Universidad Central "Marta Abreu" de las Villas
Facultad de Matemática Física y Computación

TESIS EN OPCIÓN AL TÍTULO DE MASTER EN MATEMÁTICA APLICADA

Título: *"Utilización de la transformada y matrices de Hadamard en las funciones booleanas y en el Criptoanálisis"*

Autor: Lic. Guillermo Sosa Gómez
Tutores: MSc. Oristela Cuellar Jústiz
MSc. Luis A. Perfetti Villamil

Santa Clara
2010

Hago constar que el presente trabajo para optar por el Titulo de Master en Matemática Aplicada ha sido realizado en la Facultad de Matemática Física y Computación de la Universidad Central "Marta Abreu" de Las Villas como parte de la culminación de los estudios de la Maestría en Matemática Aplicada, autorizando a que el mismo sea utilizado por la institución, para los fines que estime conveniente, tanto de forma parcial como total y que además no podrá ser presentado en eventos ni publicado sin la autorización de la Universidad.

_____

Firma del autor

Los abajo firmantes, certificamos que el presente trabajo ha sido realizado según acuerdos de la dirección de nuestro centro y el mismo cumple con los requisitos que debe tener un trabajo de esta envergadura referido a la temática señalada.

_____ _____

Firma del tutor *Firma del jefe del Seminario*

A mi abuela Mima

que ya no está presente.

"La mayoría de las ideas fundamentales de la ciencia son esencialmente sencillas y, por regla general pueden ser expresadas en un lenguaje comprensible para todos."

Einstein, Albert

Agradecimientos

Con la culminación de este trabajo se termina una etapa de nuestra vida y en este preciso momento le vienen a la mente todas aquellas personas que de una manera u otra han apoyado la culminación exitosa del mismo.

Debo agradecer:

A mis padres por todo el apoyo brindado durante toda la vida y mi hermana que es mi fuente de inspiración.

A Oristela por su paciencia y apoyo en la culminación de este trabajo.

A Perfetti y Antonio porque como amigos míos siempre me están enseñando a andar por la vida.

A los miembros del Departamento de Matemática por dejarme ser partes de ellos.

A la Dra. Yanet Rodríguez Sarabia por obligarme a entrar en el mundo de la Criptografía.

A los especialistas rusos del Octavo Centro del Servicio Federal de Seguridad Ruso por las enseñanzas transmitidas durante los postgrados.

A la Dirección de Criptografía, en especial al Coronel Diego García y a los Teniente Coroneles Pablo, Nelson y Diwaldo.

Resumen

En esta tesis se presentan de manera breve los conceptos y definiciones fundamentales de las funciones booleanas, la transformada y matrices de Hadamard. Se abordan y describen matemáticamente las diferentes propiedades que presentan las matrices de Hadamard. Se hace una revisión de la aplicabilidad de esta transformada a dos problemas fundamentales. El primero de ellos está relacionado con la búsqueda de funciones booleanas criptográficamente deseables, dándose una serie de propiedades que deben cumplir las mismas para este propósito desde el punto de vista de la transformada de Hadamard. El segundo se basa en cómo ayudar a un criptoanalista a descifrar los generadores pseudoaleatorios del cifrado en flujo utilizando la transformada de Hadamard. Por último para validar los resultados de estas aplicaciones se utilizó una herramienta computacional de propósito general como el Mathcad.

Abstract

In this thesis, we briefly present the basic concepts and definitions of Boolean functions, transform and Hadamard matrices. Are discussed and mathematically describe the different properties which have Hadamard matrices. A review of the applicability of this transform to two major problems. The first one is related to the search for desirable cryptographic Boolean functions, giving a series of properties that must meet the same for this purpose from the point of view of the Hadamard transform. The second is based on how to help a cryptanalyst to decipher the pseudorandom generators of the stream cipher using the Hadamard transform. Finally to validate the results of these applications used a general purpose computational tool such as Mathcad.

Contenido

Introducción

Aun cuando las cartas no contienen información sensible o muy personal, a muchos de nosotros nos gusta pensar que el contenido de nuestra correspondencia personal es privado y que sellando el sobre lo protegemos de todos, excepto del destinatario intencional. Si nosotros enviáramos nuestras cartas con los sobres abiertos cualquiera podría leer su contenido. Para muchas personas el uso de correo electrónico es en la actualidad una alternativa para enviar las cartas a través del correo postal[1]; es unos de los medios más rápidos de comunicación pero, no hay ningún sobre para proteger los mensajes. De hecho se dice a menudo que enviar los mensajes mediante correo electrónico es como enviar una carta sin sobre. Claramente cualquiera que quiera enviar mensajes confidenciales, o quizá incluso simplemente personales, vía correo electrónico debe encontrar algún medio de protegerlos. Una solución común es usar la criptografía y encriptar el mensaje. El uso de la encriptación para proteger los correos electrónicos no está extendido, pero se está extendiendo y es probable que esta proliferación continúe. De hecho en mayo del 2001 un grupo del bloque europeo recomendó a los usuarios de Europa encriptar todos sus correos electrónicos, para evitar ser espiados en lo adelante por el Reino Unido o EE.UU. que escuchan detrás de las puertas de la red.[2]

La Criptografía es una ciencia bien establecida que ha tenido una influencia histórica significante por más de 2,000 años. Tradicionalmente sus usuarios principales eran los gobiernos y el ejército.

El impacto de la Criptografía en la historia está bien documentado. Uno de los primeros libros es indudablemente El Codebreakers por David Kahn. Este libro tiene más de 1,000 páginas y se publicó en 1967. Se ha descrito como “La primera historia comprensiva de comunicación confidencial” y hace la lectura absorbente. Más recientemente Simón Singh ha escrito un libro más corto llamado El Libro del Código, este no es tan comprensivo como el libro de Kahn, pero se piensa que estimula el interés del hombre común por el asunto. Los dos son libros excelentes muy recomendados.

Antes de los años setenta, la criptografía era un arte negro, para entendidos y prácticamente sólo para uso del personal gubernamental y militar[3]. Es ahora una disciplina académica bien establecida que se enseña en muchas universidades. También está extensamente disponible para el uso por las compañías e individuos. Ha habido muchas fuerzas que han influido en esta transición. Dos de las más obvias han sido el movimiento hacia el negocio automatizado y el establecimiento de la Internet como un cauce de comunicación. Las compañías quieren comerciar entre sí ahora y con sus clientes que usan la Internet. Los gobiernos quieren comunicarse con sus ciudadanos vía la Internet para que, por ejemplo, puedan someterse a los ingresos del impuesto electrónicamente.[1]

Aunque no hay ninguna duda que el comercio electrónico está poniéndose en aumento popular, se citan a menudo miedos sobre la seguridad por ser uno de los aspectos más difíciles para su aceptación completa.

La Criptografía moderna ha evolucionado considerablemente durante las últimas tres décadas. No sólo ha cambiado la tecnología, sino que hay un rango más amplio de aplicaciones. Además, es probable que todos seamos usuarios directos o nos afectemos por su uso. Todos nosotros necesitamos entender cómo funciona y lo que se puede lograr.

La idea de un sistema cifrado es que se puede enmascarar la información confidencial de tal manera que su significado sea incompresible a una persona desautorizada. La mayoría de los usos comunes es, probablemente, guardar los datos firmemente en un archivo de la computadora o transmitirlo por un cauce inseguro como la Internet. En cualquier escenario el hecho que el documento se encripta no previene que las personas desautorizadas tengan el acceso a él pero, más bien, asegura que ellos no puedan entender lo que ellos ven.

Cualquier persona que intercepta un mensaje durante la transmisión se llama, no sorprendentemente, un interceptor. Otros autores usan diferentes nombres, como “el intruso”, “el enemigo”, “el adversario”, o incluso “el tipo malo”. Sin embargo, debe reconocerse que, en ocasiones, los interceptores pueden ser los “tipos buenos”. Aun cuando ellos saben el algoritmo de desencriptar, los

interceptores no saben, en general, la llave de desencriptación. Es esta falta de conocimiento, la que impide saber el texto claro. La Criptografía es la ciencia de diseñar sistemas cifradores, considerando al criptoanálisis como el proceso de deducir la información sobre el texto claro del texto cifrado sin conocerse la llave apropiada. Criptología es el término colectivo para Criptografía y Criptoanálisis.

En la terminología criptográfica al mensaje para ser cifrado se le conoce como texto claro; al proceso de codificación al que se somete al mensaje para que no pueda ser develado por entidades no autorizadas se le llama cifrado; al documento que resulta de cifrar el mensaje se le conoce como criptograma; al proceso de recuperar el mensaje en claro a partir del criptograma se le llama descifrado [4]. Finalmente, el término llave o clave se refiere a un valor numérico utilizado para alterar la información haciéndola segura y visible únicamente a los individuos que tienen la llave correspondiente para recuperar dicha información [1].

Formalmente un críptosistema puede ser definido como una quíntupla $\{P, C, K, E, D\}$, donde [4]:

P es el conjunto finito de los posibles textos claros.

C es el conjunto finito de los posibles textos cifrados.

K es el espacio de llaves y es un conjunto finito de todas las llaves posibles. $\forall k \in K, \exists\ E_k \in E(\text{regla de cifrado})\ \exists\ D_k \in D(\text{regla de descifrado})$

Cada $E_k: P \to C$ y $D_k: C \to P$ son funciones tales que $\forall\ x \in P, D_k(E_k(x)) = x$

Un hecho importante es que el conocimiento de la llave de encriptación no es necesario para obtener el criptograma. Esta observación simple es la base del artículo de Diffie-Hellman, que ha tenido un impacto dramático en la criptología moderna y ha llevado a una división natural en dos tipos de sistemas de cifrado: simétrico y asimétrico.

Uno de los objetivos de estudiar la Criptografía es permitir diseñar o llevar a cabo un sistema de cifrado para evaluar si cualquier sistema, es bastante seguro para la aplicación particular.

Nuestro trabajo se dedica totalmente a los sistemas de cifrados simétricos, los llamados Cifrados en Flujo y en Bloque.

Las técnicas de Cifrado en Flujo se basan en una transformación variante en el tiempo de los símbolos del texto claro. La diferencia fundamental entre el Cifrado en Flujo y el Cifrado en Bloque consiste en la presencia o no de memoria interna en el sistema, así como en el tamaño de la unidad mínima a cifrar[1].

En general, un cifrador en flujo consiste en un generador de clave cuya secuencia pseudoaleatoria de salida (llamada secuencia cifrante o cifradora) se suma módulo dos (operación binaria idéntica a la puerta OR-exclusiva) con los bits del mensaje, para formar la secuencia de bits de salida. Cada bit de salida de la secuencia cifradora pseudoaleatoria depende del estado interno del generador en ese momento[1].

A la hora de diseñar estos cifradores, deben cuidarse una serie de propiedades en la secuencia utilizada. Al margen de conseguir que las secuencias generadas parezcan aleatorias, la secuencia debe tener un comportamiento lo más impredecible posible. Es decir, a partir de una fracción de la secuencia cifrante no debe poder predecirse el resto, ya que en tal caso se facilitaría la labor del criptoanalista.

Parte de este trabajo se dedica a realizar una fundamentación teórica para hacer ataques estadísticos buscando auto correlaciones en los bits de salida de los cifradores en flujo. Como antes se había dicho el Criptoanálisis es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido. El término "Criptoanálisis" también se utiliza para referirse a cualquier intento de sortear la seguridad de distintos tipos de algoritmos y protocolos criptográficos en general, y no solamente el cifrado. Aunque el objetivo ha sido siempre el mismo, los métodos y técnicas del criptoanálisis han cambiado drásticamente a través de la historia de la criptografía, adaptándose a una creciente complejidad criptográfica, que abarca desde los métodos de lápiz y papel del pasado, pasando por máquinas como Enigma hasta llegar a los sistemas basados en computadoras del presente.

Una transformada representa el cambio de un dominio hacia otro, y que debido a sus propiedades, reduce la complejidad de problemas matemáticos. Este tipo de herramienta ha sido muy útil y fundamental en la solución de problemas en distintos campos y de diversa naturaleza. Entre estas transformadas, está la de Hadamard que nos será útil en el criptoanálisis de los cifradores en flujo.

Una subclase importante de algoritmos de llave simétrica está conformada por los cifradores simétricos por bloque que se caracterizan por dividir el texto claro en bloques de longitud fija, los cuales pueden ser o no procesados de forma independiente de acuerdo al modo de operación en que el cifrador por bloque sea utilizado. Muchos de los cifradores en bloque utilizan las S-cajas. Formalmente, una S-caja es una función o correspondencia de n bits de entrada en m bits de salida $S: Z_2^n \longrightarrow Z_2^m$, es decir, una S-caja puede ser vista como una función booleana de n bits de entrada y m bits de salida. Por ejemplo, el estándar de cifrado de datos (DES por sus siglas en inglés) emplea S-cajas en las cuales el número de bits de entrada (seis) es mayor que el número de bits de salida (cuatro)[4].

La otra parte de este trabajo se dedica a definir las distintas representaciones de las funciones booleanas junto con el espectro de Hadamard, que es una herramienta crucial para hacer la clasificación de tales funciones. Asimismo, se enuncian las principales propiedades matemáticas que deben exhibir las funciones booleanas para ser utilizadas como constructoras de S-cajas.

Esta investigación constituye un primer paso en el desarrollo y avance de una nueva ciencia en nuestro país y dentro del Departamento de Matemática de nuestra Universidad. Es una temática actual relacionada con la Criptografía y enfocada desde el punto de vista matemático. En ella se hace una profundización en el estudio de la Transformada y Matriz de Hadamard; se analizan las auto correlaciones en el código de salida de generadores pseudoaleatorios de los cifradores en flujo y las propiedades de las funciones booleanas con un enfoque nuevo de cómo utilizar esta transformada y la respectiva matriz.

Por tanto, el problema científico que se pretende resolver con esta tesis es:

“Como utilizar la Transformada y Matriz de Hadamard para determinar auto correlaciones en los bit de salida de un generador pseudoaleatorio y las propiedades criptográficamente deseables de las funciones booleanas”

Hipótesis de investigación

“La utilización de la transformada y matrices de Hadamard es una herramienta adecuada para el criptoanálisis y el análisis de las propiedades de las funciones booleanas que se utilizan en criptografía”

Como objetivo general se propone entonces: “Realizar un estudio de las funciones booleanas, de la transformada y Matrices de Hadamard así como su aplicabilidad a la Criptografía”

Para lograr dicho objetivo general, se proponen los siguientes objetivos específicos:

1. Estudiar la Transformada de Hadamard.
2. Enunciar las propiedades de las Matrices de Hadamard.
3. Estudiar las funciones Booleanas y sus propiedades criptográficamente deseables.
4. Aplicar las funciones booleanas, la Transformada y Matrices de Hadamard en la Criptografía.

Para dar cumplimiento a estos objetivos fue necesario plantearse y solucionar las siguientes tareas de investigación:

1. Detección del problema y recolección de la información necesaria para su posible solución.
2. Estudio de conceptos matemáticos del Álgebra, de las funciones booleanas y de la Criptografía.
3. Formulación de una teoría matemática que sustente la solución del problema planteado.

4. Implementación en paquetes de propósito general como el Mathcad para la validación de algunas aplicaciones.

El primer paso para la realización de este trabajo fue la confección del marco teórico, para ello se realizó una amplia revisión de la literatura consultando libros, artículos y páginas de internet, entre otras fuentes. Los elementos esenciales se encuentran expuestos de manera resumida en el primer capítulo de la presente tesis.

Novedad científica:

a. La elaboración de toda una teoría que permite determinar funciones booleanas deseables de manera sencilla y con menor costo computacional.

b. La introducción de una nueva herramienta matemática para el Criptoanálisis.

c. Nuevas posibilidades de aplicación de las temáticas que se abordan en la tesis en investigaciones dirigidas por la Dirección de Criptografía del MININT y generalización de estos resultados.

La tesis está estructurada en: Introducción, tres Capítulos, Conclusiones, Recomendaciones, Referencias Bibliográficas y Anexos.

En el primer capítulo abordamos la construcción sencilla de matrices de Hadamard y sus generalidades. Se ha tratado de presentar los resultados y problemas abiertos con el suficiente rigor, para que los lectores puedan obtener una visión general sin necesidad de un profundo conocimiento de los antecedentes algebraicos. Se incluyen las definiciones básicas y las propiedades de las matrices de Hadamard, en forma abreviada.
La emoción puramente intelectual y el desafío de encontrar nuevas matrices de Hadamard y la confirmación de la conjetura de Hadamard se ve reforzada por el conocimiento de que son maravillosamente útiles.

En el segundo capítulo se presenta lo relacionado con el mundo de las funciones booleanas y las propiedades criptográficamente deseables. Además, se explica cómo es el funcionamiento de las S-cajas dentro de la criptografía simétrica.

El tercer capítulo está dedicado a la aplicación que tienen las mismas en la Criptografía y las Funciones Booleanas, donde entre otros aspectos se refleja como Las matrices de Hadamard actúan sobre la información estadística de la distribución de las entradas y salidas de secuencias, permitiendo el alto error de distancia de corrección de los códigos y las secuencias de correlación baja.

Capítulo 1. Transformada y matrices de Hadamard.

Introducción

En la literatura las referencias de la Transformada de Hadamard, las matrices de Hadamard y las funciones relacionadas con ellas son extensas. Estas referencias abarcan los asuntos de procesamiento de señal, la codificación y transmisión de imagen, el análisis estadístico, el procesamiento y codificación de la voz, los circuitos lógicos, la filtración, las olas electromagnéticas, los dispositivos ópticos y su modelado matemático, el procesamiento de radar, la sismología, la holografía, el reconocimiento de patrones, la compresión de datos y el análisis químico[5].

La serie de funciones de Hadamard puede aplicarse a muchas áreas dónde las técnicas sinusoidales habían dominado anteriormente. Esto es, por ejemplo, en el diseño de equipamiento digital para la comunicación y aplicaciones computacionales[6].

En el procesamiento de imágenes y el reconocimiento de patrones la motivación para usar otras transformadas como la de Fourier es que reduce el tiempo computacional para una resolución dada, o para aumentar la resolución sin incurrir en la penalidad de tiempo de cómputo largo. La transformada de Hadamard se ha usado de manera efectiva para satisfacer estos requisitos. Un acercamiento general al reconocimiento de patrones es llevar a cabo una transformación de un modelo de patrones y la auto correlación de conjuntos transformados de valores para determinar el grado de reconocimiento, en lugar de intentar encontrar auto correlaciones de las señales originales. Pueden encontrarse ahorros sustanciales en el tiempo de cómputo de esta manera. Usada de la manera correcta, la transformada de Hadamard puede reducir la complejidad de dos procesos dimensionales al nivel de adiciones y substracciones de coeficientes.[7]

1.1. Transformada de Hadamard

La Transformada de Hadamard es quizás la más conocida de las transformadas ortogonales no sinusoidales. La Transformada de Hadamard ha ganado la prominencia en las aplicaciones en el procesamiento de señales digitales, dado que sólo usa sumas y substracciones para computar. Por consiguiente, su implementación en el hardware es muy simple[8].

Definición 1.1. La transformada de Hadamard de una función f en V_n (donde los valores de f pueden ser 0 y 1) es una aplicación $H(f): V_n \to \mathbb{R}$, definida por

$$H(f)(h) = \sum_{x \in V_n} f(x)(-1)^{h \cdot x}, \quad (1.1)$$

En la cual se definen los coeficientes de f con respecto a las bases orto normales del carácter de grupo $Q_x(h) = (-1)^{h \cdot x}$; f puede ser recuperada por la transformada inversa de Hadamard

$$f(x) = 2^{-n} \sum_{h \in V_n} H(f)(h)(-1)^{h \cdot x} \quad (1.2)$$

El espectro de Hadamard de f es una lista de los 2^n coeficientes de Hadamard dado por (1.1) con h variable. Las funciones booleanas simples son funciones constantes 0 y 1. Obviamente, $H(0)(u) = 0$ y los coeficientes de Hadamard para la función 1 son dados por el siguiente lema enunciado en [9].

Lema 1.1. Si $h \in \mathbb{V}_n$, tenemos $\sum_{u \in V_n} (-1)^{u \cdot h} = \begin{cases} 2^n, & \text{si } h = 0 \\ 0, & \text{en otro caso} \end{cases}$

Demostración

Primero, si $h = 0$, entonces todos los sumandos son 1. Ahora, asumamos que $h \neq 0$, y consideremos el hiperplano $M = \{u \in \mathbb{V}_n : u \cdot h = 0\}, \bar{M} = \{u \in \mathbb{V}_n : u \cdot h = 1\}$. Obviamente, estos hiperplanos constituyen una partición de $\mathbb{V}_n$. Aun más, para cualquier $u \in M$, el sumando es

1, y para cualquier $u \in \bar{M}$, el sumando es -1. La cardinalidad de $M, \bar{M}$ son las mismas, que es 2^{n-1}, así tenemos el lema[10].

Un cálculo directo del espectro de Hadamard completo utilizando (1.1) implica una complejidad de N^2 pasos, con $N = 2^n$. Sin embargo tal y como ocurre con la transformada rápida de Fourier (ver en [11]), es posible definir un procedimiento rápido para el cálculo de la transformada de Hadamard que puede ser computado con únicamente $NLog(N)$ pasos. Para lograr esa aceleración, la Transformada Rápida de Hadamard (TRH) utiliza el concepto de *diagrama de mariposa.* Un diagrama de mariposa de tamaño 2 (el tamaño más pequeño), toma dos bits de entrada(x_0, x_1), y produce dos bits de salida (y_0, y_1), de la siguiente manera:

$$\begin{cases} y_0 = x_0 + x_1 \\ y_1 = x_0 - x_1 \end{cases}$$

En general, la TRH divide recursivamente el cálculo de un vector de tamaño $n = r\ m$, en *r* transformaciones más pequeñas de tamaño *m,* donde *r* es la base de la transformación. Estas *r* transformaciones pequeñas son combinadas utilizando diagramas de mariposa de tamaño *r*, las cuales a su vez, son TRH de tamaño r.

1.2 Cálculo algorítmico de la Transformada de Hadamard

La transformada unidimensional de Hadamard de una secuencia se ha calculado para un vector genérico a partir de la evaluación valor a valor de la misma. Se ha demostrado que el algoritmo funciona correctamente para cualquier secuencia.

Algoritmo para el cálculo de la transformada directa de Hadamard (tomado de [8, 12])

```
function y=hdt(x)
Calcula la transformada de Hadamard de la secuencia x
[m,N]=size(x); %Obtiene el tamaño de la matriz
t=round(log10(N)/log10(2)); %Calcula el valor de t tal que N=2^t
for u=1:N
  B=0;
  for n=1:N
    A=0;
    for l=0:t-1
      a=dec2bin(n-1,t); %Paso a binario
      b=dec2bin(u-1,t); %Paso a binario
      A=A+(a(t-l)*b(t-l));
    end
    B=B+x(n)*((-1)^A);
  end
  y(u)=B;
end
y=y/N;
```

Algoritmo para el cálculo de la transformada inversa de Hadamard (tomado de [8, 12])

```
function y=ihdt(x)
%Calcula la transformada inversa de Hadamard de la secuencia x
```

```
[m,N]=size(x); %Obtiene el tamaño de la matriz
t=round(log10(N)/log10(2)); %Calcula el valor de t tal que N=2^t
for u=1:N
  B=0;
  for n=1:N
    A=0;
    for l=0:t-1
      a=dec2bin(n-1,t); %Paso a binario
      b=dec2bin(u-1,t); %Paso a binario
      A=A+(a(t-l)*b(t-l));
    end
    B=B+x(n)*((-1)^A);
  end
  y(u)=B;
end
```

Al ser una transformada simétrica, la transformada inversa se calcula igual excepto por el valor de multiplicación 1/N.

1.3. Las matrices de Hadamard

Introducción

Una matriz de Hadamard es una matriz H de orden $n \times n$ con las entradas ± 1 qué satisface $H\,H^t = n\,I$, donde H es real, simétrica y las filas y las columnas de las mismas son ortogonales dos a dos.[6].

Estas matrices deben su nombre a un teorema del propio Hadamard:

Teorema 1.1. Sea $X = (x_{ij})$ una matriz real de orden $n \times n$ cuyas entradas satisfacen que $|x_{ij}| \leq 1$ para toda i, j. Entonces $|det(X)| \leq n^{\frac{n}{2}}$. La igualdad se tiene si y solo si X es una matriz de Hadamard[7].

Sea $x_1, \dots, x_n$ las filas de X, entonces por la geometría euclidiana simple, $|det(X)|$ es el volumen del paralelepípedo con lados $x_1, \dots, x_n$; así $|det(X)| \leq |x_1| \cdots |x_n|$, donde $|x_i|$ es la longitud euclidiana de x_i ; la igualdad se tiene si y solo si $x_1, \dots, x_n$ son mutuamente perpendiculares.

Por hipótesis, $|x_i| = ({x_{i1}}^2 + \cdots + {x_{in}}^2)^{1/2} \leq n^{1/2}$, con igualdad si y solo si $|x_{ij}| = 1$ para toda j.

¿Para qué valores de orden n existen matrices de Hadamard? Hay una importante Condición necesaria:

Teorema 1.2. Si una matriz de Hadamard de orden n existe, entonces $n = 1$ o $n = 2$ o $n \equiv 0 (mod\ 4)$.

Para ver esto, observamos primero que cambiando el signo de cada entrada en una columna de una matriz de Hadamard se obtiene otra matriz de Hadamard. Cambiando los signos de todas las columnas en que la entrada de la primera fila sea $-$, nosotros asumimos que todas las entradas en la primera fila son $+$.

$$\begin{array}{cccc} \overbrace{+ \cdots +}^{a} & \overbrace{+ \cdots +}^{a} & \overbrace{+ \cdots +}^{a} & \overbrace{+ \cdots +}^{a} \\ + \cdots + & + \cdots + & - \cdots - & - \cdots - \\ + \cdots + & - \cdots - & + \cdots + & - \cdots - \end{array}$$

Figure 1.1: Tres filas de una matriz de Hadamard

Como cada una de las otras filas es ortogonal a la primera, se tiene que cada fila tiene m entradas $+$ y m entradas$-$, dónde $n = 2\,m$. Y si $n > 2$, las primeras tres filas son como en Figura 1, con $n = 4\,a$.

Si es así la condición necesaria dada en el teorema 1.2 es suficiente. El múltiplo más pequeño de 4 para el cual se ha construido una matriz es actualmente 428[13].

1.4. Equivalencia de matrices de Hadamard

Las matrices de Sylvester y Paley de órdenes 4 y 8 son equivalentes - hay esencialmente de hecho una única matriz de cada uno de estos órdenes. Para todos los órdenes más grandes para que ambas matrices existan tiene que cumplirse, $n = p + 1$, dónde p es un primo de Mersenne. En los otros casos ellas no son equivalentes[7].

En las matrices de Hadamard se realizan varias operaciones. De estas las que conservan la propiedad de Hadamard son:

a) Permutar filas, y cambiar el signo de algunas de ellas;
b) Permutar columnas, y cambiar el signo de algunas de ellas;
c) Transponer

Dos matrices de Hadamard H_1 y H_2 son equivalentes si una puede ser obtenida a partir de otra por operaciones de tipo a) y b); es decir, si $H_2 = P^{-1}H_1Q$, donde P y Q son matrices monomiales (tienen solamente un elemento no nulo en cada fila o columna) con entradas no nulas ± 1.

El grupo de automorfismo de una matriz de Hadamard H consiste en el grupo de todos los pares (P, Q) de matrices monomiales con entradas no nulas ± 1 satisfaciendo $H = P^{-1}HQ$; la operación de grupo está dada por $(P_1, Q_1) \circ (P_2, Q_2) = (P_1P_2, Q_1Q_2)$[14].

Note que hay siempre un automorfismo $(-I, -I)$, el cual queda en el centro del grupo de automorfismo[15].

1.5. Construcciones Sencillas

Las investigaciones en el área de las matrices de Hadamard y sus aplicaciones han ido creciendo rápidamente, especialmente durante las tres últimas décadas. Estas matrices pueden ser transformadas para producir los diseños de bloques incompletos, los t-diseños, los diseños de Youden, los diseños ortogonales de F-cuadrado, el diseño óptimo de peso, el conjunto maximal de dos a dos conjuntos de variables aleatorias independientes con la medida uniforme, el error, la corrección y la detección de los códigos, las funciones de Walsh, y otros objetos matemáticos y estadísticos. En este trabajo se estudia la existencia de matrices de Hadamard y algunas de sus aplicaciones[5].

Muy a menudo los problemas más difíciles se pueden afirmar con sencillez engañosa. Esto es particularmente cierto en las matemáticas, y muchos problemas bien conocidos son de este tipo. Típicos son:

- El último teorema de Fermat, que si el entero n es de tres o más, no existen soluciones enteras x, y, z distintas de cero para la ecuación $x^n + y^n = z^n$.
- Conjetura de los cuatros colores de Guthie para mapas del plano, las regiones de cualquier mapa en el plano pueden ser coloreadas con cuatro o menos colores de modo que no hay dos regiones adyacentes que tengan asignadas el mismo color.
- La conjetura de Van Der Waerden, que la permanente de una matriz cuadrada doblemente estocástica de n lados es al menos $n!\, n^{-n}$.

- Conjetura de GoldbacKs, de que cada entero par mayor que 2 es una suma de dos números primos.

Todos estos problemas se conocen desde hace mucho tiempo. Aquí se trata de una conjetura similar, que ha estimulado el interés de los matemáticos y estadísticos en los últimos años. Esta es la conjetura de la matriz de Hadamard, denominada a veces como la conjetura de Paley, aunque está implícito en algunos escritos de antes de la época de Paley. Si n es un entero positivo divisible por 4, hay una matriz H cuadrada de orden n, con todas sus entradas, +1 o -1, tal que $HH^t = n\, I$[5].

Los cuatro primeros problemas mencionados son peculiares por el hecho de que se ha argumentado que su valor real se encuentra en la matemática de subproductos, o sea, es el resultado de la falta de resolverlos. Estos resultados han sido a menudo empleado más útil que sería la solución de estos problemas por sí mismas por medios elementales. Por ejemplo, los intentos de probar el último teorema de Fermat y los otros problemas teóricos numéricos han llevado a la teoría de números algebraicos, al concepto de los ideales en los anillos, así como a una serie de puntos de vistas hermosos de la naturaleza de los números primos.

Sin embargo, la conjetura de la matriz Hadamard es de distinta naturaleza. A pesar de que una serie de ideas asociadas se han desarrollado en la búsqueda de matrices Hadamard, la existencia misma de estas matrices tiene amplias consecuencias en muchos campos de investigación, tales como la teoría del diseño óptimo, la teoría de la información y la teoría de grafos[7].

La construcción más simple de nuevas matrices de Hadamard son las llamadas matrices de Sylvester-Hadamard que se construyen a través del producto de Kronecker. En general, si $A = (a_{ij})$ y $B = (b_{kl})$ son matrices de tamaño $m \times n$ y $p \times q$ respectivamente, el producto de Kronecker $A \otimes B$ es la matriz $mp \times nq$ hecha de bloques de tamaño $p \times q$, donde el bloque (i, j) es $a_{ij}B$. Entonces, la matriz de Sylvester $S(k)$ de orden 2^kes el producto de Kronecker iterado de k copias de la matriz de Hadamard $\begin{pmatrix} + & + \\ + & - \end{pmatrix}$ de orden 2[9].

Podemos expresar ahora la Transformada de Hadamard en términos de las matrices de Sylvester-Hadamard $\mathrm{H_n}$, es decir,

$\mathrm{H(f) = f\,H_n}$; donde $(-1)^{\mathrm{u\cdot v}}$ es la entrada en la posición $\mathrm{(u,v) \in V_n \times V_n}$, en la matriz $\mathrm{H_n}$. Consecuentemente,

$$\mathrm{f = \frac{1}{2^n}\ H(f)H_n} \quad \text{ó} \quad \mathrm{f(u) = \frac{1}{2^n} \sum_{v \in V_n} (-1)^{u\cdot v}\ H(f)(v)}$$

Similarmente, si ζ es una secuencia $(1,-1)$ en $\mathrm{V_n}$, entonces la transformada de Hadamard es definida por

$H_\zeta = \zeta H_n$

Lema 1.2. Si la matriz de Sylvester-Hadamard H_n está dada por

$H_n = \begin{pmatrix} l_0 \\ l_1 \\ \vdots \\ l_{2^n-1} \end{pmatrix}$, donde l_i es una fila de H_n, entonces l_i como un vector es $l_i = ((-1)^{\alpha_i \cdot \alpha_0}, (-1)^{\alpha_i \cdot \alpha_1}, \dots, (-1)^{\alpha_i \cdot \alpha_{2^n-1}})$, donde α_i es la representación binaria de i, $0 \leq i \leq 2^n - 1$, escrito como un vector de longitud 2^n .

Demostración

Por inducción en n.

Para $n = 1$, tenemos $H_1 = \begin{bmatrix} + & + \\ + & - \end{bmatrix}, l_0 = (+ \quad +)$, la sucesión de $\langle 0, x \rangle$ y $l_1 = (+ \quad -)$, la sucesión de $\langle 1, x \rangle$ donde $x \in \mathbb{V}_1$.

Supongamos que el lema es verdadero para $n = 1,2, \dots, k-1$

Puesto que, $H_k = H_1 \otimes H_{k-1}$, donde $\otimes$ es el producto de Kronecker, cada fila de H_k puede ser expresada como $\delta \otimes l$ donde $\delta = (+ \quad +)$ ó $(+ \quad -)$, y l es una fila de H_{k-1}. Asumiendo que l es la sucesión de una función, decimos $h(x) = \langle \alpha , x \rangle$ donde $\alpha, x \in V_{k-1}$. De esta manera $\delta \otimes l$ es la sucesión de $\langle \beta , y \rangle$ donde $y \in V_k$, $\beta = (0 \quad \alpha)$ ó $(1 \quad \alpha)$ acordando como $\delta = (+ \quad +)$ ó $(+ \quad -)$. Así el lema es verdadero para $n = k$

Definiendo $l_{i+2^n} = -l_i$. Entonces como una consecuencia del lema anterior, se tiene tenemos que todas las secuencias afines se encuentran entre las filas de $\pm H_n$, es decir, $l_0, \dots, l_{2^{n+1}-1}$.

Corolario 1.1. [16]Hay una matriz de Hadamard de orden 2^k para cada entero positivo k

Demostración

Utilizando la definición de producto de Kronecker y definiendo a la matriz de orden 2^k de forma recursiva como $H_n = H_{n-1} \otimes \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ con $H_0 = 1$.

Teorema 1.3.Paley (1933). Si p^αes una potencia prima(es una potencia de entero positivo de un número primo) y $p^\alpha + 1 \equiv 0 \ (mod\ 4)$, entonces hay una matriz de Hadamard de orden $p^\alpha + 1$[2].

Demostración

Supongamos que los miembros del campo $GF(\ p^\alpha)$ están etiquetados $a_0, a_1, a_2, \ldots$, en algún orden. Una matriz Q de orden p^α es definida como sigue: la entrada (i,j) de Q igual $\chi(a_i - a_j)$, donde χ es el carácter cuadrático en $GF(\ p^\alpha)$, es decir,

$$\chi(a) = \begin{cases} 0\ , & a = 0 \\ 1, & a = b^2\ para\ algún\ b \in GF(p^\alpha) \\ -1, & en\ otro\ caso \end{cases}$$

Entonces, escribiremos

$$S = \begin{bmatrix} 0 & 1 \\ -1 & Q \end{bmatrix},\ H = I + S$$

H es una matriz de Hadamard

Ejemplo 1.1. Para construir una matriz de Hadamard de orden 12, observamos que $12 = 11 + 1$. Los elementos cuadráticos de $GF(11)$ son $1,3,4,5\ y\ 9$; usando el orden natural $a_0 = 0, a_1 = 1, \ldots, a_{10} = 10$, Q y H son:

$$Q = \begin{bmatrix} 0 & - & + & - & - & - & + & + & + & - & + \\ + & 0 & - & + & - & - & - & + & + & + & - \\ - & + & 0 & - & + & - & - & - & + & + & + \\ + & - & + & 0 & - & + & - & - & - & + & + \\ + & + & - & + & 0 & - & + & - & - & - & + \\ + & + & + & - & + & 0 & - & + & - & - & - \\ - & + & + & + & - & + & 0 & - & + & - & - \\ - & - & + & + & + & - & + & 0 & - & + & - \\ - & - & - & + & + & + & - & + & 0 & - & + \\ + & - & - & - & + & + & + & - & + & 0 & - \\ - & + & - & - & - & + & + & + & - & + & 0 \end{bmatrix}$$

$$H = \begin{bmatrix} + & + & + & + & + & + & + & + & + & + & + & + \\ - & + & - & + & - & - & - & + & + & + & - & + \\ - & + & + & - & + & - & - & - & + & + & + & - \\ - & - & + & + & - & + & - & - & - & + & + & + \\ - & + & - & + & + & - & + & - & - & - & + & + \\ - & + & + & - & + & + & - & + & - & - & - & + \\ - & + & + & + & - & + & + & - & + & - & - & - \\ - & - & + & + & + & - & + & + & - & + & - & - \\ - & - & - & + & + & + & - & + & + & - & + & - \\ - & - & - & - & + & + & + & - & + & + & - & + \\ - & + & - & - & - & + & + & + & - & + & + & - \\ - & - & + & - & - & - & + & + & + & - & + & + \end{bmatrix}$$

Teorema 1.4. Si p^{α} es una potencia prima y $p^{\alpha} + 1 \equiv 2 \ (mod\ 4)$. entonces hay una matriz de Hadamard de orden $2(p^{\alpha} + 1)$[7].

Demostración

Usando el carácter cuadrático χ en $GF(p^{\alpha})$, una matriz Q es construida como en el Teorema 1.3, y

$$S = \begin{bmatrix} 0 & 1 \\ 1 & Q \end{bmatrix},$$

Entonces

$$H = S \otimes \begin{bmatrix} + & + \\ + & - \end{bmatrix} + I \otimes \begin{bmatrix} + & - \\ - & - \end{bmatrix}$$

Es la requerida matriz de Hadamard.

Ejemplo 1.2. Como $12 = 2(5+1)$, donde 5 es primo y $5+1 \equiv 2\ mod(4)$, podemos usar el Teorema 1.4 para construir una matriz de orden 12. Los elementos cuadráticos en $GF(5)$ son 1 y 4, así

$$Q = \begin{bmatrix} 0 & + & - & - & + \\ + & 0 & + & - & - \\ - & + & 0 & + & - \\ - & - & + & 0 & + \\ + & - & - & + & 0 \end{bmatrix} \quad S = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & + & - & - & + \\ 1 & + & 0 & + & - & - \\ 1 & - & + & 0 & + & + \\ 1 & - & - & + & 0 & + \\ 1 & + & - & - & + & 0 \end{bmatrix}$$

$$H = \begin{bmatrix} + & - & + & + & + & + & + & + & + & + & + & + \\ - & - & + & - & + & - & + & - & + & - & + & - \\ + & + & + & - & + & + & - & - & - & - & + & + \\ + & - & - & - & + & - & - & + & - & + & + & - \\ + & + & + & + & + & - & + & + & - & - & - & - \\ + & - & + & - & - & - & + & - & - & + & - & + \\ + & + & - & - & + & + & + & - & + & + & - & - \\ + & - & - & + & + & - & - & - & + & - & - & + \\ + & + & - & - & - & - & + & + & + & - & + & + \\ + & - & - & + & - & + & + & - & - & - & + & - \\ + & + & + & + & - & - & - & - & + & + & + & - \\ + & - & + & - & - & + & - & + & + & - & - & - \end{bmatrix}$$

Gruner en los años (1939-40) mostró que una matriz de Hadamard de orden $n = k^2$ puede ser construida si $k-1$ y $k+1$ son ambos potencias primas. El caso $k = 18$ da una matriz de Hadamard de orden 324; este orden no se había sido construido hasta ese momento.

Williamson en el año (1944) generalizó los teoremas 1.3 y 1.4 a:

Teorema 1.5. Si existe una matriz de Hadamard de orden $h, h > 1$, y p^α es una potencia prima impar, entonces existe una matriz de Hadamard de orden $h(p^\alpha + 1)$. La demostración puede encontrarse en [5]

Conclusiones del Capítulo

En este capítulo se han presentado de manera resumida los conceptos y definiciones fundamentales de la transformada y matriz de Hadamard. En cualquier caso no hemos pretendido hacer un análisis exhaustivo ya que nuestro interés se centra únicamente en exponer las herramientas matemáticas para llevar a cabo el desarrollo de los próximos capítulos. Estas fundamentaciones teóricas y recomendaciones prácticas, pueden tener aplicaciones en muchos otros campos, y por tanto, un alcance mucho más allá del presente trabajo.

Capítulo 2. Funciones booleanas.

¡Tome lo que usted necesite; actué como debe, y va a obtener aquello para lo que quiera!

René Descartes (1596–1650)

2.1. Definiciones básicas en las funciones booleanas.

El propósito de este capítulo es dar algunas definiciones preliminares sobre las funciones de Boole para introducir una herramienta para la Criptografía, es decir, la transformada de Hadamard. El uso de la transformada de Hadamard hace que el cálculo de la no linealidad, y muchas de las propiedades de cifrado de una función booleana, sea una tarea muy fácil y agradable. Otros temas necesarios en los capítulos siguientes se presentarán también aquí[9].

Sea $\mathbb{V}_n$ el espacio vectorial de dimensión n sobre el campo binario $GF(2)$. Para dos vectores $a = (a_1,\ldots,a_n)$ y $b = (b_1,\ldots,b_n)$ de $\mathbb{V}_n$, nosotros definimos el producto escalar $a \cdot b = a_1 b_1 \oplus \cdots \oplus a_n b_n$, dónde la multiplicación y suma $\oplus$ (llamada XOR) son sobre $GF(2)$ (no debe confundirse con el producto directo de espacios del vector, pero eso va a estar claro en el contexto). También definimos la operación $*$ por $a * b = (a_1 b_1, \ldots, a_n b_n)$. Dado un vector $\mathbf{a}$, siempre será un vector fila a menos que el contexto exija obviamente que sea un vector columna.

Definición 2.1. Una función booleana f de n variables es una aplicación que va de $\mathbb{V}_n$ a $GF(2)$. La secuencia de $(0,1)$ definida por $(f(v_0), f(v_1), \ldots, f(v_{2^n-1}))$ es llamada tabla de verdad de f, donde $v_0 = (0,\ldots,0,0), v_1 = (0,\ldots,0,1), \ldots, v_{2^n-1} = (1,\ldots,1,1)$, ordenado por el orden lexicográfico. (A menudo, cuando hay un peligro de confusión debido a una

anotación similar, nosotros escribiremos $\alpha_i$en lugar de v_i. La secuencia de $(1,-1)$ de f definida por $((-1)^{f(v_0)},\dots,(-1)^{f(v_{2^n-1})})$ es la tabla de verdad polar de f. El álgebra de todas las funciones booleanas en V_n se denotará por $\mathfrak{B}_n$[17].

Obviamente, $v_i = \alpha_i = b(i)$, dónde $b(i)$ es la representación binaria de i, $0 \le i \le 2^n - 1$, escrito como un vector de longitud 2^n.

Una función booleana en $\mathbb{V}_n$ puede expresarse como un polinomio en $GF(2)[x_1,\dots,x_n]/({x_1}^2 - x_1,\dots,{x_n}^2 - x_n)$, la forma normal algebraica (ANF abreviatura en ingles), es decir, $f(x) = \sum_{a\in V_n} c_a {x_1}^{a_1}\cdots {x_n}^{a_n}$, donde $c_a \in GF(2)$ y $a = (a_1,\dots,a_n)$. Es más, $c_a = \sum_{x\le a} f(x)$, donde $x \le a$ significa que $x_i \le a_i$, para toda $1 \le i \le n$(decimos a veces que **a** cubre a **x**).

El número de variables en el monomio del orden más alto con el coeficiente no nulo se llama grado algebraico, o simplemente el grado de f. Se dice que una función booleana es homogénea si su ANF sólo contiene condiciones del mismo grado. La negación lógica o complemento de una función booleana f es $\bar{f} = f \oplus 1$.

Sea f una función en $\mathbb{V}_n$ y sea U un subespacio de $\mathbb{V}_n$. La restricción de f a U, denotado por f_U, es una función en U, definida por la regla $f_U(u) = f(u)$ para cada $u \in U$.

La dimensión de un subespacio vectorial U de $\mathbb{V}_n$ es denotado por $\dim(U)$. Una función afín $l_{a,c}$ en $\mathbb{V}_n$ es una función que toma la forma siguiente:

$l_{a,c}(x) = a\cdot b \oplus c = a_1x_1 \oplus \cdots \oplus a_nx_n \oplus c,$ Donde $a = (a_1,\dots,a_n) \in \mathbb{V}_n$ $c \in GF(2)$. Si $c = 0$, entonces $l_{a,0} = l_a$ es una función lineal.

A cada función booleana $f: \mathbb{V}_n \rightarrow GF(2)$ le asociamos su forma característica, o función signo o función polar, denotada por $\hat{f}: \mathbb{V}_n \rightarrow \{1,-1\}$ y definida por $\hat{f}(x) = (-1)^{f(x)}$.

El comportamiento de la función signo de la suma y del producto de funciones booleanas, se muestra en la siguiente proposición.

Proposición 2.1. Si f, g son funciones booleanas en $\mathbb{V}_n$, entonces las afirmaciones siguientes son válidas:

1. $\widehat{f \oplus g} = \hat{f}\,\hat{g}$
2. $2\widehat{fg} = 1 + \hat{f} + \hat{g} - \hat{f}\,\hat{g}$

Demostración

$$\widehat{f \oplus g} \equiv (-1)^{f(x)\oplus g(x)} = (-1)^{f(x)} \cdot (-1)^{g(x)} \equiv \hat{f}\,\hat{g}$$

Esta afirmación se desprende de la observación que $\hat{f}(x) = 1 - 2\,f(x)$

$2\widehat{fg} = 2\,(1 - 2f(x)g(x)) = 2 - 4\,f(x)g(x)$. Por otro lado se tiene que

$$\begin{aligned} 1 + \hat{f} + \hat{g} - \hat{f}\,\hat{g} &= 1 + (1 - 2f(x)) + (1 - 2\,g(x)) - (1 - 2f(x))(1 - 2\,g(x)) \\ &= 3 - 2f(x) - 2g(x) - (1 - 2f(x) - 2g(x) + 4f(x)g(x)) \\ &= 2 - 4f(x)g(x) \end{aligned}$$

Definición 2.2. El peso de Hamming definido en [18] de un vector $x \in \mathbb{V}_n$, denotado por $wt(x)$, es el número de $1s$ en el vector x.

Para una función booleana en $\mathbb{V}_n$, sea $\Omega_f = \{x \in \mathbb{V}_n : f(x) = 1\}$ el soporte de f. El peso de Hamming de una función f es el peso de Hamming de su tabla de verdad, es decir, la cardinalidad de $f^{-1}(1)$, o equivalente $wt(f) = |\Omega_f|$ tomado de [19]. La distancia de Hamming entre dos funciones $f, g: \mathbb{V}_n \rightarrow GF(2)$, denotado por $d(f,g)$ es definida como $d(f,g) = wt(f \oplus g)$.

La no linealidad de una función f, denotada por $\mathcal{N}_f$ y enunciada en [20-22], es definida como $\mathcal{N}_f = \min_{\phi \in \mathcal{A}_n} d(f, \phi)$, donde $\mathcal{A}_n$ es la clase de todas las funciones afines en $\mathbb{V}_n$. Una función de n variables es llamada balanceada si su peso es exactamente 2^{n-1}.

Lema 2.1. [23]El peso y la distancia de Hamming satisfacen las siguientes propiedades:

1. $wt(x \oplus y) = wt(x) + wt(y) - 2\, wt(x * y);$
2. $d(f,g) = |\{x \in \mathbb{V}_n : f(x) \neq g(x)\}|;$
3. $d(f,g) + d(g,h) \geq d(f,h);$
4. $d(f,g) = 2^n - \frac{1}{2} \sum_x \hat{f}(x) \cdot \hat{g}(x)$
5. $d(f,\bar{g}) = 2^n - d(f,g)$

2.2. Función de Autocorrelación

Definición 2.3. [24-26]La función de Autocorrelación $\hat{r}_f(a)$ es definida como

$$\hat{r}_f(a) = \sum_{x \in \mathbb{V}_n} \hat{f}(x) \cdot \hat{f}(x \oplus a).$$

En lo adelante escribiremos $\hat{r}(a)$ si no hay ningún riesgo de confusión. Note que $\hat{r}(0)$es igual a 2^n. El valor de correlación entre dos funciones booleanas g y h es definido por[9]

$$c(g,h) = 1 - \frac{d(g,h)}{2^{n-1}}$$

Nosotros definimos la función de correlación cruzada entre $f, g: \mathbb{V}_n \to GF(2)$ por

$$c(\hat{f},\hat{g})(y) = \sum_{x \in \mathbb{V}_n} \hat{f}(x) \cdot \hat{g}(x \oplus y)$$

Una relación muy importante afirma que la transformada inversa de la función polar es la función de autocorrelación.

Teorema 2.1.[27]Una función booleana en $\mathbb{V}_n$ satisface

$H(\hat{r})(h) = H(\hat{f})^2(h)$, para toda $h \in \mathbb{V}_n$.

Ya que $\Pr\left(\hat{f}(x) \neq \hat{f}(x \oplus a)\right) = \frac{1}{2} - \frac{\hat{r}(a)}{2^{n+1}}$ para valores grandes de n, este teorema permite un cómputo eficiente de estas probabilidades, requiriendo $O(n\,2^n)$ operaciones, en vez de $O(2^{2n})$ para un cálculo directo.

La relación principal entre la transformada de Hadamard de f y $\hat{f}$ es mostrada en el siguiente lema.

Lema 2.2. Tenemos

$$H(\hat{f})(h) = -2H(f)(h) + 2^n\delta(h),$$

o

$$H(f)(h) = 2^{n-1}\delta(h) - \frac{1}{2}H(\hat{f})(h),$$

Donde $\delta(h) = \begin{cases} 1, & h = 0 \\ 0, & h \neq 0 \end{cases}$

Demostración

A partir de la parte izquierda, obtenemos

$$H(\hat{f})(h) = \sum_{x \in V_n} (-1)^{(f(x) \oplus (h \cdot x))} = \sum_{x \in V_n} (1 - 2f(x))(-1)^{(h \cdot x)} =$$

$$= \sum_{x \in V_n} (-1)^{(h \cdot x)} - 2\sum_{x \in V_n} f(x)(-1)^{(h \cdot x)} = 2^n\delta(h) - 2H(f)(h)$$

Por el lema 1.1

2.3. Transformada de Hadamard en subespacios.

Uno puede encontrar una ecuación muy importante entre $H(f)$ y f restringido a un subespacio arbitrario de $\mathbb{V}_n$, llamada Fórmula de Suma de Poisson, tomado de [28].

Teorema 2.2. Sea $f: \mathbb{V}_n \to GF(2)$ y $H(f)$ su transformada de Hadamard. Sea S un subespacio arbitrario de $\mathbb{V}_n$ y sea $S^{\perp}$ el dual de S, es decir, $S^{\perp} = \{x \in \mathbb{V}_n : x \cdot s = 0, \forall s \in S\}$.Entonces

$$\sum_{u \in S} H(f)(u) = 2^{\dim(S)} \sum_{u \in S^{\perp}} f(u)$$

Demostración

Tenemos $\sum_{u \in S} H(f)(u) = \sum_{u \in S}\left(\sum_{v \in \mathbb{V}_n} f(v)(-1)^{u \cdot v}\right) =$

$$= \sum_{v \in \mathbb{V}_n} f(v)\left(\sum_{u \in S}(-1)^{u \cdot v}\right) = 2^{\dim(S)} \sum_{v \in S^{\perp}} f(v)$$

Corolario 2.1. Para cualquier función booleana $f: V_n \to GF(2)$

$$\sum_{u \leq v} H(f)(u) = 2^{wt(v)} \sum_{u \leq \bar{v}} f(u),$$

Donde $u \leq v$ significa que si $u_i = 1$, entonces $v_i = 1$, para cada $1 \leq i \leq n$.

2.4. Transformaciones Lineales y la función signo

Lema 2.3. Si la función booleana f puede ser obtenida desde g por una transformación afín de la entrada , es decir, $g(v) = f(A\,v \oplus b)$, donde A es una matriz inversible y $b \in \mathbb{V}_n$, entonces las transformadas de Hadamard de f y g están relacionadas por

$$H(g)(u) = \pm H(f)(u\,A^{-1})$$

Demostración

Primero, $H(g)(u) = \sum_{v \in V_n} g(v)(-1)^{u \cdot v} = \sum_{v \in V_n} (-1)^{u \cdot v} f(A\,v \oplus b)$

Por definición $v = (A^{-1})\,w \oplus (A^{-1})b$ y $u' = u\,A^{-1}$, tenemos

$H(g)(u) = \sum_w (-1)^{u \cdot A^{-1} w} (-1)^{u \cdot A^{-1} b} f(w) = \pm \sum_w (-1)^{u' \cdot w} f(w) = \pm H(f)(u')$, con la cual probamos el lema.

Sea la función lineal $l_a(x) = a \cdot x$.

Teorema 2.2. Las siguientes afirmaciones son verdaderas:

1. $H(\widehat{f \oplus 1})(x) = H(\hat{f})(x)$
2. Si $g(x) = f(x) \oplus l_a(x)$, entonces $H(\hat{g})(x) = H(\hat{f})(x \oplus a)$
3. Si $g(x) = f(x \oplus a)$, entonces $H(\hat{g})(x) = (-1)^{a \cdot x} H(\hat{f})(x)$
4. Si $g(x) = f(xA)$, A es una matriz no singular, entonces $H(\hat{g})(x) = H(\hat{f})(x\,A^{-t})$ (A^{-t} es la transpuesta de la matriz inversa)
5. Si $h(x) = f(x) \oplus g(x)$ en $\mathbb{V}_n$, entonces $H(\hat{h})(x) = \frac{1}{2} \sum_{v \in V_n} H(\hat{f})(v)\, H(\hat{g})(x \oplus v)$
6. Si $h(x,y) = f(x) \oplus g(y)$, f en $\mathbb{V}_n$ y g en $\mathbb{V}_m$, entonces $H(\hat{h}) = H(\hat{f})(x)\, H(\hat{g})(y)$
7. Si $k(x) = f(x)\, g(x)$ y $h(x) = f(x) \oplus g(x)$, entonces $H(\hat{h})(x) = \frac{1}{2}\left(2^n \delta(x) + H(\hat{f})(x) + H(\hat{g})(x) - H(\hat{h})(x)\right)$, donde δ es la función delta de Kronecker.

Tomemos $g, h,$ dos funciones booleanas en n variables, tal que $h(x) = g(Ax \oplus a)$, donde A es una matriz $n \times n$ sobre $GF(2)$.

En la transformada de Hadamard para g, $H(g)(w) = \sum_{x \in V_n} g(x)\,(-1)^{w \cdot x}$, si reemplazamos x por $(y \oplus a)(A^{-1})^t$, $g(x)$ por $h(x)$ y la suma sobre y en vez de x.

Obtenemos (para facilitar la escritura se denota la transpuesta $(A^{-1})^t = A^{-t}$)

$$H(g)(w) = \sum_x g(x)(-1)^{w \cdot x} = \sum_y (-1)^{w A^{-t} \cdot (y \oplus a)} h(y) =$$
$$\sum_y (-1)^{w A^{-t} \cdot y} (-1)^{w A^{-t} \cdot a} h(y) =$$
$$(-1)^{w A^{-t} \cdot a} \sum_y (-1)^{w A^{-t} \cdot y} h(y) = (-1)^{w A^{-t} \cdot a} H(y)(A^{-t} w)$$

De una manera similar, $H(h)(w) = (-1)^{w \cdot a} H(g)(w A^t)$

Por lo tanto, tenemos la versión más precisa después del lema 2.4.

Definición 2.4. Dos funciones booleanas g, h en V_n son llamadas equivalentes si $g(x) = h(Ax \oplus a) \oplus (b \cdot x) \oplus c$, donde $a, b \in V_n$, $c \in GF(2)$ y A es una matriz no singular de $n \times n$. Si tal transformación no existe, entonces g, h son no equivalentes.

2.5. Ecuación de Parseval

De la definición de la Transformada de Hadamard deducimos que $H(\hat{f})(u)$ es igual al número de ceros menos el número de unos en el vector binario $f \oplus l_u$ y entonces,

$$H(\hat{f})(u) = 2^n - 2\, d(f, l_u(v))$$

$$d(f, l_u(v)) = \frac{1}{2}\,(2^n - H(\hat{f})(u)) \quad (2.1)$$

$$d(f, 1 \oplus l_u(v)) = \frac{1}{2}\,(2^n + H(\hat{f})(u))$$

Resumiremos esto en el siguiente teorema.

Teorema 2.3. La no linealidad de f es determinada por la transformada de Hadamard de f, es decir, $\mathcal{N}_f = 2^{n-1} - \frac{1}{2} \max_{u \in V_n} |H(\hat{f})(u)|$

Demostración

En una sección 2.1 se había definido la no linealidad como

$\mathcal{N}_f = \min_{l_u(v)\in \mathcal{A}_n} d(f, l_u(v)) = \min_{l_u(v)\in \mathcal{A}_n} wt(f \oplus l_u(v))$ y sustituyendo (2.1) en la definición

$\mathcal{N}_f = \min_{l_u(v)\in \mathcal{A}_n} \left\{\frac{1}{2}\left(2^n - H(\hat{f})(u)\right)\right\} = 2^{n-1} - \frac{1}{2}\max_{u\in V_n}\left|H(\hat{f})(u)\right|$. Por lo que queda demostrado.

Lema 2.4.

$$\sum_{u\in V_n} H(\hat{f})(u)\, H(\hat{f})(u\oplus v) = \begin{cases} 2^{2n}, v = 0 \\ 0 \quad , v \neq 0 \end{cases}$$

Demostración

Tenemos

$$\begin{aligned}\sum_{u\in V_n} H(\hat{f})(u)\, H(\hat{f})(u\oplus v) &= \sum_{u\in V_n}\sum_{w\in V_n} (-1)^{u\cdot w}\hat{f}(w) \sum_{x\in V_n} (-1)^{(u\oplus v)\cdot x}\hat{f}(x) \\ &= \sum_{w\in V_n}\sum_{x\in V_n} (-1)^{v\cdot x}\hat{f}(w)\hat{f}(x) \sum_{u\in V_n} (-1)^{u\cdot(w\oplus x)} \\ &= 2^n \sum_{w\in V_n} (-1)^{v\cdot w}\hat{f}(w)^2 = 2^n \sum_{w\in V_n} (-1)^{v\cdot w} = 2^n 2^n = 2^{2n}\end{aligned}$$

Donde $\hat{f}(w)^2 = 1$ y queda probado el lema.

Corolario 2.2. [29](Ecuación de Parseval). Para una función booleana f en n variables, la siguiente ecuación es válida

$$\sum_{u\in V_n} H(\hat{f})(u)^2 = 2^{2n}$$

Una consecuencia inmediata de este resultado es que $\max_{u\in V_n}\left|H(\hat{f})(u)\right| \geq 2^{n/2}$.

Basado en esta observación se definen las funciones curvas o de Bent, las cuales son funciones booleanas de n variables de entradas tales que,

$H(\hat{f})(h) = 2^{n/2}, \forall\, h \in 0, \ldots, 2^n - 1$ (2.2)

Las relaciones dadas en (2.1) sirven para encontrar una función afín para f (en términos de la distancia de Hamming): $l_{u,a_0}(v) = a_0 \oplus u \cdot v$, donde $\left|H(\hat{f})(u)\right|$ es grande.

Ejemplo 2.1. Definamos la función booleana en V_3 por $f(x_1,x_2,x_3) = 1 \oplus x_1 \oplus x_2 \oplus x_2x_3 \oplus x_1x_2x_3$

La tabla de verdad es 11010011 y en ese mismo orden los coeficientes de Hadamard de la función polar son $-2,2,2,-2,-2,2,-6,-2$. Pues $\left|H(\hat{f})(\alpha_6)\right| = 6$, entonces la función $l_{a_6,1} = 1 \oplus x_1 \oplus x_2$, es una función cercana a la función f. Se puede chequear fácilmente que $d(f, l_{a_6,1}) = 1$

2.6. Resultados asintóticos en los Coeficientes de Hadamard

Definamos V_∞ como el espacio de sucesiones infinitas sobre $GF(2)$ con todos los elementos cero excepto para una cantidad finita. Se define $\mathfrak{B}$ como el álgebra de las funciones booleanas en V_∞, y diremos que $\mathfrak{B}_n$ es el álgebra de funciones booleanas en V_n. Sea la amplitud espectral de una función booleana definida por[5, 7, 28-30]:

$$S(f) = \max_{v \in V_n} \left|H(\hat{f})(v)\right|$$

Teorema 2.4. Para toda función booleana f en $\mathfrak{B}$, denotamos como f_n, a toda f de V_n que satisface

$$\sqrt{2\log(2)} - \frac{5\log(n)}{n} \leq \frac{S(f_n)}{2^{n/2}\sqrt{n}} \leq \sqrt{2\log(2)} + \frac{4\log(n)}{n}$$

La demostración de este teorema se puede ver en [31]

Corolario 2.3. . Para toda función booleana f en $\mathfrak{B}$, denotamos como f_n, a toda f de V_n que satisface

$$\lim_{n\to\infty} \frac{S(f_n)}{2^{n/2}\sqrt{n}} = \sqrt{2\log(2)}$$

2.7. Distribuciones de Probabilidad

Sea $i(w)$ el índice $i-ésimo$ de la componente no nula de un vector $w \in V_n$. Suponiendo que las componentes de entrada $(x_1, \dots, x_n)$ de una función booleana $f(x)$ en V_n son variables aleatorias binarias independientes con distribución de probabilidad $Pr(x_i = 1) = \frac{1}{2} - \epsilon_i$, así, $Pr(x_i = 0) = \frac{1}{2} + \epsilon_i$, $i = 1,2, \dots, n$. La conexión entre la distribución de probabilidad de una función booleana f y la distribución de probabilidad de sus argumentos puede ser expresada en términos de la Transformada de Hadamard, bajo la condición de no uniformidad de la entrada[32].

Teorema 2.5. Si f es una función booleana arbitraria en V_n , entonces

$$\frac{1}{2} - Pr(f = 1) = \frac{1}{2^{n+1}}\left[\hat{H}(\hat{f})(0) + \sum_{s=1}^{n} \sum_{\substack{w\in V_n \\ wt(w)=s}} 2^s \hat{H}(\hat{f})(w)\epsilon_{1(w)} \dots \epsilon_{n(w)}\right]$$

Demostración

Sea $a = (a_1, \dots, a_n)$. Tenemos

$$Pr(f = 1) = \sum_{\substack{a\in V_n \\ f(a)=1}} Pr(x_1 = a_1, \dots, x_n = a_n) =$$

$$= \sum_{\substack{a\in V_n \\ f(a)=1}} Pr(x_1 = a_1), \dots, Pr\,(x_n = a_n) = \sum_{\substack{a\in V_n \\ f(a)=1}} \left(\frac{1}{2} + (-1)^{a_1}\epsilon_1\right) \dots \left(\frac{1}{2} + (-1)^{a_n}\epsilon_n\right) =$$

$$= \frac{1}{2^n}\mathrm{wt}(f) + \sum_{\substack{a\in V_n \\ f(a)=1}} \sum_{s=1}^{n} \frac{1}{2^{n-s}} \sum_{\substack{w\in V_n \\ \mathrm{wt}(w)=s}} (-1)^{a\cdot w} \epsilon_{1(w)} \cdots \epsilon_{n(w)} =$$

$$= \frac{1}{2^n}\mathrm{wt}(f) + \sum_{s=1}^{n} \frac{1}{2^{n-s}} \sum_{\substack{w\in V_n \\ \mathrm{wt}(w)=s}} \sum_{\substack{a\in V_n \\ f(a)=1}} (-1)^{a\cdot w} \epsilon_{1(w)} \cdots \epsilon_{n(w)}$$

Usando el Lema 2.2 y el hecho que $H(\hat{f})(0) = 2^n - 2\mathrm{wt}(f)$, tenemos el corolario.

Corolario 2.4. Si f es una función booleana, entonces

$$\Delta_f(\epsilon) := \max_{\substack{|\epsilon_i|\le\epsilon \\ 1\le i\le n}} \left|\frac{1}{2} - \Pr(f=1)\right| = \frac{1}{2^{n+1}} \max_{x\in V_n} \left| \sum_{w\in V_n} (-1)^{x\cdot w} H(\hat{f})(w) (2\epsilon)^{\mathrm{wt}(w)} \right|$$

Diremos que la función booleana f en V_n es balanceada si la tabla de verdad contiene tanto unos como ceros. Equivalentemente, f es balanceada si $\mathrm{wt}(f) = |\Omega_f| = 2^{n-1}$. Usando el Corolario anterior, podemos decir fácilmente que f es balanceada si y solo si $\Delta_f(\epsilon) = o(1)$

Lema 2.5. Las siguientes igualdades son válidas:

1. Si $l_{a,a_0}(x) = a\cdot x \oplus a_0$ en V_n, entonces $\Delta_{l_{a,a_0}}(\epsilon) = \frac{1}{2}(2\epsilon)^{\mathrm{wt}(a)}$
2. Si $g(x) = f(x)\oplus 1$, entonces $\Delta_g(\epsilon) = \Delta_f(\epsilon)$
3. Si $g(x) = f(x\oplus a)$, entonces $\Delta_g(\epsilon) = \Delta_f(\epsilon)$

De la Definición 2.1., deducimos que si f, g son funciones booleanas en V_n cuyas secuencias son η_f, η_g, respectivamente, entonces

$$d(f,g) = 2^{n-1} - \frac{1}{2}\,\eta_f \cdot \eta_g.$$

Sea f una función booleana en V_n, cuya secuencia es $\eta_f = (a_1, \ldots, a_n)$ y Φ_i es una función afín cuya secuencia es l_i. De la observación anterior se infiere que

$$(\eta_f \cdot l_i)^2 = 2^n + 2\sum_{j<k} a_j a_k\, h_{ij} h_{ik}.$$

Sumándose para $i = 1,2,\ldots,2^n$, deducimos

$\sum_{i=1}^{2^n}(\eta_f \cdot l_i)^2 = 2^{2n} + 2\sum_{i=1}^{2^n}\sum_{j<k} a_j a_k\, h_{ij}h_{ik} = 2^{2n} + 2\sum_{j<k} a_j a_k \sum_{i=1}^{2^n} h_{ij}h_{ik} = 2^{2n}$,

la cual es una variante de la ecuación de Parseval. Por lo tanto, existe un índice i tal que:

$(\eta_f \cdot l_i)^2 = (\eta_f \cdot l_{i+2^n})^2 \geq 2^n$,

Así que $\eta_f \cdot l_i \geq 2^{n/2}$ ó $\eta_f \cdot l_{i+2^n} \geq 2^{n/2}$. Sin pérdida de generalidad podemos asumir que $\eta_f \cdot l_i \geq 2^{n/2}$.

Pero $d(f,g) = 2^{n-1} - \frac{1}{2}\eta_f \cdot \eta_g$, de aquí que

$d(f,\phi_i) \leq 2^{n-1} - 2^{\frac{n}{2}-1}$.

Esto muestra el próximo resultado crucial[5, 9].

Teorema 1.6. [18, 31, 33, 34]La no linealidad $\mathcal{N}_f$ satisface

$\mathcal{N}_f \leq 2^{n-1} - 2^{\frac{n}{2}-1}$, para cualquier función booleana f en V_n.

2.8. Relación entre las funciones booleanas y las S-Cajas

Las cajas de sustitución (S-cajas) constituyen la piedra angular en Criptografía para lograr que los cifradores por bloque exhiban la ineludible propiedad de no linealidad. En efecto, si la o las S-cajas de un determinado cifrador por bloque no alcanzan una alta no linealidad, entonces se considera que tal algoritmo no podrá ofrecer una seguridad adecuada para impedir que la información confidencial pueda ser develada por entidades no autorizadas [4].

Formalmente, una S-caja es una función o correspondencia de n bits de entrada a m bits de salida $S: Z_2^n \longrightarrow Z_2^m$, es decir, una S-caja puede ser vista como una función booleana de n bits de entrada y m bits de salida. Cuando n = m la función es inversible y por lo tanto biyectiva. Sin embargo en muchas ocasiones, las S-cajas de los cifradores por bloque no son biyectivas. Por ejemplo, el estándar de cifrado de datos (DES por sus siglas en inglés) emplea

S-cajas en las cuales el número de bits de entrada (seis) es mayor que el número de bits de salida (cuatro)[35-37].

Dada su definición, es claro que el número de funciones booleanas elegibles para diseñar una S-caja de n bits de entrada y m bits de salida está dado por 2^{m2^n} , de tal manera que para valores moderados de n y m el tamaño del espacio de búsqueda de este problema tiene un tamaño desmesurado (por ejemplo para el algoritmo DES el total de funciones booleanas candidatas es un número con 78 dígitos decimales)[37].

Sin embargo, no todas las funciones booleanas son apropiadas para construir buenas S-cajas. Además de la ya mencionada propiedad de no linealidad, otras de las principales propiedades criptográficas requeridas para dichas funciones booleanas son: balance, alto grado algebraico, criterio de avalancha estricto, orden de inmunidad, etc.

En general, los métodos para diseñar y construir funciones booleanas y S-cajas pueden ser divididos en tres tipos de estrategias: la generación aleatoria, la construcción algebraica y los diseños heurísticos [38].

El método de generación aleatoria evita con facilidad una variedad de propiedades combinatorias que son consideradas debilidades criptográficas. Pero, las funciones booleanas generadas por este método no suelen tener buenas propiedades de no linealidad. En contraste, las construcciones algebraicas pueden brindar propiedades combinatorias específicas y una muy alta no linealidad, no obstante, tienden a tener mala calidad en aquellas características que no fueron específicamente consideradas durante su diseño [18, 20, 39, 40].

Una tercera estrategia para diseñar funciones booleanas y S-cajas se basa en diseños heurísticos [17, 41-44]. En este caso, las técnicas evolutivas han sido particularmente útiles debido, especialmente, a su alto poder exploratorio, que les permite evaluar a partir de una población de soluciones potenciales amplias regiones del espacio de diseño sin necesidad de agotar exhaustivamente todo el universo de posibilidades [38]. Entre los principales logros obtenidos en el problema del diseño eficiente de S-cajas por parte de las heurísticas evolutivas se encuentran: el hallazgo de funciones booleanas con hasta nueve entradas

de máxima no linealidad, la confirmación o refutación de conjeturas sobre la máxima no linealidad alcanzable con funciones no lineales de siete, ocho, nueve y diez entradas, etc.[17, 37, 42-48].

En este epígrafe se explican las aplicaciones de las S-cajas en la llamada criptografía de llave secreta o simétrica, se describen los principios matemáticos básicos que sustentan el diseño de funciones booleanas con buenas propiedades criptográficas y se explican varios métodos de búsqueda de dichas funciones basados en técnicas heurísticas.

En el capítulo siguiente se definen las distintas representaciones de las funciones booleanas junto con el espectro de Hadamard, que es una herramienta crucial para hacer la clasificación de tales funciones. Asimismo, se enumeran las principales propiedades matemáticas que deben exhibir las funciones booleanas a ser utilizadas como constructoras de S-cajas.

2.8.1. Uso de las S-cajas en la Criptografía de llave simétrica

Las técnicas científicas para la implementación de la seguridad computacional son desarrolladas por la Criptografía, la cual puede resumidamente ser definida como el estudio del problema de cómo establecer un intercambio de información seguro a través del uso de un canal de comunicación que no lo es[37].

De manera general, los métodos de cifrado/descifrado pueden clasificarse en dos categorías: Criptografía de llave simétrica y Criptografía de llave pública. En el resto de esta sección se describen los aspectos de diseño más destacados de la primera clase.

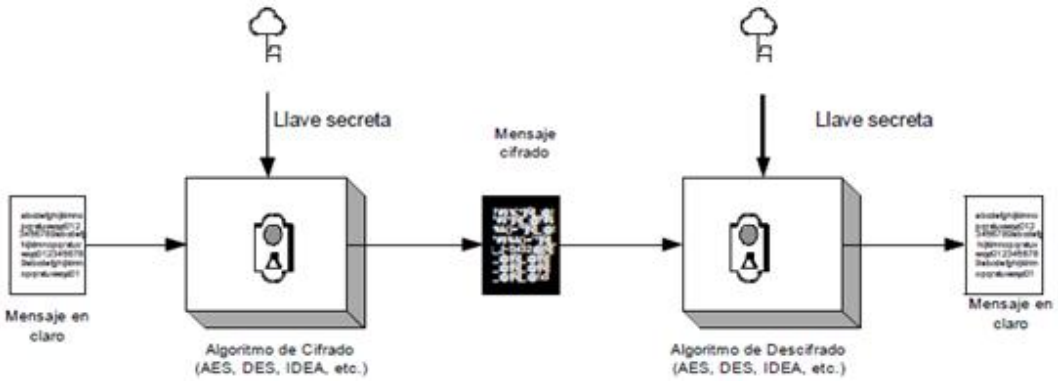


Figura 2.1. Modelo convencional de cifrado con llave simétrica

La figura muestra esquemáticamente el proceso de cifrado y descifrado llevado a cabo en un sistema simétrico. En los algoritmos de llave simétrica (o secreta) se presupone que cada una de las partes legítimamente involucradas en la comunicación son las únicas entidades que tienen conocimiento de la llave empleada en el proceso de cifrado/descifrado. El conocimiento de esta llave permite el descifrado del texto, de ahí la razón de que ésta deba permanecer en el más estricto secreto.

En la terminología criptográfica al mensaje a ser cifrado se le conoce como texto claro; al proceso de codificación al que se somete al mensaje para que no pueda ser develado por entidades no autorizadas se le llama cifrado; al documento que resulta de cifrar el mensaje se le conoce como criptograma; al

proceso de recuperar el mensaje en claro a partir del criptograma se le llama descifrado [4]. Finalmente, el término llave o clave se refiere a un valor numérico utilizado para alterar la información haciéndola segura y visible únicamente a los individuos que tienen la llave correspondiente para recuperar dicha información [1].

Algunos ejemplos famosos de cifradores por bloque son: el venerable estándar de cifrado de datos (DES) adoptado en el año 1974 [4, 24, 49], y su sucesor, el estándar avanzado de encriptación (AES), escogido en octubre de 2000 por el Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés) como el estándar oficial en Estados Unidos para cifrar/descifrar documentos [35, 37]. La principal ventaja de este tipo de esquema es la sencillez matemática y consecuente eficiencia computacional de sus algoritmos, y su principal debilidad el manejo y distribución de las llaves secretas entre las partes interesadas. Los tamaños de las llaves utilizadas para cifrar/descifrar varían desde los 64 bits (aun cuando hoy en día se necesitan al menos 80 bits para ser consideradas realmente seguras) hasta 256 bits.

En el caso del estándar DES, se utiliza una longitud de llave de apenas 56 bits. A pesar que en el tiempo de su creación esta longitud de llave fue considerada muy segura, los avances tecnológicos han permitido el desarrollo de técnicas para encontrar las llaves por búsqueda exhaustiva en tiempos relativamente cortos. Por ejemplo, ya desde 1999 un proyecto de cómputo distribuido rompió el DES en un tiempo de 22 horas con 15 minutos. Debido a ello, desde hace mucho tiempo el DES no es considerado suficientemente robusto para aplicaciones de alta seguridad, por lo que en la práctica profesional se utiliza una variante conocida como triple DES, la cual brinda una seguridad equivalente a la proporcionada por una llave de 112 bits[4].

Los cifradores por bloque ofrecen diversos grados de seguridad, determinados esencialmente por el ya mencionado tamaño en bits de la llave secreta y por la propia calidad criptográfica del diseño de cada cifrador. Hoy en día, muchos de los diseños más importantes de cifradores por bloque siguen el modelo de Feistel. Ello se debe a que este modelo se caracteriza por su simplicidad, buenas propiedades criptográficas y una robustez inherente. Por otro lado, los cifradores por bloque de Feistel han adquirido un enorme prestigio tras resistir

exitosamente el escrutinio exhaustivo que sobre ellos ha realizado la comunidad criptográfica de manera implacable a lo largo de los últimos treinta años [24].

Los cifradores de Feistel utilizan transformaciones lineales en forma de corrimientos lógicos, operadores booleanos a nivel de bits, etc., y transformaciones no lineales que son implementadas con bloques de sustitución de bits, conocidos en la literatura especializada como S-cajas. Dado que las S-cajas son los únicos bloques no lineales presentes en el modelo de Feistel, se acepta de manera general que la calidad en eficiencia y seguridad de un algoritmo cifrador depende en buena medida del buen diseño de dichos módulos.

Conclusiones del Capítulo

En este capítulo se han abordado y descrito matemáticamente las definiciones y propiedades de las funciones booleanas utilizando la transformada de Hadamard. Se dedica un epígrafe a las S-cajas como funciones booleanas útiles en el cifrado en bloque. Además, se aborda la relación existente entre la transformada y las matrices de Hadamard.

Capítulo 3. Aplicaciones.

3.1. La aplicación de la Transformada y de las matrices de Hadamard en el Cifrado en Flujo.

En este epígrafe se expone el resultado obtenido en la aplicación de la Transformada de Hadamard en el criptoanálisis, y en particular, para ver con que probabilidad se pueden descifrar diferentes Generadores Pseudoaleatorios de Números que se utilizan en el Cifrado en Flujo y la importancia del uso de la transformada de Hadamard en este tipo de problema.

El Criptoanálisis es el estudio de los métodos para obtener el sentido de una información cifrada, sin acceso a la información secreta requerida para obtener este sentido normalmente.[50] Típicamente, esto se traduce en conseguir la clave secreta. En el lenguaje no técnico, se conoce esta práctica como **romper o forzar el código**, aunque esta expresión tiene un significado específico dentro del argot técnico.

Aunque el objetivo ha sido siempre el mismo, los métodos y técnicas del criptoanálisis han cambiado drásticamente a través de la historia de la criptografía, adaptándose a una creciente complejidad criptográfica.

Los resultados del criptoanálisis [51] han cambiado también: ya no es posible tener un éxito ilimitado al romper un código, y existe una clasificación jerárquica de lo que constituye un ataque en la práctica.

En la denominación de secuencias aleatorias se engloban todas aquéllas que han sido generadas mediante procesos físicos intrínsecamente aleatorios, es decir, basados en el supuesto de la existencia de procesos al azar en la naturaleza. En múltiples aplicaciones es preciso poder disponer de la misma secuencia (aparentemente aleatoria) en dos puntos

distintos, por lo cual es necesario utilizar algoritmos deterministas que sean reproducibles. En tal caso, se denominan secuencias pseudoaleatorias.

Las secuencias pseudoaleatorias según [52] son utilizadas en diversos entornos relacionados con el mundo de las telecomunicaciones. Entre otros ámbitos de aplicación, podemos encontrar la transmisión de datos (dígase para aleatorizar símbolos).

En el Criptoanálisis es muy importante conocer qué relación existe entre los elementos de la salida para a partir de estos divagar sobre un posible texto claro, entonces la idea *es como facilitar* el cálculo de una probabilidad que relaciona varios términos de una salida y en la medida que dicha probabilidad sea más alta mejor será para descifrar el texto claro.

Estamos hablando de la siguiente probabilidad.

$P\left(z_i\varepsilon_1 + z_{i+1}\varepsilon_2 + \ldots + z_{i+k-1}\varepsilon_k = 0 \right)$, donde $\vec{\varepsilon} \in V_k(2) \setminus \{\vec{0}\}$ y los z_i son las salidas de los Generadores Pseudoaleatorios.

Para el cálculo de esta probabilidad nos basamos en lo siguiente

Si designamos a

$$n_0 = \left| \{ i \mid z_i\varepsilon_1 + z_{i+1}\varepsilon_2 + \ldots + z_{i+k-1}\varepsilon_k = 0 \} \right|$$

$$n_1 = \left| \{ i \mid z_i\varepsilon_1 + z_{i+1}\varepsilon_2 + \ldots + z_{i+k-1}\varepsilon_k = 1 \} \right|$$

$$n_0 + n_1 = V$$

Entonces, por la definición de probabilidad clásica tenemos que

$$P\left(z_i\varepsilon_1 + z_{i+1}\varepsilon_2 + \ldots + z_{i+k-1}\varepsilon_k = 0 \right) = \frac{n_0}{V}$$

Ahora, hacemos ciertas transformaciones y para ello planteamos la siguiente razón

$$\frac{1}{V}\sum_{i=1}^{V}(-1)^{z_i\varepsilon_1+z_{i+1}\varepsilon_2+\ldots+z_{i+k-1}\varepsilon_k}=\Delta_\varepsilon \qquad \textbf{(2.3)}$$

¿Pero cómo esta magnitud está relacionada con nuestra búsqueda?

La expresión $(-1)^{z_i\varepsilon_1+z_{i+1}\varepsilon_2+\ldots+z_{i+k-1}\varepsilon_k}$ **(2.4)** es -1 si el exponente es 1 y es 1 si el exponente es 0.

Resulta que la suma (2.3) con exponente que pertenezca a n_0 va hacer n_0 y la suma (2.3) con exponente que pertenezca a n_1 va a hacer -n_1. Esto es consecuencia de las propiedades de las series

$$\sum_{i=1}^{m}(-1)^{2i}=m \quad y \quad \sum_{i=1}^{m}(-1)^{2i-1}=-m$$

Por ello, nosotros podemos reescribir (2.3) de la siguiente manera

$$\Delta_\varepsilon=\frac{n_0-n_1}{n_0+n_1}$$

El problema es conocido Δ_ε encontrar los valores de n_0 y n_1, lo cual conduce a una ecuación diofántica que por las condiciones de las variables anteriores hace que sea necesario acudir a recursos tales como el teorema de Kronecker el cual a su vez hace muy complicada la solución del problema. La idea entonces es utilizar una transformada que como es conocido representa el cambio de un dominio hacia otro, y que debido a sus propiedades, *reduce la complejidad de problemas matemáticos.* Este tipo de herramienta ha sido muy útil y fundamental en la solución de problemas en distintos campos, y de diversa naturaleza. La transformada de Hadamard nos permite resolver el problema planteado.

La transformada de Hadamard puede también definirse según [8, 12] con la expresión de la $\mathrm{H(u)}$:

$H(z) = \frac{1}{N}\sum_{n=0}^{N-1} x[n]\cdot(-1)^{\sum_{i=0}^{t-1} b_i(n)\cdot b_i(z)}$, donde:

N es el número de muestras

t se corresponde con $N=2^t$

$b_k(z)$ es el bit k- ésimo en la representación binaria de z

La sumatoria es módulo 2

Resulta que al encontrar una relación entre Δ_ε, n_0 y n_1

$$1+\Delta_\varepsilon = \frac{n_0 - n_1}{n_0 + n_1} + 1 = \frac{2n_0}{n_0 + n_1} \Rightarrow \frac{1+\Delta_\varepsilon}{2} = \frac{n_0}{V}$$

Entonces la probabilidad que queremos hallar quedaría

$$P\{z_i\varepsilon_1 + z_{i+1}\varepsilon_2 + \ldots + z_{i+k}\varepsilon_k = 0\} = \frac{n_0}{} = \frac{1+\Delta_\varepsilon}{}$$

Para calcular la probabilidad deseada basta con hallar Δ_ε

Supongamos ahora que tenemos la sucesión de salida, que se puede escribir en forma matricial

$z_1^{(1)} \ldots\ldots z_v^{(1)}$
$z_1^{(2)} \ldots\ldots z_v^{(2)}$
$\ldots\ldots\ldots\ldots\ldots$
$z_1^{(k)} \ldots\ldots z_v^{(k)}$

Estas son sucesiones binarias o vectores binarios, ***v*** puede ser una cifra bastante grande.

Entonces hay que calcular la siguiente estadística

$$n_{\varepsilon} = \sum_{i=1}^{v} (-1)^{z_i^{(1)}\varepsilon_1 + z_i^{(2)}\varepsilon_2 + \ldots + z_i^{(k)}\varepsilon_k} \qquad \forall \vec{\varepsilon} \in V_k(2)$$

Veamos ahora lo siguiente:

Para diferente ***i*** tendremos diferentes vectores los cuales cumplen que

$\left\{ i : z_i^{(1)}, \ldots\ldots, z_i^{(k)} = \alpha \right\}$ (*), donde el vector $\alpha \in V_k(2)$ es fijo.

Precisamente en este tacto la expresión será igual a $(-1)^{(\alpha,\varepsilon)}$

En este caso la suma se puede reescribir

$$\sum_{\alpha \in V_k} \sum_{(*)} (-1)^{(\alpha,\varepsilon)} = \sum_{\alpha \in V_k} (-1)^{(\alpha,\varepsilon)} n_{\alpha}$$ **(2.5)**, donde

$n_{\alpha} = \left| \left\{ i : z_i^{(1)}, \ldots\ldots, z_i^{(k)} = \alpha \right\} \right|$

Para calcular la expresión **(2.5)** debemos crear un arreglo de memoria que tenga un tamaño de 2^k, lo inicializamos $\Pi[\alpha] = 0,\ \alpha \in V_k(2)$

Se convierte cada columna de la matriz en la cifra Y

$Y = \sum_{n=0}^{k-1} z_n^{(j)} \cdot 2^n$, después hacemos la operación

$\Pi[Y] = \Pi[Y] + 1$, este es el contador de cuantas columnas son la cifra Y,

$n_{\alpha} = \Pi[\alpha]$

Ahora, hagamos $\hat{n}_{\varepsilon} = \sum_{\alpha \in V_k} (-1)^{(\alpha,\varepsilon)} n_{\alpha}$

Entonces para calcular $\hat{n}_\varepsilon, \varepsilon \in V_k(2)$ y resolver (2.5), utilizaremos la Transformada Discreta de Hadamard.

Si tomamos $n_\alpha = x$ y a

$(-1)^{\sum_{i=0}^{t-1} b_i(\alpha) b_i(\varepsilon)} = (-1)^{(\alpha,\varepsilon)}$, la transformada se puede reescribir en la propia definición y quedaría

$H(\varepsilon) = \frac{1}{V} \sum_{\alpha \in V_k} n_\alpha \cdot (-1)^{(\alpha,\varepsilon)}$, donde entonces $N = V$ ya que V es la cantidad de columnas de matriz de salida y es a su vez la cantidad de operaciones que va a realizar el operador suma.

$$\Delta_\varepsilon = \frac{\hat{n}_\varepsilon}{V} = H(\varepsilon)$$

Si utilizamos la matriz de Hadamard que desde el punto de vista computacional aumenta la cantidad de trabajo pero se hace más fácil el cálculo de los Δ_ε.

El máximo orden de esta matriz es de 256 y para calcular $\Delta_\varepsilon = \frac{H_{2^n}\,\Pi(\alpha)}{V}$

Con esto ya hemos determinado una manera menos engorrosa de calcular Δ_ε que nos permitirá determinar cuál es el valor de ε que hace que la probabilidad sea la más alta posible para descifrar.

3.2 Funciones booleanas.

Como se mencionó en el Capítulo 2, una S-caja de n bits × m bits es una relación tal que $S: Z_2^n \rightarrow Z_2^m$. Así, una S-caja puede ser representada como 2^n números de m bits, denotados por $r_0, \ldots, r_{2^n-1}$, en donde $S(x) = r_x$, $0 \leq x \leq 2^n$ y donde r_x representa los renglones de la caja S. Alternativamente, una S-caja puede también representarse

mediante una matriz binaria M de $2^n \times m$ bits, donde la entrada i, j es el bit j del renglón i-ésimo.

En la práctica, resulta suficiente estudiar S-cajas de n variables de entrada con un solo bit de salida, a las que llamaremos por simplicidad funciones booleanas de n variables, y las cuales serán el objeto de estudio en el resto de este epígrafe.

Una función booleana de n variables, $f(x): Z_2^n \to Z_2$ es entonces una relación de n entradas binarias a una sola salida binaria. Llamaremos B_n al conjunto de las

2^{2^n} funciones booleanas de n variables.

3.2.1. Ejemplos.

En esta subsección se ilustran las definiciones dadas en el capitulo precedente con varios ejemplos.

Tabla 3.1. Número de funciones balanceadas en B_n

N	B_n	Func. Balanceadas	Porcentaje
1	$2^2 = 4$	$\binom{2^1}{2^0} = \binom{2}{1} = 2$	50
2	$2^4 = 16$	$\binom{2^2}{2^1} = \binom{4}{2} = 6$	37.5
3	$2^8 = 256$	$\binom{2^3}{2^2} = \binom{8}{4} = 70$	27.3
4	$2^{16} = 64\ Kilos$	$\binom{2^4}{2^3} = \binom{16}{8} = 12870$	19.6
5	$2^{32} = 4\ Gigas$	$\binom{2^5}{2^4} = \binom{32}{16} \approx 601\ Meg$	14.0
6	$2^{64} = 16\ Exas$	$\binom{2^6}{2^5} = \binom{64}{32} \approx 1.6\ exas$	9.9

Ejemplo 3.1: Número de funciones balanceadas.

La tabla 3.1 muestra el número de funciones booleanas balanceadas y su respectivo porcentaje en el total de B_n funciones booleanas para n=1,2,…,6. Como puede apreciarse, hay una gran cantidad de funciones balanceadas en el enorme universo de funciones booleanas B_n, que sin embargo decrece rápidamente cuando n aumenta.

Ejemplo 3.2: Función booleana de tres entradas, balanceada y de máxima no linealidad.

Consideremos la función booleana f de tres entradas descrita algebraicamente como:

$f(x) = x_2x_1 + x_3x_1 + x_3x_2$

Tabla 3.2. Ejemplo de una función booleana de tres entradas

x_3	x_2	x_1	$f(x)$	$\hat{f}(x)$	$H(\hat{f})$
0	0	0	0	1	0
0	0	1	0	1	4
0	1	0	0	1	4
0	1	1	1	-1	0
1	0	0	0	1	4
1	0	1	1	-1	0
1	1	0	1	-1	0
1	1	1	1	-1	-4

La tabla 3.2 presenta la tabla de verdad de la función f en su versión tradicional y polar, junto con su respectivo espectro de Hadamard. El espectro de f puede ser hallado a través de la ecuación 1.1, o aún mejor, utilizando la Transformada Rápida de Hadamard mostrada esquemáticamente en la figura 4.

El espectro $\mathrm{H(f)}$ de una función booleana f brinda una rica información sobre las características de dicha función. Por ejemplo, el espectro de Hadamard de la tabla 3.2 nos indica que f es una función balanceada, puesto que el primer coeficiente del espectro,$\mathrm{H(0)}$ tiene valor cero. Asimismo, se determina que f tiene no linealidad 2 puesto que:

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2}\max_{u \in V_n}\left|\mathrm{H}\left(\hat{f}\right)(u)\right| = 2^2 - \frac{1}{2}\,4 = 2$$

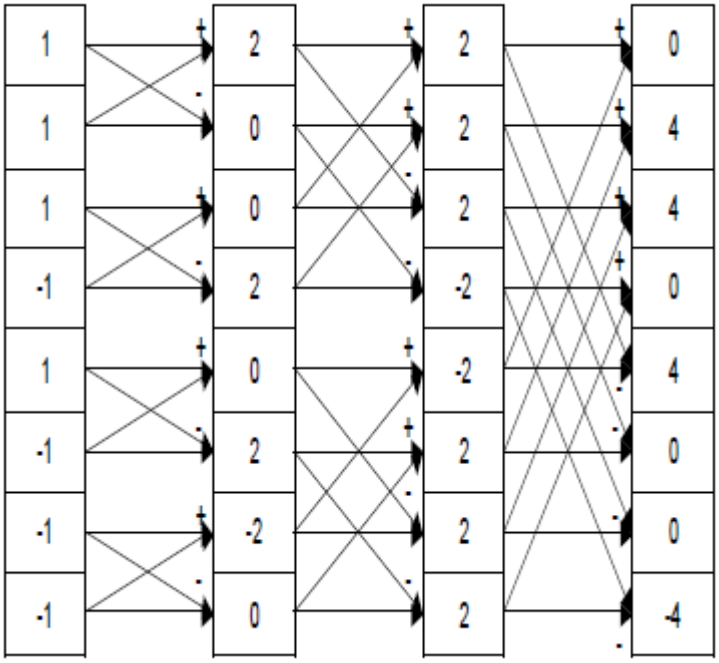


Figura 3.1. Transformada rápida de Hadamard para la función

$$f(x) = x_2x_1 + x_3x_1 + x_3x_2$$

Ejemplo 3.3: Función curvas de 4 entradas.

Consideremos la función booleana f de cuatro entradas descrita algebraicamente como:

$$f(x) = \overline{x_4}\,\overline{x_3}x_2x_1 + x_4x_3(\overline{x_2} + \overline{x_1}) + \overline{x_2}\,\overline{x_1}(x_3 + x_4)$$

La tabla 3.3 presenta la tabla de verdad de la función f en su versión tradicional y polar, junto con su respectivo espectro de Hadamard. Del espectro de Hadamard de la tabla 3.3 podemos deducir que la función booleana f, satisface la definición de función curva de la ecuación 2.2. Nótese que la tabla de verdad de f corresponde a la de una función booleana no balanceada con máxima no linealidad 6, puesto que:

$$\mathcal{N}_f = 2^{n-1} - \frac{1}{2}\max_{u \in V_n}\left|H(\hat{f})(u)\right| = 2^3 - \frac{1}{2}\,4 = 6$$

Tabla 3.3 Tabla de verdad de una función curva de 4 entradas

x_4	x_3	x_2	x_1	$f(x)$	$\hat{f}(x)$	$H(\hat{f})$
0	0	0	0	0	1	4
0	0	0	1	0	1	-4
0	0	1	0	0	1	-4
0	0	1	1	1	-1	-4
0	1	0	0	1	-1	4
0	1	0	1	0	1	4
0	1	1	0	0	1	4
0	1	1	1	0	1	-4
1	0	0	0	1	-1	4
1	0	0	1	0	1	4
1	0	1	0	0	1	4
1	0	1	1	0	1	-4
1	1	0	0	1	-1	-4
1	1	0	1	1	-1	4
1	1	1	0	1	-1	4
1	1	1	1	0	1	4

3.3 Propiedades criptográficas deseables en las funciones booleanas.

En la práctica profesional para diseñar S-cajas con buenas propiedades criptográficas se tienen en cuenta varios criterios, los principales de ellos consideran que estas deben tener las propiedades que se enumeran a continuación:

1. Balance: Esta propiedad es muy deseable para evitar ataques cripto-diferenciales tales como los introducidos por A. Shamir contra el algoritmo DES [4, 24].

2. **Alta no linealidad**: Esta propiedad reduce el efecto de los ataques por criptoanálisis lineal. Como se discutió, la no linealidad de una función booleana puede ser calculada directamente utilizando la transformada de Hadamard (a través de la ecuación 1.1).

3. **Auto correlación**: Este valor es proporcional al desbalance de todas las derivadas de primer orden de la función booleana. Los valores pequeños son considerados como buenos mientras que un valor grande es considerado un símbolo de debilidad. Las funciones curvas, gozan de una autocorrelación mínima, por lo que optimizan esta propiedad.

4. **Indicador absoluto:** Este indicador es denotado por $\mathrm{M(f)}$ y está dado por el máximo valor absoluto en $\hat{\mathrm{r}}_{\mathrm{f}}(\mathrm{a})$ (véase definición 2.3). Se considera que una función booleana con un $\mathrm{M(f)}$ pequeño es criptográficamente deseable. Las funciones curvas tienen una autocorrelación óptima pues su indicador absoluto es cero [1,3,11].

5. **Efecto avalancha**: Está relacionado con la autocorrelación y se define con respecto a un bit específico de entrada tal que al complementarlo resulta un cambio en el bit de salida con una probabilidad de 1/2. El criterio de avalancha estricto (SAC por sus siglas en inglés), requiere los efectos avalancha de todos los bits de entrada. Se dice que una función booleana satisface el criterio de avalancha estricto si al complementar un solo bit de entrada resulta un cambio en un bit de salida con una probabilidad de 1/2. Puede demostrarse fácilmente que una función booleana f con función de autocorrelación $\hat{\mathrm{r}}_{\mathrm{f}}(\mathrm{a})$, satisface el criterio de avalancha estricto si y sólo si $\hat{\mathrm{r}}_{\mathrm{f}}(\mathrm{a}) = 0, \forall\, \mathrm{a}$ con peso de Hamming $wt(a) = 1$ [3, 53].

6. **Grado algebraico**: El grado algebraico de una función f, denotado como $\deg(\mathrm{f})$, es el número de entradas más grande que aparece en cualquier producto de la forma normal algebraica. Esto es $x_1 \oplus x_2$ tiene grado 1 (es decir, es lineal) mientras que $x_1 \oplus x_1x_2x_3$ tiene grado 3 [17, 42, 44].

7. **Orden de Inmunidad de Correlación**: Una función f tiene un orden de inmunidad de correlación m si y sólo si [39]:

$$H(\hat{f}) = 0\,; 1 \leq H(f) \leq m$$

8. **Resistencia:** Una función f que tiene inmunidad de correlación de orden m, es resistente si y sólo si también es balanceada [39] o sea si:

$H(\hat{f}) = 0 \; ; 0 \leq H(f) \leq m$

Estos son los principales criterios utilizados en la práctica profesional para diseñar S-cajas con buenas propiedades criptográficas para los cifradores en bloque.

Conclusiones del Capítulo

En este capítulo hemos mostrado algunas aplicaciones de la transformada y matrices de Hadamard en las funciones booleanas, en la búsqueda de funciones criptográficamente deseables y en el criptoanálisis de los generadores pseudoaleatorios del cifrado en flujo.

Se ilustró primeramente con detalles matemáticos, el cálculo de la probabilidad de la correlación entre los bit de salida de un generador pseudoaleatorio, mientras que más adelante se mostró matemáticamente a través de ejemplos como podemos utilizar la transformada de Hadamard para buscar funciones booleanas deseables criptográficamente.

Conclusiones

- El presente trabajo aborda una nueva ciencia en nuestro país, la Criptografía y en particular el uso en ella de la transformada y matrices de Hadamard quedando demostrada la utilidad de estas en la búsqueda de funciones criptográficamente deseables y en el criptoanálisis.
- Se estudió la teoría de las funciones booleanas y las propiedades criptográficamente deseables de las mismas.
- Se estudió y presentó de manera organizada la teoría relacionada con la transformada y matrices de Hadamard.
- Se explicaron las relaciones entre la transformada de Hadamard y las propiedades de las funciones booleanas.
- Se determinó matemáticamente como utilizar la transformada y matrices de Hadamard en el criptoanálisis de los generadores pseudoaleatorios.

Recomendaciones

El presente trabajo abre una temática de investigación dentro del Departamento de Matemática de la Facultad de Matemática Física y Computación de la Universidad Central Marta Abreu de Las Villas específicamente dentro del Seminario de Criptografía por lo que se recomienda:

1. Ampliar este estudio a otras ramas de la Criptografía como es la Teoría de la Información.
2. Profundizar en el estudio de la transformada de Hadamard buscando otras aplicaciones dentro de la Criptología.
3. Implementar sobre el Mathcad o sobre el Mathematica todas las propiedades criptográficamente deseables de las funciones booleanas.

Bibliografía

1. Menezes, A.J.V.O., P. C. Vanstone, S. A., *Handbook of Applied Cryptography*. 1997, CRC Press.
2. Institute for Studies in Theoretical Physics and Mathematics, I. 2010; Available from: http://math.ipm.ac.ir.
3. Hernández-Luna, E., *Documento de Propuesta Doctoral*. 2005.
4. F. Rodríguez-Henríquez, N.A.S., A. Díaz Pérez y Ç. K. Koç. (2006) *Cryptographic Algorithms on Reconfigurable Hardware*. Springer First Edition, 362.
5. Hedayat, A., Wallis, W.D., *Hadamard matrices and their applications.* Ann. Stat, 1978. **6**: p. 1184–1238.
6. EW., W. *Hadamard matrix*. 2010; Available from: http://mathworld.wolfram.com/HadamardMatrix.html.
7. Yamada, J.S.a.M., *Hadamard matrices, sequences and block designs.* J. H. Dinitz and D. R. Stinson, 1992.
8. Marlon J. Luján Paredes, E.M.P.R., Klebes R. Arias Quispe, *IMPLEMENTACIÓN DE LA TRANSFORMADA BIDIMENSIONAL DE HADAMARDEN UN FPGA.*
9. Stanica, T.W.C.a.P., *Cryptographic Boolean Functions and Applications.*
10. Bernasconi A, C.B., Simon J., *On the Fourier analysis of Boolean functions.* 1996: p. 1-24.
11. Henríquez, F.R., *De la búsqueda de funciones booleanas con buenas propiedades criptográficas.*
12. Desconocido, *La Tranformada de Hadamard*
13. Tayfeh-Rezaie, H.K.a.B., *A Hadamard matrix of order 428.* J. Combinatorial Designs 13, 2005: p. 435-440.
14. M. Hall, J., *Note on the Mathieu group M_{12}.* Arch. Math. 13 1962: p. 334-340.
15. Kantor, W.M., *Automorphism Groups of Hadamard Matrices.* 1967.
16. Sylvester, J.J., *Thoughts on inverse orthogonal matrices, simultaneous sign successions, and tessellated pavements in two or more colours, with applications to Newton's rule, ornamental tile-work, and the theory of numbers.* 1867.
17. J. A. Clark, J.L.J., S. Maitra, y P. Stnic., *Almost boolean functions: The design of boolean functions by spectral inversion.* In Computational Intelligence 20, 2004. **3**: p. 450-462.
18. Carlet, C., et al., *Algebraic immunity for cryptographically significant Boolean functions: analysis and construction.* #IEEE_J_IT#, 2006. **52 %6**(7): p. 3105-3121 %&.
19. Clark, J.A., et al., *Evolving boolean functions satisfying multiple criteria*, in *In INDOCRYPT 2002, LNCS 2551*. 2002, Springer. p. 246--259.
20. Sarkar, K.C.G.y.P., *Improved construction of nonlinear resilient s-boxes*, in *8th International Conference on the Theory and Application of Cryptology and Information Security*. 2002, Springer-Verlag. p. 466-483.
21. Seberry J, Z.X.-M., Zheng Y., *Nonlinearity and propagation characteristics of balanced Boolean functions.* Inform Comput, 1995. **119**: p. 1-13.
22. Meier W, S.O., *Nonlinearity criteria for cryptographic functions.* Adv. in crypt.–Eurocrypt '89, 1990. **434**: p. 54-62.
23. Carlet, C., *On the degree, nonlinearity, algebraic thickness, and nonnormality of Boolean functions, with developments on symmetric functions.* #IEEE_J_IT#, 2004. **50 %6**(9): p. 2178-2185 %&.
24. Schneier, B., ed. *Protocols, Algorithms, and Source Code in Applied Cryptography*. 2 ed. 1996.
25. Carlet, C., *Recursive Lower Bounds on the Nonlinearity Profile of Boolean Functions and Their Applications.* #IEEE_J_IT#, 2008. **54 %6**(3): p. 1262-1272 %&.
26. K., M., *Spectral analysis of Boolean functions under nonuniformity of arguments.* 2002.

27. Seberry J, Z.X.-M., *Highly nonlinear 0–1 balanced Boolean functions satisfying strict avalanche criterion.* Adv. in crypt.–Auscrypt '92, 1993. **765**: p. 45-55.
28. Beauchamp, K.G. and L. Debnath, *Walsh Functions and Their Applications.* #IEEE_J_SMC#, 1979. **9 %6**(1): p. 67 %&.
29. Sloane, N. *A library of Hadamard matrices*. 2010; Available from: http://www.research.att.com/~njas/hadamard/.
30. Yuen, C.K., *Walsh functions and their applications.* #IEEE_J_PROC#, 1977. **65** (2): p. 285.
31. F., R., *Asymptotic nonlinearity of Boolean functions,Coding and cryptography–WCC 2003*

2003.
32. MacWilliams FJ, S.N., *The theory of error-correcting codes.* North-Holland Publishing Company, 1978.
33. Carlet, C., D.K. Dalai, and S. Maitra. *Cryptographic Properties and Structure of Boolean Functions with Full Algebraic Immunity*. 2006.
34. Carlet, C. and P. Charpin. *Cubic Boolean functions with highest resiliency*. 2004.
35. NIST, *Announcing the Advanced Encryption Standard (AES).* 2001, Federal Information Standards Publication.
36. Rijmen, J.D.y.V., *The Design of Rijndael.* Springer-Verlag, 2002.
37. E. López-Trejo, F.R.-H.y.A.D.-P., *An Efficient FPGA implementation of CCM Using AES.*, in *The 8th International Conference on Information Security and Cryptology (ICISC'05),*. 2005. p. 208-215.
38. J. C. Hernández-Castro, P.I., y C. Luque del Arco-Calderón., *Finding efficient nonlinear functions by means of genetic programming.*, in *KES 2003, Seventh International Conference on Knowledge-Based Intelligent Information & Engineering Systems*. 2003. p. 1192-1198.
39. Forré, R. (1990) *Methods and instruments for designing s-boxes*. J. of Cryptology, 115–130.
40. Maitra, P.S.y.S., *Nonlinearity bounds and construction of resilient Boolean functions*, in *In Advances in Cryptology - Crypto 2000*, Springer-Verlag, Editor. 2000, Lecture Notes in Computer Science: Berlin
41. House, A.W.H. and H.M. Heys. *Design of a flexible cryptographic hardware module*. 2004.
42. S. Kavut, S.M., S. Sarkar y M. D. Yücel., *Enumeration of 9-Variable Rotation Symmetric Boolean Functions Having Nonlinearity > 240*, in *INDOCRYPT 2006, 7th International Conference on Cryptology in India*. 2006, Springer. p. 266-279.
43. J. Fuller, W.M., y E. Dawson, *Multiobjective optimization of bijective sboxes*, in *CEC 2004: International Conference on Evolutionary Computation*, IEEE, Editor. 2004: Portland OR, USA. p. 1525-1532.
44. S. Kavut, S.M.y.S.S., *There exist Boolean functions on n (odd) variables having nonlinearity* $> 2^{n-1} - 2^{n-1/2}$ *if and only if n > 7*. 2006.
45. W. Millan, J.F., y E. Dawson, *Evolutionary generation of bent functions for cryptography*, I.C.S. Press, Editor. 2003.
46. J. A. Clark, J.L.J., S. Stepney, S. Maitra, y W. Millan. *Evolving boolean functions satisfying multiple criteria*. in *Third International Conference on Cryptology*. 2002.
47. Millan, W., J. Fuller, and E. Dawson. *New concepts in evolutionary search for Boolean functions in cryptology*. 2003.
48. Z. Saber, M.F.U., *A. Youssef: On the existence of (9, 3, 5, 240) resilient functions.* IEEE Transactions on Information Theory, 2006. **52**(2): p. 2269-2270.
49. A. Díaz-Pérez, N.A.S., y F. Rodríguez-Henríquez., *Some Guidelines for Implementing Symmetric-Key Cryptosystems on Reconfigurable-Hardware.*, in *IV Jornadas de Computación Reconfigurable y Aplicaciones*. 2004. p. 379-387.
50. ; Available from: http://es.wikipedia.org/wiki/.
51. Schneier, B., *A SELF-STUDY COURSE IN BLOCK-CIPHER CRYPTANALYSIS.*
52. Soriano Ibañez, M.G.D., Raúl, *Generación y análisis de secuencias pseudoaleatorias.* Ediciones UPC, 1999.
53. Hernández-Luna, E., *Criterio de avalancha estricto en funciones booleanas*. 2005.

Anexos

Anexo 1. Ejemplo de Criptoanálisis en el Mathcad

$n_0 := 7$ Lo da el grado del polinomio

$i := 0 .. n_0 - 1$

$a_i := floor(rnd(1) + 0.5)$ Genera sucesión X aleatoria de 0 y 1 de 7 elementos.

$n_1 := 2^{n_0} - 1$

$a_{n_1+n_0} := 0$

Polinomio Primitivo

$z^7 + z^4 + 1$

A la i se le da un valor grande

$i := 0 .. n_1 \cdot 3000$

$a_{i+n_0} := mod(a_{i+4} + a_i, 2)$

Se le agrega a la sucesión X una sucesión de 0 y 1 de acuerdo a la forma del polinomio

$n_2 := 6$

$i := 0 .. n_2 - 1$

$su_i := floor(rnd(1) + 0.5)$

$n_3 := 2^{n_2} - 1$

$su_{n_3+n_1} := 0$

$z^6 + z^4 + z^3 + z + 1$

$i := 0 .. n_3 \cdot 1300$

$su_{i+6} := mod(su_{i+4} + su_{i+3} + su_{i+1} + su_i, 2)$

Este es el Generador Compresor

```
Compresor(a, su) := | 1 ← 0
                    | for i ∈ 0.. rows(su) − 1
                    |     if su_i = 1
                    |         z_l ← a_i
                    |         l ← l + 1
                    |     break if l > rows(a) − 1
                    | z
```

$z := Compresor(a, su)$

$rows(z) = 4.16 \times 10^4$

$n_4 := 8$

$i := 0.. rows(z) - n_4$

$$vz_i := \sum_{j=0}^{n_4-1} \left[z_{(i+j)} \cdot 2^{n_4-1-j} \right]$$

$markz_{2^{n_4}-1} := 0$

$t := 0.. rows(z) - n_4$

$markz_{(vz_t)} := markz_{(vz_t)} + 1$

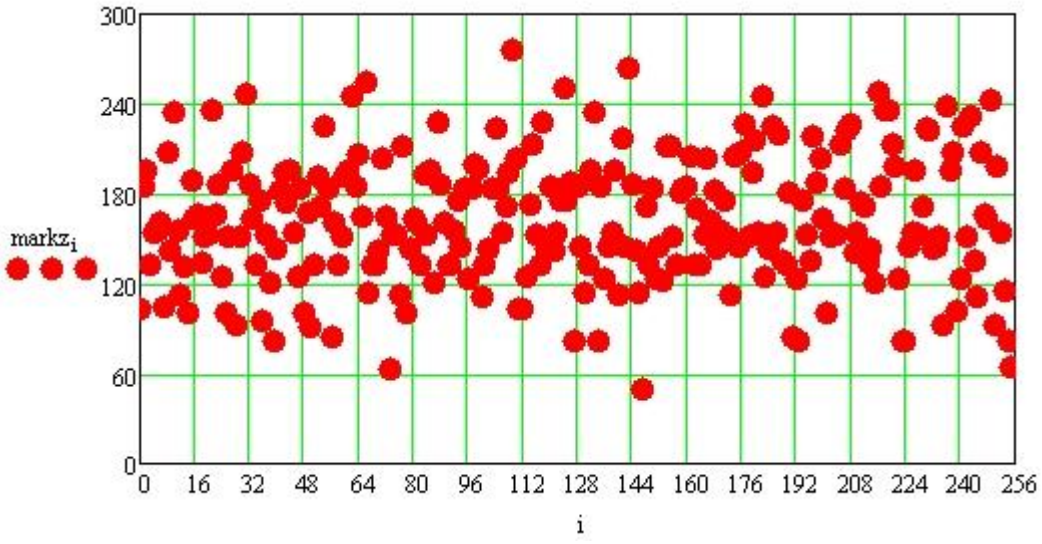


Diagrama donde se muestra la cantidad de repeticiones de los números entre 0 y 256

markz =

	0
0	103
1	185
2	196
3	133
4	154
5	156
6	161
7	105
8	207
9	142
10	235
11	156
12	112
13	131
14	101
15	...

Matriz columna que representa la cantidad de repeticiones de los números entre 0 y 256.

Matrices de Hadamard

$$H_1 := \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

$$H_2 := \text{kronecker}(H_1, H_1) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$H_4 := \text{kronecker}(H_2, H_2)$ Producto de Kronecker

$H_8 := \text{kronecker}(H_4, H_4)$

$v := \text{rows}(z) - n_4$

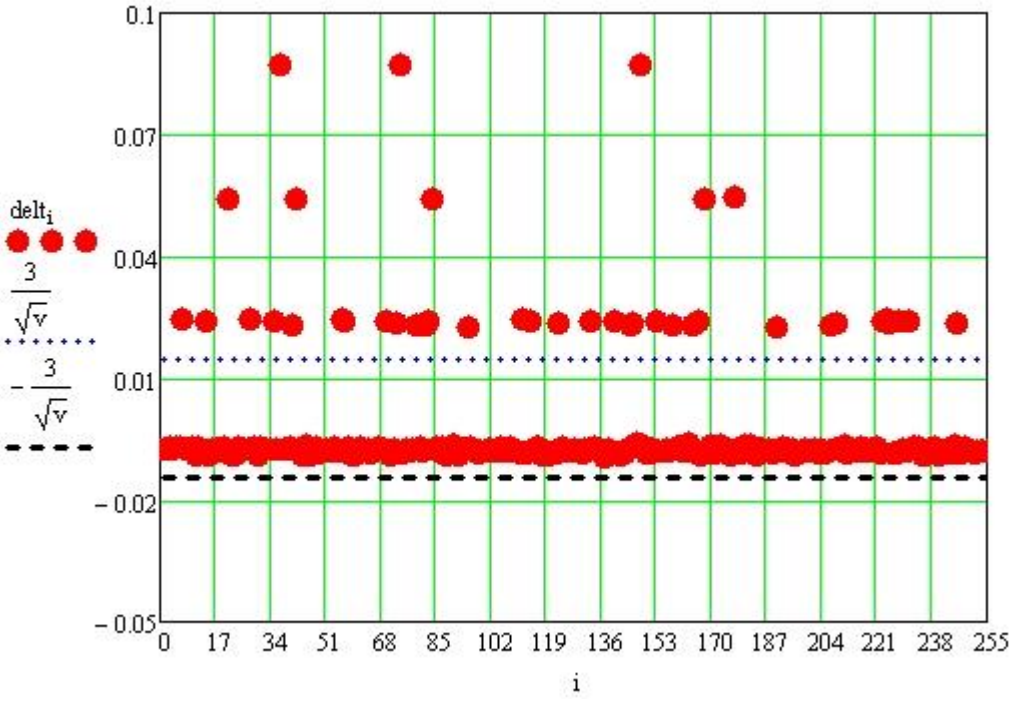
$$\text{delt} := \frac{H_8 \cdot \text{markz}}{v}$$

$\text{delt}_0 := 0$

$i := 1 .. 2^{n_4} - 1$

delt =

	0
0	0
1	-0.008
2	-0.008
3	-0.007
4	-0.008
5	-0.007
6	-0.007
7	0.024
8	-0.008
9	-0.008
10	-0.007
11	-0.009
12	-0.007
13	-0.008
14	0.024
15	...



Representación de la probabilidad

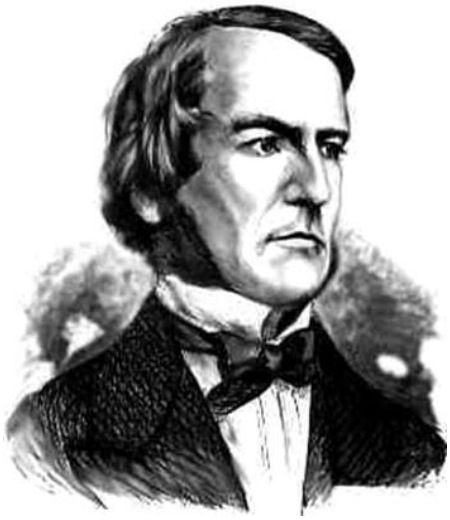
max(delt) = 0.087

37 100101

$$\frac{1 + delt_{37}}{2} = 0.544 \qquad \frac{\sum_{i=0}^{v} (-1)^{z_i + z_{i+3} + z_{i+5}}}{v} = 0.087 \qquad delt_{37} = 0.087$$

Anexo 2. Un poco de Historia.

GEORGE BOOLE (1815–1864)



George Boole, el hijo de un comerciante de clase baja, nació en Lincoln, Inglaterra, a finales de noviembre de 1815. Su padre le dio lecciones de matemáticas y le inculcó el amor por el aprendizaje. Un amigo de la familia (un bibliotecario local) le enseñó lo básico del latín. Boole estaba traduciendo poesía a la edad de 12 años. A los 14 ya hablaba con fluidez en alemán, italiano y francés, también. Le gustaban especialmente las novelas y la poesía.

Sus habilidades en las matemáticas superiores no se presentaron hasta que tenía 17 años de edad (que leyó su primer libro de matemáticas avanzadas, de Lacroix y Cálculo Diferencial e Integral). Debido a que el negocio de su padre quebró, se vio obligado a trabajar para mantener a su familia. A los 16 años se convirtió en asistente de maestro en una escuela privada en Doncaster, y antes de que él tuviera 20 años abrió su propia escuela. En 1838, Boole se ofreció para hacerse cargo de la Academia de Hall en Waddington, después de su fundador, Robert Hall, murió. Su familia se mudó a Waddington y lo ayudó a dirigir la escuela.

Usando revistas matemáticas tomados del Instituto local de la Mecánica, Boole lee “Principia” de Isaac Newton y las obras de los matemáticos franceses Pierre-Simon Laplace (1749-1827) y Joseph Louis Lagrange (1736-1813).

Después de aprender de lo que escribieron estos autores anteriores, Boole a los 24 años, publicó su primer artículo (Investigaciones sobre la teoría de las transformaciones de análisis) en el Diario Matemáticas de Cambridge (CMJ). Se desató una amistad entre George Boole y el editor del CMJ, Duncan F. Gregory, que duró hasta la muerte prematura de Gregory en 1844.

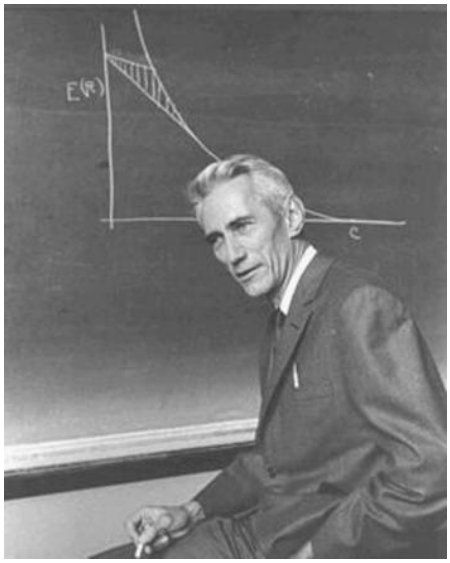
Gregory influenció a Boole para que estudiara Álgebra. Debido a la situación financiera de su familia, Boole fue incapaz de seguir el consejo de Gregory y matriculó los cursos de auditoría en Cambridge. De hecho, en el verano de 1840 abrió una escuela en Lincoln y otra vez toda la familia se mudó de nuevo con él. Después de que su padre murió, Boole tomó, en 1849, un puesto en la Cátedra de Matemáticas en el Queen's College de Cork, donde permaneció y enseñó durante el resto de su vida. Allí, conoció a una sobrina de Sir George Everest, con el nombre de María del Everest. Ella era 17 años más joven que él, pero se hicieron amigos al instante. George empezó a darle clases a María de cálculo diferencial, y en 1855, después de que su padre murió, se casó con ella. Eran muy felices juntos y tuvieron cinco hijas nacieron: Mary Ellen (n. 1856), Margarita (n. 1858), Alicia Stott (n. 1860), Lucy Everest (n. 1862), y Ethel Lilian (n. 1864).

Las obras de Boole se encuentran en alrededor de 50 artículos y en algunas otras publicaciones. Una lista de las memorias de Boole y documentos sobre temas de lógica y matemáticas, se encuentra en el catálogo de las Memorias de científicos publicados por la Royal Society, y en un volumen sobre ecuaciones diferenciales (editado por I. Todhunter). Boole escribió 22 artículos en el Diario Matemáticas de Cambridge y su sucesora la Revista Matemática Dublin, 16 documentos en la Revista de Filosofía, seis memorias en las Philosophical Transactions (Real Sociedad), y algunos otros en las Transacciones de la Royal Society de Edimburgo y de la Real Academia de Irlanda, en el Petersburgo de la Academia de St-Boletín (en 1862, bajo el seudónimo de G. Boldt), y en Crelle, y un documento sobre la base matemática de la lógica publicado en la Revista Mecánica (1848). En 1844, la Real Sociedad le dio una medalla por sus contribuciones al análisis, debido a su trabajo sobre el uso del Álgebra y cálculo para analizar las cifras infinitamente grandes y pequeñas. El cálculo de razonamiento, que preocupaba a Boole,

encontró su camino en el trabajo de 1847, el análisis matemático de la Lógica, que amplió el trabajo del matemático alemán Gottfried Wilhelm Leibniz (1646-1716) y que impulsó la idea de que la lógica era una disciplina matemática, en lugar de la filosofía. Este trabajo le valió la admiración del lógico distinguido Augustus de Morgan, y un lugar en la Facultad de Queen's College de Irlanda. En 1854, Boole, publicó una investigación sobre las leyes del pensamiento, en que se basan las teorías matemáticas de la lógica y las probabilidades, que es quizás su obra más importante. Boole aproximó la lógica en una nueva forma, reduciéndola a un álgebra simple, incorporando lógica en las matemáticas, y sentando las bases del enfoque binario ahora famoso. Las expresiones lógicas están ahora representados mediante un formulario matemático llamado en su honor Álgebra de Boole. El genio de Boole fue reconocido y recibió grados honoríficos de las universidades de Dublín y Oxford y fue elegido miembro de la Royal Society en 1857. Dado que su trabajo finalmente llevó a la gente de la Luna a la tierra, es natural que Boole sea el nombre de un cráter lunar. Un día, en 1864, Boole fue caminando desde su casa a la universidad y fue atrapado en una tormenta de lluvia. Dio conferencias con la ropa mojada y cogió un resfriado. Por eso, es lamentable para las matemáticas que murió cuando tenía sólo 49 años de edad.

Boole en el trabajo sobre la lógica matemática fue criticado y / o ignorado por sus contemporáneos, a excepción de un lógico estadounidense Charles Sanders Peirce (1839-1914), quien pronunció un discurso en la Academia Americana de las Artes y las Ciencias, describiendo las ideas de Boole. Peirce pasó más de 20 años trabajando en estas ideas y sus aplicaciones en circuitos electrónicos. Lamentablemente, el álgebra de Boole y Peirce sus trabajos siguieron siendo en su mayoría desconocidos y no utilizados, hasta 1940, cuando un joven estudiante llamado Claude Elwood Shannon recogió los trabajos de Boole y Peirce y reconoció su importancia para el diseño de la electrónica.

CLAUDE ELWOOD SHANNON (1916–2001)



Claude E. Shannon nació en Petoskey, Michigan, el 30 de abril de 1916. Su padre era un hombre de negocios y, por un período, Juez de Testamentos. Su madre era una profesora de idiomas y por varios años directora de Gaylord High School, en Gaylord, Michigan. Shannon permaneció en Gaylord, hasta que tenía 16 años cuando se graduó de la escuela secundaria. Él mostró una inclinación por la ciencia y las matemáticas, y se mantuvo ocupado en la construcción de modelos de aviones, radio control, modelo de barco, y un sistema telegráfico para un amigo, a media milla de distancia. Después de su hermana, en 1932 entró en la Universidad de Michigan (UM), donde se interesó por la obra de George Boole. Shannon se graduó de la UM en 1936 con la doble Licenciatura Grados de Ciencias en Ingeniería Eléctrica y de Ciencias Matemáticas. Enseguida, aceptó un puesto de asistente de investigación en el Massachusetts Institute of Technology para mantenerse a sí mismo, comenzando sus estudios de posgrado. Se graduó en 1940 con un master en Ingeniería Eléctrica y un doctorado en Matemáticas. Su tesis de master, Un Análisis Simbólico de Parada y Cambia Circuitos es un exitoso intento de usar el álgebra de Boole para analizar parada cambia circuitos, mientras su tesis doctoral trata de genéticas de la población. Una versión de su tesis de Maestría. Se publicó en Transactions of the American Institute of Electrical Engineers (1940), y le valió el Premio Noble Alfred. Después de pasar un año en el Instituto de Estudios Avanzados, en 1941 Shannon se unió a

Teléfonos AT & T Bell en Nueva Jersey como un matemático investigador para trabajar en sistemas de control de incendios y Criptografía. Permaneció afiliado a los Laboratorios Bell, hasta 1972, ocupando también otros puestos en (MIR; Centro para el estudio de las Ciencias del Comportamiento en Palo Alto, el Instituto de Estudios Avanzados de Princeton, miembro visitante en All Souls College, Oxford, la Universidad de California, el IEEE y la Real Sociedad). En 1949, se casó con Mary Elizabeth Shannon Moore y tuvieron tres hijos y una hija: Robert, James, Andrew Moore, y Margarita. En una de sus obras más importantes, Teoría Matemática de la Comunicación, Shannon fundamenta el tema de la teoría de la información y propuso un modelo esquemático lineal de un sistema de comunicaciones. Esta era una idea revolucionaria ya que no había ya ninguna necesidad de que las ondas electromagnéticas se envían por un cable, uno podía comunicarse mediante el envío de secuencias de bits 0 y 1. En el año siguiente, escribió otro artículo fundamental, Teoría de la Comunicación de los Sistemas Secretos, que es el primer análisis de Criptografía. Los trabajos clasificados se basan en los sistemas de secreto realizado por Shannon, en el último año de la Segunda Guerra Mundial. Shannon murió en 2001 después de una larga lucha con la enfermedad de Alzheimer.

Jacques Salomón Hadamard (1865-1963)

Su padre Amédée Hadamard, se casó con Marie Claire Jeanne Picard, el 6 de junio de 1864, era de origen judío y fue un maestro que enseñó varias materias, tales como los clásicos, la Gramática, Historia y Geografía. La madre de Jacques daba clases particulares de piano en su casa. En el momento en que Jacques nació Amédée daba clases en el Imperial Liceo Versalles, pero su familia se trasladó a París cuando él tenía tres años y su padre ocupaba un puesto en el Lycée Charlemagne.

Jacques comenzó sus estudios en el Lycée Charlemagne. En sus primeros años en la escuela era bueno en todas las asignaturas, salvo matemáticas. Se destacó en particular, en griego y latín. Él escribió en 1936:

... en aritmética, hasta el quinto grado, fui el ultimo.

No era preciso en esta declaración porque, aunque en un primer momento es cierto que él era débil en la aritmética, ya en la quinta clase se coloca segundo. En esa época (1875) fue ganador de premios en muchos temas en el Concurso

General, el concurso nacional para los alumnos de la escuela. Fue un buen profesor de matemáticas el que lo enamoró de las matemáticas y la ciencia.

En 1884 Hadamard realizó exámenes de ingreso a la Escuela Politécnica y la Escuela Normal, fue el primer lugar en ambos exámenes. Él escogió la escuela Normal Superior, donde pronto se hizo amigo de sus compañeros de estudios como Duhem y Painlevé. Entre sus maestros tendría a: Hermite, Darboux, Appell, Goursat y Emile Picard. Ya en esta etapa comenzó a realizar investigaciones, investigó el problema de encontrar una estimación para el factor determinante generado por los coeficientes de una serie de potencias. Se graduó en la Escuela Normal Superior, el 30 de octubre de 1888.

Hadamard obtuvo su doctorado en 1892 con una tesis sobre las funciones definidas por series de Taylor. Este trabajo sobre las funciones de una variable compleja fue uno de los primeros en examinar la teoría general de las funciones analíticas.

En el mismo año Hadamard recibió el Gran Premio de Ciencias. El tema propuesto para el premio llenaba las lagunas del trabajo de Riemann sobre las funciones zeta y presentado por Hermite. Stieltjes había reclamado en 1885 haber probado la hipótesis de Riemann, pero nunca había publicado su "prueba" y, después de que el tema del premio fue anunciado en 1890, Stieltjes descubrió una laguna en su "prueba" que él fue incapaz de llenar. Nunca presentó una entrada para el premio, pero Hadamard, entre el momento de presentación de su tesis y su examen oral, se dio cuenta que sus resultados podrían aplicarse a las funciones zeta. Su papel en las funciones enteras y las funciones zeta obtuvo el primer premio.

Tal vez su resultado más importante demostrado durante este tiempo fue el teorema de los números primos que demostró en 1896.

Este teorema se conjeturó en el siglo XVI, pero no se demostró hasta 1896, cuando Hadamard independientemente de Charles de la Vallée Poussin, utilizó el análisis complejo. La prueba había sido esbozada por Riemann en 1851, pero las herramientas necesarias no se habían desarrollado en ese momento. Este problema fue una de las motivaciones principales para el desarrollo del análisis complejo desde 1851 hasta 1896.

Otro resultado que Hadamard publicado durante su tiempo en Burdeos fue la desigualdad del máximo determinante. Matrices cuyo determinante satisfacen dicha igualdad en la relación anterior hoy se llaman matrices de Hadamard, y son importantes en la teoría de las ecuaciones integrales, teoría de la codificación y otras áreas.

Hadamard recibió el Premio Poncelet en 1898 por sus logros de investigación durante los últimos diez años. A pesar de que su investigación estuvo orientada más hacia la física matemática, siempre sostuvo firmemente que él fue un matemático, y no físico. En particular, trabajó en las ecuaciones en derivadas parciales de la física matemática produciendo resultados de gran importancia. En 1898 su famoso trabajo sobre geodésicas en superficies de curvatura negativa sentó las bases de la dinámica simbólica. Entre los temas que él consideraba eran elasticidad, la óptica geométrica, la hidrodinámica y los problemas de valores en la frontera. Él introdujo el concepto de un bien planteado el valor inicial y problema de valor límite.

Durante los primeros cinco años en París, otros tres niños nacieron, en primer lugar otro hijo Mathieu y luego dos hijas Cécile y Jacqueline. Siguió recibiendo premios por su investigación y fue honrado en 1906 con la elección como Presidente de la Sociedad Francesa de Matemáticas. En 1909 fue nombrado catedrático de mecánica en el Colegio de Francia. En el año siguiente publicó Lecciones sobre Calculo de Variaciones que ayudó a sentar las bases de análisis funcional (introdujo la palabra funcional). Luego, en 1912 fue nombrado profesor de análisis en la Escuela Politécnica.

Continuó produciendo libros y papeles de la más alta calidad, la publicación de tal vez su texto más famoso de Conferencias sobre el problema de Cauchy en Ecuaciones Diferenciales Parciales en 1922. El libro se basa en un ciclo de conferencias que dio en la Universidad de Yale en los Estados Unidos. También participó en nuevos temas, escribiendo varios artículos sobre la Teoría de las Probabilidades, en particular en las cadenas de Markov. También publicó numerosos artículos sobre Educación Matemática y la Educación en general.

Después de la guerra se convirtió en un activo defensor de la paz y se requirió el apoyo firme de los matemáticos en los EE.UU. que le permitió entrar en el Congreso Internacional en Cambridge, Massachusetts en 1950. Fue nombrado presidente honorario del Congreso.

Una tragedia, Hadamard fue golpeado antes de su muerte. En 1962, cuando tenía 96 años, su nieto Étienne fue muerto en un accidente de alpinismo. Esto parecía finalmente matar el espíritu de Hadamard y no salió de su casa después de esto, casi esperando la muerte.

En la conferencia para celebrar el centenario de su nacimiento, uno de sus alumnos dijo que había sido enseñado por:

... un maestro que estaba en activo, vivo, cuyo razonamiento se combinaba con exactitud y dinamismo. Así, la conferencia se convirtió en una lucha y una aventura. Sin sufrir el rigor, la importancia de la intuición fue devuelta a nosotros, y los mejores alumnos estaban encantados.

Laurent Schwartz habló de Hadamard en esta ceremonia para celebrar el centenario del nacimiento de Hadamard: --

Creo que él tuvo una influencia fantástica en su tiempo, y que todos los analistas de vida fueron modelados por él, directa o indirectamente.