Una nueva construcción de funciones bent de $2k$ variables a partir de una base de $\mathbb{F}_2^{2k}$

Joan-Josep Climent
Departament d'Estadística i Investigació Operativa. Universitat d'Alacant
Email: jcliment@ua.es

Francisco J. García
Departament de Mètodes Quantitatius i Teoria Econòmica. Universitat d'Alacant
Email: francisco.garcia@ua.es

Verónica Requena
Departament d'Estadística i Investigació Operativa. Universitat d'Alacant
Email: vrequena@ua.es

***Resumen*—Sea k un entero positivo. A partir de una base del espacio vectorial $\mathbb{F}_2^{2k}$ construimos, de forma iterativa, unos subconjuntos de $\mathbb{F}_2^{2k}$ que resultan ser los soportes de funciones bent de $2k$ variables. Proporcionamos también el número de funciones bent que podemos obtener con esta técnica y vemos que podemos obtener todas las funciones bent de 4 variables.**

***Palabras clave*—Función boolena, función bent, soporte, criptografía, base.**

I. Introducción

Las funciones booleanas se utilizan en distintas aplicaciones criptográficas tales como cifrado en bloque, cifrado en flujo y funciones hash [1], [4], [14], [16]. Para un número par n de variables, las funciones booleanas de máxima no linealidad son las llamadas funciones *bent* [7], [22], [24]. El nombre *bent* para dichas funciones se debe a Rothaus [21], aunque su origen se remonta a un artículo de McFarland [15] sobre conjuntos de diferencias en grupos no cíclicos. Existen diferentes métodos para obtener funciones bent, la mayoría de ellos están basados en la forma normal algeraica de una función booleana (véase, por ejemplo, [3], [5], [6], [11], [12], [13], [15], [17], [21], [24], [26]). Sin embargo, hay muy pocas construcciones de funciones bent basadas en el soporte (o equivalentemente, en la tabla de verdad) de funciones booleanas (por ejemplo, la clase de funciones bent conocida como *partial spread* introducida por Dillon [11]). Una construcción explícita de este tipo de funciones bent puede verse en [9].

Tanto el uso de la forma normal algebraica como la tabla de verdad tienen ventajas y desventajas. Por ejemplo, la forma normal algebraica de una función booleana $f(\boldsymbol{x})$ de n variables proporciona directamente su grado y, si éste es mayor que $n/2$, podemos afirmar que $f(\boldsymbol{x})$ no es una función bent (véase [21]); sin embargo, no conocemos el número de elementos de su soporte (es decir, su peso). Por otro lado, si conocemos la tabla de verdad de $f(\boldsymbol{x})$, entonces sabemos si su poporte tiene el número de elementos para ser una función bent o no, aunque no conocemos su grado. Para ver la relación entre la forma normal algebraica de una función booleana y su soporte, véase, por ejemplo [8].

El resto del artículo está organizado como sigue. Primero, en la sección II introducimos algunas definiciones básicas y la notación que utilizaremos en lo sucesivo. En la sección III, partiendo de una base de $\mathbb{F}_2^{2k}$ introducimos unos subconjuntos de $\mathbb{F}_2^{2k}$ que son los soportes de funciones bent de $2k$ variables e introducimos algunos resultados que nos permitirán contar el número de funciones bent que podemos obtener mediante dichos conjuntos. En la sección IV ampliamos la construcción de la sección III y finalmente, en la sección V, presentamos algunas conclusiones y algunos problemas abiertos.

II. Preliminares

Sea $\mathbb{F}_2$ el cuerpo binario con la adición denotada por $\oplus$ y la multiplicación denotada por yuxtaposición. Para cualquier entero positivo n, es bien conocido que $\mathbb{F}_2^n$ es un espacio vectorial sobre $\mathbb{F}_2$ con la adición usual (denotada también por $\oplus$). Si para $i = 0, 1, 2, \ldots, 2^n - 1$, denotamos por $\boldsymbol{i}$ la expansión binaria de i de n dígitos, entonces $\mathbb{F}_2^n = \{\boldsymbol{i} \mid 0 \leq i \leq 2^n - 1\}$. Además, denotamos por $\mathrm{Env}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_l\}$ el subespacio vectorial de $\mathbb{F}_2^n$ generado por los vectores $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_l \in \mathbb{F}_2^n$. Decimos que el conjunto $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_l\}$ es una **base de Gauss-Jordan de cardinalidad** l si la matriz cuyas filas son los vectores $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_l$ está en forma escalonada reducida (véase también [2], [10]). Además, si $S \subseteq \mathbb{F}_2^n$ y $\boldsymbol{a} \oplus S = \{\boldsymbol{a} \oplus \boldsymbol{u} \mid \boldsymbol{u} \in S\}$ para $\boldsymbol{a} \in \mathbb{F}_2^n$, entonces es evidente que $\left|\boldsymbol{a} \oplus S\right| = \left|S\right|$, donde $\left|S\right|$ denota el número de elementos de S. Utilizaremos esta propiedad sin mencionarla explícitamente.

Una **función booleana** de n variables es una aplicación $f : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2$. El conjunto de todas las funciones booleanas de n variables se denota por $\mathcal{B}_n$ y es un espacio vectorial con la adición (denotada también por $\oplus$) de dimensión 2^n sobre $\mathbb{F}_2$. La función complementaria de $f \in \mathcal{B}_n$ es la función booleana $1 \oplus f$.

Si $f \in \mathcal{B}_n$, llamamos **tabla de verdad** de f (véase, por ejemplo, [18], [19]), a la secuencia binaria de longitud 2^n dada por

$$\boldsymbol{\xi} = (f(\mathbf{0}), f(\mathbf{1}), \ldots, f(\mathbf{2^n - 1})).$$

Llamamos **soporte** de f, y escribimos $\mathrm{Sop}\,(f)$, al conjunto de vectores de $\mathbb{F}_2^n$ cuya imagen por f es 1, es decir,

$$\mathrm{Sop}\,(f) = \{\boldsymbol{a} \in \mathbb{F}_2^n \mid f(\boldsymbol{a}) = 1\}.$$

Además, llamamos **peso** de f, y lo denotamos por $w(f)$, al número de 1 de la tabla de verdad de f y, por tanto, $w(f) = \left|\,\mathrm{Sop}\,(f)\,\right|$.

Si $f, g \in \mathcal{B}_n$, es fácil comprobar que $\mathrm{Sop}\,(f \oplus g) = \mathrm{Sop}\,(f)\,\Delta\,\mathrm{Sop}\,(g)$, donde Δ denota la diferencia simétrica de

conjuntos. En consecuencia, $\mathrm{Sop}\,(1 \oplus f) = \mathbb{F}_2^n \setminus \mathrm{Sop}\,(f)$ y, por tanto, $w(1 \oplus f) = 2^n - w(f)$.

Además, si $f \in \mathcal{B}_n$ y $\boldsymbol{a} \in \mathbb{F}_2^n$, entonces $\mathrm{Sop}\,(g_{\boldsymbol{a}}) = \boldsymbol{a} \oplus \mathrm{Sop}\,(f)$, donde $g_{\boldsymbol{a}} \in \mathcal{B}_n$ es la función booleana de n variables dada por $g_{\boldsymbol{a}}(\boldsymbol{x}) = f(\boldsymbol{a} \oplus \boldsymbol{x})$ para todo $\boldsymbol{x} \in \mathbb{F}_2^n$.

Decimos que $f \in \mathcal{B}_n$ es **equilibrada** si $w(f) = 2^{n-1}$. Es evidente que f es equilibrada si y sólo si $1 \oplus f$ es equilibrada.

Decimos que $f \in \mathcal{B}_n$ es una **función afín** si

$$f(\boldsymbol{x}) = \langle \boldsymbol{a}, \boldsymbol{x} \rangle \oplus b,$$

donde $\boldsymbol{a} \in \mathbb{F}_2^n$, $b \in \mathbb{F}_2$ y $\langle \boldsymbol{a}, \boldsymbol{x} \rangle$ es el producto escalar usual de los vectores $\boldsymbol{a}$ y $\boldsymbol{x}$. Si $b = 0$, decimos que f es una **función lineal**. Las funciones afines son equilibradas, pero no todas las funciones equilibradas son afines.

Definimos la **no linealidad** de una función $f \in \mathcal{B}_n$ como

$$\mathrm{NL}(f) = \min\{d(f, \varphi) \mid \varphi \in \mathcal{A}_n\}$$

donde $\mathcal{A}_n$ es el conjunto de todas las funciones afines y $d(f, \varphi) = w(f \oplus \varphi)$ es la distancia entre f y φ. La no linealidad de f está acotada superiormente (véase [16], [24]) por

$$\mathrm{NL}(f) \leq 2^{n-1} - 2^{\frac{n}{2}-1}.$$

Llamamos **funciones bent** a las funciones booleanas que alcanzan la máxima no linealidad (véase [16], [24]). Por tanto, las funciones bent solamente existen para n par.

El resultado siguiente proporciona una caracterización de las funciones bent.

Teorema 1 ([23], [24]): *Sea $f(\boldsymbol{x})$ una función booleana de n variables con n par. Son equivalentes:*

(a) *$f(\boldsymbol{x})$ es una función bent.*
(b) *La función booleana $f(\boldsymbol{x}) \oplus f(\boldsymbol{a} \oplus \boldsymbol{x})$ es equilibrada para todo $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$.*
(c) *El número de 1 en la tabla de verdad de la función booleana $f(\boldsymbol{x}) \oplus \langle \boldsymbol{a}, \boldsymbol{x} \rangle$ es $2^{n-1} \pm 2^{\frac{n}{2}-1}$ para todo $\boldsymbol{a} \in \mathbb{F}_2^n$.*

Ahora, como consecuencia del resultado anterior, tenemos la siguiente caracterización del soporte de una función bent.

Corolario 1: *Supongamos que $S \subseteq \mathbb{F}_2^n$ con n par. Entonces S es el soporte de una función bent de n variables si y sólo si $S\,\Delta(\boldsymbol{a} \oplus S)$ es el soporte de una función equilibrada de n variables para todo $\boldsymbol{a} \in \mathbb{F}_2^n \setminus \{\boldsymbol{0}\}$.*

Otra consecuencia del teorema 1 es que si $f \in \mathcal{B}_n$ es una función bent, entonces $w(f) = 2^{n-1} \pm 2^{\frac{n}{2}-1}$. Además, $1 \oplus f \in \mathcal{B}_n$ es una función bent y $w(1 \oplus f) = 2^{n-1} \mp 2^{\frac{n}{2}-1}$.

III. Resultados principales

En esta sección introducimos un proceso iterativo que nos permitirá obtener los soportes de algunas funciones bent de n variables a partir de una base de $\mathbb{F}_2^n$. A partir de ahora, suponemos que $n = 2k$ y que $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ es una base de $\mathbb{F}_2^n$. Para $i = 1, 2, \ldots, k$, consideramos los subespacios vectoriales

$$G_i = \mathrm{Env}\,\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\},$$

$$H_i = \mathrm{Env}\,\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\},$$

de $\mathbb{F}_2^n$. Claramente, $\dim G_i = 2i$ y $\dim H_i = 2$. Además, si suponemos que $G_0 = \{\boldsymbol{0}\}$, entonces

$$G_i = G_{i-1} \oplus H_i \quad \text{y} \quad G_{i-1} \cap H_i = \{\boldsymbol{0}\},$$

con lo que G_i es la suma directa de G_{i-1} y H_i. En particular, $G_1 = H_1$.

Por conveniencia en la notación, nos referiremos a los elementos de H_i, para $i = 1, 2, \ldots, k$, como

$$\boldsymbol{a}_0^{(i)} = \boldsymbol{0},\ \boldsymbol{a}_1^{(i)} = \boldsymbol{u}_{2i-1},\ \boldsymbol{a}_2^{(i)} = \boldsymbol{u}_{2i} \text{ y } \boldsymbol{a}_3^{(i)} = \boldsymbol{u}_{2i-1} \oplus \boldsymbol{u}_{2i}.$$

Utilizando los conjuntos G_{i-1} y los elementos de H_i, para $i = 1, 2, \ldots, k$, definimos unos subconjuntos de G_i con ciertas propiedades de manera que, al final del proceso, los subconjuntos de G_k son los soportes de funciones bent de $2k$ variables.

Para $p \in \{0, 1, 2, 3\}$ consideremos los conjuntos

$$B(p) = \left\{\boldsymbol{a}_p^{(1)}\right\} \quad \text{y} \quad \widehat{B}(p) = \bigcup_{\substack{q=0 \\ q \neq p}}^{3} \left\{\boldsymbol{a}_q^{(1)}\right\}.$$

Es evidente que

$$G_1 = B(p) \cup \widehat{B}(p) \quad \text{y} \quad B(p) \cap \widehat{B}(p) = \emptyset.$$

Además, si $r, s \in \{0, 1, 2, 3\}$ con $r \neq s$, entonces $B(r) \neq B(s)$.

Ahora, sea $(p_1, p_2, \ldots, p_{i-1}, p_i) \in \{0, 1, 2, 3\}^i$ y supongamos que hemos definido los conjuntos $B(p_1, p_2, \ldots, p_{i-1})$ y $\widehat{B}(p_1, p_2, \ldots, p_{i-1})$. Entonces, definimos

$$B(p_1, p_2, \ldots, p_{i-1}, p_i) = \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right), \tag{1}$$

$$\widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i) = \left(\boldsymbol{a}_{p_i}^{(i)} \oplus B(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{B}(p_1, p_2, \ldots, p_{i-1})\right). \tag{2}$$

Nuestro objetivo es probar que para todo $(p_1, p_2, \ldots, p_k) \in \{0, 1, 2, 3\}^k$, los conjuntos

$$B(p_1, p_2, \ldots, p_k) \quad \text{y} \quad \widehat{B}(p_1, p_2, \ldots, p_k)$$

son los soportes de dos funciones bent de $2k$ variables, de manera que una es la función complementaria de la otra. Los lemas siguientes, cuya demostración se puede hacer por inducción, permiten simplificar el resultado antes mencionado.

Lema 1: *Si $i \in \{1, 2, \ldots, k\}$ y $(p_1, p_2, \ldots, p_i) \in \{0, 1, 2, 3\}^i$, entonces:*

(a) $G_i = B(p_1, p_2, \ldots, p_i) \cup \widehat{B}(p_1, p_2, \ldots, p_i)$,
(b) $B(p_1, p_2, \ldots, p_i) \cap \widehat{B}(p_1, p_2, \ldots, p_i) = \emptyset$.
(c) $\left|B(p_1, p_2, \ldots, p_i)\right| = 2^{2i-1} - 2^{i-1}$,
(d) $\left|\widehat{B}(p_1, p_2, \ldots, p_i)\right| = 2^{2i-1} + 2^{i-1}$.

Lema 2: *Si* $i \in \{1,2,\ldots,k\}$, $(p_1,p_2,\ldots,p_i) \in \{0,1,2,3\}^i$ *y* $\boldsymbol{u} \in G_i \setminus \{\mathbf{0}\}$, *entonces:*

(a) $\left|B(p_1,\ldots,p_i) \cap \left(\boldsymbol{u} \oplus B(p_1,\ldots,p_i)\right)\right| = 2^{2i-2} - 2^{i-1}$,
(b) $\left|\widehat{B}(p_1,\ldots,p_i) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p_1,\ldots,p_i)\right)\right| = 2^{2i-2} + 2^{i-1}$,
(c) $\left|B(p_1,p_2,\ldots,p_i) \cap \left(\boldsymbol{u} \oplus \widehat{B}(p_1,p_2,\ldots,p_i)\right)\right| = 2^{2i-2}$,
(d) $\left|\widehat{B}(p_1,p_2,\ldots,p_i) \cap \left(\boldsymbol{u} \oplus B(p_1,p_2,\ldots,p_i)\right)\right| = 2^{2i-2}$.

Estos resultados permiten probar que los conjuntos $B(p_1,p_2,\ldots,p_k)$ y $\widehat{B}(p_1,p_2,\ldots,p_k)$ son los soportes de una función bent de $2k$ variables y su complementaria, respectivamente.

Teorema 2: *Si* $(p_1,p_2,\ldots,p_k) \in \{0,1,2,3\}^k$, *los conjuntos*

$$B(p_1,p_2,\ldots,p_k) \quad y \quad \widehat{B}(p_1,p_2,\ldots,p_k)$$

son los soportes de dos funciones bent de $2k$ *variables de manera que una es la función complementaria de la otra.*

Demostración: Supongamos que $\boldsymbol{u} \in \mathbb{F}_2^{2k} \setminus \{\mathbf{0}\}$. Puesto que $\mathbb{F}_2^{2k} = G_k$, por los lemas 1 y 2 tenemos que

$$\begin{aligned}
&\left|B(p_1,p_2,\ldots,p_k)\,\Delta\,(\boldsymbol{u} \oplus B(p_1,p_2,\ldots,p_k))\,\right| \\
&\quad = \left|B(p_1,p_2,\ldots,p_k)\right| + \left|\boldsymbol{u} \oplus B(p_1,p_2,\ldots,p_k)\right| \\
&\qquad - 2\left|B(p_1,p_2,\ldots,p_k) \cap (\boldsymbol{u} \oplus B(p_1,p_2,\ldots,p_k))\,\right| \\
&\quad = 2^{2k-1} - 2^{k-1} + 2^{2k-1} - 2^{k-1} - 2\left(2^{2k-2} - 2^{k-1}\right) \\
&\quad = 2^{2k-1},
\end{aligned}$$

con lo que el conjunto

$$B(p_1,p_2,\ldots,p_k)\,\Delta(\boldsymbol{u} \oplus B(p_1,p_2,\ldots,p_k))$$

es el soporte de una función equilibrada de $2k$ variables. Ahora, por el corolario 1, concluimos que $B(p_1,p_2,\ldots,p_k)$ es el soporte de una función bent $f(\boldsymbol{x})$ de $2k$ variables y, por el lema 1, tenemos que $\widehat{B}(p_1,p_2,\ldots,p_k)$ es el soporte de la función complementaria $1 \oplus f(\boldsymbol{x})$. ■

Para contar el número de funciones bent proporcionadas por el teorema 2 necesitamos el resultado siguiente, cuya demostración se sigue fácilmente por inducción.

Teorema 3: *Supongamos que* $i \in \{1,2,\ldots,k\}$ *y consideremos* $(p_1,p_2,\ldots,p_i),(q_1,q_2,\ldots,q_i) \in \{0,1,2,3\}^i$. *Si existe* $l \in \{1,2,\ldots,i-1\}$ *tal que* $p_1 = q_1$, $p_2 = q_2$, …, $p_l = q_l$, *pero* $p_{l+1} \neq q_{l+1}$, *entonces*

$$\begin{aligned}
&B(p_1,p_2,\ldots,p_l,p_{l+1},p_{l+2},\ldots p_{l+m}) \\
&\qquad \neq B(p_1,p_2,\ldots,p_l,q_{l+1},q_{l+2},\ldots q_{l+m}), \\
&\widehat{B}(p_1,p_2,\ldots,p_l,p_{l+1},p_{l+2},\ldots p_{l+m}) \\
&\qquad \neq \widehat{B}(p_1,p_2,\ldots,p_l,q_{l+1},q_{l+2},\ldots q_{l+m})
\end{aligned}$$

para $m = 1,2,\ldots,i-l$.

Así, como consecuencia de este resultado obtenemos el número de soportes de funciones bent que podemos construir.

Corolario 2: *Para una base de* $\mathbb{F}_2^{2k}$, *el número de funciones bent de* $2k$ *variables que podemos construir de acuerdo con el proceso descrito anteriormente es* 2^{2k+1}.

(p_1,p_2)	$B(p_1,p_2)$	$\widehat{B}(p_1,p_2)$
$(0,0)$	$\mathbf{1,2,3,4,8,12}$	$\mathbf{0,5,6,7,9,10,11,13,14,15}$
$(0,1)$	$\mathbf{0,5,6,7,8,12}$	$\mathbf{1,2,3,4,9,10,11,13,14,15}$
$(0,2)$	$\mathbf{0,4,9,10,11,12}$	$\mathbf{1,2,3,5,6,7,8,13,14,15}$
$(0,3)$	$\mathbf{0,4,8,13,14,15}$	$\mathbf{1,2,3,5,6,7,9,10,11,12}$
$(1,0)$	$\mathbf{0,2,3,5,9,13}$	$\mathbf{1,4,6,7,8,10,11,12,14,15}$
$(1,1)$	$\mathbf{1,4,6,7,9,13}$	$\mathbf{0,2,3,5,8,10,11,12,14,15}$
$(1,2)$	$\mathbf{1,5,8,10,11,13}$	$\mathbf{0,2,3,4,6,7,9,12,14,15}$
$(1,3)$	$\mathbf{1,5,9,12,14,15}$	$\mathbf{0,2,3,4,6,7,8,10,11,13}$
$(2,0)$	$\mathbf{0,1,3,6,10,14}$	$\mathbf{2,4,5,7,8,9,11,12,13,15}$
$(2,1)$	$\mathbf{2,4,5,7,10,14}$	$\mathbf{0,1,3,6,8,9,11,12,13,15}$
$(2,2)$	$\mathbf{2,6,8,9,11,14}$	$\mathbf{0,1,3,4,5,7,10,12,13,15}$
$(2,3)$	$\mathbf{2,6,10,12,13,15}$	$\mathbf{0,1,3,4,5,7,8,9,11,14}$
$(3,0)$	$\mathbf{0,1,2,7,11,15}$	$\mathbf{3,4,5,6,8,9,10,12,13,14}$
$(3,1)$	$\mathbf{3,4,5,6,11,15}$	$\mathbf{0,1,2,7,8,9,10,12,13,14}$
$(3,2)$	$\mathbf{3,7,8,9,10,15}$	$\mathbf{0,1,2,4,5,6,11,12,13,14}$
$(3,3)$	$\mathbf{3,7,11,12,13,14}$	$\mathbf{0,1,2,4,5,6,8,9,10,15}$

TABLA I
SOPORTES DE LAS FUNCIONES BENT CONSTRUIDAS CON LA BASE $\mathcal{U}$ DEL EJEMPLO 1

Surge ahora, de modo natural, la siguiente pregunta: ¿si $\mathcal{U}$ y $\mathcal{V}$ son dos bases distintas de $\mathbb{F}_2^{2k}$, las 2^{2k+1} funciones bent obtenidas a partir de la base $\mathcal{U}$ son distintas de las 2^{2k+1} funciones bent obtenidas a partir de la base $\mathcal{V}$? Puesto que el número de bases distintas de $\mathbb{F}_2^{2k}$ (véase [25, página 46]) es $\prod_{i=0}^{2k-1}(2^{2k} - 2^i)$, podemos construir

$$2^{2k+1} \prod_{i=0}^{2k-1} (2^{2k} - 2^i)$$

funciones bent de $2k$ variables. Así, para $k = 2$, podemos construir $645\,120$ funciones bent. Sin embargo, es bien conocido que solamente hay 896 funciones bent distintas de 4 variables. Por tanto, deben haber bases distintas que proporcionan las mismas funciones bent, tal como vemos en el ejemplo siguiente.

Ejemplo 1: Supongamos que $k = 2$ y consideremos las bases $\mathcal{U} = \{\mathbf{1},\mathbf{2},\mathbf{4},\mathbf{8}\}$ y $\mathcal{V} = \{\mathbf{6},\mathbf{7},\mathbf{9},\mathbf{13}\}$ de $\mathbb{F}_2^4$. Las tablas I y II recogen los soportes de las funciones bent que podemos construir con dichas bases utilizando el procedimiento descrito en esta sección. Como podemos ver, obtenemos las mismas funciones bent en ambos casos, aunque para diferentes valores de $(p_1,p_2) \in \{0,1,2,3\}^2$. □

Si necesitamos poner de manifiesto que hemos utilizado la base $\mathcal{U} = \{\boldsymbol{u}_1,\boldsymbol{u}_2,\ldots,\boldsymbol{u}_{2k-1},\boldsymbol{u}_{2k}\}$ en la construcción de los conjuntos de las expresiones (1) y (2), escribimos

$$B_{\mathcal{U}}(p_1,p_2,\ldots,p_k) \quad y \quad \widehat{B}_{\mathcal{U}}(p_1,p_2,\ldots,p_k).$$

Además, si nos fijamos detenidamente en las expresiones (1) y (2) vemos que los conjuntos anteriores dependen de los subespacios vectoriales $H_i = \mathrm{Env}\,\{\boldsymbol{u}_{2i-1},\boldsymbol{u}_{2i}\}$, para $i = 1,2,\ldots,k$, más que de la base $\{\boldsymbol{u}_{2i-1},\boldsymbol{u}_{2i}\}$ considerada. Por tanto, podemos establecer el siguiente resultado.

Lema 3: *Supongamos que* $\mathcal{U} = \{\boldsymbol{u}_1,\boldsymbol{u}_2,\ldots,\boldsymbol{u}_{2k-1},\boldsymbol{u}_{2k}\}$ *y* $\mathcal{V} = \{\boldsymbol{v}_1,\boldsymbol{v}_2,\ldots,\boldsymbol{v}_{2k-1},\boldsymbol{v}_{2k}\}$ *son dos bases de* $\mathbb{F}_2^{2k}$. *Si existe* $r \in \{1,2,\ldots,k\}$ *tal que*

- $(\boldsymbol{v}_{2i-1},\boldsymbol{v}_{2i}) = (\boldsymbol{u}_{2i-1},\boldsymbol{u}_{2i})$ *para* $i \in \{1,2,\ldots,k\} \setminus \{r\}$,

(p_1, p_2)	$B(p_1, p_2)$	$\widehat{B}(p_1, p_2)$
$(0,0)$	$\mathbf{3,7,11,12,13,14}$	$\mathbf{0,1,2,4,5,6,8,9,10,15}$
$(0,1)$	$\mathbf{0,1,2,7,11,15}$	$\mathbf{3,4,5,6,8,9,10,12,13,14}$
$(0,2)$	$\mathbf{0,4,9,10,11,12}$	$\mathbf{1,2,3,5,6,7,8,13,14,15}$
$(0,3)$	$\mathbf{0,5,6,7,8,12}$	$\mathbf{1,2,3,4,9,10,11,13,14,15}$
$(1,0)$	$\mathbf{0,4,8,13,14,15}$	$\mathbf{1,2,3,5,6,7,9,10,11,12}$
$(1,1)$	$\mathbf{1,2,3,4,8,12}$	$\mathbf{0,5,6,7,9,10,11,13,14,15}$
$(1,2)$	$\mathbf{3,7,8,9,10,15}$	$\mathbf{0,1,2,4,5,6,11,12,13,14}$
$(1,3)$	$\mathbf{3,4,5,6,11,15}$	$\mathbf{0,1,2,7,8,9,10,12,13,14}$
$(2,0)$	$\mathbf{0,1,3,6,10,14}$	$\mathbf{2,4,5,7,8,9,11,12,13,15}$
$(2,1)$	$\mathbf{2,6,10,12,13,15}$	$\mathbf{0,1,3,4,5,7,8,9,11,14}$
$(2,2)$	$\mathbf{1,4,6,7,9,13}$	$\mathbf{0,2,3,5,8,10,11,12,14,15}$
$(2,3)$	$\mathbf{1,5,8,10,11,13}$	$\mathbf{0,2,3,4,6,7,9,12,14,15}$
$(3,0)$	$\mathbf{0,2,3,5,9,13}$	$\mathbf{1,4,6,7,8,10,11,12,14,15}$
$(3,1)$	$\mathbf{1,5,9,12,14,15}$	$\mathbf{0,2,3,4,6,7,8,10,11,13}$
$(3,2)$	$\mathbf{2,4,5,7,10,14}$	$\mathbf{0,1,3,6,8,9,11,12,13,15}$
$(3,3)$	$\mathbf{2,6,8,9,11,14}$	$\mathbf{0,1,3,4,5,7,10,12,13,15}$

TABLA II
SOPORTES DE LAS FUNCIONES BENT CONSTRUIDAS CON LA BASE $\mathcal{V}$ DEL EJEMPLO 1

- $\operatorname{Env}\{\boldsymbol{v}_{2r-1}, \boldsymbol{v}_{2r}\} = \operatorname{Env}\{\boldsymbol{u}_{2r-1}, \boldsymbol{u}_{2r}\}$,

entonces

(a) $B_{\mathcal{U}}(p_1, p_2, \ldots, p_k) = B_{\mathcal{V}}(p_1, p_2, \ldots, p_k)$,
(b) $\widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_k) = \widehat{B}_{\mathcal{V}}(p_1, p_2, \ldots, p_k)$.

para todo $(p_1, p_2, \ldots, p_k) \in \{0,1,2,3\}^k$.

Además, el orden en el que cada par de vectores aparece en la base no es importante, como establecemos en el resultado siguiente.

Lema 4: *Supongamos que* $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ *y* $\mathcal{V} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{2k-1}, \boldsymbol{v}_{2k}\}$ *son dos bases de* $\mathbb{F}_2^{2k}$. *Si existen* $r, s \in \{1, 2, \ldots, k\}$ *(con* $r < s$*) tales que*

- $(\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}) = (\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i})$, *para* $i \neq r, s$,
- $(\boldsymbol{v}_{2r-1}, \boldsymbol{v}_{2r}) = (\boldsymbol{u}_{2s-1}, \boldsymbol{u}_{2s})$,
- $(\boldsymbol{v}_{2s-1}, \boldsymbol{v}_{2s}) = (\boldsymbol{u}_{2r-1}, \boldsymbol{u}_{2r})$,

entonces

$$\begin{aligned} &B_{\mathcal{U}}(p_1, p_2, \ldots, p_r, \ldots, p_s, \ldots, p_k) \\ &\qquad = B_{\mathcal{V}}(p_1, p_2, \ldots, p_s, \ldots, p_r, \ldots, p_k), \\ &\widehat{B}_{\mathcal{U}}(p_1, p_2, \ldots, p_r, \ldots, p_s, \ldots, p_k) \\ &\qquad = \widehat{B}_{\mathcal{V}}(p_1, p_2, \ldots, p_s, \ldots, p_r, \ldots, p_k), \end{aligned}$$

para todo $(p_1, p_2, \ldots, p_k) \in \{0,1,2,3\}^k$.

Ahora, como consecuencia de los lemas 3 y 4 tenemos el resultado siguiente.

Teorema 4: *Supongamos que* $\mathcal{U} = \{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ *y* $\mathcal{V} = \{\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots, \boldsymbol{v}_{2k-1}, \boldsymbol{v}_{2k}\}$ *son bases de* $\mathbb{F}_2^{2k}$ *tales que* $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$ *y* $\{\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}\}$ *son bases de Gauss-Jordan de cardinalidad* 2. *Si* σ *es una permutación de* $\{1, 2, \ldots, k\}$ *tal que*

$$(\boldsymbol{v}_{2i-1}, \boldsymbol{v}_{2i}) = (\boldsymbol{u}_{2\sigma(i)-1}, \boldsymbol{u}_{2\sigma(i)}) \quad \textit{para} \quad i = 1, 2, \ldots, k,$$

entonces $\mathcal{U}$ *y* $\mathcal{V}$ *proporcionan los soportes de las mismas funciones bent de* $2k$ *variables.*

Por tanto, a partir de ahora, además de suponer que $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$ es una base de Gauss-Jordan de cardinalidad 2, supondremos también que $\boldsymbol{u}_{2i-1} > \boldsymbol{u}_{2j-1}$ (en orden lexicográfico) si $i < j$. Puesto que cada subespacio de dimensión 2 tiene 6 bases diferentes, pero solamente una de ellas es una base de Gauss-Jordan de cardinalidad 2, tenemos que el número de bases de $\mathbb{F}_2^{2k}$ que satisfacen dichas condiciones es

$$\frac{\prod_{i=0}^{2k-1}(2^{2k} - 2^i)}{6^k \cdot k!}.$$

En particular, para $k = 2$ tenemos 280 bases que satisfacen dichas condiciones. En consecuencia, de acuerdo con el corolario 2, podemos construir $2^5 \cdot 280 = 8960$ funciones bent de 4 variables. Recordemos que el número de funciones bent distintas de 4 variables es 896 (448 con peso 6 y otras 448 con peso 10). Una búsqueda exhaustiva por ordenador permite obtener las 896 funciones bent a partir de las siguientes 28 bases de $\mathbb{F}_2^4$:

$$\begin{array}{llll} \{\mathbf{8,7;5,3}\}, & \{\mathbf{8,7;4,2}\}, & \{\mathbf{8,7;4,1}\}, & \{\mathbf{8,7;2,1}\}, \\ \{\mathbf{8,6;5,2}\}, & \{\mathbf{8,6;4,3}\}, & \{\mathbf{8,6;4,1}\}, & \{\mathbf{8,6;2,1}\}, \\ \{\mathbf{8,5;6,1}\}, & \{\mathbf{8,5;4,3}\}, & \{\mathbf{8,5;4,2}\}, & \{\mathbf{8,5;2,1}\}, \\ \{\mathbf{8,4;6,1}\}, & \{\mathbf{8,4;5,3}\}, & \{\mathbf{8,4;5,2}\}, & \{\mathbf{8,4;2,1}\}, \\ \{\mathbf{8,3;6,1}\}, & \{\mathbf{8,3;5,2}\}, & \{\mathbf{8,3;4,2}\}, & \{\mathbf{8,3;4,1}\}, \\ \{\mathbf{8,2;6,1}\}, & \{\mathbf{8,2;5,3}\}, & \{\mathbf{8,2;4,3}\}, & \{\mathbf{8,2;4,1}\}, \\ \{\mathbf{8,1;5,3}\}, & \{\mathbf{8,1;5,2}\}, & \{\mathbf{8,1;4,3}\}, & \{\mathbf{8,1;4,2}\}. \end{array}$$

Por tanto, nuestra construcción permite obtener todas las funciones bent de 4 variables, cosa que no ocurre con otras construcciones.

Para $k = 3$ no es posible obtener una clasificación completa similar a la clasificación anterior, ya que el número de bases que satisfacen las condiciones requeridas es, en este caso, 15 554 560. Por otro lado, en el supuesto de que las funciones bent obtenidas a partir de cada una de dichas bases fueran distintas (cosa bastante improbable visto lo que ocurre para 4 variables), tendríamos $2^{2\cdot 3+1} \cdot 15\,554\,560 = 1\,990\,983\,680$ funciones bent de 6 variables, pero como el número de funciones bent distintas de 6 variables es 5 425 430 528 (véase, [6], [20]), podemos afirmar que nuestra construcción no permite obtener todas las funciones bent de 6 variables y, por tanto, tampoco las funciones bent con más de 8 variables. En la sección IV veremos cómo mejorar el proceso descrito en esta sección.

k	Segundos	Número de soportes
2	0.0276	2^5
3	0.2923	2^7
4	4.7412	2^9
5	74.5827	2^{11}
6	1215.0815	2^{13}
7	21347.9378	2^{15}

TABLA III
PARA UNA BASE DADA, TIEMPO NECESARIO (EN SEGUNDOS) PARA OBTENER TODOS LOS SOPORTES DE FUNCIONES BENT DE $2k$ VARIABLES PARA DIFERENTES VALORES DE k

Finalmente, en la tabla III, vemos el tiempo (en segundos) necesario para obtener, en un ordenador personal, los 2^{2k+1}

soportes de funciones bent de $2k$ variables a partir de la misma base de $\mathbb{F}_2^n$. Es importante mencionar que el tiempo medio necesario para obtener de forma aleatoria los soportes de 100 funciones bent de 4 variables (es decir, para $k = 2$) fue de 6.56 segundos; sin embargo, después de más de 250 horas de cálculo, no obtuvimos (de forma aleatoria), ningún soporte correspondiente a una función bent de 6 variables (es decir, para $k = 3$).

IV. Más resultados

En toda esta sección suponemos que k y l son dos enteros fijos tales que $3 \leq l < k$. Sea B_{2l} el conjunto de todas las funciones bent de $2l$ variables y denotemos por $\mathsf{B}_{2l}^{(1)}$ el conjunto de todas las funciones bent de $2l$ variables que podemos obtener mediante la construcción introducida en la sección III. Claramente $\mathsf{B}_{2l}^{(1)} \subseteq \mathsf{B}_{2l}$ y, de acuerdo con lo dicho al final de dicha sección, la inclusión anterior es estricta, con lo que $\mathsf{B}_{2l}^{(2)} = \mathsf{B}_{2l} \backslash \mathsf{B}_{2l}^{(1)} \neq \emptyset$ es el conjunto de todas las funciones bent que no podemos obtener mediante dicha construcción. Sea $f \in \mathsf{B}_{2l}^{(2)}$ tal que $w(f) = 2^{2l-1} - 2^{l-1}$ y denotemos por A y $\widehat{A}$ los soportes de f y $1 \oplus f$ respectivamente.

Por otro lado, si identificamos el vector $\boldsymbol{v} \in \mathbb{F}_2^{2l}$ con el vector $(\mathbf{0}_{2(k-l)}, \boldsymbol{v}) \in \mathbb{F}_2^{2k}$, podemos suponer que $G_l = \mathbb{F}_2^{2l}$ es un subespacio vectorial de dimensión $2l$ de $\mathbb{F}_2^{2k}$. De esta forma, los subconjuntos A y $\widehat{A}$ de G_l satisfacen las propiedades:

- $G_l = A \cup \widehat{A}$ y $A \cap \widehat{A} = \emptyset$,
- $\left|A\right| = 2^{2l-1} - 2^{l-1}$ y $\left|\widehat{A}\right| = 2^{2l-1} + 2^{l-1}$.

Sea $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2l-1}, \boldsymbol{u}_{2l}\}$ una base de G_l y consideremos $\boldsymbol{u}_{2l+1}, \boldsymbol{u}_{2l+2}, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k} \in \mathbb{F}_2^{2k}$ de manera que:

- $\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2l-1}, \boldsymbol{u}_{2l}, \boldsymbol{u}_{2l+1}, \boldsymbol{u}_{2l+2}, \ldots, \boldsymbol{u}_{2k-1}, \boldsymbol{u}_{2k}\}$ es una base de $\mathbb{F}_2^{2k}$,
- $\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\}$, para $i = l+1, l+2, \ldots, k$, es una base de Gauss-Jordan de cardinalidad 2,
- $\boldsymbol{u}_{2i-1} > \boldsymbol{u}_{2j-1}$ (en orden lexicográfico), si $l + 1 \leq i < j \leq k$.

Para $i = l + 1, l + 2, \ldots, k$, consideramos los subespacios vectoriales

$$G_i = \operatorname{Env}\{\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_{2l-1}, \boldsymbol{u}_{2l}, \ldots, \boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\},$$
$$H_i = \operatorname{Env}\{\boldsymbol{u}_{2i-1}, \boldsymbol{u}_{2i}\},$$

de $\mathbb{F}_2^{2k}$. Claramente, $\dim G_i = 2i$ y $\dim H_i = 2$. Además,

$$G_i = G_{i-1} \oplus H_i \quad \text{y} \quad G_{i-1} \cap H_i = \{\mathbf{0}\},$$

con lo que G_i es la suma directa de G_{i-1} y H_i.

Igual que en la sección III, por conveniencia en la notación, nos referiremos a los elementos de H_i, para $i = l + 1, l + 2, \ldots, k$, como

$$\boldsymbol{a}_0^{(i)} = \mathbf{0},\ \boldsymbol{a}_1^{(i)} = \boldsymbol{u}_{2i-1},\ \boldsymbol{a}_2^{(i)} = \boldsymbol{u}_{2i} \text{ y } \boldsymbol{a}_3^{(i)} = \boldsymbol{u}_{2i-1} \oplus \boldsymbol{u}_{2i}.$$

Para $p \in \{0, 1, 2, 3\}$ consideramos los conjuntos

$$C(p) = \left(\boldsymbol{a}_p^{(l+1)} \oplus \widehat{A}\right) \cup \bigcup_{\substack{q=0 \\ q \neq p}}^{3} \left(\boldsymbol{a}_q^{(l+1)} \oplus A\right),$$

$$\widehat{C}(p) = \left(\boldsymbol{a}_p^{(l+1)} \oplus A\right) \cup \bigcup_{\substack{q=0 \\ q \neq p}}^{3} \left(\boldsymbol{a}_q^{(l+1)} \oplus \widehat{A}\right).$$

Ahora, si $(p_1, p_2, \ldots, p_{i-1}, p_i) \in \{0, 1, 2, 3\}^i$ y suponemos que hemos definido los conjuntos $C(p_1, p_2, \ldots, p_{i-1})$ y $\widehat{C}(p_1, p_2, \ldots, p_{i-1})$, podemos definir

$$C(p_1, p_2, \ldots, p_{i-1}, p_i) = \left(\boldsymbol{a}_{p_i}^{(i)} \oplus \widehat{C}(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus C(p_1, p_2, \ldots, p_{i-1})\right),$$

$$\widehat{C}(p_1, p_2, \ldots, p_{i-1}, p_i) = \left(\boldsymbol{a}_{p_i}^{(i)} \oplus C(p_1, p_2, \ldots, p_{i-1})\right) \cup \bigcup_{\substack{q=0 \\ q \neq p_i}}^{3} \left(\boldsymbol{a}_q^{(i)} \oplus \widehat{C}(p_1, p_2, \ldots, p_{i-1})\right).$$

Así, mediante los mismos argumentos utilizados en la sección III, es fácil comprobar que los lemas 1 y 2 continúan siendo válidos si cambiamos los conjuntos $B(p_1, p_2, \ldots, p_{i-1}, p_i)$ y $\widehat{B}(p_1, p_2, \ldots, p_{i-1}, p_i)$ por los conjuntos $C(p_1, p_2, \ldots, p_{i-1}, p_i)$ y $\widehat{C}(p_1, p_2, \ldots, p_{i-1}, p_i)$ respectivamente. Además, el teorema 2 también es válido si cambiamos los conjuntos $B(p_1, p_2, \ldots, p_k)$ y $\widehat{B}(p_1, p_2, \ldots, p_k)$ por los conjuntos $C(p_1, p_2, \ldots, p_{k-l})$ y $\widehat{C}(p_1, p_2, \ldots, p_{k-l})$ respectivamente. Finalmente, el teorema 3 también permite afirmar que los soportes de las funciones bent de $2k$ variables obtenidas de esta forma son distintos de los soportes de las funciones bent de $2k$ variables obtenidos a partir de la construcción de la sección III.

V. Conclusiones y líneas futuras

En este artículo utilizamos una base de $\mathbb{F}_2^{2k}$ para construir 2^{2k+1} conjuntos en $\mathbb{F}_2^{2k}$ que son los soportes de funciones bent de $2k$ variables. La mitad de las funciones bent obtenidas son las funciones complementarias de la otra mitad.

Ponemos de manifiesto que dos bases distintas pueden proporcionar las mismas funciones bent y damos una clasificación completa para el caso $k = 2$; es decir, para las funciones bent de 4 variables. Sin embargo, no hemos podido establecer una clasificación análoga para $k > 2$, con lo que es necesario profundizar más en esta construcción para determinar bajo qué condiciones dos bases distintas proporcionan las mismas funciones bent.

Nuestra construcción permite obtener todas las funciones bent de 4 variables, pero no todas las funciones bent de más variables. Sin embargo, partiendo del soporte de una función bent de $2l$ variables, con $3 \leq l < k$, que no se pueda obtener con dicha construcción, podemos iniciar un proceso iterativo similar y otener más funciones bent. Estas nuevas funciones bent son distintas de las obtenidas con la construcción de la sección III, pero no hemos podido establecer bajo qué condiciones se da la igualdad entre las funciones bent obtenidas. Esto será objeto de un trabajo posterior.

AGRADECIMIENTOS

Este trabajo ha sido parcialmente subvencionado por el proyecto MTM2011-24858 del Ministerio de Economía y Competitividad del Gobierno de España.

REFERENCIAS

[1] A. Braeken, V. Nikov, S. Nikova y B. Preneel. On Boolean functions with generalized cryptographic properties. En A. Canteaut y K. Viswanathan, editores, *Progress in Cryptology – INDOCRYPT 2004*, volumen 3348 de *Lecture Notes in Computer Science*, páginas 120–135. Springer-Verlag, Berlin, 2004.

[2] A. Canteaut, M. Daum, H. Dobbertin y G. Leander. Finding nonnormal bent functions. *Discrete Applied Mathematics*, 154:202–218, 2006.

[3] C. Carlet y P. Guillot. A characterization of binary bent functions. *Journal of Combinatorial Theory (Series A)*, 76:328–335, 1996.

[4] C. Carlet y Y. Tarannikov. Covering sequences of Boolean functions and their cryptographic significance. *Designs, Codes and Cryptography*, 25:263–279, 2002.

[5] C. Carlet. On the secondary constructions of resilient and bent functions. *Progress in Computer Science and Applied Logic*, 23:3–28, 2004.

[6] D. K. Chang. Binary bent sequences of order 64. *Utilitas Mathematica*, 52:141–151, 1997.

[7] C. Charnes, M. Rötteler y T. Beth. Homogeneous bent functions, invariants, and designs. *Designs, Codes and Cryptography*, 26:139–154, 2002.

[8] J.-J. Climent, F. J. García y V. Requena. Cálculo del grado de una función booleana a partir de su soporte. En J. Domingo Ferrer, A. Martínez Ballesté, J. Castellà Roca y A. Solanas Gómez, editores, *Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI2010)*, páginas 7–12. Publicacions URV, Tarragona, 2010.

[9] J.-J. Climent, F. J. García y V. Requena. Construcción de funciones bent de n variables a partir de una base de $\mathbb{F}_2^n$. En J. Domingo Ferrer, A. Martínez Ballesté, J. Castellà Roca y A. Solanas Gómez, editores, *Actas de la XI Reunión Española sobre Criptología y Seguridad de la Información (RECSI2010)*, páginas 13–18. Publicacions URV, Tarragona, 2010.

[10] M. Daum, H. Dobbertin y G. Leander. An algorithm for checking normality of Boolean functions. En *Proceedings of the 2003 International Workshop on Coding and Cryptography (WCC 2003)*, páginas 133–142. mar. 2003.

[11] J. F. Dillon. *Elementary Hadamard Difference Sets*. Tesis Doctoral, University of Maryland, 1974.

[12] H. Dobbertin. Construction of bent functions and balanced Boolean functions with high nonlinearity. En B. Preneel, editor, *Fast Sofware Encription*, volumen 1008 de *Lecture Notes in Computer Science*, páginas 61–74. Springer-Verlag, Berlin, 1995.

[13] P. V. Kumar, R. A. Scholtz y L. R. Welch. Generalized bent functions and their properties. *Journal of Combinatorial Theory (Series A)*, 40:90–107, 1985.

[14] K. Kurosawa y R. Matsumoto. Almost security of cryptographic Boolean functions. *IEEE Transactions on Information Theory*, 50(11):2752–2761, 2004.

[15] R. L. McFarland. A family of difference sets in non-cyclic groups. *Journal of Combinatorial Theory (Series A)*, 15:1–10, 1973.

[16] W. Meier y O. Staffelbach. Nonlinearity criteria for cryptographic functions. En J. Quisquater y J. Vandewalle, editores, *Advances in Cryptology – EUROCRYPT'89*, volumen 434 de *Lecture Notes in Computer Science*, páginas 549–562. Springer-Verlag, Berlin, 1990.

[17] K. Nyberg. Perfect nonlinear S-boxes. En D. W. Davies, editor, *Advances in Cryptology – EUROCRYPT'91*, volumen 547 de *Lecture Notes in Computer Science*, páginas 378–386. Springer-Verlag, Berlin, 1991.

[18] D. Olejár y M. Stanek. On cryptographic properties of random Boolean functions. *Journal of Universal Computer Science*, 4(8):705–717, 1998.

[19] E. Pasalic y T. Johansson. Further results on the relation between nonlinearity and resiliency for Boolean functions. En M. Walker, editor, *Crytography and Coding*, volumen 1746 de *Lecture Notes in Computer Science*, páginas 35–44. Springer-Verlag, Berlin, 1999.

[20] B. Preneel. *Analysis and Design of Cryptographic Hash Functions*. Tesis Doctoral, Katholieke University Leuven, ene. 1993.

[21] O. S. Rothaus. On "bent" functions. *Journal of Combinatorial Theory (Series A)*, 20:300–305, 1976.

[22] P. Sarkar y S. Maitra. Construction of nonlinear Boolean functions with important cryptographic properties. En B. Preneel, editor, *Advances in Cryptology – EUROCRYPT 2000*, volumen 1807 de *Lecture Notes in Computer Science*, páginas 485–506. Springer-Verlag, Berlin, 2000.

[23] J. Seberry y X.-M. Zhang. Constructions of bent functions from two known bent functions. *Australasian Journal of Combinatorics*, 9:21–35, 1994.

[24] J. Seberry, X.-M. Zhang y Y. Zheng. Nonlinearity and propagation characteristics of balanced Boolean functions. *Information and Computation*, 119:1–13, 1995.

[25] S. A. Vanstone y P. C. van Oorschot. *An Introduction to Error Correcting Codes with Applications*. Kluwer Academic Publishers, Boston, MA, 1989.

[26] N. Y. Yu y G. Gong. Constructions of quadratic bent functions in polynomial forms. *IEEE Transactions on Information Theory*, 52(7):3291–3299, 2006.