ consultas, cuya ventaja en el experimento $\mathbf{Exp}^{\text{PRF}}$ es*

$$\mathbf{Adv}_E^{\text{PRF}}(\mathcal{A}) = \Theta\left(\frac{q(q-1)}{2N}\right)$$

Demostración. Sea $\mathcal{A}^{\mathcal{O}}$ un distinguidor que consulta entradas distintas $x_i \in Dom(\mathcal{E})$ y detecta colisiones en las respuestas $y_i \in Ran(\mathcal{E})$ de un oráculo. Su estrategia consiste de la siguiente manera: si después de q consultas $\mathcal{A}$ detecta una colisión, entonces retorna 0; de otro modo, $\mathcal{A}$

retorna 1. Adicionalmente, deje que el oráculo se comporte como una familia de permutaciones $\mathcal{E}$ en el Mundo 1 y $\rho \xleftarrow{\$} Y^Y$ en el Mundo 0.

Dada una secuencia (x^q, y^q) de pares entrada-salida $(x_i, y_i) \in \Omega$ compatibles para ambos oráculos, se presentan los siguientes casos para el Experimento 4.2.1:

Para el mundo real, E_k es una permutación. Por lo tanto, el distinguidor siempre retornará 1.

$$\begin{aligned}\Pr\left[\,\mathbf{Exp}_1^{\text{PRF}}(\mathcal{A}) \Rightarrow 1\,\right] &= \Pr\left[\,\mathcal{A}^{F_k} \Rightarrow 1\,\right] \\ &= \Pr\left[\,E_k(x^q) = y^q \text{ distinto por pares}\,\right] \\ &= 1\end{aligned}$$

Para el mundo ideal, ρ es una función aleatoria. Debido a esto, la probabilidad de que el distinguidor retorne 1 depende de la existencia de una colisión en (x^q, y^q), *i.e.*, retorna 1 si y^q es distinto por pares.

$$\begin{aligned}\Pr\left[\,\mathbf{Exp}_0^{\text{PRF}}(\mathcal{A}) \Rightarrow 1\,\right] &= \Pr\left[\,\mathcal{A}^{\rho} \Rightarrow 1\,\right] \\ &= \Pr\left[\,\rho(x^q) = y^q \text{ distinto por pares}\,\right] \\ &= 1 - C(Y, q)\end{aligned}$$

Percátese de que la probabilidad de este evento está dada por la cota de cumpleaños. Por último, el Teorema 6.1.5 implica que la ventaja del adversario es

$$\begin{aligned}\mathbf{Adv}_E^{\text{PRF}}(\mathcal{A}) &= \Pr\left[\,\mathbf{Exp}_1^{\text{PRF}}(\mathcal{A}) \Rightarrow 1\,\right] - \Pr\left[\,\mathbf{Exp}_0^{\text{PRF}}(\mathcal{A}) \Rightarrow 1\,\right] \\ &= 1 - (1 - C(Y, q)) \\ &= C(Y, q)\end{aligned}$$

De esta manera, se concluye la demostración. □

6.2. Construcción MAC

Intuitivamente, nos damos cuenta de que las funciones pseudoaleatorias son objetos muy útiles para diseñar un MAC. Imagine un equipo de emisor-receptor que conoce una familia F y selecciona al azar una clave secreta $k \xleftarrow{\$} Key(F)$. Lo único que debe hacer el emisor para enviar un mensaje m es firmar el mensaje como $y = F_k(x)$, y luego, enviarlo por un canal inseguro al receptor. Sin importar que tipo de mensaje-firma (x', y') reciba el receptor, él sólo tiene que verificar que $F_k(x') = y'$ para asegurar que el mensaje llego integro y garantizar que fue enviado por el emisor, el otro miembro que conoce la clave secreta.

Simultáneamente, un adversario que atrapa el par (x', y') se enfrenta con el siguiente problema. Suponga que en lugar de obtener mensajes con firmas producidas por una función pseudoaleatoria, obtiene firmas producidas por una función aleatoria. Reflexione sobre lo siguiente: si un modelo es entrenado con datos $y' \xleftarrow{\$} Y$ como ruido aleatorio, entonces un adversario

usando ese modelo nunca mejora sus probabilidades de lograr falsificar una firma y. Esto se debe a que los datos son basura, ya que todos los valores y' son obtenidos de una distribución uniforme completamente al azar. Contemple cómo esta conclusión es similar a las mencionadas en el Teorema 5.2.1 sobre la seguridad perfecta.

Teorema 6.2.1. *Sea Λ un esquema de autenticación cuyo MAC $F : K \times X \to Y$ es una función pseudoaleatoria y sea $\mathcal{A}$ un adversario, bajo el experimento $\mathbf{Exp}^{\text{FORGE}}$, que realiza a lo más q consultas de longitud μ. Por lo tanto, existe un adversario $\mathcal{B}$ bajo el experimento $\mathbf{Exp}^{\text{PRF}}$ tal que*

$$\mathbf{Adv}_F^{\text{FORGE}}(\mathcal{A}) \leq \mathbf{Adv}_F^{\text{PRF}}(\mathcal{B}) + \frac{q}{|Y|}$$

Demostración. Sea $\mathcal{A} \in CPA$ un adversario bajo el Experimento 6.1.1 y deje que $\rho \xleftarrow{\$} Y^X$ sea el algoritmo de cifrado relacionado con el esquema Λ. Por consiguiente,

$$\mathbf{Adv}_\rho^{\text{FORGE}}(\mathcal{A}) \ = \Pr\left[\, \mathcal{V}_k(x, y) = 1 \,\right] \ = \Pr\left[\, \rho(x) = y \,\right] \ = \frac{1}{|Y|}$$

Esto es directo, dada la Proposición 3.1.3. Suponga ahora que el algoritmo de cifrado $F \sim \Lambda$ es una función pseudoaleatoria. Entonces, existe un adversario B bajo el Experimento 4.2.1 tal que

$$\mathbf{Adv}_F^{\text{FORGE}}(\mathcal{A}) = \Pr\left[\, \mathcal{V}_k(x, y) = 1 \,\right] = \Pr\left[\, F_k(x) = y \,\right] \leq \Pr\left[\, \mathbf{Exp}_1^{\text{PRF}}(\mathcal{B}) \ \Rightarrow \ 1 \,\right]$$

Observe cómo calcular la probabilidad del evento $F_k(x) = y$ es una estrategia particular que puede emplear $\mathcal{B}$, no obstante, pueden existir mejores estrategias que retornen 1 para F_k.

$$\therefore \quad \mathbf{Adv}_F^{\text{FORGE}}(\mathcal{A}) - \mathbf{Adv}_\rho^{\text{FORGE}}(\mathcal{A}) \leq \Pr\left[\, \mathcal{B}^{F_k} \ \Rightarrow \ 1 \,\right] - \Pr\left[\, \mathcal{B}^{\rho} \ \Rightarrow \ 1 \,\right]$$

Así, por definición de función pseudoaleatoria,

$$\mathbf{Adv}_F^{\text{FORGE}}(\mathcal{A}) \leq \mathbf{Adv}_F^{\text{PRF}}(\mathcal{B}) + \frac{1}{|Y|}$$

En conclusión, si la ventaja de $\mathcal{B}$ es negligible, entonces F es un MAC infalsificable. □

El resultado anterior es bastante estrecho, pues la seguridad del MAC está reducida a la seguridad de una PRF. No obstante, para garantizar este nivel de seguridad es necesario que la PRF tenga una entrada de tamaño arbitrario. Los MAC generalmente se diseñan haciendo uso de primitivas criptográficas como los BC que sólo pueden procesar un bloque de tamaño fijo a la vez. Debido a esto, un algoritmo MAC debe considerar cómo comprimir un mensaje a un tamaño de bloque fácil de procesar para el cifrador por bloques, y que a su vez el algoritmo tenga un comportamiento indistinguible de una función aleatoria.

Cuando los mensajes son más grandes que la longitud de los bloques, se procesa el mensaje empleando **modos de operación para cifradores por bloques**. Los principales modos de operación, es decir, **libro de código electrónico** (*Electronic Code Book*, ECB), **cadena de bloques cifrados** (*Cipher Block Chaining*, CBC) y el **modo contador** (*Counter mode*, CTR), nos indican la manera en que un cifrador por bloques puede ser utilizado para cifrar mensajes muy grandes sin comprometer su seguridad.

6.2.1. Relación entre funciones y permutaciones pseudoaleatorias

Como discutimos en la sección anterior, la construcción habitual de un MAC emplea cifradores por bloques y permutaciones públicas que se pueden modelar como familias de permutaciones. Entre las permutaciones y las funciones pseudoaleatorias existe una estrecha relación muy importante de conocer al diseñar un MAC. La relación PRP-PRF es un resultado que se refleja del teorema del ataque de cumpleaños, el cual estipula que

Lema 6.2.2. ***[Lema PRF-PRP]*** *Sea* $E : \{E_k : Y \to Y \mid k \in K\}$ *una familia de funciones con* $|Y| = N$ *y sea* $\mathcal{A}$ *un adversario que realiza a lo más* q *consultas. Dado* $k \xleftarrow{\$} K$ *y* $\rho \xleftarrow{\$} Y^Y$*, entonces*

$$\| \mathcal{A}^{\rho} - \mathcal{A}^{E_k} \| \leq \frac{q(q-1)}{2N}$$

Como consecuencia, para cualquier adversario bajo $\mathbf{Exp}^{\text{PRF}}$ *se tiene que,*

$$|\, \mathbf{Adv}_E^{\text{PRF}}(\mathcal{A}) - \mathbf{Adv}_E^{\text{PRP}}(\mathcal{A}) \,| \leq \frac{q(q-1)}{2N}$$

Demostración. Para demostrar esta proposición se hará uso de la técnica de coeficientes H enunciada por Patarin (2009). En el siguiente capítulo, se abordará con más detalle qué son estos coeficientes, por el momento considere lo siguiente:

Sea $\mathbb{O}_1$ el comportamiento del oráculo como una permutación aleatoria $\pi \xleftarrow{\$} Y^{\dagger}$ y sea $\mathbb{O}_0$ su comportamiento como función aleatoria $\rho \xleftarrow{\$} Y^Y$, $|Y| = N$. Entonces, dado un transcrito $w = (x^q, y^q) \in \Omega$,

$$\begin{aligned} \frac{\Pr[\,\mathbb{O}_0 = w\,]}{\Pr[\,\mathbb{O}_1 = w\,]} = \frac{\Pr[\,\pi(x^q) = y^q\,]}{\Pr[\,\rho(x^q) = y^q\,]} &= \frac{(N)_q}{N^q} = \frac{1}{N} \cdot \frac{2}{N} \cdots \frac{N-q-1}{N} \\ &= \prod_{i=1}^{q-1} \left(\frac{N-i}{N} \right) \leq 1 - C(N,q) \end{aligned}$$

Note cómo se ha empleado el resultado de la cota de cumpleaños (6.2), y que una permutación sólo genera una secuencia y^q de elementos distintos por pares. Por lo tanto, el cociente entre una función aleatoria sobre una permutación aleatoria resulta en la cota de cumpleaños.

Ahora, suponga que $\mathcal{A}^{\mathbb{O}}$ es un distinguidor para un experimento PRF y PRP respectivamente. Entonces,

$$\frac{\Pr[\,\mathcal{A}^{\rho} \Rightarrow 1\,]}{\Pr[\,\mathcal{A}^{\pi} \Rightarrow 1\,]} \geq \frac{(N)_q}{N^q} = 1 - C(\Omega, q) \geq 1 - \frac{q(q-1)}{2N}$$

Luego, al despejar la variable aleatoria $\mathcal{A}^{\rho}$ se sigue que

$$\Pr[\,\mathcal{A}^{\rho} \Rightarrow 1\,] \geq \left(1 - \frac{q(q-1)}{2N}\right) \cdot \Pr[\,\mathcal{A}^{\pi} \Rightarrow 1\,] \geq \Pr[\,\mathcal{A}^{\pi} \Rightarrow 1\,] - \frac{q(q-1)}{2N}$$

Al aplicar las propiedades de la distancia estadística 1.4.6,

$$\| \mathcal{A}^{\rho} - \mathcal{A}^{\pi} \| \leq \frac{q(q-1)}{2N}$$

Por último, considere un distinguidor para una familia de funciones E compatible con los transcritos.

$$\begin{aligned} \therefore \quad \frac{q(q-1)}{2N} &\geq \Pr\left[\mathcal{A}^{\rho} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\pi} \Rightarrow 1\right] \\ &\geq \Pr\left[\mathcal{A}^{\rho} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{E} \Rightarrow 0\right] - (\Pr\left[\mathcal{A}^{\rho} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{E} \Rightarrow 0\right]) \\ &\geq \mathbf{Adv}_{E}^{\text{PRF}}\mathcal{A} - \mathbf{Adv}_{E}^{\text{PRP}}\mathcal{A} \end{aligned}$$

Es notorio que

$$\frac{-q(q-1)}{2N} \leq \mathbf{Adv}_{E}^{\text{PRP}}(\mathcal{A}) - \mathbf{Adv}_{E}^{\text{PRF}}(\mathcal{A})$$

Por lo tanto, la indistingubilidad de una PRP como PRF está acotada. □

Este resultado es bastante útil, pues asegura que una función pseudoaleatoria y una permutación pseudoaleatoria (que modelan un BC) pueden ser empleados para construir un MAC, además de que cualquier MAC basado en un cifrador por bloques tiene una seguridad limitada por el teorema del cumpleaños.

6.3. Más allá de la cota de cumpleaños

El lema PRP-PRF declara que la ventaja del adversario crece de manera asintótica al cuadrado de las consultas $O(q^2/N)$. Esto implica que una clave de 128 bits solamente garantiza 64 bits de seguridad. Normalmente, lo anterior no es un problema, ya que solamente hay que considerar claves de 256 para obtener la seguridad deseada de 128 bits. El problema es que existen entornos de recursos limitados que no tienen el lujo de poder gastar más en recursos de los que ya usan sus aplicaciones, como para permitirse almacenar claves mucho más grandes. Los dispositivos como relojes, marcapasos, sensores inteligentes, accesorios "wearables" y en general "El internet de las cosas" son entornos de bajos recursos (Dar et al., 2021; Naito, 2017).

La comunidad criptográfica ha hecho grandes esfuerzos para mejorar la seguridad de los MAC, sin degradar el rendimiento del proceso de autenticación, a través de construcciones seguras "más allá de la cota de cumpleaños" (*BBB* por sus siglas en inglés). Esto significa que las construcciones MAC BBB son confiables para más de $2^{n/2}$ consultas, donde n es el tamaño de bloque del cifrador subyacente. La primera solución para superar la limitación de cumpleaños es incorporar una estructura aleatoria para el procesamiento de cada parte del mensaje. Sin embargo, los esquemas existentes requieren propiedades de cifrado de bloque muy sólidas: un patrón de cifrado perfecto, resistencia a los ataques de claves asociadas o una cantidad relativamente grande de entropía (Cogliati & Seurin, 2016). Una opción es implementar el método

de transformación de PRP a PRF, como la construcción pEDM, que utiliza una sola permutación de n nits para construir una PRF con dos llamadas que no requieren la invertibilidad de la permutación (Dutta et al., 2021).

6.3.1. Estado del arte

El primer MAC BBB demostrable conocido como SUM-ECBC fue propuesto por Yasuda (2010). Este MAC está basado en un diseño genérico llamado "Digesto de Doble bloque luego Suma" o DbHtS (*Doble-block Hash then Sum*), que genera dos digestos G y H de un mensaje M, para luego sumar los dos bloques cifrados y entregar la salida DbHtS$(M) = G(M) \oplus H(M)$. A partir de este diseño genérico, se propusieron distintos diseños de MAC BBB, por ejemplo: PMAC+, una versión modificada de PMAC que opera con tres claves; LightMAC+ (Naito, 2017), una modificación de LightMAC independiente de la longitud del mensaje y con un rendimiento mejorado, y GCM-SIV2, un modo de operación con memoria (*stateful*) o MACRX (Bellare et al., 1999), una construcción que suma bits entre mensajes de manera aleatoria.

Una generalización del diseño DbHtS conocida como "Digesto de Doble bloque luego Función" o *DbHtF* (*Double-block Hash-then-Function*) calcula la salida a partir de una función F que toma 2 digestos G y H de entrada, para obtener *DbHtF*$(M) = F(G(M), H(M))$. Por ejemplo: NI+MAC (Dutta et al., 2015), una modificación del NI MAC basada en una función de comprensión, con dos tuberías en paralelo para calcular la firma, y 3kf9 (Zhang et al., 2012), una construcción basada en el modo CBC que emplea la estructura $f9$ para calcular la salida. En general, todos los cifradores mencionados anteriormente se consideran DbHtF, de acuerdo a Guo et al. (2020).

Un diseño genérico descubierto por Liskov et al. (2011) consiste en crear un MAC basado en un TBC. Un TBC puede ser construido a través de emplear el modo de operación *Xor-Encrypt-Xor* (XEX) con un BC, y al mismo tiempo, un TBC puede generar un MAC a partir de un diseño dedicado como el propuesto por Iwata et al. (2017). Estos diseños suelen ser más seguros que PMAC y logran procesar bloques de $n+t$-bits por llamada de cifrador. En general, es importante encontrar funciones MAC más seguras y eficientes, que brinden seguridad más allá del límite de cumpleaños, por lo tanto, los TBC son una propuesta sobresaliente.

La Tabla 6.3.1 resume las características y las construcciones MAC BBB relacionadas con las funciones pseudoaleatorias. Las primitivas de subyacentes de cada sistema se denotan PP (permutación pública), BC (cifrador por bloques), CF (Función de compresión) y las recientes TBC (Cifrador por bloques entonable). Cabe mencionar que la seguridad mostrada en las tablas son las cotas más estrechas demostradas para el momento, en específico, para la seguridad de CLRW2 que fue demostrada por Jha y Nandi (2020).

Se describe la seguridad de cada MAC con la notación de complejidad, el número de consultas q, el tamaño de bits n por bloque, la longitud del mensaje l y, particularmente para MACRX, la cantidad de t bits tomados al azar (Bellare et al., 1999). Todas estas construcciones se utilizan para proteger los datos en entornos con recursos limitados que exceden de manera confiable el límite de cumpleaños.

MAC	Llaves	Complejidad	Seguridad	Paralelo	Primitiva	Referencia
SUM-ECBC	4	$O(l^4q^3/2^{2n})$	$2n/3$	$\times$	BC	(Yasuda, 2010)
PMAC+	3	$O(l^3q^3/2^{2n})$	$2n/3$	✓	BC	(Yasuda, 2011)
GCM-SIV2	2	$\theta(l^2q^3/2^{2n})$	$2n/3$	$\times$	BC	(Iwata & Minematsu, 2016)
3kf9	3	$O(l^3q^3/2^{2n})$	$2n/3$	$\times$	BC	(Zhang et al., 2012)
CLRW2	3	$O(q^3/2^{n+t})$	$(n+t)/3$	$\times$	TBC	(Landecker et al., 2012)
NI+	1	$O(l^2q^2/2^{2n})$	$2n/3$	$\times$	CF	(Dutta et al., 2015)
LightMAC+	3	$\theta(q^3/2^{2n})$	$2n/3$	✓	BC	(Naito, 2017)
ZMAC	1	$\theta(q^3/2^{n+t})$	$(n+t)/2$	✓	TBC	(Iwata et al., 2017)
HPxHP	2	$O(q^3/2^{2n})$	$2n/3$	✓	PP	(Moch & List, 2019)
nEHtM	2	$\theta(q^3/2^{2n}$	$2n/3$	$\times$	PP	(Dutta et al., 2019)
pEDM	2	$\theta(q^3/2^{2n})$	$2n/3$	$\times$	PP	(Dutta et al., 2021)
EliMAC	1	$\theta(\sqrt{q^2/2^{2n-s}})$	$(n-s)/2$	✓	BC	(Dobraunig et al., 2023)

6.3.2. Funciones HASH universales

Como ya se mencionó, existen distintas propuestas para mejorar la indistinguibilidad de una construcción basada en BC como PRF. A continuación se describe una construcción genérica bastante importante que nos permitirá diseñar un modo de operación resistente a las colisiones denominada "casi xor universal", o AXU por sus siglas en inglés.

Sea $\mathcal{H} : \{H_k \mid k \in K\}$ una familia de funciones con dominio X y rango Y para las siguientes definiciones.

Proposición 6.3.1. *La función $\mathcal{H}$ es llamada **hash-casi-universal** ($\epsilon-$AU), si para todo $x, x' \in X$ se satisface que*

$$\max_{x' \neq x} \Pr_{k \leftarrow K} \left[H_k(x) = H_k(x') \right] \leq \epsilon$$

donde ϵ es una función negligible.

En tal caso, si el valor de ϵ es nulo, entonces $\mathcal{H}$ es una **función hash universal**.

Proposición 6.3.2. *Sea $(Y, \oplus)$ un grupo abeliano. Luego, H es llamada una **función casi-xor-universal** ($\epsilon-$AXU), si para todo $\Delta \in Y$ y cualesquiera $x, x' \in X$ se tiene que*

$$\max_{x' \neq x} \Pr_{k \leftarrow K} \left[H_k(x) \oplus H_k(x') = \Delta \right] \leq \epsilon(n)$$

Observe que si una función es AXU, entonces también es $\epsilon-$AU. Por último,

Proposición 6.3.3. *Sea $Y = \{0,1\}^n \times \{0,1\}^t$. Entonces $\mathcal{H}$ es llamada una **función casi-parcial-xor-universal** ($(n,t,\epsilon)-$pAXU), si para todo $x, x' \in X$ y $\Delta \in \{0,1\}^n$ se cumple que*

$$\max_{x' \neq x} \Pr_{k \leftarrow K} \left[H_k(x) \oplus H_k(x') = (\Delta, 0^t) \right] \leq \epsilon(n,t)$$

Las funciones AXU y pAXU son requerimientos esenciales para la construcción de los MAC BBB. Sin embargo, es pertinente hacer las preguntas ¿Existen funciones AXU y pAXU que superen la cota de cumpleaños? ¿En qué casos pueden existir? ¿Si existen, cómo las construimos?

En los siguientes capítulos, se dará respuesta a estas preguntas mediante el estudio de la técnica de los coeficientes H (que se mencionó brevemente en el Lema 6.2.2) y al analizar una pAXU empleado por el esquema ZMAC dado más adelante.

Capítulo 7

Herramientas de la técnica-H

En el capítulo anterior, se hizo uso práctico de la técnica propuesta de los coeficientes H para demostrar el Lema PRF-PRP. Ahora, se estudiará de manera minuciosa los teoremas de suficiencia descubiertos por Patarin (2009). Esta técnica es uno de los logros más importantes del enfoque moderno, sobre todo para el desarrollo de esquemas simétricos.

En este capítulo, vamos a unir todos las ideas estudiadas hasta ahora para entender por fin la técnica principal que tanto buscábamos. Como se mencionó al final del Capítulo 2, no se buscan listas de condiciones inagotables sobre cómo diseñar cifradores por bloques o códigos de autenticación. Lo que se busca es una condición muy fuerte, que al cumplirse obtenga un esquema con todas las propiedades de seguridad que hemos estudiado a lo largo de los Capítulos 5 y 6.

7.1. Condiciones de suficiencia

Antes de abordar los resultados principales de esta teoría, es importante tener en claro algunos conceptos que enunciamos a continuación:

Definición 7.1.1. *Sea $\mathcal{A}$ un adversario y $\mathbb{O}$ un oráculo. Un **transcrito** es una variable aleatoria $\tau(\mathcal{A}^{\mathbb{O}}) := (x^q, y^q)$, tal que para toda $i \leq q$ cada instancia x_i, y_i es dada recursivamente como*

$$(x_i, y_i) := \big(\mathcal{A}(y^{i-1}), \mathbb{O}(x^i)\big)$$

Podemos advertir que para cualquier transcrito $(x^q, y^q) \in \Omega$,

$$\Pr\left[\, \tau(\mathcal{A}^{\mathbb{O}}) = (x^q, y^q) \,\right] = \Pr\left[\, \mathcal{A}(y^q) = x^q,\ \mathbb{O}(x^q) = y^q \,\right]$$

Recuerde que un oráculo y un adversario se modelan como sistemas probabilísticos, ambos con sus respectivos espacios de probabilidad asociados a un espacio de monedas en particular. Aunque no sea evidente en la definición, está implícito que tanto el adversario $\mathcal{A}$ como el oráculo $\mathbb{O}$ son sistemas independientes.

El transcrito es una abstracción que permite entender la interacción entre ambos sistemas como un sólo conjunto de tuplas que conforman su comportamiento de entrada-salida (x^q, y^q) de Ω. De esta manera, se puede hacer un análisis puramente probabilístico para realizar pruebas de seguridad incondicional.

Definición 7.1.2. *Deje que $\mathcal{A}^{\mathrm{O}} \in ATK$ sea un distinguidor genérico. Para dos funciones distintas F y G, la **ventaja incondicional** del distinguidor es*

$$\langle F, G\rangle := \left| \Pr\left[\mathcal{A}^{F_k} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{G} \Rightarrow 1\right] \right|$$

Además, para cada experimento de pseudoaletoriedad se tiene que

$$\mathbf{Adv}_F^{\text{PRF}} := \max_{KPA} \Delta(F; \rho)$$

$$\mathbf{Adv}_F^{\text{PRP}} := \max_{CPA} \Delta(F; \rho)$$

$$\mathbf{Adv}_F^{\text{SPRP}} := \max_{CCA} \Delta(F^{\pm}; \rho^{\pm})$$

$$\mathbf{Adv}_F^{\text{TPRP}} := \max_{CPA} \Delta(\widehat{F}; \widehat{\rho})$$

$$\mathbf{Adv}_F^{\text{TSPRP}} := \max_{CCA} \Delta(\widehat{F}^{\pm}; \widehat{\rho}^{\pm})$$

*es la **seguridad incondicional** de F como PRF, o como PRP en sus respectivas versiones fuertes y entonables.*

Contemple cómo la seguridad incondicional es la ventaja máxima con la que se puede distinguir una familia. Esta ventaja se calcula sobre el mejor de los distinguidores posibles en un modo de ataque, el cual está definido previamente por alguno de los experimentos vistos en el Capítulo 4. Cabe agregar, que la seguridad incondicional de una función pseudoaleatoria es análoga al concepto de indiferenciabilidad de una función quasi-aleatoria introducida por Maurer (2002).

Encontrar al más poderoso de los adversarios bajo teoría de la información podría parecer una tarea bastante difícil, sin embargo, es aquí en donde aplicaremos los resultados obtenidos sobre la distancia estadística en el Capítulo 1.

Corolario 7.1.3. *Sea Ω_1 el soporte del distinguidor $\mathcal{A}$. Dado un transcrito $\tau(\mathcal{A}^{\mathrm{O}})$. Entonces, para cualesquiera dos familias F y G, se tiene que*

$$\langle F, G\rangle \leq \| \boldsymbol{\tau}_F - \boldsymbol{\tau}_G \|$$

Más aún, la ventaja del distinguidor es óptima cuando

$$(x^q, y^q) \in \Omega_1 \Leftrightarrow \Pr\left[\tau(\mathcal{A}^{F_k}) = (x^q, y^q)\right] \geq \Pr\left[\tau(\mathcal{A}^{G}) = (x^q, y^q)\right]$$

Demostración. Considere un distinguidor genérico $\mathcal{A}^{\mathbb{O}}$ y sea $\tau = (x^q, y^q)$ un transcrito cualquiera. Entonces,

$$\begin{aligned}
\Pr\left[\, \mathcal{A}^{\mathbb{O}} \Rightarrow 1 \,\right] &= \Pr\left[\, \tau(\mathcal{A}^{\mathbb{O}}) \in \mathbf{Sop}\, \mathcal{A} \,\right] \\
&= \Pr\left[\, \mathcal{A}(y^q) = x^q, \mathbb{O}(x^q) = y^q, \flat = 1 \,\right] \\
&= \Pr\left[\, \flat(\mathcal{A}(y^q)) = 1, \mathfrak{B} = (x^q, y^q) \,\right] \\
&= \sum_{(x^q, y^q) \in \mathbf{Sop}\, \mathcal{A}} \Pr\left[\, \mathfrak{B} = (x^q, y^q) \,\right] \\
&= \mathbb{P}_{\tau}^{\mathfrak{B}}(\Omega_1)
\end{aligned}$$

Como el distinguidor parte el conjunto de los transcritos, la clase Ω_1 y Ω_0, se cumple la desigualdad anterior. Luego, para dos funciones distintas, se sigue que

$$\begin{aligned}
\langle F, G \rangle &= \left| \Pr\left[\, \mathcal{A}^F \Rightarrow 1 \,\right] - \Pr\left[\, \mathcal{A}^G \Rightarrow 1 \,\right] \right| && (7.1) \\
&= \left| \mathbb{P}_X^F(\Omega_1) - \mathbb{P}_X^G(\Omega_1) \right| && (7.2) \\
&\leq \max_{\Omega_1} \left| \mathbb{P}_X^F(\Omega_1) - \mathbb{P}_X^G(\Omega_1) \right| && (7.3) \\
&\leq \left\| \mathbb{P}_X^F - \mathbb{P}_X^G \right\| = \| \boldsymbol{\tau}_F - \boldsymbol{\tau}_G \| && (7.4)
\end{aligned}$$

Rememoré la Definición 1.4.6 sobre la notación para funciones de probabilidad o para variables aleatorias que usamos en (7.4). Ahora, supongamos un distinguidor óptimo tal que

$$\max_{ATK} \langle F, G \rangle = \| \boldsymbol{\tau}_F - \boldsymbol{\tau}_G \| \tag{7.5}$$

$\Rightarrow$) Considere un transcrito en el soporte del distinguidor $\omega_1 \in \mathbf{Sop}\, \mathcal{A}$. Luego, de (7.5) se deduce que

$$\| \boldsymbol{\tau}_F - \boldsymbol{\tau}_G \| = \max_{ATK} \langle F, G \rangle = \max_{\Omega_1} \left| \mathbb{P}_X^F(\Omega_1) - \mathbb{P}_X^G(\Omega_1) \right|$$

Por el Lema 1.4.8, se cumple que $\Omega_1 \subseteq \Omega_{\geq}$.

$$\therefore \quad \Pr\left[\, \tau(\mathcal{A}^{F_k}) = \omega_1 \,\right] \geq \Pr\left[\, \tau(\mathcal{A}^G) = \omega_1 \,\right]$$

$\Leftarrow$) Ahora, considere un transcrito $\omega \in \Omega_{\geq}$ para dos funciones distintas. Entonces,

$$\begin{aligned}
\| \boldsymbol{\tau}_F - \boldsymbol{\tau}_G \| &= \sum_{\tau \in \Omega} \max\{0, \Pr\left[\, \tau(\mathcal{A}^{F_k}) = \omega \,\right] - \Pr\left[\, \tau(\mathcal{A}^G) = \omega \,\right]\} \\
&= \sum_{\tau \in \Omega_{\geq}} \left| \Pr\left[\, \tau(\mathcal{A}^{F_k}) = \omega \,\right] - \Pr\left[\, \tau(\mathcal{A}^G) = \omega \,\right] \right| \\
&= \left| \mathbb{P}_X^F(\Omega_{\geq}) - \mathbb{P}_X^G(\Omega_{\geq}) \right|
\end{aligned}$$

Al aplicar (7.5), se resuelve que

$$\left|\ \mathbb{P}_X^F(\Omega_{\geq}) - \mathbb{P}_X^G(\Omega_{\geq})\ \right| \ = \ \max_{ATK} \langle F,\, G \rangle \ = \ \left|\ \mathbb{P}_X^F(\Omega_1) - \mathbb{P}_X^G(\Omega_1)\ \right|$$

Por lo tanto, el transcrito pertenece al soporte del distinguidor $\omega \in \Omega_1$.

Dado que se cumple la suficiencia y la necesidad, se concluye la prueba. □

7.1.1. Coeficientes H

Uno de los mayores problemas al desarrollar un sistema criptográfico es cómo destilar una familia de funciones de tal manera que su distribución sea uniforme. Se sabe que a pesar de que existen múltiples maneras para construir una familia de funciones específica, obtener una familia cuyas instancias generen una distribución uniforme entre su dominio y rango es una tarea monumental. Por este motivo, en el Capítulo 6 se introdujeron las funciones AXU.

Resumiendo, una función AXU no garantiza uniformidad, pero asegura que las irregularidades entre instancias esté acotada. De esta manera, Patarín desarrolla una serie de resultados para secuencias de transcritos con probabilidad acotada, como las funciones AXU, a partir de una medida nombrada coeficiente H.

Definición 7.1.4. *Sea $G : (\mathfrak{I}_q, X \to X, K, \mathfrak{B})$ un sistema de respuesta y deje que $(a^q, b^q) \in \mathfrak{B}_{i/o}$ sea una secuencia de parejas $(a_i, b_i) \in X$, $i = 1, \ldots, q$ en el comportamiento, tal que cada a_i es distinta por pares. Se define el* ***coeficiente*** *H de G como*

$$H(a^q, b^q) := \left|\left\{k \in K \mid (a_i, b_i, k) \in \mathfrak{B},\ \forall i \leq q\right\}\right|$$

donde $\mathfrak{B}$ es el comportamiento interno de G.

Aprecie como el sistema G define a su vez una aplicación $G : K \to X^X$. De este modo, los coeficientes H también corresponden con la cardinalidad del conjunto

$$\left\{k \in K \mid G_K(a_i) = b_i\ \forall i \leq q\right\}$$

En consecuencia, se denota H como la cantidad de instancias que mapean una secuencia a^q a exactamente una salida b^q, *i.e.*, la medida del espacio latente K.

Las herramientas de los coeficientes H constituyen 5 teoremas fundamentales que garantizan seguridad incondicional bajo distintos modos de ataque: KPA, CPA, CCA y sus versiones adaptativas. A continuación, se enuncian las condiciones de suficiencia para cada caso.

7.1.2. Seguridad bajo ataque de texto plano conocido

Teorema 7.1.5. [***Condición de suficiencia contra KPA***] *Sean α, β números reales positivos y $|X| = N$. Si para valores aleatorios $(a^q, b^q) \in \Omega$ (los elementos a_i distintos por pares) con $\Pr[\,\tau = (a^q, b^q)\,] \geq (1 - \beta)$ siempre sucede que,*

$$H \geq \frac{|K|}{N^q}(1 - \alpha)$$

entonces, la seguridad incondicional de una familia F es

$$\mathbf{Adv}_F^{\mathrm{KPA}} \leq \alpha + \beta$$

contra cualquier adversario $\mathcal{A} \in KPA$ con q textos conocidos.

Demostración. Se denota D al conjunto de elementos $a^q \in X^{(q)}$, tal que los elementos a_i son distintos por pares. Enseguida, considere un adversario $\mathcal{A} \in KPA$ y tome un $a^q \in D$ fijo para los siguientes casos:

$\leq$) Sea Ω_1 el soporte del distinguidor $\mathcal{A}$. Por lo tanto, para el mundo ideal:

$$\Pr\left[\, \mathcal{A}^{\rho} \Rightarrow 1 \,\right] = \Pr\left[\, \natural\left(\mathcal{A}(y^q)\right) = 1,\ \rho(x^q) = y^q \,\right] \tag{7.6}$$

$$= \sum_{b^q \in \Omega_1(a^q)} \Pr\left[\, \rho(a^q) = b^q \,\right] \tag{7.7}$$

$$= \sum_{b^q \in \Omega_1(a^q)} \frac{1}{N^q} \tag{7.8}$$

$$= \frac{|\, \Omega_1(a^q) \,|}{N^q} \tag{7.9}$$

donde $\Omega_1(a^q) = \left\{ b^q \mid (a^q, b^q) \in \mathbf{Sop}\, \mathcal{A} \right\}$. Vea en (7.8) cómo se aplica la Proposición 3.3.7 sobre las URF. Luego, para el mundo real:

$$\Pr\left[\, \mathcal{A}^{F_k} \Rightarrow 1 \,\right] = \sum_{b^q \in \Omega_1(a^q)} \Pr\left[\, F_k(a^q) = b^q \,\right]$$

$$= \sum_{b^q \in \Omega_1(a^q)} \prod_{1 \leq j < i}^{q} \Pr\left[\, F_k(x_i) = y_i \middle|\, F_k(x_j) = y_j \,\right]$$

Debido a que F_k es una función, $\Pr\left[\, F(k, x_i) = (y_i) \,\right]$ y $\Pr\left[\, F(k, x_j) = (y_j) \,\right]$ son independientes. Adicionalmente, ya que F_k es una función probabilística,

$$\Pr\left[\, \mathcal{A}^{F_k} \Rightarrow 1 \,\right] = \sum_{b^q \in \Omega_1(a^q)} \prod_{i=1}^{q} \sum_{\substack{\hat{k} \in K \,: \\ F(\hat{k},\, a_i) \,=\, b_i}} \Pr\left[\, \hat{k} = k \,\right]$$

Advierta de que K es el espacio de claves asociado al comportamiento $\mathbb{F} : X^{(q)} \to X^{(q)}$ de la función criptográfica F.

$$\therefore \quad \Pr\left[\, \mathcal{A}^{F_k} \Rightarrow 1 \,\right] = \sum_{b^q \in \Omega_1(a^q)} \sum_{\substack{\hat{k} \in K,\, i \,\leq\, q \,: \\ F(\hat{k},\, a_i) \,=\, b_i}} \frac{1}{|K|} \tag{7.10}$$

$$= \sum_{b^q \in \Omega_1(a^q)} \frac{H(a^q, b^q)}{|K|} \tag{7.11}$$

Observe cómo el coeficiente H se obtiene a partir de (7.10). Ahora, se define $\mathbb{B}$ como la cantidad de transcritos $(a^q, b^q) \in \Omega$ tales que

$$H(a^q, b^q) \geq \frac{|K|}{N^q}(1-\alpha)$$

Por hipótesis,

$$(1-\beta) \leq \frac{|\mathbb{B}|}{|D| \cdot N^q}$$

Para un a^q fijo, se define $\mathbb{B}(a^q)$ como el conjunto de b^q que satisface la hipótesis anterior.

$$\therefore \quad |\mathbb{B}| = \sum_{a^q \in D} |\mathbb{B}(a^q)| \geq |D| \cdot N^q(1-\beta) \tag{7.12}$$

De (7.11) se sigue que

$$\Pr\left[\, \mathcal{A}^{F_k} \;\Rightarrow\; 1 \,\right] \geq \frac{\gamma}{|K|} \sum_{\Omega_1(a^q) \,\cap\, \mathbb{B}(a^q)} H(a^q, b^q) \tag{7.13}$$

$$\geq (1-\alpha) \cdot \frac{|\Omega_1(a^q) \;\cap\; \mathbb{B}(a^q)|}{N^q} \tag{7.14}$$

$$\geq (1-\alpha) \cdot \frac{|\,\Omega_1(a^q)\,| - |\,\mathbb{B}^{\complement}(a^q)\,|}{N^q} \tag{7.15}$$

De (7.9) y (7.15),

$$\Pr\left[\, \mathcal{A}^{F_k} \;\Rightarrow\; 1 \,\right] \geq (1-\alpha) \cdot \frac{|\Omega_1(a^q)| - |\mathbb{B}^{\complement}(a^q)|}{N^q} \tag{7.16}$$

$$= (1-\alpha) \cdot \left(\frac{|\Omega_1(a^q)|}{N^q} - \frac{|\mathbb{B}^{\complement}(a^q)|}{N^q} \right) \tag{7.17}$$

$$= (1-\alpha) \cdot \left(\Pr\left[\, \mathcal{A}^{\rho} \;\Rightarrow\; 1 \,\right] - \frac{|\mathbb{B}^{\complement}(a^q)|}{N^q} \right) \tag{7.18}$$

$$\geq (1-\alpha) \cdot \left(\Pr\left[\, \mathcal{A}^{\rho} \;\Rightarrow\; 1 \,\right] - \frac{|\mathbb{B}^{\complement}(a^q)|}{N^q} \right) - \alpha \cdot \frac{|\mathbb{B}^{\complement}(a^q)|}{N^q} \tag{7.19}$$

$$\geq \Pr\left[\, \mathcal{A}^{\rho} \;\Rightarrow\; 1 \,\right] - \alpha \cdot \Pr\left[\, \mathcal{A}^{\rho} \;\Rightarrow\; 1 \,\right] - \frac{|\mathbb{B}^{\complement}(a^q)|}{N^q} \tag{7.20}$$

$$\geq \Pr\left[\, \mathcal{A}^{\rho} \;\Rightarrow\; 1 \,\right] - \alpha - \frac{|\mathbb{B}^{\complement}(a^q)|}{N^q} \tag{7.21}$$

Dado que $1 \geq \Pr\left[\, \mathcal{A}(b^q) = a^q \,\right]$ y $1 \geq \Pr\left[\, \mathcal{A}^{\rho} \;\Rightarrow\; 1 \,\right]$, minimizamos (7.20). Enseguida, al calcular la cantidad de $b^q \notin \mathbb{B}(a^q)$,

$$\sum_{a^q \in D} |\mathbb{B}^{\complement}(a^q) + \mathbb{B}(a^q)| \;= \sum_{a^q \in D} |X^{(q)}| \;= |D| \cdot N^q$$

De (7.12), se obtiene que

$$\mathrm{Ex}\left[\mathbb{B}^{\mathfrak{C}}(a^q)\right] = \frac{1}{|D|}\sum_{a^q\in D}|\mathbb{B}^{\mathfrak{C}}(a^q)| \;= N^q - \frac{1}{|D|}\sum_{a^q\in D}|\mathbb{B}(a^q)| \tag{7.22}$$

$$\leq N^q - N^q(1-\beta) \;= \beta\cdot N^q \tag{7.23}$$

Luego, al aplicar (7.23) en (7.21),

$$\mathrm{Ex}\left[\mathcal{A}^{F_k} \;\Rightarrow\; 1\right] \geq \frac{1}{|D|}\sum_{a^q\in D}\left[\Pr\left[\,\mathcal{A}^{\rho} \;\Rightarrow\; 1\,\right] - \alpha - \frac{|\mathbb{B}^{\mathfrak{C}}(a^q)|}{N^q}\right] \tag{7.24}$$

$$= \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 1\right] - \mathrm{Ex}\left[\alpha\right] - \mathrm{Ex}\left[\tfrac{|\mathbb{B}^{\mathfrak{C}}(a^q)|}{N^q}\right] \tag{7.25}$$

$$= \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 1\right] - \alpha - \frac{1}{N^q}\cdot\mathrm{Ex}\left[\mathbb{B}^{\mathfrak{C}}(a^q)\right] \tag{7.26}$$

$$\geq \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 1\right] - \alpha - \beta \tag{7.27}$$

Aquí sobresale cómo hemos aplicado las propiedades lineales de la esperanza para obtener (7.27).

$$\therefore \quad \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 1\right] - \mathrm{Ex}\left[\mathcal{A}^{F_k} \;\Rightarrow\; 1\right] \leq \alpha + \beta \tag{7.28}$$

Esto satisface la cota superior.

$\geq$) Ahora, considere el complemento del distinguidor Ω_0. Dado que $\mathbb{B}$ se calcula de manera independiente al distinguidor, se puede replicar el mismo análisis hasta (7.27) tal que

$$\mathrm{Ex}\left[\mathcal{A}^{F_k} \;\Rightarrow\; 0\right] \geq \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 0\right] - \alpha - \beta$$

Esto es válido, puesto que se podría pensar en un distinguidor $\Phi^{\mathfrak{C}}$ como en uno genérico que responde 1 cuando Φ responde 0.

$$\therefore \quad \alpha+\beta \geq \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 0\right] - \Pr\left[\,\mathcal{A}^{F_k} \;\Rightarrow\; 0\,\right] \tag{7.29}$$

$$\geq 1 - \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 0\right] - \left(1 - \mathrm{Ex}\left[\mathcal{A}^{F_k} \;\Rightarrow\; 0\right]\right) \tag{7.30}$$

$$\geq \mathrm{Ex}\left[\mathcal{A}^{F_k} \;\Rightarrow\; 1\right] - \mathrm{Ex}\left[\mathcal{A}^{\rho} \;\Rightarrow\; 1\right] \tag{7.31}$$

Por último, al aplicar el Corolario 7.1.3 en (7.28) y (7.31) se satisface que

$$\mathbf{Adv}_F^{\mathrm{PRF}} \;=\; \max_{KPA}\left(\mathrm{Ex}\left[\mathcal{A}^{F_k} - \mathcal{A}^{\rho}\right]\right) \;\leq\; \alpha+\beta$$

En conclusión, la ventaja de cualquier adversario con una cantidad finita de textos planos conocidos está acotada del modo deseado.

□

7.1.3. Seguridad bajo ataque de texto plano elegido

El segundo y tercer teorema de los coeficientes H toman en cuenta un distinguidor bajo un ataque de texto plano elegido.

Teorema 7.1.6. [***Condición de suficiencia contra CPA-1***] *Sean α, β números reales positivos. Siempre que exista un subconjunto $\mathbb{B}(a^q) \subseteq Y^{(q)}$ con cardinalidad $|\mathbb{B}(a^q)| \geq (1-\beta) \cdot N^q$ para cada secuencia $a^q \in X^{(q)}$ con elementos distintos por pares, tal que además para toda $b^q \in \mathbb{B}(a^q)$ se cumpla que*

$$H \geq \frac{|K|}{N^q}(1-\alpha)$$

entonces, la seguridad incondicional de una familia F es

$$\mathbf{Adv}_F^{\text{CPA}} \leq \alpha + \beta$$

contra cualquier adversario no adaptativo $\mathcal{A} \in CPA$ realizando a lo más q consultas de textos planos.

Note cómo la diferencia principal entre KPA y CPA radica en la definición de $\mathbb{B}(a^q)$. En el Teorema 7.1.5 se calculan las posibles secuencias $b^q \in \mathbb{B}(a^q)$ específicamente sobre la probabilidad con que se toma un transcrito al azar dada una secuencia de entradas a^q en el transcrito. Esto restringe la estrategia del adversario a condiciones muy estrictas, tales como en un ataque KPA.

En el Teorema 7.1.6, se toman todas las $\mathbb{B}(a^q)$ correspondientes a cada secuencia a^q, por lo que la cantidad de posibles secuencias de salida $b^q \in \mathbb{B}(a^q)$ se calcula a partir de la cardinalidad de este subconjunto, y no de la probabilidad dada de un transcrito. En este resultado, se consideran todas las posibles secuencias de textos elegidos que puede seleccionar un adversario bajo CPA.

Teorema 7.1.7. [***Condición de suficiencia contra CPA-2***] *Sean α, β números reales positivos y $\mathbb{B} \subseteq Y^{(q)}$ un subconjunto con cardinalidad $|\mathbb{B}| \geq (1-\beta) \cdot N^q$. Si para todo transcrito $(a^q, b^q) \in \Omega$ (con los elementos de a^q distintos por pares) tal que $b^q \in \mathbb{B}$ se cumple que*

$$H \geq \frac{|K|}{N^q}(1-\alpha)$$

entonces, la seguridad incondicional de una familia F es

$$\mathbf{Adv}_F^{\text{CPA}} \leq \alpha + \beta$$

contra cualquier adversario $\mathcal{A} \in CPA$, realizando a lo más q consultas de textos planos.

Advierta cómo el conjunto $\mathbb{B}$ ahora no está relacionado con alguna secuencia a^q en específico. Más aún, sabemos que la cardinalidad de cualquier subconjunto de $Y^{(q)}$ está acotado. Esto significa que este resultado es independiente de cualquier entrada a_i seleccionada por un adversario bajo CPA. El Teorema 7.1.7 es mucho más fuerte que el Teorema 7.1.6, ya que el adversario podría elegir la secuencia de pares óptima e incluso así, su ventaja estaría acotada.

Para entender mejor este resultado se realiza la demostración:

Demostración. Sea $(a^q, b^q) \in \Omega$ un transcrito definido como 7.1.1 y deje que $\mathcal{A}^{\Theta}$ sea un distinguidor genérico bajo PRF. Entonces, para el mundo ideal:

$$\Pr\left[\,\mathcal{A}^{\rho} \;\Rightarrow\; 1\,\right] \;=\; \sum_{(a^q,b^q)\in\Omega_1} \Pr\left[\,\rho(a^q) = b^q\,\right] \;=\; \frac{|\Omega_1|}{N^q} \tag{7.32}$$

Recuerde que permitir al adversario consultar texto plano después de conocer el resultado del oráculo, implica que su comportamiento es un sistema determinista. Luego, para el mundo real:

$$\Pr\left[\,\mathcal{A}^{F_k} \;\Rightarrow\; 1\,\right] = \sum_{(a^q,b^q)\in\Omega_1} \Pr\left[\,F_k(a^q) = b^q\,\right] \tag{7.33}$$

$$= \sum_{\tau\in\Omega_1} \frac{1}{|K|} \prod_{i=1}^{q} \left|\,\left\{k \in K \;\mid\; F_k(a_i) = b_i\right\}\,\right| \tag{7.34}$$

$$= \sum_{\tau\in\Omega_1} \frac{H(a^q, b^q)}{|K|} \tag{7.35}$$

Observe cómo en (7.34) se aplica el coeficiente H. Por hipótesis, se tiene que cualquier subconjunto $\mathbb{B} \subseteq Y^{(q)}$ relacionado con H está dentro del compacto $(1-\beta)\cdot N^q \leq \mathbb{B} \leq N^q$. Por lo tanto, existen a lo más $\beta \cdot N^q$ elementos $b \notin \mathbb{B}$. De (7.35) y (7.32) se deduce que

$$\Pr\left[\,\mathcal{A}^{F_k} \;\Rightarrow\; 1\,\right] \geq (|\Omega_1| - \beta N^q) \cdot \frac{H(a^q, b^q)}{|K|} \tag{7.36}$$

$$\geq \frac{|\Omega_1| - \beta N^q}{|K|} \cdot \frac{|K|}{N^q}(1-\alpha) \tag{7.37}$$

$$\geq \left(\frac{|\Omega_1|}{N^q} - \beta\right) \cdot (1-\alpha) \tag{7.38}$$

$$\geq \Pr\left[\,\mathcal{A}^{\rho} \;\Rightarrow\; 1\,\right] - \beta - \alpha \tag{7.39}$$

Replicando el mismo análisis para el complemento del distinguidor, se consideran los transcritos en $\Omega_1^{\complement}$. Entonces, al calcular las probabilidades de ambos mundos,

$$\Pr\left[\,\mathcal{A}^{F_k} \;\Rightarrow\; 0\,\right] \geq \Pr\left[\,\mathcal{A}^{\rho} \;\Rightarrow\; 0\,\right] - \beta - \alpha \tag{7.40}$$

Esto se cumple, puesto que la hipótesis es simétrica para ambos conjuntos de transcritos.

$$\therefore \quad \Pr\left[\,\mathcal{A}^{\rho} \;\Rightarrow\; 1\,\right] \geq \Pr\left[\,\mathcal{A}^{F_k} \;\Rightarrow\; 1\,\right] - \beta - \alpha \tag{7.41}$$

Al aplicar el Corolario 7.1.3 en (7.39) y (7.41),

$$\mathbf{Adv}_F^{\text{PRF}} \;=\; \max_{CPA} \langle F; \rho \rangle \;\leq\; \alpha + \beta$$

En conclusión, la ventaja de cualquier adversario escogiendo adaptativamente textos planos está acotada de la manera afirmada. □

7.2. Técnica H generalizada

Los Teoremas 4 y 5 del artículo (Patarin, 2009) enuncian las condiciones de suficiencia contra los ataques de texto cifrado escogido. Ambos teoremas consideran un adversario adaptativo bajo CCA. Por lo tanto, en lugar de enunciar los últimos dos teoremas, se describe una proposición equivalente (sin pérdida de generalidad) que resume los teoremas de los coeficientes H para cualquier tipo de adversario, pero antes tenga en cuenta la siguiente definición:

Definición 7.2.1. *Sean $H_0 \sim \mathbb{O}_0$ y $H_1 \sim \mathbb{O}_1$ los coeficientes H relacionados con cada oráculo respectivamente. Se define el conjunto de* ***transcritos buenos*** *respecto a $\alpha, \beta \in [0,1]$ como*

$$\mathbb{B} := \left\{ \tau(\mathcal{A}^{\mathbb{O}}) \;\middle|\; \tfrac{H_1(\tau)}{H_0(\tau)} \geq 1-\alpha \right\}$$

tal que

$$\Pr\left[\, \tau(\mathcal{A}^{\mathbb{O}}) \in \mathbb{B} \,\right] \;\geq\; 1-\beta$$

En el complemento, los transcritos $\tau \notin \mathbb{B}$ se denominan ***transcritos malos****.*

Así, el parámetro β limita la cantidad de transcritos malos posibles

$$\beta \geq \Pr\left[\, \tau(\mathcal{A}^{\mathbb{O}}) \notin \mathbb{B} \,\right]$$

Mientras que el parámetro α son las claves que satisfacen

$$\alpha \geq 1 - \frac{H_1}{H_0}$$

De estas relaciones, podemos hallar la siguiente equivalencia:

Proposición 7.2.2. *Dados dos oráculos F y G, para todo transcrito bueno se satisface*

$$\frac{\Pr\left[\, F(a^q) = b^q \,\right]}{\Pr\left[\, G(a^q) = b^q \,\right]} \geq 1-\alpha \quad \text{y} \quad \Pr\left[\, \tau(\mathcal{A}^{G}) \notin \mathbb{B} \,\right] \leq \beta$$

donde $(a^q, b^q) \in \mathbb{B}$.

Demostración. Sean dos oráculos con espacio de claves $K_1 \sim F$ y $K_0 \sim G$, respectivamente. Acorde a la Definición 7.1.4, se deduce que

$$1 \geq \frac{H_1}{|K_1|} \geq \frac{H_0}{|K_0|}$$

Sin perdida de generalidad, asumimos que la relación entra la cantidad de claves que satisface el coeficiente de F puede ser mayor que la relación con las claves de G, no obstante, podríamos realizar una prueba equivalente para el otro caso. Luego, de la Definición 7.2.1,

$$\begin{aligned} H_1 &\geq H_0 \cdot (1-\alpha) \\ \frac{H_1}{|K_1|} &\geq \frac{H_0}{|K_0|} \cdot (1-\alpha) \\ \Pr\left[\, F(a^q) = b^q \,\right] &\geq \Pr\left[\, G(a^q) = b^q \,\right] \cdot (1-\alpha) \end{aligned}$$

donde H_1, H_0 son los coeficientes respectivos de F, G. Conjuntamente, se satisface que la probabilidad de $\tau(\mathcal{A}^G) \in \mathbb{B}^{\complement}$ es menor o igual a β.

□

Como mencionamos, en virtud de que α es arbitrario, se puede demostrar el caso contrario

$$1 \geq \frac{H_0}{|K_0|} \geq \frac{H_1}{|K_1|}$$

Incluso, existen α' y β' para acotar la relación $\mathbb{P}^G \geq \mathbb{P}^F$ y la probabilidad de $\tau(\mathcal{A}^F) \notin \mathbb{B}$, respectivamente. Adicionalmente, juzgue cómo los transcritos buenos cumplen con la hipótesis $\Omega_> \subseteq \mathbb{B} \subseteq \Omega_\geq$ del Lema 1.4.8 empleado en la distancia estadística.

Corolario 7.2.3. [***Suficiencia de seguridad incondicional***] *Sean dos oráculos F y G. Entonces, para todo transcrito bueno se cumple que*

$$\| F - G \| \leq \alpha + \beta$$

Demostración. A continuación, emplearemos la prueba dada por Jha y Nandi (2022) en su Lema 3, para visualizar mejor cómo los resultados de Patarin convergen a esta conclusión.

Sea (a^q, b^q) un transcrito bueno. Entonces existen α y β tales que

$$\begin{aligned}
\| F - G \| &= \sum_{(a^q,b^q)\in\Omega} \text{máx}\left\{0,\ \mathbb{P}^F_{a^q}(b^q) - \mathbb{P}^G_{a^q}(b^q)\right\} \\
&\leq \sum_{(a^q,b^q)\in\Omega_>} \mathbb{P}^F_{a^q}(b^q) - \mathbb{P}^G_{x^q}(y^q) \\
&\leq \sum_{(a^q,b^q)\in\Omega_>} \mathbb{P}^F_{a^q}(b^q) \cdot \left(1 - \frac{\mathbb{P}^F_{a^q}(b^q)}{\mathbb{P}^G_{a^q}(b^q)}\right) \\
&\leq \alpha \cdot \sum_{(a^q,b^q)\in\mathbb{B}} \mathbb{P}^F_{a^q}(b^q) + \alpha \cdot \sum_{(a^q,b^q)\notin\mathbb{B}} \mathbb{P}^G_{a^q}(b^q) \\
&\leq \alpha + \sum_{(a^q,b^q)\notin\mathbb{B}} \mathbb{P}^G_{a^q}(b^q) \leq \alpha + \beta
\end{aligned}$$

donde obtenemos la primera igualdad conforme a los Lemas 1.4.7 y 1.4.8 de la distancia estadística. Al aplicar el Corolario 7.1.3, incluso, se concluye que

$$\mathbf{Adv}^{\text{Exp}}_F \leq \| F - G \| \leq \alpha + \beta$$

para cualquier adversario $\mathcal{A} \in ATK$ haciendo q consultas.

□

Cabe mencionar, que este corolario resume los resultados de los teoremas de Patarin (2009) con base al conjunto de transcritos buenos. Asimismo, la forma de seleccionar un transcrito con buenos parámetros depende del experimento de indistinguibilidad que se considere. En particular:

- Para $\mathcal{A} \in KPA$, se deduce que

$$\frac{\Pr\left[\, F_k(a^q) = b^q \,\right]}{\Pr\left[\, \rho(a^q) = b^q \,\right]} \geq 1 - \alpha$$

  tal que $|\mathbb{B}| \leq |D| \cdot N^q \cdot (1 - \beta)$.

- Para $\mathcal{A} \in CPA$, se colige que

$$\frac{\Pr\left[\, F_k(a^q) = b^q \,\right]}{\Pr\left[\, \rho(a^q) = b^q \,\right]} \geq 1 - \alpha$$

  tal que $|\mathbb{B}| \leq N^q \cdot (1 - \beta)$.

- Para $\mathcal{A} \in CCA$, se resuelve que

$$\frac{\Pr\left[\, F_k^{\pm}(a^q) = b^q \,\right]}{\Pr\left[\, \pi^{\pm}(a^q) = b^q \,\right]} \geq 1 - \alpha$$

  tal que $|\mathbb{B}| \leq |D| \cdot N^{2q} \cdot (1 - \beta)$.

A continuación, describiremos la manera de modificar este resultado para considerar experimentos con permutaciones entonables pseudoaleatorias.

7.2.1. Condición de suficiencia extendida

Como se mencionó, la técnica de los coeficientes H es bastante amplia, ya que puede ser empleada en cualquier experimento PRF o SPRP; no obstante, se puede ampliar el uso de la técnica para analizar los cifradores por bloques entonables. Recordemos que un TBC se modela como una TPRP

$$\overline{P} = \left\{ \overline{P}_k^t : X \to X \mid (t, k) \in K \times T \right\}$$

que es una familia de permutaciones extendida por un espacio adjunto denominado espacio de tonos. Con este fin, considere la siguiente modificación para los transcritos, dada por Jha y Nandi (2022).

Definición 7.2.4. *Sean $\mathcal{A}$ un adversario y $\overline{\mathbb{O}} : X^{(q)} \xrightarrow{\text{⚅}} Y^{(q)} \times S$ un oráculo S-extendido. Se define el* ***transcrito extendido*** *$\overline{\tau}$ como*

$$\overline{\tau}(\mathcal{A}^{\mathbb{O}}) \;=\; \tau(\mathcal{A}^{\overline{\mathbb{O}}}) \;:=\; \big(\tau(\mathcal{A}^{\mathbb{O}}), S(x^q)\big)$$

donde $\overline{\mathbb{O}} := (\mathbb{O}, S)$ es un sistema de respuesta con variable adjunta S.

Advierta cómo el transcrito extendido revela la secuencia de pares entrada-salida, así como el tono empleado para generarlas. Esto implica que, el comportamiento observable para estudiar un TBC consiste en las entradas x_i, las salidas y_i y el tono s. La única variable latente que se considera es el espacio de claves de un TBC.

A continuación, se enuncia el teorema generalizado para la seguridad incondicional de sistemas extendidos contra cualquier adversario.

Teorema 7.2.5. [***Técnica H extendida***] *Sean $\overline{F} := (F, T)$ y $\overline{G} := (G, T')$ dos oráculos extendidos. Siempre que exista un subconjunto de transcritos buenos $\mathbb{B} \subseteq \overline{\Omega}$ en los transcritos extendidos, sucede que la ventaja para cualquier adversario $\mathcal{A} \in ATK$ es*

$$\langle F, G \rangle \;\leq\; \left\| \, \tau(\mathcal{A}^{\overline{F}}) - \tau(\mathcal{A}^{\overline{G}}) \, \right\| \;\leq\; \alpha + \beta$$

Demostración. Sea $(x^q, y^q, s) \in \overline{\Omega}$ un transcrito extendido. Dado un tono $t \in T$ fijo, se denota

$$\Omega(t) := \left\{ (x^q, y^q) \;\middle|\; (x^q, y^q, t) \in \overline{\Omega} \right\}$$

como el conjunto de transcritos simples. Luego, para un distinguidor genérico de F y G se sigue que

$$\Pr\left[\, \mathfrak{b}(\mathcal{A}y^q) = 1 \,\right] \leq \Pr\left[\, \mathfrak{b}(\mathcal{A}y^q, t) = 1 \,\right]$$

Esto se debe a que el adversario podría elegir no usar la información de t para decidir el valor de $\mathfrak{b}$.

$$\therefore \quad \langle F, G \rangle \;\leq\; \langle \overline{F}, \overline{G} \rangle \;\leq\; \left\| \, \overline{F} - \overline{G} \, \right\|$$

Enseguida, de la Proposición 7.2.2 sabemos que existe un transcrito $(x^q, y^q, t) \in \mathbb{B}$ tal que

$$\frac{\Pr\left[\, F(a^q) = b^q, T = t \,\right]}{\Pr\left[\, G(a^q) = b^q, T' = t \,\right]} \;\geq\; \frac{\Pr\left[\, F(a^q) = b^q \,\right]}{\Pr\left[\, G(a^q) = b^q \,\right]} \;\geq\; 1 - \alpha$$

Como la variable T es independiente de F y G, se cumple la desigualdad izquierda. Paralelamente, la cantidad de transcritos $\tau(\mathcal{A}^{\overline{G}}) \notin \mathbb{B}$ está acotada por β. En consecuencia, aplicando el Corolario 7.2.3 se infiere que

$$\left\| \, \overline{F} - \overline{G} \, \right\| \leq \alpha + \beta$$

En conclusión, la ventaja para distinguir cualesquiera dos sistemas está acotada de la manera deseada. □

Observe cómo hemos especificado un conjunto de transcritos buenos bien definido que nos permite acotar la distancia estadística entre dos sistemas de respuesta, en general.

Cabe mencionar que existe otra forma equivalente de formular el teorema del coeficiente H extendido propuesta por Hoang y Tessaro (2016). Esta técnica, más conocida como **método del valor esperado**, permite alcanzar una seguridad muy estrecha, al encontrar una función negligible,

$$\epsilon_{opt}\left(\overline{\tau}\right) = \begin{cases} 1 - \frac{\mathbb{P}^{\overline{F}_k}(x^q, y^q, s)}{\mathbb{P}^{\mathrm{O}}(x^q, y^q, s)} & \mathbb{P}^{\mathrm{O}}(x^q, y^q, s) > \mathbb{P}^{\overline{F}_k}(x^q, y^q, s) \\ 0 & \textit{de lo contrario} \end{cases}$$

de tal manera que un distinguidor cualquiera tiene ventaja

$$\langle F, G\rangle \;\leq\; \left\| \tau(\mathcal{A}^{\overline{F}}) - \tau(\mathcal{A}^{\overline{G}}) \right\| \;=\; \mathrm{Ex}\left[\epsilon_{opt}\left(\tau(\mathcal{A}^{\mathbb{O}})\right)\right]$$

de modo que la igualdad se cumple gracias al Corolario 7.2.3. Advierta cómo este resultado es un caso particular para los parámetros óptimos $\alpha = \epsilon_{opt}$ y $\beta = 0$ que garantizan la inexistencia de transcritos malos. Como el nombre del método lo indica, esta técnica permite alcanzar optimalidad siempre y cuando se pueda calcular el valor esperado con precisión y facilidad.

En el siguiente capítulo, veremos un ejemplo claro (el ZMAC) y mostraremos cómo elegir los parámetros adecuados para un transcrito bueno, así como su utilidad para las pruebas de seguridad en esquemas de seguridad y autenticación.

Capítulo 8

Caso de estudio

Una de las propuestas más recientes respecto a esquemas de autenticación de mensajes es el modo de operación propuesto por Iwata et al. (2017), denominado **ZMAC**. A diferencia, de otros modos de operación basados en cifradores por bloques (BC), ZMAC permite emplear cifradores por bloques entonables (TBC). Esto es una gran mejor, puesto que los MAC basados en BC solamente procesan n bits por ejecución, mientras que ZMAC nos permite alcanzar $n+t$ bits por ejecución. En resumen, ZMAC es un esquema que nos permite alcanzar seguridad más allá de la cota de cumpleaños (BBB) con mayor cantidad de bits por ejecución, completamente paralelizable y adaptable para cualquier TBC.

En este capítulo abordaremos en profundidad todos los aspectos técnicos de ZMA. Se hará énfasis en las pruebas de seguridad y extenderemos el análisis de cada prueba mostrando cómo los teoremas de los Capítulos 4, 5 y 7 nos garantizan una firma infalsificable.

Si bien, antes de exponer los resultados principales, es necesario introducir algunos conceptos esenciales para la comprensión de este capítulo.

Definición 8.0.1. *Dado un número naturales k, se define la operación **one-zero-padding** para todo mensaje $\mathbf{M} \in \{0,1\}^*$ como*

$$ozp(\mathbf{M};\, k) := \begin{cases} \mathbf{M} & \text{si } k|m, \\ \mathbf{M}\|10^{\nu} & \text{de lo contrario.} \end{cases}$$

de modo que $\nu = (m \mod n+t) - 1$ es la cantidad de ceros para rellenar el mensaje y $m = |\mathbf{M}|$ es la longitud del mensaje.

Definición 8.0.2. *Sea $\mathbf{A} = \mathbf{a}_1, \mathbf{a}_2, \ldots \mathbf{a}_n$ una cadena de bits y sea*

$$\mathbf{A}_x := \mathbf{a}_n x^{n-1} + \mathbf{a}_{n-1} x^{n-2} + \cdots + \mathbf{a}_2 x + \mathbf{a}_1$$

*su representación como elemento del campo de Galois $\mathrm{GF}(2^n)$. Entonces, se define la operación **doubling** como*

$$2\mathbf{A}_x := x \cdot \sum_{i=0}^{n} \mathbf{a}_i x^{i-1} \mod p(x)$$

donde $p(x)$ es el polinomio primitivo o generador de $\mathrm{GF}(2^n)$.

Es oportuno mencionar que el grupo constituido por $\{0,1\}^n$ y la operación XOR es isomorfo a $(\mathrm{GF}(2^n), +)$. Esto implica que siempre existe una transformación inversa entre ambas representaciones $\mathbf{A} \equiv \mathbf{A}_x$. De este modo, la operación *doubling* está bien definida para cualquier cadena de bits. En particular, para $n = 128$ se tiene el campo de Galois $GF(2^{128})$ con el polinomio generador usual $x^{128} + x^7 + x^2 + x + 1$ tal que

$$2\mathbf{A} = \begin{cases} \mathbf{A} \ll 1 & \text{si } \mathbf{a}_1 = 0, \\ (\mathbf{A} \ll 1) \oplus (0^{120}10000111) & \text{si } \mathbf{a}_1 = 1. \end{cases}$$

En donde la operación XOR (denotado $\oplus$) y el corrimiento circular $\ll$ son definidos de la manera usual. Conjuntamente,

Definición 8.0.3. *Sean $\mathbf{X} \in \{0,1\}^n$ y $\mathbf{Y} \in \{0,1\}^t$. Se define la operación $\oplus_t$ como*

$$\mathbf{X} \oplus_t \mathbf{Y} := \begin{cases} \lceil\!\lceil \mathbf{X} \rceil\!\rceil^t \oplus \mathbf{Y} & \textit{si } t \leq n, \\ \mathbf{X} \| 0^{t-n} \oplus \mathbf{Y} & \textit{si } t > n. \end{cases}$$

Por consiguiente, la longitud total $|\mathbf{X} \oplus_t \mathbf{Y}| = t$ en cualquier caso. Ahora, se formaliza el estudio de los TBC con la siguiente definición:

Definición 8.0.4. *Un TBC $\overline{\mathcal{E}} : \{0,1\}^t \times \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ es una permutación entonable con espacio de claves $\{0,1\}^n$ y espacio de tonos $\{0,1\}^t$. Análogamente, un TBC es un BC $\{0,1\}^t$-extendido.*

Esto significa que $Dom(\overline{\mathcal{E}})$ corresponde con el conjunto de textos planos y $Ran(\overline{\mathcal{E}})$ con el conjunto de textos cifrados. Adicionalmente, $\overline{\mathcal{E}}_k^t$ denota una permutación específica determinada por t y k.

8.1. ZMAC

Para las siguientes definiciones sobre ZMAC deje que $\overline{\mathcal{E}} : K \times T_\mathfrak{I} \times \{0,1\}^n \to \{0,1\}^n$ sea un TBC con espacio de tonos $T_\mathfrak{I} := T \times \mathfrak{I}_9$, en donde el espacio $T = \{0,1\}^t$ se denomina el **tono mayor** y la secuencia $\mathfrak{I}_9$ el **tono menor**. Además, dado un índice m, se denota $X = X[1], \ldots, X[m]$ como una cadena de m bloques, tal que cada bloque $X[i] \in \{0,1\}^{n+t}$.

Definición 8.1.1. *Se define ZMAC como una PRF $\mathcal{Z}_{\mathrm{MAC}[\overline{\mathcal{E}}_k]} : K \times \{0,1\}^* \to \{0,1\}^{2n}$ con un espacio de mensajes de tamaño arbitrario tal que*

ALGORITMO $\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}(\,\mathbf{M}\,)$:
  $X \leftarrow \text{ozp}(\mathbf{M};\, n+t),\;\; m \leftarrow |\,\mathbf{M}\,|$ ◁ *con* $X = X[1], \ldots X[p] \in \{0,1\}^{n+t}$
  $(\mathbf{U}, \mathbf{V}) \leftarrow \mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,](X)$
  si $(n+t)|m$ **entonces**
    regresa $\mathbf{S} \leftarrow \mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]}(0, \mathbf{U}, \mathbf{V})$
  si no
    regresa $\mathbf{S} \leftarrow \mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]}(4, \mathbf{U}, \mathbf{V})$

Algoritmo 8.1.1: Función pseudoaleatoria ZMAC

Advierta que ZMAC fue diseñado sobre la base de los esquemas Hash-then-MAC, específicamente está inspirado en PMAC (Yasuda, 2011). Para comprender mejor la arquitectura de ZMAC tenga en cuenta la siguiente definición dada por Black y Rogaway (2000).

Definición 8.1.2. *Sea* $G : K \times \{0,1\}^* \to Y$ *una función hash acorde a la Definición 6.3.1 y sea* $F : L \times Y \to S$ *una familia de funciones. Dadas las claves* $k_0 \xleftarrow{\$} K$ *y* $k_1, k_2 \xleftarrow{\$} L$*, se define la* ***construcción Carter-Wegman*** *como*

$$\text{CW3}[G_{k_0}, F_{k_1}, F_{k_2}](m) := \begin{cases} F_{k_1}(G_{k_0}(\mathbf{M})) & \textit{si } (n+t)|m, \\ F_{k_2}(G_{k_0}(\mathbf{M})) & \textit{de lo contrario.} \end{cases}$$

tal que $m = |\mathbf{M}|$ *es la longitud del mensaje.*

En particular, $\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}$ es una instancia de la construcción $\text{CW3}\big[\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,], \mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]_0}, \mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]_4}\big]$ constituido de la función ZHASH casi-universal y la función pseudoaleatoria ZFIN. Más adelante, estudiaremos con detalle el funcionamiento de estos algoritmos en particular.

Por el momento, cabe destacar las siguientes propiedades computacionales de ZMAC:

1. Emplea una única clave $k \in K$.

2. Las ejecuciones del TBC $\overline{\mathcal{E}}$ son paralelizables.

3. Procesa en promedio $n+t$ bits por bloque $X[i]$.

4. Su seguridad está demostrada para una longitud total de

$$\sigma := \sum_{i=1}^{q} \big|X[i]\big| \;\leq\; 2^{\min\{n,(n+t)/2\}}$$

   con q bloques consultados por el adversario.

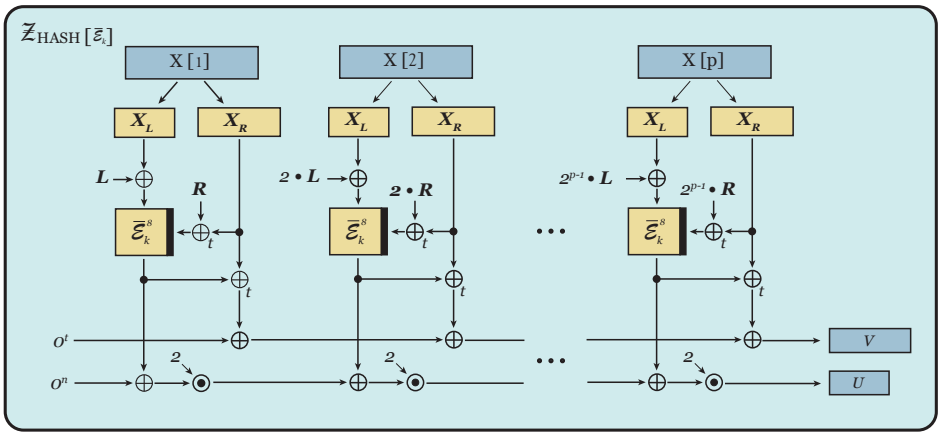

Figura 8.1: Diagrama del funcionamiento de ZHASH

8.2. ZHASH

En primer lugar, se define la función ZHASH para $t \leq n$, la que comprime las cadenas de bloques $\mathbf{X}^m$ obtenidas del mensaje. Recuerde que una función Hash es una función digesto que no puede ser invertida computacionalmente, y que posee cierta resistencia a las colisiones. En el Capítulo 6 se introdujo sobre los principios de las funciones Hash universales.

Definición 8.2.1. *Se define ZHASH como una función* $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,] : [\{0,1\}^{n+t}]^{(m)} \to \{0,1\}^n \times \{0,1\}^t$ *tal que*

ALGORITMO $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,](X)$:
  $U \leftarrow 0^n, \quad V \leftarrow 0^t$
  $\mathbf{L} \leftarrow \overline{\mathcal{E}}_k^9(0^t, 0^n), \quad \mathbf{R} \leftarrow \overline{\mathcal{E}}_k^9(0^{t-1}1, 0^n)$
  para cada $i \in \mathfrak{I}_p$ **haz**
    $(\mathbf{X}_L, \mathbf{X}_R) \leftarrow X[i]$ ◁ *Con* $|\mathbf{L}| = n$, $|\mathbf{R}| = t$ *y cada* $|X[i]| = n + t$
    $\mathbf{Z} \leftarrow \mathbf{X}_L \oplus \mathbf{L}, \quad \mathbf{T} \leftarrow \mathbf{X}_R \oplus_t \mathbf{R}$
    $\mathbf{Y}_L \leftarrow \overline{\mathcal{E}}_k^8(\mathbf{T}, \mathbf{Z})$
    $\mathbf{Y}_R \leftarrow \mathbf{Y}_L \oplus_t \mathbf{X}_R$
    $U \leftarrow 2(U \oplus \mathbf{Y}_L)$
    $V \leftarrow V \oplus \mathbf{Y}_R$
    $(\mathbf{L}, \mathbf{R}) \leftarrow (2\mathbf{L}, 2\mathbf{R})$
  regresa (U, V)

Algoritmo 8.2.1: Algoritmo de compresión ZHASH

Para entender mejor la función ZHASH, estudie el diagrama en la Figura 8.1. A continuación, explicaremos los dos casos posibles:

- Para un tono $t \leq n$, en $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,]$ se calculan dos máscaras: una izquierda $\mathbf{L} := \overline{\mathcal{E}}_k^9(0^t, 0^n)$ y una derecha $\mathbf{R} := \overline{\mathcal{E}}_k^9(0^{t-1}1, 0^n)$. Ambas de la misma longitud $|\mathbf{L}| = |\mathbf{R}| = n$.

  Dada una cadena de bloques $X := X[1], \ldots, X[p]$, el algoritmo $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,]$ divide cada bloque $\mathbf{X}[i]$ en dos partes: se define $\mathbf{X}_L[i] := \lceil\!\lceil X[i] \rceil\!\rceil^n$ como la entrada del TBC y $\mathbf{X}_R[i] := \lfloor\!\lfloor \mathbf{X}[i] \rfloor\!\rfloor_t$ como el tono del TBC. Entonces, para cada índice $i \leq p$ se calcula

$$\mathbf{Y}_L[i] = \overline{\mathcal{E}}_k^8(2^{i-1}\mathbf{R} \oplus_t \mathbf{X}_R[i],\ 2^{i-1}\mathbf{L} \oplus \mathbf{X}_L[i]) \tag{8.1}$$
$$\mathbf{Y}_R[i] = \mathbf{Y}_L[i] \oplus_t \mathbf{X}_R[i] \tag{8.2}$$

  Aprecie como las variables latentes $\mathbf{T}$ y $\mathbf{Z}$ corresponden al tono y la entrada del TBC $\overline{\mathcal{E}}^8$. Adicionalmente, $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,]$ calcula las variables U, V recursivamente:

$$U = \bigoplus_{i=1}^{p} 2^{p-i+1}\mathbf{Y}_L[i] \tag{8.3}$$
$$V = \bigoplus_{i=1}^{p} \mathbf{Y}_R[i] \tag{8.4}$$

  De esta manera, ZHASH requiere una ejecución del TBC $\overline{\mathcal{E}}$ y tres *doublings* en $\text{GF}(2^n)$ por cada bloque de $n + t$ bits. Esto, sin contar las dos ejecuciones iniciales para generar las máscaras $\mathbf{L}$ y $\mathbf{R}$.

- Para un tono $t > n$, se calculan las máscaras de la misma manera que el caso anterior. Enseguida las variables U y V se calculan conforme a las ecuaciones (8.3) y (8.4). Examine cómo $(U, \lceil\!\lceil V \rceil\!\rceil^n)$ son los variables correspondientes al caso $t = n$. En cambio, denotamos

$$W := \lfloor\!\lfloor V \rfloor\!\rfloor_{t-n} = \lfloor\!\lfloor \mathbf{X}_R[1] \rfloor\!\rfloor_{t-n} \oplus \cdots \oplus \lfloor\!\lfloor \mathbf{X}_R[m] \rfloor\!\rfloor_{t-n} \tag{8.5}$$

  como los $t - n$ bits restantes de V. Esto, lo hacemos con el fin de estudiar por separado las variables (U, V) para el caso $t = n$ y facilitar la demostración de seguridad al final de esta sección. De igual manera, vea cómo W depende únicamente de los bloques del mensaje $X[1], \ldots, X[p]$.

Observe que el algoritmo $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,]$ puede ser considerado como un algoritmo recursivo: el caso base (núcleo) calcula el par $(\mathbf{Y}_L, \mathbf{Y}_R)$ y el paso recursivo computa los valores (U, V). Por esta razón, primero describimos la siguiente construcción:

Definición 8.2.2. *Sea $\overline{\mathcal{P}} : K \times \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ una permutación entonable y sea $\mathcal{H} : \text{Ł} \times S \to \{0,1\}^n \times \{0,1\}^t$ una familia de funciones. Dadas las claves $k \xleftarrow{\$} K$ y $\ell \xleftarrow{\$} \text{Ł}$, se define el* ***esquema Xor-Tweak*** $\text{XT}[\,\overline{\mathcal{P}}, \mathcal{H}\,]$ *como*

$$\text{XT}[\,\overline{\mathcal{P}}, \mathcal{H}\,]_{k,\ell} := \overline{\mathcal{P}}_k\,(\mathbf{T}, \mathbf{W} \oplus \mathbf{X})\ \textit{con}\ \mathcal{H}_\ell(g) := (\mathbf{W},\ \mathbf{T}) \tag{8.6}$$

Este esquema *Xor-Tweak* es un diseño genérico propuesto por Minematsu y Iwata (2015) para procesar bloques en paralelo con seguridad CPA. En específico, ZHASH emplea el esquema denotado $\overline{XE} := \mathrm{XT}[\,\overline{\mathcal{E}}^{8}, \mathcal{H}\,]$, que mapea

$$\overline{XE}:\ \ (\mathbf{X}_R, (\mathbf{X}_L, i)) \mapsto \overline{\mathcal{E}}_k^8(2^{i-1}\mathbf{R} \oplus_t \mathbf{X}_R[i],\ 2^{i-1}\mathbf{L} \oplus \mathbf{X}_L[i]) \tag{8.7}$$

en donde $\overline{\mathcal{E}}_k^8$ es una permutación dada por el tono 8 y la clave k de nuestro TBC, en tanto que $\mathcal{H}$ es una función que cumple la Definición 6.3.3. Este esquema es el componente nuclear del algoritmo $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,]$ y nos permite procesar $2^n - 1$ bloques por ejecución.

Al mismo tiempo, para poder estudiar la seguridad de esta construcción, definimos el objeto ideal $\overline{XP} := \mathrm{XT}[\overline{\pi}, \mathcal{H}]$ como el esquema *Xor-Tweak* que emplea una TURP $\overline{\pi}$ como primitiva criptográfica.

8.2.1. $\mathcal{H}$ como función parcialmente Casi-Xor-Universal

Una pieza crucial para el desarrollo del esquema $\overline{XE}$ fue encontrar una familia de funciones con buena resistencia a las colisiones.

Definición 8.2.3. *Sea $\mathcal{H} : Ł \times S \to \{0,1\}^n \times \{0,1\}^t$ una familia de funciones con espacio de claves $Ł = \{0,1\}^n \times \{0,1\}^n$ y dominio $s = \{0,1\}^t \times \mathfrak{I}_{2^n-1}$. Dados $\mathbf{L}, \mathbf{R} \xleftarrow{\$} Ł$, se define*

$$\mathcal{H}_{\mathbf{L},\mathbf{R}}(\mathbf{S}, i) := (2^{i-1}\mathbf{L}, 2^{i-1}\mathbf{R} \oplus_t \mathbf{S})$$

Para evaluar la seguridad del núcleo de ZHASH, primero probaremos que $\mathcal{H}$ es una función Hash adecuada.

Lema 8.2.4. *La función $\mathcal{H}$ es pAXU respecto a (n, t, ϵ) de modo que*

$$\epsilon(n,t) = \frac{1}{2^{n+\min\{n,t\}}}$$

Demostración. Se denota la probabilidad de colisión de $\mathcal{H}$ como

$$\mathcal{C}(\mathcal{H}, T, T') := \Pr_{\mathbf{L},\mathbf{R}\leftarrow Ł}\left[\mathcal{H}_{\mathbf{L},\mathbf{R}}(\mathbf{S}, i) \oplus \mathcal{H}_{\mathbf{L},\mathbf{R}}(\mathbf{S}', j) = (\delta, 0^t)\right]$$

para dos tonos $\mathbf{S} \neq \mathbf{S}'$ distintos. Luego, tenga en cuenta los dos casos siguientes:

$(\leq)$ Suponga $t \leq n$. Entonces por la Definición 8.0.3, se sigue que

$$\begin{aligned}(\delta, 0^t) &= \left(2^{i-1}\mathbf{L},\ 2^{i-1}\mathbf{R} \oplus_t \mathbf{S}\right) \oplus \left(2^{j-1}\mathbf{L},\ 2^{j-1}\mathbf{R} \oplus_t \mathbf{S}'\right) \\ &= \left(2^{i-1}\mathbf{L},\ \left\lceil 2^{i-1}\mathbf{R}\right\rceil^t \oplus \mathbf{S}\right) \oplus \left(2^{j-1}\mathbf{L},\ \left\lceil 2^{j-1}\mathbf{R}\right\rceil^t \oplus \mathbf{S}'\right) \\ &= \left(2^{i-1}\mathbf{L} \oplus 2^{j-1}\mathbf{L},\ \left\lceil 2^{i-1}\mathbf{R} \oplus 2^{j-1}\mathbf{R}\right\rceil^t \oplus \mathbf{S} \oplus \mathbf{S}'\right)\end{aligned}$$

Como $\mathbf{R}, \mathbf{L}$ y $\mathbf{S}, \mathbf{S}'$ son independientes, entonces se pueden escribir las ecuaciones

$$\begin{aligned} \delta &= (2^{i-1} + 2^{j-1})\mathbf{L} \\ \Delta S &= \llbracket (2^{i-1} + 2^{j-1})\mathbf{R} \rrbracket^t \end{aligned}$$

en donde $\Delta S := \mathbf{S} \oplus \mathbf{S}'$, acorde a la Proposición 3.1.6. Además, denotamos $\lambda_h = 2^{i-1} + 2^{j-1}$ con $h < n$, para facilitar los cálculos. Note cómo $i = j$ implica que

$$\llbracket 2^{i-1}\mathbf{R} \rrbracket^t \oplus \llbracket 2^{i-1}\mathbf{R} \rrbracket^t \;=\; 0^t \;\neq\; \Delta S$$

Esto se debe a que $\mathbf{S}$ y $\mathbf{S}'$ son distintos. Por consiguiente, sólo es necesario tener en cuenta los $i \neq j$ para que 2^h sea un elemento distinto del nulo. También, aprecie cómo $\llbracket \lambda_h \mathbf{R} \rrbracket^t$ cumple con las características de la Proposición 3.1.7.

$$\begin{aligned} \therefore \quad \mathcal{C}(\mathcal{H}, \mathbf{S}, \mathbf{S}') &= \Pr_{\mathbf{L},\mathbf{R} \leftarrow \mathbb{L}} \begin{bmatrix} \delta = \lambda_h \mathbf{L} \\ \Delta S = \llbracket \lambda_h \mathbf{R} \rrbracket^t \end{bmatrix} \\ &= \Pr\left[\, \delta = \lambda_h \mathbf{L} \,\right] \cdot \Pr\left[\, \Delta S = \llbracket \lambda_h \mathbf{R} \rrbracket^t \,\right] \\ &= \frac{1}{2^n} \cdot \frac{1}{2^t} \;=\; \frac{1}{2^{t+n}} \end{aligned}$$

Ya que δ y ΔS son elementos fijos, el cómputo de la probabilidad se determina por la distribución de las variables $\lambda_h \mathbf{R}, \lambda_h \mathbf{L}$ sobre $GF(2^n)$.

$(>)$ Suponga $t > n$. Entonces,

$$\begin{aligned} (\delta, 0^t) &= \left(2^{i-1}\mathbf{L},\, 2^{i-1}\mathbf{R} \oplus_t \mathbf{S} \right) \oplus \left(2^{j-1}\mathbf{L},\, 2^{j-1}\mathbf{R} \oplus_t \mathbf{S}' \right) \\ &= \left(2^{i-1}\mathbf{L},\, 2^{i-1}\mathbf{R} \| 0^{t-n} \oplus \mathbf{S} \right) \oplus \left(2^{j-1}\mathbf{L},\, 2^{j-1}\mathbf{R} \| 0^{t-n} \oplus \mathbf{S}' \right) \\ &= \left(2^{i-1}\mathbf{L} \oplus 2^{j-1}\mathbf{L},\, (2^{i-1}\mathbf{R} \oplus 2^{j-1}\mathbf{R}) \| 0^{t-n} \oplus \mathbf{S} \oplus \mathbf{S}' \right) \end{aligned}$$

De manera similar al caso anterior, se escribe el sistema de ecuaciones

$$\begin{aligned} \delta &= (2^{i-1} + 2^{j-1})\mathbf{L} \\ \Delta T &= (2^{i-1} + 2^{j-1})\mathbf{R} \| 0^{t-n} \end{aligned}$$

Para computar la probabilidad de colisión, tenga en cuenta que ΔT y 0^{t-n} son elementos fijos. Esto implica que existe la posibilidad de que $\lfloor\!\lfloor \Delta S \rfloor\!\rfloor_{t-n} \neq 0^{t-n}$.

$$\begin{aligned} \therefore \quad \mathcal{C}(\mathcal{H}, T, T') &= \Pr_{\mathbf{L},\mathbf{R}} \begin{bmatrix} \delta = \lambda_h \mathbf{L} \\ \Delta S = (\!| \lambda_h \mathbf{R} \| 0^{t-n} |\!) \end{bmatrix} \\ &= \Pr\left[\, \delta = \lambda_h \mathbf{L} \,\right] \cdot \Pr\left[\, \Delta S = (\!| \lambda_h \mathbf{R} \| 0^{t-n} |\!) \,\right] \\ &\leq \frac{1}{2^n} \cdot \Pr\left[\, \llbracket \Delta S' \rrbracket^n = \lambda_h \mathbf{R} \,\right] \;\leq\; \frac{1}{2^{n+n}} \end{aligned}$$

En virtud de que descartamos la información de los últimos $t - n$ bits, podemos obtener una cota superior.

De ambos casos,

$$\max_{\mathbf{S}\neq\mathbf{S}'} \Pr_{\mathbf{L},\mathbf{R}\leftarrow Ł}\left[\mathcal{H}_{\mathbf{L},\mathbf{R}}(\mathbf{S},i)\oplus\mathcal{H}_{\mathbf{L},\mathbf{R}}(\mathbf{S}',j)=(\Delta,0^t)\right]\leq\frac{1}{2^{n+\min\{n,t\}}}$$

En conclusión, $\mathcal{H}$ es una función pAXU.

□

Ya demostrado que la construcción $\mathrm{XT}[\overline{\mathcal{E}}^8,\mathcal{H}]$ cuenta con un TBC y una función HASH, se procede a probar la seguridad del esquema completo.

8.2.2. Seguridad del esquema $\overline{XP}$

Para demostrar la seguridad del núcleo de ZHASH, considere los siguientes preliminares (únicamente para esta sección):

Sea $\mathcal{A}\in CCA$ un adversario cuyo objetivo es distinguir $\overline{XP}$ de una TURP $\widehat{P}$, usando a lo más q consultas con capacidad de cómputo ilimitada. Sin perdida de generalidad, podemos asumir un transcrito ℓ-extendido para un distinguidor genérico como

$$\tau(\mathcal{A}^{\overline{\mathrm{O}}})=((s_1,x_1,y_1),\ldots,(s_q,x_q,y_q),\ell)$$

de tal manera que cada s_i es el tono mayor, cada x_i es la entrada, cada y_i es la salida y ℓ es la clave de $\mathcal{H}$. Asimismo, la estrategia del adversario consiste en consultar de manera adaptativa secuencias (s^q,x^q) y obtener respuestas (y^q,ℓ).

Para el mundo real: $\overline{XP}$ se construye con una TURP $\overline{\pi}\xleftarrow{\$} T\times Y^\dagger$ y una función pAXU $\mathcal{H}:Ł\times S\to W\times T$, de tal manera que

$$\mathcal{H}_\ell(s_i)=(w_i,t_i) \tag{8.8}$$
$$z_i=x_i+w_i \tag{8.9}$$
$$y_i=\overline{\pi}(t_i,z_i) \tag{8.10}$$

Abusando de la notación, la ecuación (8.8) representa dos elementos $w_i\in\mathrm{GF}(2^n)$ y $t_i\in\mathrm{GF}(2^t)$ dados por la imagen de $\mathcal{H}_\ell(s_i)$. Recuerde que ésta es una representación equivalente para $W=\{0,1\}^n$ y $T=\{0,1\}^t$.

De este modo, (8.9) es el proceso de enmascarar las entradas de la TURP, tal que $x_i+w_i\in\mathrm{GF}(2^n)$. Por último, (8.10) expresa la salida de $\overline{XP}$ como $y_i\in\mathrm{GF}(2^{n+t})$.

Para el mundo ideal: $\varpi\xleftarrow{\$} S\times\mathrm{GF}(2^{n+t})^\dagger$ es una TURP que mapea

$$(s_i,x_i)\ \mapsto\ y_i=\varpi(s_i,x_i) \tag{8.11}$$

Observe que los valores (w_i,z_i,t_i) no tienen sentido alguno en el mundo ideal. Por este motivo, asuma que las variables son dependientes de una clave $\ell\xleftarrow{\$}Ł$.

Expuesto ambos mundos, aprecie cómo el transcrito τ determina de manera única los valores (w_i, z_i, t_i), de acuerdo a lo siguiente:

Definición 8.2.5. *El conjunto de transcritos buenos de $\overline{XP}$ se define como*

$$\mathbb{B} = \left\{ \tau(\mathcal{A}^{\overline{\mathrm{O}}}) \mid \forall j > i : (z_i, t_i) \neq (z_j, t_j) \right\}$$

Esta definición implica que no existen colisiones en el dominio de $\overline{\pi}$. Esto es importante, puesto que el adversario puede encontrar colisiones triviales $y_i = y_j$ en el mundo real simplemente seleccionando valores (s^q, x^q) que cumplan $(z_i, t_i) = (z_j, t_j)$.

Para asegurarnos de que $\mathbb{B}$ es también un conjunto bueno respecto a $\alpha, \beta \in [0, 1]$, se enuncian los siguientes lemas:

Lema 8.2.6. *Todo transcrito bueno de $\overline{XP}$ satisface*

$$\frac{\Pr\left[\, \overline{\mathbb{XP}} = \tau \,\right]}{\Pr\left[\, \varpi = \tau \,\right]} \geq 1$$

Demostración. Sea $\tau = (s^q, x^q, y^q)$ un transcrito bueno. Entonces, la probabilidad del oráculo ideal es

$$\begin{aligned} \Pr\left[\, \varpi = \tau \,\right] &= \Pr\left[\, \varpi(s^q, x^q) = y^q,\ L = \ell \,\right] && (8.12)\\ &= \Pr\left[\, \varpi(s^q, x^q) = y^q \,\right] \cdot \Pr\left[\, L = \ell \,\right] && (8.13)\\ &= \frac{1}{|Ł|} \prod_{i=1}^{q} \frac{1}{2^n - a_i} && (8.14) \end{aligned}$$

donde a_i es la cantidad de $i < j$ entradas consultadas con el mismo tono mayor $g_j = s_i$.

Luego, recuerde que el transcrito determina de manera única el tono menor y la entrada de $\overline{\pi}$ a través del sistema de ecuaciones anterior. Por lo cual, la probabilidad del oráculo real es

$$\begin{aligned} \Pr\left[\, \overline{\mathbb{XP}} = \tau \,\right] &= \Pr\left[\, \overline{\pi}(t^q, z^q) = y^q,\ L' = \ell \,\right] && (8.15)\\ &= \Pr\left[\, \overline{\pi}(t^q, z^q) = y^q \,\right] \cdot \Pr\left[\, L = \ell \,\right] && (8.16)\\ &= \frac{1}{|Ł|} \prod_{i=1}^{q} \frac{1}{2^n - b_i} && (8.17) \end{aligned}$$

donde b_i es la cantidad de $i < j$ entradas consultadas con el mismo tono menor $t_i = t_j$.

- Supongamos que $s_i = s_j$. De (8.8),

  $$\mathcal{H}_\ell(s_i) = (w_i, t_i) = (w_j, t_j) = \mathcal{H}_\ell(s_j)$$

  Por consiguiente, $w_i = w_j$. Por definición de $\mathbb{B}$ y de (8.9), se infiere que

  $$z_i = x_i \oplus w_i \neq x_j \oplus w_j = z_j$$

  En consecuencia, la cantidad de índices en a_i está dado por la cantidad de $x_i \neq x_j$ bajo control del adversario.

- Supongamos ahora que $t_i = t_j$. De nuevo, se deduce que $z_i \neq z_j$ acorde a la definición de transcrito bueno.

  Esto implica que la cantidad de índices en b_i depende de la cantidad de $x_i \neq x_j$ distintos o de los $w_i \neq w_j$ distintos. Paralelamente, percátese cómo cada (w_i, t_i) está en correspondencia con un s_i bajo control del adversario, gracias a la función $\mathcal{H}_\ell$.

$$\begin{aligned} \therefore \quad b_i &= \left| \left\{ i < j \mid x_i \neq x_j \right\} \cup \left\{ i < j \mid s_i \neq s_j \right\} \right| && (8.18) \\ &\geq \left| \left\{ i < j \mid x_i \neq x_j \right\} \right| = a_i && (8.19) \end{aligned}$$

Por último, al aplicar (8.14), (8.17) en (8.19)se cumple que

$$\begin{aligned} 2^n - b_i &\leq 2^n - a_i \\ \frac{1}{2^n - a_i} &\leq \frac{1}{2^n - b_i} \\ \prod_{i=1}^{q} \frac{1}{2^n - a_i} &\leq \prod_{i=1}^{q} \frac{1}{2^n - b_i} \\ \Pr\left[\varpi = \tau \right] &\leq \Pr\left[\overline{\mathbb{XP}} = \tau \right] \end{aligned}$$

En conclusión, se satisface la hipótesis para el parámetro α.

□

Adicionalmente, debemos comprobar que la Definición 8.2.5 cumple con la hipótesis de los coeficientes H.

Lema 8.2.7. *Para todo transcrito malo se satisface*

$$\Pr\left[\tau(\mathcal{A}^{\varpi}) \notin \mathbb{B} \right] \leq \frac{q^2}{2}\epsilon$$

Demostración. De la Definición 8.2.5 se sabe que el conjunto de transcritos malos es

$$\mathbb{B}^{\mathfrak{C}} = \left\{ \tau \mid \exists i < j : (z_i, t_i) = (z_j, t_j) \right\}$$

Advierta cómo cualquier estrategia del adversario para distinguir ϖ de $\overline{XP}$ implica encontrar un transcrito malo.

Entonces, en el mundo ideal, las variables s_i, t_i, w_i son dependientes de la distribución de ℓ.

$$\begin{aligned}
\therefore \quad \Pr\left[\,\tau(\mathcal{A}^{\varpi}) \notin \mathbb{B}\,\right] &\leq \max_{CCA} \Pr\left[\,\big((s^q, x^q, y^q), \ell\big) \in \mathbb{B}^{\mathfrak{C}}\,\right] \\
&= \max_{(s_i,x_i)\neq(s_j,x_j)} \sum_{i<j\leq q} \Pr\left[\,(z_i, t_i) = (z_j, t_j)\,\right] \\
&= \max_{(s_i,x_i)\neq(s_j,x_j)} \sum_{i<j\leq q} \Pr_{\ell\leftarrow \text{L}} \left[(x_i + w_i, t_i) = (x_j + w_j, t_j)\right] \\
&= \max_{(s_i,x_i)\neq(s_j,x_j)} \sum_{i<j\leq q} \Pr_{\ell\leftarrow \text{L}} \left[(w_j + w_i, t_j + t_i) = (x_j + x_i, 0)\right] \\
&= \max_{(s_i,x_i)\neq(s_j,x_j)} \sum_{i<j\leq q} \Pr_{\ell\leftarrow \text{L}} \left[(w_j, t_j) + (w_i, t_i) = (\Delta x, 0)\right] \\
&\leq \sum_{i<j\leq q} \max_{(s_i,x_i)\neq(s_j,x_j)} \Pr_{\ell\leftarrow \text{L}} \left[\mathcal{H}_\ell(s_i) + \mathcal{H}_\ell(s_j) = (\Delta x, 0)\right] \\
&\leq \sum_{i<j\leq q} \epsilon \quad = \binom{q}{2} \cdot \epsilon \quad = \frac{q \cdot (q-1)}{2}\epsilon
\end{aligned}$$

donde $\Delta x := x_i + x_j \in \text{GF}(2^n)$. Vea cómo el Lema 8.2.4 se emplea para acotar los transcritos malos. En conclusión, se satisface la hipótesis para el parámetro β.

□

De esta manera, demostramos que la definición de transcritos buenos es suficiente para garantizar la seguridad del esquema $\overline{XP}$. A continuación, terminaremos la prueba considerando el esquema nuclear de ZHASH.

Corolario 8.2.8. *Sea $\overline{XP}$ el esquema de la Definición 8.2.2, con una TURP $\overline{\pi} : \{0,1\}^t \times \{0,1\}^n \to \{0,1\}^n$ y ses $\mathcal{H}$ una función acorde a la Definición 8.2.3. Por lo tanto, la seguridad incondicional del esquema como TPRP es*

$$\mathbf{Adv}^{\text{TPRP}}_{\overline{XP}} \leq \frac{q^2}{2^{n+1+\min\{n,t\}}}$$

para todo adversario realizando a lo más q consultas.

Demostración. De los Lemas 8.2.6 y 8.2.7, se deduce que $\alpha = 0$ y $\beta = q^2\epsilon/2$. Finalmente, al aplicar el Teorema 7.2.5 se concluye la prueba.

□

Así, queda demostrada la seguridad del núcleo $\overline{XP}$. Más adelante, explicaremos cómo sustituir el esquema real $\mathcal{Z}_{\text{HASH}}[\,\overline{\mathcal{E}}\,]$ en el esquema ideal $\mathcal{Z}_{\text{HASH}}[\,\overline{\pi}\,]$. Por el momento, estudiaremos a ZHASH como si fuera el esquema ideal.

8.2.3. ZHASH como función hash universal

Como comprobamos en la sección anterior, el caso base de ZHASH es seguro, sin embargo, ZMAC pide una función hash ϵ-universal para completar la construcción Carter-Wegman.

Para ello, considere la siguiente función:

$$\mathcal{Z}_{\text{HASH}}[\,\overline{XP}\,]:\ ozp(\mathbf{M}) \mapsto XT[\pi, \mathcal{H}]_{k,\ell}(X)$$

que mapea cada mensaje $\mathbf{M}$ a un hash creado por $\overline{XP}$, de acuerdo a la Definición 8.2.2. Para mostrar que ZHASH es una función resistente a las colisiones, efectuaremos el mismo análisis realizado en el artículo Iwata et al., 2017.

Lema 8.2.9. *Para toda $m, m' \leq \sqrt{\epsilon}$, la probabilidad de colisión de $\mathcal{Z}_{\text{HASH}}[\,\overline{XP}\,]$ es*

$$\mathcal{C}(\mathcal{Z}_{\text{HASH}}[\,\overline{XP}\,], m, m') \ \leq\ \frac{4}{2^{n+\min\{n,t\}}} \ =\ \epsilon$$

Demostración. Deje que $\Delta V := V + V'$ y $\Delta U := U + U'$. Entonces, la probabilidad de colisión de ZHASH es

$$\mathcal{C}(\mathcal{Z}_{\text{HASH}}[\,\overline{XP}\,], m, m') = \Pr\left[\begin{array}{ll} \Delta U & = 0^n \\ \Delta V & = 0^t \end{array}\right]$$

Ahora, conforme a las ecuaciones (8.3) y 8.4 se tiene el sistema de ecuaciones

$$\Delta U = \bigoplus_{i=1}^{m} 2^{m-i+1}\mathbf{Y}_L[i] + \bigoplus_{j=1}^{m'} 2^{m'-j+1}\mathbf{Y}'_L[j]$$
$$\Delta V = \bigoplus_{i=1}^{m} \mathbf{Y}_R[i] + \bigoplus_{j=1}^{m'} \mathbf{Y}'_R[j]$$

Por el Corolario 8.2.8, el mapa $\overline{XP}$ es una permutación entonable aleatoria.

$$\overline{XP}:\ \big(\mathbf{X}_R, [\mathbf{X}_L, i]\big) \mapsto \overline{\pi}(2^{i-1}\mathbf{R} \oplus_t \mathbf{X}_R[i],\ 2^{i-1}\mathbf{L} \oplus \mathbf{X}_L[i]) \tag{8.20}$$

Observe cómo está es la misma Construcción 8.7 para una TURP $\overline{\pi}$. De este modo, de (8.1) y (8.2), se sigue que la variable $\mathbf{Y}_L[i]$ es independiente de cada bloque $\mathbf{X}[i] = \mathbf{X}_R[i] \| \mathbf{X}_L[i]$, a su vez, $\mathbf{Y}_L[j]$ es independiente de $\mathbf{Y}_R[i], \mathbf{Y}_L[i]$ para cada $i > j$.

Por consiguiente, evaluamos los siguientes casos con $t \leq n$:

- Para $m' = m$:
  - Suponga que existe un $h \in \mathfrak{I}_m$ tal que $\mathbf{X}[h] \neq \mathbf{X}'[h]$ y que $\mathbf{X}[i] = \mathbf{X}'[i]$ para todo $i \neq h$. Entonces,

$$\Delta U \ =\ \bigoplus_{i=1}^{m} 2^{m-i+1}\underbrace{\big(\mathbf{Y}_L[i] + \mathbf{Y}'_L[i]\big)}_{\Delta L} \ =\ 2^{m-h+1}\Delta L \ \neq\ 0^n$$

donde se deduce que $\mathbf{Y}_L[h] \neq \mathbf{Y}'_L[h]$ puesto que son una permutación de $\mathbf{X}[h]$ y $\mathbf{X}'[h]$, respectivamente. De lo contrario,

$$\Delta V \;=\; \bigoplus_{i\leq m} \underbrace{\big(\mathbf{Y}_R[i] + \mathbf{Y}'_R[i]\big)}_{\Delta R} \;=\; \Delta R[h] \;=\; \mathbf{X}_R[\ell] \oplus \mathbf{X}'_R[\ell] \;\neq\; 0^t$$

Esto implica que no puede existir una colisión para un único índice h.

- Suponga dos índices $h, s \in \mathfrak{I}_m$ que satisfacen $\mathbf{X}[h] \neq \mathbf{X}'[h]$ y $\mathbf{X}[s] \neq \mathbf{X}'[s]$. Entonces,

$$\Delta U \;=\; 2^{m-h+1}\Delta L[h] + 2^{m-s+1}\Delta L[s] + \underbrace{\bigoplus_{i\notin\{h,s\}} 2^{m-i+1}\Delta L[i]}_{\delta_1}$$

$$\Delta V \;=\; \Delta R[h] + \Delta R[s] + \underbrace{\bigoplus_{i\notin\{h,s\}} \Delta R[i]}_{\delta_2}$$

Observe que Δ_1 y Δ_2 son variables independientes de $(\Delta R[h], \Delta L[h])$ y $(\Delta R[s], \Delta L[s])$ a causa de la separación de dominios en la Construcción 8.20. Además, los índices h y s determinan tonos distintos a los tonos dependientes de i.

Deje que $\lambda_h = 2^{m-h+1}, \lambda_s = 2^{m-s+1}$ y considere una colisión

$$\begin{bmatrix} \Delta U & = 0^n \\ \Delta V & = 0^t \end{bmatrix} \Leftrightarrow \begin{bmatrix} \lambda_h\Delta L[h] \oplus \lambda_s\Delta L[s] & = \delta_1 \\ \Delta R[h] \oplus \Delta R[s] & = \delta_2 \end{bmatrix}$$
$$\Leftrightarrow \begin{bmatrix} \lambda_h\Delta L[h] \oplus \lambda_s\Delta L[s] & = \delta_1 \\ \lceil\!\lceil \Delta L[h] \oplus \Delta L[s] \rceil\!\rceil^t & = \delta_2 \oplus \mathbf{X}_R[h] \oplus \mathbf{X}'_R[h] \oplus \mathbf{X}_R[s] \oplus \mathbf{X}'_R[s] \end{bmatrix}$$

Podemos asumir el siguiente sistema equivalente:

$$\begin{pmatrix} \lambda_h & \lambda_s \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \Delta L[h] \\ \Delta L[s] \end{pmatrix} = \begin{pmatrix} \delta_1 \\ \delta_3 \end{pmatrix}$$

En virtud del caso anterior, se sabe que el determinante es $\lambda_h \oplus \lambda_s \neq 0$ porque h, s son distintos. De lo contrario, no es posible una colisión. Por ende, el mapa $\mathbf{X}[i] \mapsto (\delta_1, \delta_3)$ tiene una única solución. De este modo, la distribución de las variables se

encuentra sobre $\mathrm{GF}(2^n) \setminus \{0\}$ en el peor de los casos.

$$\begin{aligned}
\therefore \quad \Pr\begin{bmatrix} \Delta U &= 0^n \\ \Delta V &= 0^t \end{bmatrix} &\leq \max_{\substack{\delta_1 \in \mathrm{GF}(2^n) \\ \delta_2 \in \mathrm{GF}(2^t)}} \Pr\begin{bmatrix} \lambda_h \Delta L[h] \oplus \lambda_s \Delta L[s] &= \delta_1 \\ \lVert \Delta L[h] \oplus \Delta L[s] \rVert^t &= \delta_2 \end{bmatrix} \\
&\leq \max_{\substack{\delta_1 \in \mathrm{GF}(2^n) \\ \delta_2 \in \mathrm{GF}(2^t)}} \sum_{\substack{\delta_3 \in \mathrm{GF}(2^n) : \\ \lVert \delta_3 \rVert^t = \delta_2}} \Pr\begin{bmatrix} \lambda_h \Delta L[h] \oplus \lambda_s \Delta L[s] &= \delta_1 \\ \Delta L[h] \oplus \Delta L[s] &= \delta_3 \end{bmatrix} \\
&\leq \max_{\substack{\delta_1 \in \mathrm{GF}(2^n) \\ \delta_2 \in \mathrm{GF}(2^t)}} \sum_{\substack{\delta_3 \in \mathrm{GF}(2^n) : \\ \lVert \delta_3 \rVert^t = \delta_2}} \frac{1}{2^n - 1} \cdot \frac{1}{2^n - 1} \\
&\leq 2^{n-t} \cdot \frac{2}{2^n} \cdot \frac{2}{2^n} = \frac{4}{2^{n+t}}
\end{aligned}$$

- Para $m' \leq m + 1$, se tienen las ecuaciones

$$\begin{aligned}
\Delta U &= \bigoplus_{i \leq m} 2^{m-i+1} \mathbf{Y}_L[i] \oplus \bigoplus_{i \leq m+1} 2^{m+1-i+1} \mathbf{Y}'_L[i] \\
&= 2\big(\mathbf{Y}'_L[m+1] \oplus 2\mathbf{Y}'_L[m] \oplus \mathbf{Y}_L[m] \oplus \underbrace{\bigoplus_{i \leq m-1} 2^{m-i} \Delta L[i]}_{\delta_1}\big)
\end{aligned}$$

y

$$\begin{aligned}
\Delta V &= \bigoplus_{i \leq m} \mathbf{Y}_R[i] \oplus \bigoplus_{i \leq m+1} \mathbf{Y}'_R[i] \\
&= \lVert \mathbf{Y}'_L[m+1] \oplus 2\mathbf{Y}'_L[m] \oplus \mathbf{Y}_L[m] \rVert^t \oplus \underbrace{\bigoplus_{i \leq m-1} \Delta R[i]}_{\delta_2}
\end{aligned}$$

Conforme al caso anterior, se deduce que δ_1 y δ_2 son variables independientes de $\mathbf{Y}_L[m]$ y $\mathbf{Y}_L[m+1]$. Sean $A = \mathbf{Y}'_L[m+1] \oplus \mathbf{Y}_L[m]$ y $B = \mathbf{Y}_L[m]$. Entonces, se tiene que

$$\begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} A \\ B \end{pmatrix} = \begin{pmatrix} \delta_1 \\ \delta_2 \end{pmatrix} \tag{8.21}$$

Como A y B son independientes entre sí, gracias a la separación de dominios (establecida

por $m+1$) es fácil ver que este sistema tiene una única solución.

$$\begin{aligned}
\therefore \quad \Pr\left[\begin{array}{ll}\Delta U & = 0^n \\ \Delta V & = 0^t\end{array}\right] &\leq \max_{\substack{\delta_1 \in \mathrm{GF}(2^n) \\ \delta_3 \in \mathrm{GF}(2^t)}} \Pr\left[\begin{array}{ll}A + 2B & = \delta_1 \\ \left\Vert A + B \right\Vert^t & = \delta_2\end{array}\right] \\
&\leq \max_{\substack{\delta_1 \in \mathrm{GF}(2^n) \\ \delta_2 \in \mathrm{GF}(2^t)}} \sum_{\substack{\delta_3 \in \mathrm{GF}(2^n) : \\ \left\Vert \delta_3 \right\Vert^t = \delta_2}} \Pr\left[\begin{array}{ll}A + 2B & = \delta_1 \\ A + B & = \delta_3\end{array}\right] \\
&\leq \max_{\substack{\delta_1 \in \mathrm{GF}(2^n) \\ \delta_2 \in \mathrm{GF}(2^t)}} \sum_{\substack{\delta_3 \in \mathrm{GF}(2^n) : \\ \left\Vert \delta_3 \right\Vert^t = \delta_2}} \frac{1}{2^n} \cdot \frac{1}{2^n} \\
&\leq \frac{2^{n-t}}{2^{2n}} = \frac{1}{2^{n+t}}
\end{aligned}$$

En este caso, percátese que A y B son variables aleatoriamente uniformes tomadas de $\mathrm{GF}(2^n)$.

- Para el caso $m' > m$,

$$\Delta U = 2\Big(\mathbf{Y}'_L[m'] \oplus 2\mathbf{Y}'_L[m'-1] \oplus \underbrace{\bigoplus_{i \leq m'-2} 2^{m'-i+1} \Delta L[i]}_{\delta_1} \Big)$$

$$\Delta V = \left\Vert\, \mathbf{Y}'_L[m'] \oplus \mathbf{Y}'_L[m'-1] \oplus \underbrace{\bigoplus_{i \leq m'-2} \Delta R[i]}_{\delta_2} \,\right\Vert^t$$

Observe que δ_1 y δ_2 son independientes de $\mathbf{Y}'_L[m']$ y $\mathbf{Y}'_L[m'-1]$. Además, en este caso $m - 1 < m \leq m'$, de otro modo estaríamos dentro del caso anterior. Sean $A = \mathbf{Y}'_L[m']$ y $B = \mathbf{Y}'_L[m'-1]$. Entonces, se obtiene de nuevo el sistema (8.21).

$$\therefore \quad \Pr\left[\begin{array}{ll}\mathbf{Y}'_L[m'] \oplus 2\mathbf{Y}'_L[m'-1 & = \delta_1 \\ \mathbf{Y}'_L[m'] \oplus \mathbf{Y}'_L[m'-1] & = \delta_2\end{array}\right] \leq \frac{1}{2^{n+t}}$$

Reflexione cómo $\mathbf{Y}'_L[m'], \mathbf{Y}'_L[m'-1]$ son independientes en cualquier caso, gracias a la Construcción 8.20.

Para finalizar, asumimos que $t > n$ con $m' \geq m$. En este caso, se obtiene una ecuación extra acorde a lo definido en (8.5):

$$\Delta W \;=\; W + W' \;=\; \bigoplus_{i \leq m} \left\Vert \mathbf{X}_R[i] \right\Vert_{t-n} \oplus \bigoplus_{i \leq m'} \left\Vert \mathbf{X}'_R[j] \right\Vert_{t-n}$$

Inmediatamente, de las ecuaciones (8.1) y (8.2), se obtiene el nuevo sistema

$$\begin{aligned}\Delta U &= \bigoplus_{i\leq m} 2^{m-i+1}\mathbf{Y}_L[i] \oplus \bigoplus_{j\leq m'} 2^{m'-j+1}\mathbf{Y}_L[j]\\ \Delta V &= \bigoplus_{i\leq m} \mathbb{T}\Delta R[i]\mathbb{T}^n \oplus \bigoplus_{j\leq m'} \mathbb{T}\Delta R[j]\mathbb{T}^n\\ \Delta W &= \bigoplus_{i\leq m} \mathbb{L}\Delta R[i]\mathbb{L}_{t-n} \oplus \bigoplus_{j\leq m'} \mathbb{L}\Delta R[j]\mathbb{L}_{t-n}\end{aligned}$$

Advierta cómo $(\Delta U, \Delta V)$ conforma un sistema de ecuaciones independientes similar a los casos anteriores, sin olvidar que ΔW corresponde con los últimos $t-n$ bits de ΔV. Más aún, en este caso, el sistema depende de ΔW para tener una única solución.

Si $\Delta W \neq 0^{t-n}$, entonces para un índice $i \leq m'$ se cumple que $\mathbf{X}_R[i] \oplus \mathbf{X}'_R[i] \neq 0^t$, puesto que $X[i]$ y $X'[i]$ son distintos. De otro modo, el sistema no presenta solución, lo que indica que no es posible una colisión.

Dicho lo anterior, para que ocurra una colisión $(\Delta U, \Delta V, \Delta W) = (0^n, 0^n, 0^{t-n})$, podemos asumir que la probabilidad es máxima si se satisface que

$$\begin{aligned}\mathbf{Y}_L[m] \oplus 2\mathbf{Y}_L[m-1] &= \underbrace{\bigoplus_{i<m-1} 2^{m-i+1}\Delta L[i]}_{\delta_1}\\ \mathbf{Y}_L[m] \oplus \mathbf{Y}_L[m-1] &= \underbrace{\bigoplus_{i<m-1} \mathbb{T}\Delta R[i]\mathbb{T}^n \oplus \mathbf{X}_R[m] \oplus \mathbf{X}_R[m-1]}_{\delta_2}\end{aligned} \tag{8.22}$$

Observe cómo este sistema corresponde al caso $t = n$.

$$\therefore \quad \Pr\left[\begin{array}{ll}\Delta U & = 0^n\\ \Delta V & = 0^n\end{array}\right] \leq \frac{4}{2^{2n}}$$

De esta manera, podemos afirmar que en cualquier caso ϵ no es mayor que $4/2^{n+\min\{n.t\}}$.

□

Esto concluye que la probabilidad de colisión de ZHASH es negligible para un $\epsilon(n,t)$ y una cantidad de q consultas dadas. En consecuencia, se cumple el primer requisito para la construcción $\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}$.

Es oportuno mencionar que los valores $\mathbf{X}[i]$ son controlados por el adversario, así, inclusive para un TBC con longitud de tono t muy grande, no se tiene una probabilidad mayor a $1/2^{2n}$. Conjuntamente, no se puede concluir que la función ZHASH es casi-Xor-Universal. Esto se debe a qué en el primer caso $V + V' \neq 0^n$ o la suma $U + U' \neq 0^t$, lo que entra en conflicto con la Definición 6.3.2.

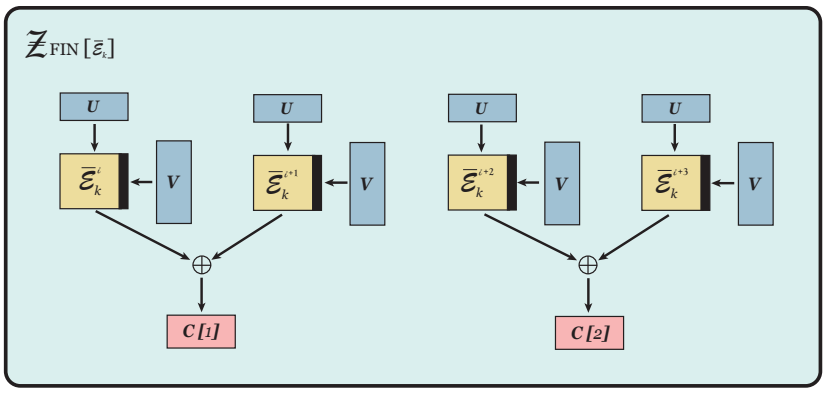

Figura 8.2: Esquema ZFIN

8.3. ZFIN

El algoritmo ZFIN es el mecanismo que nos permite generar una firma de $2n$ bits segura, desde los valores U, V obtenidos de ZHASH, de la siguiente manera:

Definición 8.3.1. *Se define ZFIN como una función* $\mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]} : \mathfrak{I}_9 \times \{0,1\}^n \times \{0,1\}^t \to \{0,1\}^n$ *tal que*

ALGORITMO $\mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]}(\, i, \mathbf{U}, \mathbf{V}\,)$:
  $\mathbf{Y}_L \leftarrow \mathcal{E}_k^i(\mathbf{V}, \mathbf{U}) \oplus \mathcal{E}_k^{i+1}(\mathbf{V}, \mathbf{U})$
  $\mathbf{Y}_R \leftarrow \mathcal{E}_k^{i+2}(\mathbf{V}, \mathbf{U}) \oplus \mathcal{E}_k^{i+3}(\mathbf{V}, \mathbf{U})$
  regresa $\mathbf{Y} \leftarrow (\!|\mathbf{Y}_L \| \mathbf{Y}_R|\!)$

Algoritmo 8.3.1: Algoritmo de salida ZFIN

Note que i es un número natural que sirve para obtener una separación de dominio entre cada permutación $\overline{\mathcal{E}}_k^i$. Siempre y cuando $|i - j| \geq 4$, las funciones $\mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]}(i, u, v)$ y $\mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]}(j, u, v)$ son distintas e independientes. Así, para el caso de un mensaje $\mathbf{M}$ que requiera *padding* se define $i = 0$ y para el otro caso se define $i = 4$.

Para demostrar que ZFIN es una función PRF, y de este modo cumplir con el segundo requisito de la construcción Carter-Wegman, se necesita definir la siguiente construcción:

Definición 8.3.2. *Sean* P_1 *y* P_2 *dos permutaciones independientes. Entonces, la función*

$$\text{SUM2}[P_1, P_2](\mathbf{X}) := P_1(\mathbf{X}) \oplus P_2(\mathbf{X})$$

se denomina ***suma de permutaciones*** *para toda entrada* $\mathbf{X} \in \{0,1\}^n$.

Esta definición es crucial para el análisis de ZMAC, ya que que ZFIN es una instancia de SUM2. En específico, se denota $\mathcal{Z}_{\text{FIN}}[\overline{P}]$ como la construcción ideal de ZFIN con una TURP

$$\overline{P} : \ (i, U, V) \mapsto \text{SUM2}[P^i, P^{i+1}](U, V) \| \text{SUM2}[P^{i+2}, P^{i+3}](U, V)$$

tal que $i \in \{0, 4\}$, y U, V son obtenidos de $\mathcal{Z}_{\text{HASH}}[\,\overline{XP}\,]$. Para entender mejor el funcionamiento de $\mathcal{Z}_{\text{FIN}[\overline{\widetilde{\varepsilon}_k}]}$ observe la Figura 8.2.

8.3.1. Seguridad PRF de ZFIN

Ya que SUM2 es un caso general de la estructura de ZFIN, se demuestra la seguridad de SUM2 haciendo uso de los coeficientes H, de manera similar al análisis propuesto por Jha y Nandi (2022).

Lema 8.3.3. *Sea $\mathcal{A}$ un adversario realizando a lo más $q \leq 2^{n-4}$ consultas. Entonces,*

$$\mathbf{Adv}^{\text{PRF}}_{\text{SUM2}} \leq \left(\frac{q}{2^n}\right)^{3/2}$$

Demostración. Sea $\tau = (x^q, y^q)$ un transcrito bueno. Luego, para cada $j < i$:

$$\begin{aligned}\Pr\left[\,\text{SUM2}[P_1, P_2](x^q) = y^q\,\right] &= \prod_{i=1}^{q} \Pr\left[\,P_1(x_i) \oplus P_2(x_i) = y_i \;\middle|\; P_1(x_j) \oplus P_2(x_j) = y_j\,\right] \\ &= \prod_{i=1}^{q} \sum_{\widehat{y}_i \in Y} \Pr\left[\,P_1(x_i) = \widehat{y}_i,\, P_2(x_i) = y_i \oplus \widehat{y}_i \;\middle|\; P_1(x_j) \oplus P_2(x_j) = y_j\,\right]\end{aligned}$$

En vista que P_1 y P_2 son distintas, se tiene el siguiente sistema independiente:

$$\begin{aligned}\Pr\left[\,\text{SUM2}[P_1, P_2](x^q) = y^q\,\right] &= \prod_{i=1}^{q} \sum_{\widehat{y}_i \in Y} \Pr\left[\begin{array}{ll} P_1(x_i) & = \widehat{y}_i \\ P_2(x_i) & = y_i \oplus \widehat{y}_i \end{array} \;\middle|\; P_1(x_j) \oplus P_2(x_j) = y_j\right] \\ &= \prod_{i=1}^{q} \sum_{\widehat{y}_i \in Y} \frac{1}{2^n - a_i} \cdot \frac{1}{2^n - b_i}\end{aligned}$$

Recuerde que a_i y b_i son la cantidad de índices j respectivos. Luego, para calcular la cantidad de elementos $\widehat{y}_i \in Y$, asumimos que se satisface a lo mucho

$$\underbrace{P_1(x_j) \oplus P_2(x_j) \oplus P_2(x_i)}_{u_j} \;\neq\; P_1(x_i) \;\neq\; \underbrace{P_1(x_j)}_{v_j}$$

Esto implica que existe un $\widehat{y}_i \notin \{u_j, v_j \mid j < i\}$ para cada índice j.

$$\begin{aligned}
\therefore \quad \Pr[\,\mathrm{SUM2}[P_1,P_2](x^q) = y^q\,] &\geq \prod_{i=1}^{q} \frac{|Y \setminus \{u_j, v_j\}|}{\big(2^n - |\{v_j\}|\big)\big(2^n - |\{u_j\}|\big)} \\
&\geq \prod_{i=1}^{q} \frac{2^n - 2(i-1)}{\big(2^n - (i-1)\big)\big(2^n - (i-1)\big)} \\
&\geq \prod_{i=1}^{q} \frac{2^n - 2(i-1)}{\big(2^n - (i-1)\big)\big(2^n - i + 1\big)} \cdot \frac{2^n}{2^n} \\
&\geq \prod_{i=1}^{q} \frac{2^{2n} - 2^{n+1}(i-1) + (i-1)\big(i-1\big)}{2^{2n} - 2^{n+1}(i-1) + (i-1)^2} \cdot \frac{1}{2^n} \\
&\geq \prod_{i=1}^{q} \left(1 - \frac{(i-1)^2}{2^{2n} - 2^{n+1}(i-1) + (i-1)^2}\right) \cdot \frac{1}{2^{nq}} \\
&\geq \prod_{i=1}^{q} \left(1 - \frac{(i-1)^2}{2^{2n-1}}\right) \cdot \frac{1}{2^{nq}}
\end{aligned}$$

Suponiendo que $2^{n+1}(i-1) < 2^{n+1} < 2^{2n-1}$, se colige que

$$\begin{aligned}
\Pr[\,\mathrm{SUM2}[P_1,P_2](x^q) = y^q\,] &\geq \left(1 - 2\sum_{i=1}^{q} \frac{(i-1)^2}{2^{2n}}\right) \cdot \frac{1}{2^{nq}} \\
&\geq \left(1 - \frac{2}{3}\frac{q^3}{2^{2n}}\right) \cdot \frac{1}{2^{nq}} \\
&\geq \left(1 - \frac{q^3}{2^n}\right) \cdot \frac{1}{2^{nq}} \\
&\geq \left(1 - \frac{q^3}{2^{2n}}\right) \cdot \Pr[\,\rho(x^q) = y^q\,]
\end{aligned}$$

tal que ρ es una TURP con rango $Y = \{0,1\}^n$. Así, aplicando el Teorema 7.1.7 con $\alpha = q^3/2^{2n}$ y $\beta = 0$, se concluye que SUM2 es segura.

□

Es suficiente con emplear la técnica H de la manera usual, para demostrar la seguridad de la suma de dos permutaciones. Por lo tanto, podemos concluir lo siguiente:

Corolario 8.3.4. *Sea $\mathcal{A}$ un adversario realizando a lo más $q \leq 2^{n-4}$ consultas contra $\mathcal{Z}_{\text{FIN}}[\overline{P}_I]$. Entonces, para cada $i \in \{0,4\}$ se satisface que*

$$\mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}}[\overline{P}_I]} \leq 2\left(\frac{q}{2^n}\right)^{3/2}$$

Demostración. Deje que $Z_i(U,V) := \mathcal{Z}_{\text{FIN}}[\overline{P}](i,U,V)$. Entonces,

$$\begin{aligned}\mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}}[\overline{P}_I]} &\leq \mathbf{Adv}^{\text{PRF}}_{Z_i+Z_{i+1}} + \mathbf{Adv}^{\text{PRF}}_{Z_{i+2}+Z_{i+3}} \\ &\leq \mathbf{Adv}^{\text{PRF}}_{SUM2[Z_i,Z_{i+1}]} + \mathbf{Adv}^{\text{PRF}}_{SUM2[Z_{i+2},Z_{i+3}]} \\ &\leq \left(\frac{q}{2^n}\right)^{3/2} + \left(\frac{q}{2^n}\right)^{3/2}\end{aligned}$$

Esto se cumple conforme al Lema 8.3.3. □

Recuerde que la construcción ZFIN consiste en una firma de $2n$-bits, que se obtiene al concatenar $Z_i + Z_{i+1} \| Z_{i+2} + Z_{i+3}$. Dicho de otra manera, el adversario requiere resolver dos veces el problema de SUM2, puesto que cada permutación $\overline{P}_I(i,U,V)$ es distinta debido a la separación de dominios que se obtiene con los tonos pequeños $i, i+1, i+2, i+3$.

8.4. Probabilidad de falsificación de ZMAC

Finalmente, después del análisis a la seguridad de ZHASH y ZFIN, estamos preparados para analizar la seguridad de la construcción ZMAC. No obstante, antes de enunciar el teorema principal es importante entender cómo se componen los dos algoritmos.

Recuerde que $\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}$ es una instancia de la construcción Carter-Wegman que a su vez es un caso particular del esquema genérico Hash-then-PRF. Éste tiene la siguiente propiedad.

Lema 8.4.1. *Sea $G : H \times M \to S$ una función hash-casi-universal ϵ–AU y sea $\rho \xleftarrow{\$} Y^Y$ una función aleatoria. Entonces*

$$\mathbf{Adv}^{\text{PRF}}_{[G,\rho]} \leq \binom{q}{2}\epsilon$$

para cualquier adversario $\mathcal{A} \in CPA$.

Demostración. Sean $\tau = (m^q, y^q, h)$ el transcrito extendido, $F := [G,\rho]$ la construcción Hash-then-PRF y $\varphi \xleftarrow{\$} M^Y$ una función aleatoria. Se define el conjunto de transcritos buenos como

$$\mathbb{B} := \left\{\tau(\mathcal{A}^{\mathcal{O}}) \mid \forall i < j : \ x_i \neq x_j\right\}$$

donde $x_i = G_h(m_i)$ es el hash de cada mensaje con clave $h \in H$. Observe cómo esto implica que la probabilidad de encontrar un transcrito malo depende de la probabilidad de colisión de G.

$$\therefore \quad \Pr[\,\tau \notin \mathbb{B}\,] \ \leq \ \max_{m_1,\ldots,m_q} \sum_{i<j} \mathcal{C}(G, m_i, m_j) \ \leq \ \binom{q}{2}\epsilon$$

Luego, para los transcritos buenos,

$$\begin{aligned}\Pr\left[\,\rho(G(m^q)) = y^q,\ H = h\,\right] &= \frac{1}{|H|}\cdot \Pr\left[\,\rho(G(m^q)) = y^q \;\middle|\; H = h\,\right]\\ &= \frac{1}{|H|}\cdot \Pr\left[\,\rho(x^q) = y^q\,\right]\\ &= \frac{1}{|H|}\cdot \frac{1}{|Y|^q}\\ &= \Pr\left[\,\varphi(m^q) = y^q,\ H' = h\,\right]\end{aligned}$$

Esto implica que $\alpha = 0$ y $\beta = \binom{q}{2}\epsilon$. Por último, la prueba se concluye con el Teorema 7.2.5. □

8.4.1. Cota de seguridad de ZMAC

Finalmente, dado los resultados anteriores, llegamos al resultado principal enunciado en el siguiente teorema:

Teorema 8.4.2. *La construcción $\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}$ es infalsificable contra cualquier adversario con ventaja*

$$\mathbf{Adv}^{\text{FORGE}}_{\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}} \leq \mathbf{Adv}^{\text{TPRP}}_{\overline{\varepsilon}} + \frac{q}{2^{2n}} + \frac{5\sigma^2/2}{2^{n+\min\{n,t\}}} + 4\left(\frac{q}{2^n}\right)^{3/2}$$

realizando a lo más $q \leq 2^{n-4}$ consultas.

Demostración. Sea $\mathcal{A}$ un adversario bajo el experimento PRF. Entonces, del Teorema 6.2.1,

$$\mathbf{Adv}^{\text{FORGE}}_{\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}} \leq \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}}(\mathcal{A}) + \frac{q}{2^{2n}} \tag{8.23}$$

Recuerde que ZMAC es una instancia de la Construcción 8.1.2. Por definición de TPRP existe un adversario $\mathcal{B}$ tal que

$$\begin{aligned}\mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}} &= \mathbf{Adv}^{\text{PRF}}_{\text{CW3}\left[\mathcal{Z}_{\text{HASH}[\overline{XE}]},\mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]_0},\mathcal{Z}_{\text{FIN}[\overline{\varepsilon}]_4}\right]}(\mathcal{A})\\ &\leq \mathbf{Adv}^{\text{PRF}}_{\text{CW3}\left[\mathcal{Z}_{\text{HASH}[\overline{XP}]},\mathcal{Z}_{\text{FIN}[\overline{\pi}]_0},\mathcal{Z}_{\text{FIN}[\overline{\pi}]_4}\right]}(\mathcal{A}) + \mathbf{Adv}^{\text{TPRP}}_{\overline{\varepsilon}}(\mathcal{B})\end{aligned}$$

Al aplicar el Lema 8.2.9 y el Corolario 8.3.4, se deduce que

$$\begin{aligned}\mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}} &\leq \mathbf{Adv}^{\text{TPRP}}_{\overline{\varepsilon}}(\mathcal{B}) + \mathbf{Adv}^{\text{PRF}}_{\text{CW3}\left[\mathcal{Z}_{\text{HASH}[\overline{XP}]},F_0,\mathcal{Z}_{\text{FIN}[\overline{\pi}]_4}\right]}(\mathcal{A}) + \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}[\overline{\pi}]_4}}\\ &\leq \mathbf{Adv}^{\text{TPRP}}_{\overline{\varepsilon}}(\mathcal{B}) + \mathbf{Adv}^{\text{PRF}}_{\text{CW3}\left[\mathcal{Z}_{\text{HASH}[\overline{XP}]},F_0,F_4\right]}(\mathcal{A}) + \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}[\overline{\pi}]_0}} + \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}[\overline{\pi}]_4}}\\ &\leq \mathbf{Adv}^{\text{TPRP}}_{\overline{\varepsilon}}(\mathcal{B}) + \mathbf{Adv}^{\text{PRF}}_{\text{CW3}[G,F_0,F_4]}(\mathcal{A}) + \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}[\overline{\pi}]_0}} + \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{FIN}[\overline{\pi}]_4}} + \mathbf{Adv}^{\text{TPRP}}_{XP}\\ &\leq \mathbf{Adv}^{\text{TPRP}}_{\overline{\varepsilon}}(\mathcal{B}) + \mathbf{Adv}^{\text{PRF}}_{\text{CW3}[G,F_0,F_4]}(\mathcal{A}) + 4\left(\frac{q}{2^n}\right)^{3/2} + \frac{q^2}{2^{n+1+\min\{n+t\}}}\end{aligned}$$

Debido a qué $\mathcal{Z}_{\text{FIN}[\overline{\pi}]_0}$ y $\mathcal{Z}_{\text{FIN}[\overline{\pi}]_4}$ son PRF, podemos reemplazarlas por dos funciones aleatorias F_0 y F_4. Por último, se aplica el Lema 8.4.1 para obtener la seguridad de CW3 y se emplea el ϵ del Lema 8.2.9 para obtener la probabilidad de colisión de ZHASH.

$$\therefore \quad \mathbf{Adv}^{\text{PRF}}_{\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}} \leq \mathbf{Adv}^{\text{TPRP}}_{\overline{\mathcal{E}}}(\mathcal{B}) + \frac{q^2}{2} \cdot \frac{4}{2^{n+\text{mín}\{n,t\}}} + \frac{q^2/2}{2^{n+\text{mín}\{n,t\}}} + 4\left(\frac{q}{2^n}\right)^{3/2} \tag{8.24}$$

De (8.23) y (8.24) se concluye la prueba.

□

De este modo, se concluye que ZMAC es una MAC segura, ya que se ha demostrado que la probabilidad de falsificar una firma generada por $\mathcal{Z}_{\text{MAC}[\overline{\varepsilon}_k]}$ es negligible.

8.5. Trabajo futuro

Una vez replicada la cota de seguridad de ZMAC y expuesto cómo emplear los teoremas demostrados en esta tesis, sobre todo la técnica H, hemos descubierto varias áreas de oportunidad para mejorar la eficiencia e incluso maximizar la seguridad de ZMAC. Resumimos nuestras observaciones con las siguientes propuestas:

8.5.1. Propuestas de modificaciones a ZMAC

Al estudiar la probabilidad de colisión de ZHASH, notamos que es posible redefinir el caso $t > n$ para obtener seguridad 2^{n+t} en cualquier caso:

En primer lugar, consideramos un TBC como (2020) tal que su espacio de tonos es mayor que su entrada. De este modo, redefinimos las ecuaciones 8.1 y 8.2 para el caso $t \geq n$:

$$\mathbf{Y}_L[i] = \overline{\mathcal{E}}^8_k(2^{i-1}\mathbf{S} \oplus \mathbf{X}_R,\ 2^{i-1}\text{Ł} \oplus \mathbf{X}_L) \tag{8.25}$$

$$\mathbf{Y}_R[i] = \left(\mathbf{Y}_L[i] \| \cdots \| \left\lceil\!\left\lceil 2^{h-1}\mathbf{Y}_L[i]\right\rceil\!\right\rceil^t\right) \oplus \mathbf{X}_R[i] \tag{8.26}$$

en donde h es el entero tal que $h - 1 < t/n \leq h$ y la máscara Ł se define de la manera usual. Además, definimos la máscara

$$\mathbf{S} := \left\lceil\!\left\lceil \mathbf{R}[1] \right\rceil\!\right\rceil \| \cdots \| \mathbf{R}[h] \left\rceil\!\right\rceil^t$$

para las variables $\mathbf{R}[j] := \overline{\mathcal{E}}^9_k(1^j 0^{t-i}, 0^n)$ con $j \leq h$. Simultáneamente, vea que este diseño puede alcanzar mayor eficiencia al procesar $n + t > 2n$ bits por ejecución del TBC.

El propósito de esta modificación es lograr que las $\left\lfloor\!\left\lfloor V \right\rfloor\!\right\rfloor_{t-n}$ sean independientes de cada bloque $X[1], \ldots, X[p]$ del mensaje. De esta manera se redefine el sistema de ecuaciones (8.22) como

$$\begin{aligned} \mathbf{Y}_L[m] \oplus 2\mathbf{Y}_L[m-1] &= \delta_1 \\ \mathbf{Y}_L[m] \| \cdots \| \left\lceil\!\left\lceil 2^{h-1}\mathbf{Y}_L[m]\right\rceil\!\right\rceil^t \oplus \mathbf{Y}_L[m-1] \| \cdots \| \left\lceil\!\left\lceil 2^{h'-1}\mathbf{Y}_L[m-1]\right\rceil\!\right\rceil^t] &= \delta_2 \end{aligned}$$

Es importante aclarar que para asegurar que este sistema tenga una única solución, se deben evaluar los casos donde

$$\llbracket 2^{h-1}\mathbf{Y}_L[m]\rrbracket^t \oplus \llbracket 2^{h'-1}\mathbf{Y}_L[m-1]\rrbracket^t \;=\; \lVert\delta_2\rVert_{t-n} \;=\; 0^{t-n}$$

para evitar conflictos con la hipótesis de $\mathbf{Y}_L[m], \mathbf{Y}_L[m-1]$ distintos. Esto dificulta el análisis, dado que el adversario puede controlar el parámetro $h = h'$ y buscar colisiones internas con la definición.

Una solución más general, consiste en redefinir la relación (8.26) como una función hash que mapea

$$\mathcal{G} :\; (\mathbf{S}, \mathbf{X}_R[i]) \mapsto \mathbf{T}$$

los valores de la máscara y los últimos t bits del bloque $\mathbf{X}$ (para generar un tono adecuado para ZFIN). Buscar dicha función es una tarea complicada y va más allá del alcance de esta tesis

Otra manera sencilla para modificar ZMAC es encontrar una función pAXU que sea más eficiente que la función $\mathcal{H}$ descrita en la Definición 8.2.3. Esto se debe a que observamos que la demostración de seguridad de la Construcción 8.2.2 es independiente del Lema 8.2.4.

8.5.2. Propuesta para la técnica H

Como definimos en el Capítulo 7, la Definición 7.2.1 describe un trascrito bueno para el comportamiento de cualquier sistema probabilístico. Es importante destacar que la definición original de comportamiento dada por Polderman y Willems (1997) está definida sobre cualquier sistema dinámico, incluyendo espacios continuos y diferenciables.

Esto es de particular importancia para esquemas basados en sistemas caóticos, puesto que la relación

$$\frac{H_1(\tau)}{H_0(\tau)} \geq 1 - \alpha$$

permite acotar el comportamiento de cualesquiera dos sistemas probabilísticos con cantidad de claves H_1 y H_0.

Por el momento, la Definición 7.1.4 solamente contempla sistemas probabilísticos con espacio finito:

$$H(a^q, b^q) := \left|\left\{k \in K \mid (a_i, b_i, k) \in \mathfrak{B},\ \forall i \leq q\right\}\right|$$

No obstante, como acabamos de mencionar, la probabilidad de un transcrito $(a^q, b^q) \in \Omega$ con $i \leq q; a_i, b_i \in \mathbb{R}$, puede ser calculada si hacemos uso de un σ-álgebra de Borel para construir un sistema probabilístico.

Claro, es necesario analizar si la construcción de dicho sistema probabilístico con un espacio de tiempo T, un espacio muestral $\Omega \subseteq \mathbb{R} \times \mathbb{R}$, un espacio latente K y un comportamiento $\mathfrak{B} \subseteq \left(\Omega \times K\right)^T$, no entra en contradicción con alguna de las suposiciones que realizamos en nuestras demostraciones de seguridad.

En nuestro trabajo demostramos, que partir de un transcrito en el comportamiento de un sistema probabilístico, podemos obtener las mismas conclusiones de suficiencia que mostraron Patarin (2009) y Jha y Nandi (2022). Por ello pensamos que generalizar la técnica H para conjuntos continuos es posible de realizar, introduciendo conceptos avanzados de probabilidad como las σ-álgebras.

8.5.3. Conclusión

Este trabajo presenta una introducción bastante detallada sobre la seguridad demostrable en cifradores por bloque, en específico en esquemas de autenticación. Incluso, explicamos conceptos avanzados sobre la Técnica H y las pruebas de seguridad.

Se ha realizado un estudio extenso de distintos artículos, con pruebas rigurosas, enlazando y homogeneizando los distintos resultados que en ellos se encuentran. Esperamos que la tesis sea de gran utilidad para criptógrafos e informáticos que deseen estudiar más a fondo las construcciones PRF y sus aplicaciones.

Bibliografía

(2020). *IACR Transactions on Symmetric Cryptology*, *2020*(S1), 88-131. https://doi.org/10.13154/tosc.v2020.iS1.88-131

Bellare, M., Goldreich, O., & Krawczyk, H. (1999). Stateless Evaluation of Pseudorandom Functions: Security beyond the Birthday Barrier. *Advances in Cryptology - CRYPTO '99, 19th Annual International Cryptology Conference, Santa Barbara, California, USA, August 15-19, 1999, Proceedings*, *1666*, 270-287. https://doi.org/10.1007/3-540-48405-1_17

Bellare, M., & Rogaway, P. (1993). Random oracles are practical: a paradigm for designing efficient protocols. *Proceedings of the 1st ACM Conference on Computer and Communications Security*, 62-73. https://doi.org/10.1145/168588.168596

Bellare, M., & Rogaway, P. (2005). *Introduction to Modern Cryptography* (1.ª ed.). Department of Computer Science; Engineering, University of California at San Diego. https://cseweb.ucsd.edu/~mihir/papers/br-book.pdf

Bellare, M., & Rogaway, P. (2006). The Security of Triple Encryption and a Framework for Code-Based Game-Playing Proofs. *Proceedings of the 24th Annual International Conference on The Theory and Applications of Cryptographic Techniques*, 409-426. https://doi.org/10.1007/11761679_25

Bennett, C. H., & Gill, J. (1981). Relative to a Random Oracle A, $\mathbf{P}^A \neq \mathbf{NP}^A \neq$ co-$\mathbf{NP}^A$ with Probability 1. *SIAM Journal on Computing*, *10*(1), 96-113. https://doi.org/10.1137/0210008

Bhattacharjee, A., Dutta, A., List, E., & Nandi, M. (2020). CENCPP* - Beyond-birthday-secure Encryption from Public Permutations [https://eprint.iacr.org/2020/602]. https://eprint.iacr.org/2020/602

Black, J., & Rogaway, P. (2000). CBC MACs for Arbitrary-Length Messages: The Three-Key Constructions. *Proceedings of the 20th Annual International Cryptology Conference on Advances in Cryptology*, 197-215.

Cogliati, B., & Seurin, Y. (2016). EWCDM: An Efficient, Beyond-Birthday Secure, Nonce-Misuse Resistant MAC [https://eprint.iacr.org/2016/525]. https://eprint.iacr.org/2016/525

Dar, A. B., Lone, M. J., & Hussain, N. (2021). Revisiting Lightweight Block Ciphers: Review, Taxonomy and Future directions [https://eprint.iacr.org/2021/476]. https://eprint.iacr.org/2021/476

Dobraunig, C., Mennink, B., & Neves, S. (2023). EliMAC: Speeding Up LightMAC by around 20 %. *IACR Transactions on Symmetric Cryptology*, *2023*(2), 69-93. https://doi.org/10.46586/tosc.v2023.i2.69-93

Dutta, A., Nandi, M., & Paul, G. (2015). One-Key Compression Function Based MAC with Security beyond Birthday Bound [https://eprint.iacr.org/2015/1016]. https://eprint.iacr.org/2015/1016

Dutta, A., Nandi, M., & Talnikar, S. (2019). Beyond Birthday Bound Secure MAC in Faulty Nonce Model. *11476*, 437-466. https://doi.org/10.1007/978-3-030-17653-2_15

Dutta, A., Nandi, M., & Talnikar, S. (2021). Permutation Based EDM: An Inverse Free BBB Secure PRF. *IACR Transactions on Symmetric Cryptology*, *2021*(2), 31-70. https://doi.org/10.46586/tosc.v2021.i2.31-70

Goldwasser, S., & Micali, S. (1984). Probabilistic encryption. *Journal of Computer and System Sciences*, *28*(2), 270-299. https://doi.org/https://doi.org/10.1016/0022-0000(84)90070-9

Guo, T., Wang, P., Hu, L., & Ye, D. (2020). Attacks on Beyond-Birthday-Bound MACs in the Quantum Setting [https://eprint.iacr.org/2020/1595]. https://eprint.iacr.org/2020/1595

Hoang, V. T., & Tessaro, S. (2016). Key-Alternating Ciphers and Key-Length Extension: Exact Bounds and Multi-user Security. En M. Robshaw & J. Katz (Eds.), *Advances in Cryptology - CRYPTO 2016 - 36th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2016, Proceedings, Part I* (pp. 3-32, Vol. 9814). Springer. https://doi.org/10.1007/978-3-662-53018-4_1

Iwata, T., & Kurosawa, K. (2003). OMAC: One-Key CBC MAC. En *FSE* (pp. 129-153).

Iwata, T., & Minematsu, K. (2016). Stronger Security Variants of GCM-SIV [https://eprint.iacr.org/2016/853]. https://eprint.iacr.org/2016/853

Iwata, T., Minematsu, K., Peyrin, T., & Seurin, Y. (2017). ZMAC: A Fast Tweakable Block Cipher Mode for Highly Secure Message Authentication. *IACR Cryptology ePrint Archive*, *2017*, 535. http://dblp.uni-trier.de/db/journals/iacr/iacr2017.html#IwataMPS17

Jha, A., & Nandi, M. (2020). Tight Security of Cascaded LRW2. *Journal of Cryptology*, *33*, 1272-1317. https://doi.org/10.1007/s00145-020-09347-y

Jha, A., & Nandi, M. (2022). A Survey on Applications of H-Technique: Revisiting Security Analysis of PRP and PRF. *Entropy*, *24*(4). https://doi.org/10.3390/e24040462

Katz, J., & Lindell, Y. (2014). *Introduction to Modern Cryptography, Second Edition* (2nd). Chapman & Hall/CRC.

Landecker, W., Shrimpton, T., & Terashima, R. S. (2012). Tweakable Blockciphers with Beyond Birthday-Bound Security. *Advances in Cryptology - Crypto 2012*, *7417*, 14-30. https://doi.org/10.1007/978-3-642-32009-5_2

Liskov, M., Rivest, R. L., & Wagner, D. (2011). Tweakable Block Ciphers. *J. Cryptology*, *24*, 588-613. https://doi.org/10.1007/s00145-010-9073-y

Maurer, U. (2002). Indistinguishability of Random Systems. *Advances in Cryptology - EUROCRYPT 2002, International Conference on the Theory and Applications of Crypto-*

graphic Techniques, Amsterdam, The Netherlands, April 28 - May 2, 2002, Proceedings, *2332*, 110-132. https://doi.org/10.1007/3-540-46035-7_8

Maurer, U., Pietrzak, K., & Renner, R. (2006). Indistinguishability Amplification [https://eprint.iacr.org/2006/456]. https://eprint.iacr.org/2006/456

Minematsu, K., & Iwata, T. (2015). Tweak-Length Extension for Tweakable Blockciphers [https://eprint.iacr.org/2015/888]. https://eprint.iacr.org/2015/888

Moch, A., & List, E. (2019). Parallelizable MACs Based on the Sum of PRPs with Security Beyond the Birthday Bound [https://eprint.iacr.org/2019/422]. https://eprint.iacr.org/2019/422

Naito, Y. (2017). Blockcipher-based MACs: Beyond the Birthday Bound without Message Length [https://eprint.iacr.org/2017/852]. https://eprint.iacr.org/2017/852

Patarin, J. (2009). The "Coefficients H" Technique. En R. M. Avanzi, L. Keliher & F. Sica (Eds.), *Selected Areas in Cryptography* (pp. 328-345). Springer Berlin Heidelberg.

Polderman, J. W., & Willems, J. C. (1997). *Introduction to mathematical systems theory: a behavioral approach*. Springer-Verlag.

Rogaway, P. (2004). Efficient Instantiations of Tweakable Blockciphers and Refinements to Modes OCB and PMAC. *Advances in Cryptology - ASIACRYPT 2004, 10th International Conference on the Theory and Application of Cryptology and Information Security, Jeju Island, Korea, December 5-9, 2004, Proceedings*, *3329*, 16-31. https://doi.org/10.1007/978-3-540-30539-2_2

Savage, N. (2013). Proofs probable. *Commun. ACM*, *56*(6), 22-24. https://doi.org/10.1145/2461256.2461265

Shannon, C. E. (1949). Communication theory of secrecy systems. *The Bell System Technical Journal*, *28*(4), 656-715. https://doi.org/10.1002/j.1538-7305.1949.tb00928.x

Shimeall, T. J., & Spring, J. M. (2014). Chapter 8 - Resistance Strategies: Symmetric Encryption. En T. J. Shimeall & J. M. Spring (Eds.), *Introduction to Information Security* (pp. 155-186). Syngress. https://doi.org/https://doi.org/10.1016/B978-1-59749-969-9.00008-0

Shoup, V. (2004). Sequences of games: a tool for taming complexity in security proofs [https://eprint.iacr.org/2004/332]. https://eprint.iacr.org/2004/332

Yasuda, K. (2010). The Sum of CBC MACs is a Secure PRF. *Proceedings of the 2010 International Conference on Topics in Cryptology*, 366-381. https://doi.org/10.1007/978-3-642-11925-5_25

Yasuda, K. (2011). A New Variant of PMAC: Beyond the Birthday Bound. *Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference*, *6841*, 593. https://doi.org/10.1007/978-3-642-22792-9_34

Zhang, L., Wu, W., Sui, H., & Wang, P. (2012). 3kf9: Enhancing 3GPP-MAC beyond the Birthday Bound. En X. Wang & K. Sako (Eds.), *Advances in Cryptology – ASIACRYPT 2012* (pp. 296-312). Springer Berlin Heidelberg.