Ciencias Matemáticas, Vol. 33, No. 1, Pag. 62-65, 2019

S-cajas Afines con Igual Varianza del Coeficiente de Confusión
Affine S-boxes with the Same Confusion Coefficient Variance

Ismel Martínez-Díaz[1]*, Alejandro Freyre [1], Eziel Ramos [1], C.M. Legón[1]

Resumen Las propiedades de no-linealidad y varianza del coeficiente de confusión son de gran importancia en las S-cajas, componentes principales de los cifradores de bloques. Es necesario agrupar las S-cajas de modo que todas posean el mismo valor de no-linealidad y el mismo valor de varianza del coeficiente de confusión. En este trabajo se demuestra experimentalmente como, a partir de una S-caja inicial, se puede construir un subconjunto de S-cajas affines que tienen igual varianza del coeficiente de confusión. Se muestra además que las S-cajas pertenecientes a dicho subconjunto no reflejan la misma fuga hipotética de potencia bajo el modelo de fuga: peso de *Hamming*.

Abstract Properties as non-linearity and confusion coefficient variance are important in S-box design. In this work we show a new method that construct an affine subset of S-boxes from an initial S-box. This subset contains S-boxes with the same confusion coefficient variance but not the same hypothetical leakage under the Hamming weight leakage model.

Palabras Clave
S-cajas — No-linealidad — Varianza del coeficiente de confusión

[1] *Instituto de Criptografía, Facultad de Matemática y Computación, Universidad de la Habana, Habana, Cuba, ismel@matcom.uh.cu, a.freyre@estudiantes.matcom.uh.cu, e.ramos@estudiantes.matcom.uh.cu, clegon58@gmail.com*
***Autor para Correspondencia**

1. Introducción

En la criptografía simétrica, en particular en el diseño de cifradores de bloques, es de especial importancia las componentes conocidas como S-cajas o cajas de sustitución. Para asegurar la seguridad en el cifrado es necesario que las S-cajas posean buenos valores de ciertas propiedades criptográficas. Entre estas propiedades criptográficas destacan: la propiedad de no-linealidad NL (*Non-linearity*) [1] ante los ataques lineales y diferenciales, y la propiedad de varianza del coeficiente de confusión CCV (*Confusion Coefficient Variance*) [7] ante los ataques de canal colateral por consumo de potencia bajo el modelo de fuga: peso de *Hamming*.

Existen varios métodos para conformar S-cajas con buenos valores de NL o CCV. En general estos métodos se pueden agrupar en: métodos por construcción algebraica [4], métodos heurísticos (incluida la búsqueda aleatoria) [5, 9] o métodos mixtos [2].

Mientras más altos sean los valores de estas dos propiedades, más resistente es la S-caja ante distintos ataques criptográficos [10], sin embargo, cuando aumenta el valor de NL, disminuye el valor de CCV, y viceversa [7]. De acuerdo con lo anterior, es muy complejo obtener S-cajas con buenos valores de NL y CCV al mismo tiempo. Si se obtiene una S-caja con estas características, es útil contar con un algoritmo que pueda generar S-cajas semejantes. En la literatura actual no se conocen algoritmos de este tipo.

Es conocido además que las transformaciones afines matienen invariante el valor de NL [3] y que las S-cajas pueden reflejar la misma resistencia ante los ataques de canal colateral por consumo de potencia según el modelo de fuga: peso de *Hamming* [8].

En este trabajo se investiga la existencia de transformaciones afines que mantengan invariantes ambos parámetros (NL y CCV). Se identifica un subconjunto de transformaciones afines que no alteran el valor de la varianza del coeficiente de confusión. Se presenta un nuevo método que permite, dado una S-caja inicial, obtener S-cajas que poseen los mismos valores de NL y CCV que la S-caja inicial. Se demuestra experimentalmente el buen funcionamiento del método en el espacio de S-cajas de 8 bits y 4 bits. Finalmente, se muestra que a pesar de poseer el mismo valor de CCV, las S-cajas del conjunto no reflejan la misma resistencia ante los ataques de canal colateral por consumo de potencia bajo el modelo de fuga: peso de *Hamming*.

1.1 Nociones básicas

Una S-caja es una función vectorial booleana biyectiva definida como $S : \{0,1\}^n \to \{0,1\}^n$. Las S-cajas afines a una S-caja S son aquellas S-cajas $S_{a,b} = S(x \oplus a) \oplus b, \forall x \in \{0,1\}^n$

donde $a,b \in \{0,1\}^n$, en el caso particular de $a = 0, b = 0$, entonces $S_{0,0} = S$.

Toda S-caja afín $S_{a,b}$ a una S-caja S poesee el mismo valor NL que S [3].

Dos S-cajas S_a, S_b poseen la misma fuga hipotética de potencia bajo el modelo de fuga: peso de *Hamming* si $HW(S_a(x)) = HW(S_b(x)), \forall x \in \{0,1\}^n$ [8], donde la función de peso de *Hamming* $HW(y), y \in \{0,1\}^n$, calcula la cantidad de unos en el vector booleano y.

Tanto el valor de la propiedad NL y como de la propiedad CCV de una S-caja S, pueden ser calculadas mediante la herramienta SET (*S-box Evaluation Tool*) presentada en [6].

2. Resultados y discusión

A fin de encontrar alguna S-caja con alto valor CCV manteniendo la NL, se analizan todas las S-cajas afines a la mejor S-caja presentada en [7]. No se encuentra S-caja alguna con dicha característica, en particular porque la S-caja inicial es una S-caja obtenida por computación evolutiva y representa un óptimo local. Pero se pudo comprobar que todas las S-cajas afines obtenidas cuando $b = 0$ o $b = 255$ poseen el mismo valor CCV que la S-cajas inicial.

Lo anterior sugiere plantear:

Conjetura 1. Sea S una S-caja. El subconjunto de S-cajas afines $A = \{S_{a,b} | S_{a,b}(x) = S(x \oplus a) \oplus b\}, \forall x \in \{0,1\}^n$, donde $a \in \{0,1\}^n$, $b \in \{0\}^n \cup \{1\}^n$, cumple que $CCV(S_{a,b}) = CCV(S), \forall S_{a,b} \in A$.

El conjunto A posee un tamaño de $2 * (2^n - 1)$ S-cajas afines con igual valor de CCV a la S-caja inicial S. Esta cantidad crece en un orden exponencial con respecto a la cantidad de bits n (ver Tab. 1).

Para estudiar experimentalmente la correctitud de la conjetura, se presenta un nuevo método para obtener S-cajas con igual valor de NL e igual valor de CCV a una S-cajas inicial. Dicho método se describe de acuerdo a los siguientes pasos (ver Alg. 1):

Algorithm 1 Método para obtener S-cajas con igual NL e igual CCV

Require: S, S-caja.
Ensure: R, conjunto de S-cajas con igual NL y CCV que S.

```
1:  R ← ∅
2:  for a ∈ {0,1}^n \ {0}^n do
3:      for b ∈ {0}^n ∪ {1}^n do
4:          for x ∈ {0,1}^n do
5:              S_{a,b}(x) ← S(x ⊕ a) ⊕ b
6:          end for
7:          R ← R ∪ {S_{a,b}}
8:      end for
9:  end for
10: return R
```

2.1 Experimentos realizados

Para evaluar el nuevo método presentado se realizó el siguiente experimento:

1. En los espacios de S-cajas de 8 bits ($n = 8$) y 4 bits ($n = 4$).
2. Se generan 10000 S-cajas aleatorias iniciales.
3. Por cada S-caja aleatoria inicial se aplica el método 1 y se crea su conjunto de transformaciones afines correspondiente.
4. Se calcula el valor CCV de todas las S-cajas pertenecientes a cada conjunto de S-cajas resultante.

Los resultados obtenidos mostraron experimentalmente el correcto funcionamiento del método. Se pudo comprobar que todas las S-cajas de los conjuntos resultantes poseían igual valor CCV que cada una de las S-cajas iniciales al aplicarse respectivamente 10000 veces el método.

Seguidamente se muestra la S-caja $SPicek_{8,0}$, perteneciente al conjunto resultante de aplicar el Algoritmo 1 a la S-caja presentada en [7]. En particular $SPicek_{8,0}$ se obtuvo con los valores $a = 8$ y $b = 0$; es un ejemplo de S-caja con altos valores de NL y CCV ya que su S-caja inicial exhibe estas características.

$SPicek_{8,0}$ = (55, 4f, ac, dd, 3d, b0, 13, cc, 59, d2, 7f, 48, 08, 8f, d1, 94, 0a, 97, 1e, 7d, cb, 71, bc, 83, 7b, 19, 4e, 93, 54, cd, 20, 1f, 4a, f7, 5b, f2, 17, 5a, 2f, 22, eb, 10, 8d, 67, a5, 25, 04, e3, 4c, 2d, 86, ec, 75, 29, 38, 2c, d8, 70, f5, 07, 41, ef, a6, 9c, 1b, 2e, 8c, f6, 76, 06, 96, c2, a3, 45, fc, 51, 40, b7, c9, e0, 3a, be, 74, e2, 4d, 69, bd, c0, ff, 0c, 7a, d4, ea, 3c, 21, 73, a2, ab, 6a, b3, ad, 58, dc, a0, f3, 2a, 57, 34, a4, 46, 89, e6, 53, 2b, 8a, af, cf, 88, 62, 90, f8, 79, fd, 43, 44, ee, 47, 42, b1, d6, 91, 5f, 77, 50, 8b, a8, f0, c8, 3e, 0d, 84, 35, 85, 52, 23, fb, 87, 65, 99, 68, 6b, 82, df, 05, 5d, e4, 9b, 15, 32, 7e, 98, 9f, 36, d5, ca, 16, e9, 24, db, 64, 6d, 95, 92, 3b, 03, 6f, 27, 5e, 1c, 3f, b9, 02, 8e, a1, ba, 66, fa, 18, 60, ce, c3, 11, 4b, ae, 81, fe, bb, 12, c1, b8, e8, aa, ed, b4, 28, f4, 31, c5, 14, de, 9d, d9, d0, 78, c7, 00, f9, a9, da, b5, 49, d3, 0b, f1, 09, e7, e5, 0f, 6c, 56, 6e, 80, bf, 0e, e1, 1d, c6, 33, 30, d7, 5c, 9e, 1a, 37, a7, 01, 63, 61, 7c, b2, 9a, 26, c4, b6, 72, 39)

Aunque las S-cajas de A poseen el mismo valor de CCV, no poseen la misma fuga hipotética de potencia bajo el modelo de fuga: peso de *Hamming*.

Para demostrar lo anterior se define el siguiente experimento:

1- Se crea mediante el Algorimo 1 el subconjunto de S-cajas afines A_{aes} a la S-caja del cifrador AES que poseen su mismo valor CCV.

$$A_{aes} = \{S_{a,b} | S_{a,b}(x) = S_{aes}(x \oplus a) \oplus b\}, \forall x \in \{0,1\}^n \quad (1)$$

donde $a \in \{0,1\}^n$, $b \in \{0\}^n \cup \{1\}^n$.

Cuadro 1. Tamaño del conjunto A en relación con el tamaño de bits n

Cantidad de bits	Cantidad de elementos del conjunto
4	30
8	510

2- Para cada S-caja $S_{a,b} \in A_{aes}$ se calcula su distancia euclideana:

$$ED(S_a, S_b) = \sqrt{\sum_{x \in \{0,1\}^8} (HW(S_a(x)) - HW(S_b(x)))^2} \quad (2)$$

y su distancia de *Hamming*:

$$HD(S_a, S_b) = \sum_{x \in \{0,1\}^8} \begin{cases} 1 & HW(S_a(x)) \neq HW(S_b(x)), \\ 0 & \text{e.o.c} \end{cases} \quad (3)$$

con respecto a la S-caja S_{AES}.

Los resultados obtenidos comprueban lo esperado. Las S-cajas del conjunto A_{aes} poseen distinta fuga hipotética de la S-caja S_{AES}. Incluso distan de dicha S-caja con valores diferentes (ver figuras 1. y 2.) según distancias tan disímiles como son la distancia euclidiana y la distancia de *Hamming*. En el caso de la distancia euclideana se puede ver que: $ED(S_{a,b}, S_{AES}) > 25, \forall S_{a,b} \in A_{aes}$. Mientras que para la distancia de *Hamming*: $HD(S_{a,b}, S_{AES}) > 150, \forall S_{a,b} \in A_{aes}$.

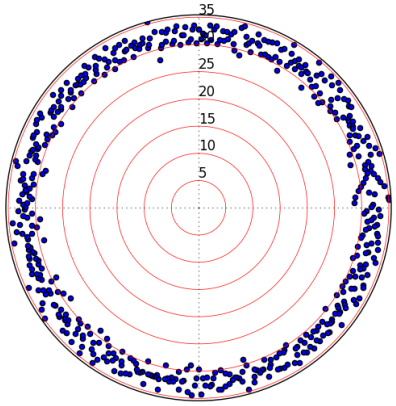

Figura 1. ED entre cada S-caja que pertence al conjunto (1) - puntos alrededor - y la S-caja del cifrador AES - punto central -

Conclusiones

Se define un nuevo conjunto de S-cajas que poseen igual no-linealidad e igual varianza del coeficiente de confusión y se presenta un método para generar dicho conjunto a través de una S-caja inical. Como trabajo futuro se pretende utilizar

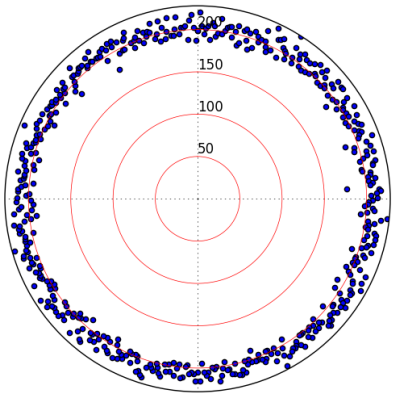

Figura 2. HD entre cada S-caja que pertence al conjunto (1) - puntos alrededor - y la S-caja del cifrador AES - punto central -

dicho conjunto de S-cajas para estudiar mejor el espacio de búsqueda de todas las S-cajas. Queda como problema abierto encontrar S-cajas afines que posean la misma fuga hipotética de potencia bajo el modelo de fuga: peso de *Hamming*.

Referencias

[1] Claude Carlet and Cunsheng Ding. Nonlinearities of s-boxes. *Finite fields and their applications*, 13(1):121–135, 2007.

[2] Reynier Antonio de la Cruz Jiménez. On some methods for constructing almost optimal s-boxes and their resilience against side-channel attacks. *IACR*, (618), 2018.

[3] Gregor Leander and Axel Poschmann. On the classification of 4 bit s-boxes. *Arithmetic of Finite Fields*, (159-76), 2007.

[4] Kaisa Nyberg. Diffrentially uniform mappings for cryptography. In *Advances in Cryptology - EUROCRYPT 93, Workshop on the Theory and Application of Cryptographic Techniques*, pages 55–64. Springer, 1994.

[5] Stjepan Picek. *Applications of evolutionary computation to cryptology*. sn: SI, 2015.

[6] Stjepan Picek, Lejla Batina, Domagoj Jakobović, Barış Ege, and Marin Golub. S-box, set, match: a toolbox for s-box analysis. In *IFIP International Workshop on*

Information Security Theory and Practice, pages 140–149. Springer, 2014.

[7] Stjepan Picek, Kostas Papagiannopoulos, Barış Ege, Lejla Batina, and Domagoj Jakobovic. Confused by confusion: Systematic evaluation of dpa resistance of various s-boxes. In *International Conference in Cryptology in India*, pages 374–390. Springer, 2014.

[8] Ricardo Sánchez. Generación de s-cajas equivalentes según su resistencia a los ataques por análisis diferencial de potencia. Tesis de diploma, Facultad de Ingeniería Informática, Universidad Tecnológica de la Habana, 2016.

[9] Dania Tamayo. Algoritmos heurísticos híbridos para el diseño de s-cajas. Master's thesis, Facultad de Matemática y Computación, Universidad de la Habana, 2017.

[10] Henk CA Van Tilborg and Sushil Jajodia. *Encyclopedia of cryptography and security*. Springer Science & Business Media, 2014.