Ciencias Matemáticas, Vol. 32, No. 1, Pag. 17-21, 2018
Recibido 11-2017

Varianza del coeficiente de confusión y no-linealidad de S-cajas dentro de las clases *Hamming Weight*
Confusion coefficient variance and non-linearity of S-boxes inside Hamming Weight classes

Ismel Martínez Díaz[1]*, Dianne Miyares Moreno[2], C.M. Legón[1]

Resumen Existen varias métricas teóricas para medir la resistencia de una S-caja ante ataques diferencial de potencia, entre las cuales destaca la varianza del coeficiente de confusión. Recientemente se ha definido una relación de equivalencia que permite dividir el espacio de S-cajas en clases de según el modelo de fuga peso de Hamming. En este trabajo se demuestra teórica y experimentalmente que el valor de la varianza del coeficiente de confusión se mantiene constante para las S-cajas que pertenecen a una misma clase de equivalencia. También se estudia experimentalmente el comportamiento de la propiedad de no-linealidad dentro de las clases observándose que posee un comportamiento asimétrico, lo cual aporta nuevos elementos a la comprensión de la relación entre la varianza del coeficiente de confusión y la no-linealidad.

Abstract There are different theoretic metrics to measure the differential power attacks resistance of S-boxes. One of the most important is the confusion coefficient variance. Recently was defined a new equivalence relation such that all S-boxes inside one class have the same power leakage under the Hamming Weight model. In this paper we have been proved that the confusion coefficient variance is constant inside each class and, at the other hand, non-linearity is asymmetric inside each class, getting a more compression about their relationship.

Palabras Clave
S-caja — HW — CCV

[1] *Instituto de Criptografía, Facultad de Matemática y Computación, Universidad de la Habana, Habana, Cuba, ismel@matcom.uh.cu, clegon58@gmail.com*
[2] *Dirección de Calidad, Universidad Tecnológica de la Habana, Habana, Cuba, dmiyares93@gmail.com*
***Autor para Correspondencia**

Introducción

En la actualidad existen una variedad de dispositivos de cómputo que se interconectan para crear, consumir e intercambiar datos. En este intercambio es muy importante el uso de la criptografía simétrica y en particular de cifradores de bloques que permitan la seguridad e integridad de los datos [1, 2].

El componente no lineal más importante de los cifradores de bloques son las S-cajas o cajas de sustitución, funciones vectoriales booleanas que garantizan la confusión en el cifrado. Los cifradores de bloques, como por ejemplo el cifrador AES (*Advanced Encryption Standard*), se encuentran ante la amenaza de ataques diferencial de potencia DPA (*Differential Power Attacks*), los cuales tienen como objetivo obtener las claves a partir de las fugas de potencia observadas por el atacante en el proceso de evaluación de la S-caja [3]. El éxito de estos ataques se debe a la existencia de correlación estadística entre la fuga de potencia real y la fuga de potencia hipotética simulada mediante diversos modelos como el modelo peso de *Hamming* [1], el cual calcula el peso de la salida de la S-caja.

Para contrarrestar estos ataques es necesario una búsqueda constante de nuevas S-cajas resistentes ante DPA [4], en esta búsqueda de S-cajas el espacio es de grandes dimensiones. En [5] se define una nueva relación de equivalencia que permite particionar el espacio de búsqueda en clases de equivalencias. Las S-cajas que pertenecen a una misma clase poseen la misma fuga hipotética de potencia según el modelo de fuga peso de *Hamming*. Estas clases son nombradas como clases *Hamming Weight*.

Existen varias métricas teóricas para medir la resistencia DPA de una S-caja [6], entre las cuales destaca la varianza del coeficiente de confusión [7], la cual denotaremos como CCV (*Confusion Coefficient Variance*). En la Sección 2.1 de este trabajo se demuestra que está métrica se mantiene constante dentro de las clases *Hamming Weight*. En la Sección 2.2 se presenta también el estudio del comportamiento de la propiedad no-linealidad, se concluye que no es constante y que posee un comportamiento asimétrico.

1. Preliminares

En esta sección se presentan los elementos necesarios para la comprensión del trabajo.

1.1 S-cajas y clases *Hamming Weight*

Una S-caja es una función vectorial booleana biyectiva $F : \{0,1\}^n \to \{0,1\}^m$.

La función de peso de *Hamming* $HW(x), x \in \{0,1\}^m$, calcula la cantidad de unos en el vector booleano x de m componentes [1].

Uno de los modelos comúnmente utilizados para representar la fuga de potencia en los cifradores de bloque es el modelo de fuga peso de *Hamming* [1]. En este modelo se interpreta como fuga hipotética del consumo de potencia cuando se cifra, al resultado de la función $HW(F(in \oplus k))$, donde F es la S-caja, *in* representa el texto claro y k la subclave con la cual se realiza el cifrado.

En [5] se definen las S-cajas *HW*-equivalentes a partir de los conjuntos $C(F)_w$ de entradas x cuyas salidas $F(x)$ poseen peso w, $C(F)_w = \{x | HW(F(x)) = w, \forall x \in \{0,1,...,2^n - 1\}\}$. Siendo F_A y F_B dos S-cajas definidas en los mismos dominio $\{0,1\}^n$ e imagen $\{0,1\}^m$, estas S-cajas son *HW*-equivalentes sí y solo sí $C(F_A)_w = C(F_B)_w, \forall w \in \{0,1,...,m\}$. La clase de equivalencia asociada a la S-caja F_A se denota como $< F_A >= \{F_B | C(F_B)_w = C(F_A)_w, \forall w \in \{0,1,...,m\}\}$. Una clase $< F_A >$ está determinada por los $(m+1)$ conjuntos $C(F_A)_w, \forall w \in \{0,1,...,m\}$. Estas clases reciben el nombre de clases *Hamming Weight*.

Ejemplo, la clase $< F_{AES} >$ a la cual pertenece la S-caja del cifrador AES, está determinada por los siguientes conjuntos de entradas con representación hexadecimal:

$C(F_{AES})_0 = \{75\}$

$C(F_{AES})_1 = \{53,57,76,9A,C8,CC,E9,EA\}$

$C(F_{AES})_2 = \{$ 05,06,09,24,50,54,5C,5F,
71,72,7A,7D,7E,7F,91,9D,
B3,B8,C0,C3,C4,CB,CF,E2,
E6,ED,F3,FF $\}$

$C(F_{AES})_3 = \{$ 01,02,0A,0B,0E,20,23,27,
2B,2C,2F,45,51,52,58,5B,
5E,64,68,6B,6F,70,73,77,
79,7B,7C,90,92,96,99,9B,
9C,9E,B0,B7,BB,BC,BE,BF,
C2,C5,C7,C9,CE,D1,DA,DE,
E0,E1,E4,E5,EE,F0,F8,FC $\}$

$C(F_{AES})_4 = \{$ 00,03,04,07,08,0C,0D,0F,
1B,1C,1F,21,22,28,29,2D,
2E,31,36,3D,41,42,46,4A,
4D,55,56,59,5A,5D,60,63,
67,6C,74,78,80,84,88,8B,
8C,93,94,95,97,98,A6,A7,
A9,AA,B1,B2,B4,B6,B9,BD,
C6,CA,D0,D6,DD,E3,E7,E8,
EB,EC,EF,F4,F7,FB $\}$

$C(F_{AES})_5 = \{$ 10,13,14,17,18,19,1E,25,
26,2A,32,35,37,3A,3B,3E,
43,47,48,49,4B,4C,4E,61,
62,65,66,69,6A,6E,83,87,
8F,9F,A0,A1,A2,A5,AD,AE,
B5,BA,C1,CD,D2,D3,D4,D5,
D7,D8,D9,F5,F9,FA,FD,FE $\}$

$C(F_{AES})_6 = \{$ 12,15,16,1D,30,33,38,39,
3C,3F,40,44,4F,6D,82,85,
89,8A,8E,A3,A4,AB,AC,DC,
DF,F1,F2,F6 $\}$

$C(F_{AES})_7 = \{11,1A,34,81,86,A8,AF,DB\}$

$C(F_{AES})_8 = \{8D\}$

A partir de la representación de la clase $< F_A >$ mediante los conjuntos $C(F(x))_w$ en [5] se propone un algoritmo que se denotará por **HwSboxGenerator**, el cual partiendo de una S-caja F_A genera otras que pertenecen a su misma clase $< F_A >$. En esencia este algoritmo construye los conjuntos $C(F_A(x))_w$ a partir de la S-caja F_A y para cada conjunto permuta aleatoriamente las salidas correspondientes a los elementos de ese conjunto.

Este algoritmo **HwSboxGenerator**, es finito en el número de conjuntos a permutar, y asegura que la S-caja obtenida pertenece a la misma clase $< F_A >$.

1.2 Resistencia práctica dentro de las clases de equivalencia ante el ataque por correlación de potencia

El ataque por correlación de potencia CPA(*Correlation Power Analysis*) [1] utiliza el coeficiente de correlación lineal como distinguidor **D** para cuantificar la dependencia estadística entre la fuga de potencia real generada a partir de la clave **K** y la fuga hipotética calculada con el modelo a partir de la clave supuesta **J**, como se ilustra en la Fig. 1.

Para comprobar en la práctica que las S-cajas de una misma clase poseen la misma resistencia ante el ataque CPA, en [5] se generan con el algoritmo **HwSboxGenerator** S-cajas pertenecientes a la clase $< F_{AES} >$. Al realizar un ataque CPA a estas S-cajas usando para cada una sus propias fugas hipotéticas pero con las mismas fugas reales generadas por el cifrador AES, se obtienen los mismos resultados para todas las S-cajas. Este resultado práctico sugiere que cualquier métrica teórica que pretenda medir la resistencia DPA en este escenario debería tener una valor constante dentro de la clase.

[1] x puede ser representado como un número entero no negativo, en particular como un byte si $m = 8$

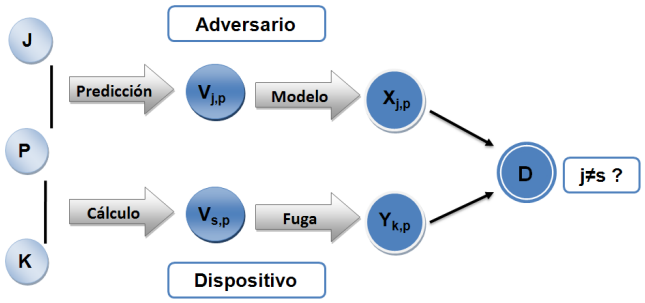

Figura 1. Representación del ataque CPA

1.3 Varianza del coeficiente de confusión

En [8] se presenta el coeficiente de confusión como una métrica para medir la resistencia teórica de una S-caja ante ataques DPA. Esta métrica se calcula para dos subclaves k_i y k_j, y se define como:

$$\kappa(k_i,k_j) = E[(V|k_i - V|k_j)^2] \tag{1}$$

Donde en (1), $V|k$ representa la función de fuga al cifrar con una subclave k.

Posteriormente, para eliminar la dependencia de las subclaves, en [7] se propone la métrica CCV utilizando el coeficiente de confusión (1) y el modelo de fuga peso de Hamming para simular la fuga $V|k$, sin depender de las subclaves. Su cálculo, teniendo en cuenta todo par de subclaves $k_i, k_j, k_i \neq k_j$ y todo texto claro in, es:

$$CCV(F) = Var(E[(HW(F(in \oplus k_i)) - HW(F(in \oplus k_j)))^2]) \tag{2}$$

En la Sección 2.1 se demuestra que esta métrica es constante dentro de la clase, lo cual se corresponde con los resultados prácticos de la Sección anterior y constituye uno de los aportes de este trabajo.

1.4 No-linealidad

La no-linealidad NL(*Non-Linearity*) es una propiedad asociada a una S-caja que determina su resistencia ante ataques lineales. En [9] se formula el cálculo de la NL como:

$$NL(F) = 2^{n-1} - \frac{1}{2} \max_{v \in \{0,1\}^m - \{0\}^m; w \in \{0,1\}^n} \left| \sum_{x \in \{0,1\}^n} (-1)^{v \cdot F(x) + w \cdot x} \right| \tag{3}$$

Donde $u \cdot v = \sum_i u_i v_i$ es el usual producto interno entre u y v.

En [10] se definen clases de equivalencias afines a partir de las propiedades algebráicas de las S-cajas, entre ellas la no-linealidad.

Es de interes encontrar S-cajas con alto valor de CCV buscando resistencia ante los ataques DPA y alto valor de NL para garantizar resistencia ante los ataques lineales, sin embargo hay pocos resultados de este tipo. La relación contradictoria entre CCV y NL ha sido discutida en [11, 4]; no existen reportes sobre la forma funcional explícita de esta relación, lo cual es un tema abierto de investigación.

En la sección 2 se investiga esta relación en un nuevo escenario: el interior de las clases de equivalencia. Como se esperaba el valor de CCV se mantiene constante dentro de la clase, sin embargo el valor de NL está lejos de ser constante y su distribución no es ni siquiera simétrica.

2. Resultados y discusión

En esta sección se presentan los resultados de este trabajo y se realiza una discusión de los mismos.

2.1 Comportamiento constante del CCV dentro de la clase *Hamming Weight*

Como resultado principal de este trabajo se demuestra que CCV es constante dentro de las clases *Hamming Weight* y se realiza un experimento con la S-cajas que pertencen a la clase del AES que confirma este resultado teórico.

Proposición 1. Sean F_A y F_B dos S-cajas definidas en los mismos dominio $\{0,1\}^n$ e imagen $\{0,1\}^m$. Si F_A y F_B son HW-equivalentes entonces $CCV(F_A) = CCV(F_B)$

Demostración. En (2) se puede notar que dos S-cajas HW-equivalentes poseen el mismo valor de CCV debido a que los pesos de hamming de sus salidas coinciden para la misma entrada $HW(F_A(x)) = HW(F_B(x))$, donde $x = in \oplus k$.

Para verificar experimentalmente el comportamiento del CCV dentro de una clase, se generaron 10000 S-cajas HW-equivalentes a la S-caja del cifrador AES utilizando el algoritmo **HwSboxGenerator**. Posteriormente se calculó el CCV para cada una de dichas S-cajas, utilizando la herramienta SET (*S-box Evaluation Tool*) presentada en [12]. Para las 10000 S-cajas se obtiene exactamente el mismo valor constante de CCV dentro de la clase, ver la Fig. 2.

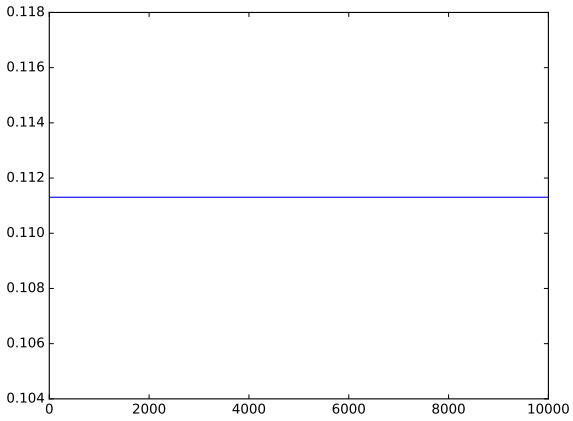

Figura 2. Valor de CCV para 10000 S-cajas HW-equivalentes a la S-caja del cifrador AES

Aunque las S-cajas *HW*-equivalentes poseen el mismo valor de CCV, esto no ocurre así en el sentido contrario; existen S-cajas que posen el mismo valor de CCV y sin embargo no pertencen a la misma clase *Hamming Weight*. Para demostrar lo anterior se definió y evaluó el siguiente conjunto A de S-cajas afines:

$$A = \{F_C | F_C(x) = F_{AES}(x \oplus a) \oplus b\} \quad (4)$$

Donde $a \in \{0,1\}^8 \setminus \{0\}^8$, $b \in \{0\}^8 \cup \{1\}^8$ y F_{AES} es la S-caja del cifrador AES.

Se puede comprobar, mediante la construción de estas S-cajas y cálculo de su CCV, que todas las S-cajas del conjunto A (4) poseen valor CCV igual al de la S-caja F_{AES}, sin embargo pertenecen a clases *Hamming Weight* distintas a la clase $< F_{AES} >$ presentada en la Sección 1.1.

2.2 Comportamiento asimétrico de NL dentro las clases *Hamming Weight*

Para estudiar el comportamiento de la NL dentro de las clases *Hamming Weight* se generaron en total 40000 S-cajas, 10000 S-cajas *HW*-equivalentes a cada una de las S-cajas: AESCC, SCREAM, AES y STRIBOB, presentadas en [13] y se evaluó la propiedad NL utilizando la herramienta SET.

Como se puede notar en las Fig. 3, 4, 5, 6, la distribución de los valores de NL dentro de las respectivas clases Hamming Weight no es constante y no es simétrica. A pesar de que la CCV es constante dentro de la clase, la nolinealidad no lo es. Este resultado aporta nuevos elementos a la comprensión de la relación entre CCV y NL.

Note además que: Al comparar entre sí los cuatro casos, el valor de CCV va descendiendo 0.149, 0.122, 0.111, 0.111, sin embargo se observan pocos cambios en el histograma de frecuencias, solo hay una ligera diferencia en la altura de algunos histogramas. En todos los casos la cola izquierda es más amplia que la derecha, lo cual significa que dentro de las clases la cantidad de S-cajas con no-linealidad baja es mayor que las de S-cajas con no-linealidad alta. Se deja como problema abierto la determinación de la distribución exacta de la NL dentro de las clases.

Conclusiones

Se demostró que dentro de las clases *Hamming Weight*, el CCV se comporta de manera constante mientras que el NL no es constante y sigue una distribución asimétrica con la cola izquierda más amplia que la derecha. Este resultado aporta nuevos elementos a la comprensión de la relación entre CCV y NL. Se deja como problema abierto la determinación de la distribución exacta de la NL dentro de las clases.

Para trabajos futuros se pretende construir un nuevo escenario en el cual el valor de NL sea constante para estudiar la distribución de CCV y también estudiar el comportamiento dentro de las clases *Hamming Weight* de la propiedad conocida como orden de transparencia redefinido MTO(*Modified Transparency Order*) [14].

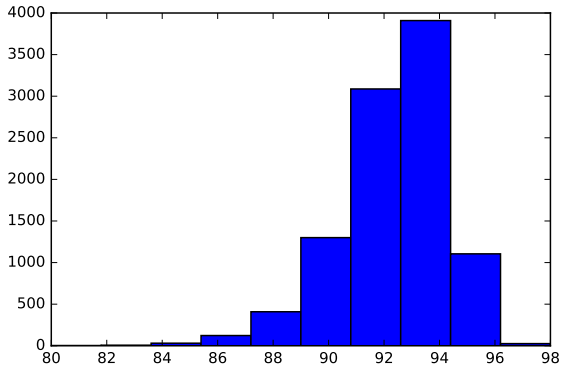

Figura 3. Histograma de los valores NL para 10000 S-cajas *HW*-equivalentes a la S-caja AESCC con CCV = 0.149

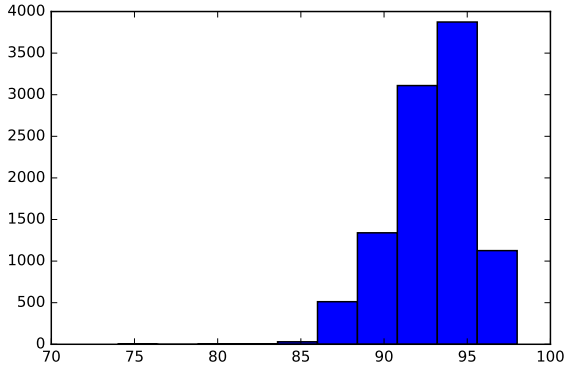

Figura 4. Histograma de los valores NL para 10000 S-cajas *HW*-equivalentes a la S-caja SCREAM con CCV = 0.122

Referencias

[1] Van Tilborg HC. *Encyclopedia of cryptography and security*; Springer; 2005.

[2] Sehrawat D, Gill NS. *Lightweight Block Ciphers for IoT based applications: A Review*; International Journal of Applied Engineering Research; 2018.

[3] Prouff E. *DPA attacks and S-boxes*; International Workshop on Fast Software Encryption; Springer; 2005.

[4] Picek S. *Applications of evolutionary computation to cryptology*; Radboud University; 2015.

[5] Sánchez R. *Generación de S-cajas equivalentes, según su resistencia a los ataques diferenciales de potencia*; Universidad Tecnológica de la Habana; 2016.

[6] Stoffelen K. *Intrinsic Side-Channel Analysis Resistance and Efficient Masking*; Radboud University; 2015.

[7] Picek S, Papagiannopoulos K, Ege B, Batina L, Jakobovic D. *Confused by confusion: Systematic evaluation of DPA*

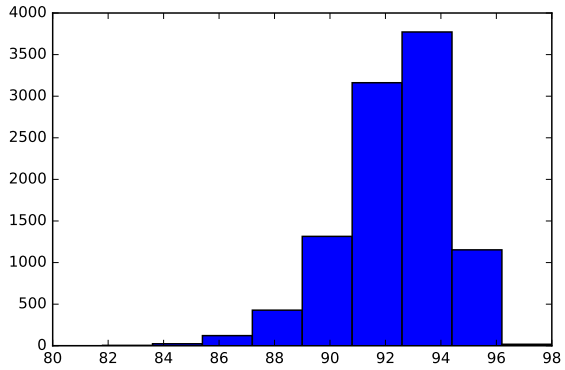

Figura 5. Histograma de los valores NL para 10000 S-cajas *HW*-equivalentes a la S-caja AES con CCV = 0.111

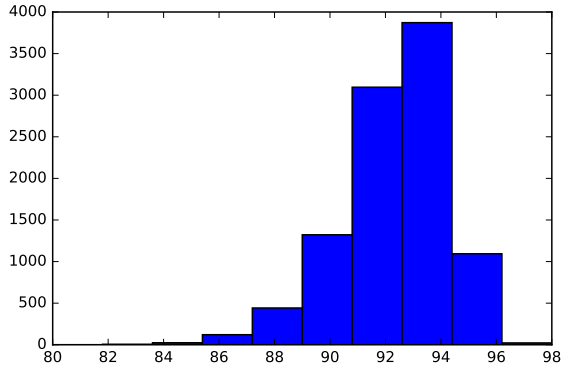

Figura 6. Histograma de los valores NL para 10000 S-cajas *HW*-equivalentes a la S-caja STRIBOB con CCV = 0.098

resistance of various s-boxes; International Conference in Cryptology in India; Springer; 2014.

[8] Fei Y, Ding AA, Lao J, Zhang L. *A Statistics-based Fundamental Model for Side-channel Attack Analysis*; IACR Cryptology ePrint Archive; 2014.

[9] Carlet C, Ding C. *Nonlinearities of S-boxes*; Finite fields and their applications; 2007.

[10] Leander G, Poschmann A. *On the classification of 4 bit s-boxes*; Arithmetic of Finite Fields; 2007

[11] Heuser A, Rioul O, Guilley S. *A theoretical study of Kolmogorov-Smirnov distinguishers*; International Workshop on Constructive Side-Channel Analysis and Secure Design; Springer; 2014.

[12] Picek S, Batina L, Jakobovic D, Ege B, Golub M. *S-box, SET, match: a toolbox for S-box analysis*; IFIP International Workshop on Information Security Theory and Practice; Springer; 2014.

[13] Lerman L, Markowitch O, Veshchikov N. *Comparing Sboxes of ciphers from the perspective of side-channel attacks*; Hardware-Oriented Security and Trust (Asian-HOST), IEEE Asian; IEEE; 2016.

[14] Chakraborty K, Sarkar S, Maitra S, Mazumdar B, Mukhopadhyay D, Prouff E. *Redefining the transparency order*; Designs, Codes and Cryptography; 2016.