Biuletyn WAT
Vol. LVII, Nr 4, 2008

Symetryczne względem cyklicznego przesunięcia argumentów funkcje boolowskie o nieparzystej liczbie zmiennych

TOMASZ KIJKO

Wojskowa Akademia Techniczna,
Wydział Cybernetyki, Instytut Matematyki i Kryptologii
00-908 Warszawa, ul. S. Kaliskiego 2

Streszczenie. Artykuł zawiera opis strategii znajdowania symetrycznych względem cyklicznego przesunięcia argumentów funkcji boolowskich o określonych własnościach kryptograficznych. Zawiera on także podstawowe definicje i twierdzenia dotyczące funkcji boolowskich i najistotniejszych parametrów kryptograficznych. Dodatkowo przedstawione zostały wyniki zastosowania opisanej strategii do znajdowania funkcji o parametrach (9,3,5,240).
Słowa kluczowe: funkcje boolowskie, funkcje boolowskie symetryczne względem cyklicznego przesunięcia argumentów, własności kryptograficzne
Symbole UKD: 519.714.7

1. Wstęp

W systemach kryptograficznych wykorzystujących funkcje boolowskie wymaga się od tych funkcji spełnienia odpowiednich kryteriów. Interesujące ze względu na własności kryptograficzne okazały się funkcje symetryczne względem cyklicznego przesunięcia argumentów (Rotation Symmetric Boolean Functions - RSBF) (patrz [5]). W artykule przedstawione zostaną najważniejsze własności kryptograficzne powyższych funkcji. Zaprezentowany zostanie także zaproponowany przez Alexandra Maximova, Martina Hella i Subhamoya Maitrę (patrz [8]) praktyczny algorytm znajdowania

symetrycznych względem cyklicznego przesunięcia argumentów funkcji boolowskich o nieparzystej liczbie zmiennych, będących funkcjami typu „plateaued" i charakteryzujących się wymaganymi własnościami kryptograficznymi.

2. Podstawowe definicje i twierdzenia

Niech $\mathbb{Z}$ oznacza pierścień liczb całkowitych, zaś $(\mathbb{Z}_2, \oplus, \circ)$ dwuelementowe ciało binarne. Przez $(\mathbb{Z}_2^n, \oplus)$ oznaczamy n-wymiarową przestrzeń liniową nad ciałem $\mathbb{Z}_2$, jest to zbiór ciągów binarnych o długości n:

$$x \in \mathbb{Z}_2^n, \qquad x = (x_1, \ldots, x_n)\,.$$

Działaniem w przestrzeni $\mathbb{Z}_2^n$ jest dodawanie modulo 2 po współrzędnych wektorów.

Będziemy oznaczali (numerowali) elementy (wektory) $\mathbb{Z}_2^n$ poprzez ich reprezentację dziesiętną:

$$\begin{aligned} \alpha_0 &= (00\cdots00) \\ \alpha_1 &= (00\cdots01) \\ &\vdots \\ \alpha_{2^n-1} &= (11\cdots11)\,. \end{aligned}$$

Funkcja boolowska (ang. Boolean function) jest przekształceniem

$$f : \mathbb{Z}_2^n \to \mathbb{Z}_2 \qquad f(x) = y, \quad x \in \mathbb{Z}_2^n,\ y \in \mathbb{Z}_2.$$

Dla danej funkcji boolowskiej ciąg binarny

$$(\, f(\alpha_0), f(\alpha_1), \cdots, f(\alpha_{2^n-1})\,).$$

nazywamy **tablicą prawdy** (ang. truth table) funkcji f.

Definicja 2.1. Wagą Hamminga binarnego wektora $\alpha \in \mathbb{Z}_2^n$, oznaczaną $wt(\alpha)$, nazywamy liczbę jedynek w tym wektorze (w binarnym ciągu n-elementowym).

Wagą Hamminga funkcji boolowskiej jest waga Hamminga jej tablicy prawdy.

Definicja 2.2. Odległość Hamminga między tymi funkcjami jest zdefiniowana jako:

$$d(f,g) = wt\,(f(x) \oplus g(x))\,,$$

gdzie prawa strona jest wagą Hamminga tablicy prawdy funkcji $f(x) \oplus g(x)$.

Każdą funkcję boolowską f n-zmiennych można przedstawić w postaci zwanej **algebraiczną postacią normalną**:

$$f(x) = a_0 \oplus \bigoplus_{1 \leqslant i \leqslant n} a_i x_i \oplus \bigoplus_{1 \leqslant i < j \leqslant n} a_{i,j} x_i x_j \cdots \oplus a_{1,2,\ldots,n} x_1 x_2 \cdots x_n,$$

gdzie wszystkie współczynniki należą do $\mathbb{Z}_2$ a symbol $\bigoplus$ oznacza sumowanie w ciele $\mathbb{Z}_2$. Jeśli **stopień** iloczynu i zmiennych zdefiniujemy jako równy i, to mamy następującą definicję:

Definicja 2.3. Stopień algebraiczny $ord(f)$ funkcji boolowskiej f równy jest największej wartości stopni poszczególnych iloczynów o niezerowych współczynnikach w algebraicznej postaci normalnej funkcji f.

Silnym kryterium „nieliniowości" funkcji boolowskiej jest jej odległość w sensie wagi Hamminga do zbioru funkcji afinicznych i do zbioru funkcji ze strukturami liniowymi.

Definicja 2.4. Niech f będzie funkcją boolowską n zmiennych. Odległość funkcji f do zbioru funkcji afinicznych:

$$\{A_{b,b_0}, \quad b \in \mathbb{Z}_2^n, \quad b_0 \in \mathbb{Z}_2\},$$

zdefiniowana jest jako

$$\delta(f) = \min_{b,b_0} d\,(f, A_{b,b_0})\,.$$

Definicja 2.5. Niech f będzie funkcją rzeczywistą n-zmiennych binarnych. **Transformatą Walsha-Hadamarda** funkcji f nazywamy funkcję rzeczywistą $\widehat{F}$ z dziedziną $\mathbb{Z}_2^n$ określoną wzorem

$$\widehat{F}(w) = \sum_x (-1)^{f(x) \oplus <x,w>},$$

gdzie iloczyn $< x, w >$ równy jest

$$\langle x, w \rangle = x_1 w_1 \oplus \cdots \oplus x_1 w_n .$$

Korzystając ze wzoru na odległość Hamminga między dwiema funkcjami wyrażoną przez transformaty Walsha-Hadamarda tych funkcji:

$$d(f, g) = 2^{n-1} - 2^{-n-1} \sum_{w} \widehat{F}(w)\widehat{G}(w),$$

otrzymujemy użyteczny praktycznie wzór:

$$\delta(f) = 2^{n-1} - \frac{1}{2} \max_{w} \left| \widehat{F}(w) \right| .$$

Ważną własnością funkcji boolowskiej jest jej zrównoważenie. Oznacza ono, że funkcja dla połowy argumentów przyjmuje wartość 1 (w tablicy prawdy funkcji występuje tyle samo 0 i 1). Własność tę można wyrazić za pomocą transformaty Walsha-Hadamarda funkcji, tj. funkcja boolowska f jest zrównoważona, wtedy i tylko wtedy, gdy $\widehat{F}(0) = 0$.
Ponadto ze względu na zastosowania kryptograficzne wyróżnia się klasy funkcji boolowskich, spełniające kryterium odporności korelacyjnej rzędu m (CI(m)), a także funkcje „resilient". Poniższe stwierdzenie wiąże odporność korelacyjną rzędu m (odpowiednio m-resilient) z wartościami transformaty Walsha-Hadamarda:

Stwierdzenie 2.1. *Niech f będzie funkcją boolowską n zmiennych. Funkcja f jest klasy $CI(m)$ (m-resilient) wtedy i tylko wtedy, gdy*

$$\widehat{F}(w) = 0 \quad \text{dla każdego } w : \ 1 \leqslant hwt(w) \leqslant m \ (0 \leqslant hwt(w) \leqslant m).$$

3. Funkcje symetryczne względem rotacji RSBF (Rotation Symmetric Boolean Functions)

Niech $x_i \in \mathbb{Z}_2$ dla $1 \leqslant i \leqslant n$. Dla $1 \leqslant k \leqslant n$, zdefiniujmy permutację $\rho_n^k(x_i)$ jako

$$\rho_n^k(x_i) = \begin{cases} x_{i+k} & \text{jeżeli } \ i + k \leqslant n \\ x_{i+k-n} & \text{jeżeli } \ i + k > n \end{cases}$$

Niech $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$. Możemy rozszerzyć powyższą definicję na n-bitowy wektor:

$$\rho_n^k(x_1, x_2, \ldots, x_n) = (\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n)).$$

Definicja 3.1. Funkcję boolowską f nazywamy symetryczną względem rotacji (Rotation Symmetric), jeżeli dla każdego argumentu $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}_2^n$ zachodzi:

$$f(\rho_n^k(x_1), \rho_n^k(x_2), \ldots, \rho_n^k(x_n)) = f(x_1, x_2, \ldots, x_n) \text{ dla } 1 \leqslant k \leqslant n.$$

Argumenty funkcji boolowskiej symetrycznej wględem operacji rotacji można podzielić na rozłączne podzbiory (klasy) w ten sposób, że każdy podzbiór zawiera wszystkie argumenty, będące cyklicznym przesunięciem jednego argumentu. Klasa jest generowana przez

$$G_n(x_1, x_2, \ldots, x_n) = \{\rho_n^k(x_1, x_2, \ldots, x_n) | 1 \leqslant k \leqslant n\}.$$

Oznaczmy liczbę wszystkich klas przez g_n. Wynika z tego, że ilość wszystkich funkcji RSBF wynosi 2^{g_n}. Liczbę g_n klas możemy wyznaczyć ze wzoru:

$$g_n = \frac{1}{n} \sum_{k|n} \phi(k) 2^{\frac{n}{k}},$$

gdzie $\phi(k)$ jest to funkcja *phi* Eulera (patrz [8]).

Każda klasa (podzbiór) może być reprezentowana przez pewien element $\Lambda_{n,i}$. Jest to „najmniejszy" względem porządku leksykograficznego element należący do danej klasy.
Jeżeli reprezentantów klas uporządkujemy leksykograficznie, to możemy zdefiniować tablicę prawdy funkcji RSBF jako wektor g_n elementowy:

$$[f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_n-1})].$$

Ważną własnością funkcji RSBF jest to, że $\widehat{F}(u) = \widehat{F}(v)$, jeżeli $u \in G_n(v)$.

Wykorzystując powyższą własność oraz fakt, że funkcja RSBF przyjmuje tę samą wartość dla wszystkich elementów tej samej klasy, możemy przekształcić macierz Walsha-Hadamarda do macierzy kwadratowej ${}_nA$ stopnia g_n postaci:

$${}_nA_{i,j} = \sum_{x \in G_n(\Lambda_{n,i})} (-1)^{<x, \Lambda_{n,j}>}.$$

Korzystając z macierzy ${}_nA$, możemy przedstawić transformatę WHT funkcji f w postaci:

$$\widehat{F}(\Lambda_{n,j}) = \sum_{i=0}^{g_n-1} (-1)^{f(\Lambda_{n,i})} {}_nA_{i,j}$$

a w postaci macierzowej:

$$\widehat{F} = [f(\Lambda_{n,0}), f(\Lambda_{n,1}), \ldots, f(\Lambda_{n,g_n-1})]_n A$$

4. Transformata Walsha-Hadamarda

Rozpatrzmy macierz ${}_nA$ w przypadku, gdy liczba zmiennych funkcji f jest nieparzysta. W tym przypadku liczba klas, dla których $wt(\Lambda_{n,i})$ jest wartością parzystą, jest równa liczbie klas, dla których $wt(\Lambda_{n,i})$ jest nieparzyste.
Jeżeli rozpatrzymy wszystkie $\Lambda_{n,i}$ o parzystej wadze Hamminga, a przez $\bar{\Lambda}_{m,i}$ oznaczymy reprezentanta klasy zawierającej dopełnienie elementu $\Lambda_{m,i}$, to można pokazać, że $G_n(\Lambda_{m,i}) \neq G_n(\bar{\Lambda}_{nj})$ dla dowolnych i i j. W związku z tym możemy podzielić wszystkie klasy na dwa rozłączne podzbiory: zawierające elementy o parzystej i nieparzystej wadze Hamminga.

Wprowadźmy permutację π elementów macierzy ${}_nA$ (otrzymamy w ten sposób macierz ${}_nA^{\pi}$) w następujący sposób:

— pierwsze $g_n/2$ wierszy macierzy ${}_nA^{\pi}$ odpowiada wierszom macierzy ${}_nA$ dla parzystych $wt(\Lambda_{m,i})$ uporządkowanych leksykograficznie.
— kolejne $g_n/2$ wiersze odpowiadają wierszom macierzy ${}_nA$ dla nieparzystych
$wt(\Lambda_{m,i})$ $(\bar{\Lambda}_{m,i})$ w kolejności odpowiadających im $\Lambda_{m,i}$, tj. $\Lambda_{m,i} = \bar{\Lambda}_{m,i-g_n/2}$ dla $i = \frac{g_n}{2}, \ldots, g_n - 1$.

Identyczną permutację stosujemu do kolumn macierzy ${}_nA$.

Przykład 4.1. Macierz ${}_nA$ dla $n = 5$.

$$ {}_nA = \left(\begin{array}{cccc|cccc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 5 & 3 & 1 & 1 & -1 & -1 & -3 & -5 \\ 5 & 1 & 1 & -3 & 1 & -3 & 1 & 5 \\ 5 & 1 & -3 & 1 & -3 & 1 & 1 & 5 \\ \hline 5 & -1 & 1 & -3 & -1 & 3 & 1 & -5 \\ 5 & -1 & -3 & 1 & 3 & -1 & 1 & -5 \\ 5 & -3 & 1 & 1 & 1 & 1 & -3 & 5 \\ 1 & -1 & 1 & 1 & -1 & -1 & 1 & -1 \end{array}\right) \begin{array}{c} (00000) \\ (00001) \\ (00011) \\ (00101) \\ \hline (00111) \\ (01011) \\ (01111) \\ (11111) \end{array} $$

Macierz ${}_nA^{\pi}$ dla $n = 5$.

$$
{}_nA^{\pi} = \left(\begin{array}{cccc|cccc}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
5 & 1 & -3 & 1 & 5 & 1 & -3 & 1 \\
5 & -3 & 1 & 1 & 5 & -3 & 1 & 1 \\
5 & 1 & 1 & -3 & 5 & 1 & 1 & -3 \\
\hline
1 & 1 & 1 & 1 & -1 & -1 & -1 & -1 \\
5 & 1 & -3 & 1 & -5 & -1 & 3 & -1 \\
5 & -3 & 1 & 1 & -5 & 3 & -1 & -1 \\
5 & 1 & 1 & -3 & -5 & -1 & -1 & 3
\end{array}\right)
\begin{array}{c}
(00000) \\ (00011) \\ (00101) \\ (01111) \\ \hline (11111) \\ (00111) \\ (01011) \\ (00001)
\end{array}
$$

Przedstawimy teraz dwa twierdzenia wraz z dowodami, pozwalające na szybsze wyznaczanie transformanty Walsha-Hadamarda dla funkcji RSBF (patrz [8]).

Lemat 4.1. *Niech* $A = (a_1, a_2, \ldots, a_n) \in \mathbb{Z}_n^2$ *i* $B = (b_1, b_2, \ldots, b_n) \in \mathbb{Z}_n^2$. *Jeżeli* $wt(A)$ *i* $wt(B)$ *są parzyste i* n *jest nieparzyste, to*

$$\bigoplus_{i=1}^{n}(a_i \wedge b_i) = \bigoplus_{i=1}^{n}(\bar{a}_i \wedge b_i) = \bigoplus_{i=1}^{n}(a_i \wedge \bar{b}_i) = 1 \oplus \bigoplus_{i=1}^{n}(\bar{a}_i \wedge \bar{b}_i).$$

Dowód. Mamy $(X \wedge Y) \oplus (\bar{X} \wedge Y) = (X \oplus \bar{X}) \wedge Y = 1 \wedge Y = Y$.
Stąd z równości

$$\bigoplus_{i=1}^{n}((a_i \wedge b_i) \oplus (\bar{a}_i \wedge b_i)) = \bigoplus_{i=1}^{n} b_i = 0$$

otrzymujemy

$$\bigoplus_{i=1}^{n}(a_i \wedge b_i) = \bigoplus_{i=1}^{n}(\bar{a}_i \wedge b_i).$$

Drugą równość dowodzimy w ten sam sposób. W przypadku ostatniej równości, z

$$\bigoplus_{i=1}^{n}((a_i \wedge \bar{b}_i) \oplus (\bar{a}_i \wedge \bar{b}_i)) = \bigoplus_{i=1}^{n} \bar{b}_i = 1$$

otrzymujemy

$$\bigoplus_{i=1}^{n}(a_i \wedge \bar{b}_i) = 1 \oplus \bigoplus_{i=1}^{n}(\bar{a}_i \wedge \bar{b}_i).$$

Twierdzenie 4.1. *Jeżeli n jest nieparzyste, to macierz ${}_nA^{\pi}$ jest postaci:*

$$ {}_nA^{\pi} = \begin{pmatrix} {}_nH & {}_nH \\ {}_nH & -{}_nH \end{pmatrix} $$

gdzie ${}_nH$ jest macierzą stopnia $\frac{g_n}{2}$.

Dowód.
Macierz ${}_nA^{\pi}$ jest zapisana w postaci, gdzie element $\Lambda_{m,i}$ odpowiada wierszowi (kolumnie) i a element $\bar{\Lambda}_{m,i}$ odpowiada wierszowi (kolumnie) $g_n/2+i$. Dzięki temu dla $0 \leqslant r, c < g_n/2$, możemy zapisać:

$$ \begin{aligned}
{}_nA^{\pi}_{r,c} &= \sum_{x \in G_n(\Lambda_{n,r})} (-1)^{<x,\Lambda_{n,c}>} \\
&= \sum_{x \in G_n(\Lambda_{n,r})} (-1)^{\bigoplus_{i=1}^{n}(x_i \wedge \Lambda_{(n,s)_i})} \\
{}_nA^{\pi}_{r,c+g_n/2} &= \sum_{x \in G_n(\Lambda_{n,r})} (-1)^{<x,\Lambda_{n,c}+g_n/2>} \\
&= \sum_{x \in G_n(\Lambda_{n,r})} (-1)^{\bigoplus_{i=1}^{n}(x_i \wedge \bar{\Lambda}_{(n,c)_i})} \\
{}_nA^{\pi}_{r+g_n/2,c} &= \sum_{x \in G_n(\Lambda_{n,r}+g_n/2)} (-1)^{<x,\Lambda_{n,c}>} \\
&= \sum_{x \in G_n(\Lambda_{n,r})} (-1)^{\bigoplus_{i=1}^{n}(\bar{x}_i \wedge \Lambda_{(n,s)_i})} \\
{}_nA^{\pi}_{r+g_n/2,c+g_n/2} &= \sum_{x \in G_n(\Lambda_{n,r}+g_n/2)} (-1)^{<x,\Lambda_{n,c}+g_n/2>} \\
&= \sum_{x \in G_n(\Lambda_{n,r})} (-1)^{\bigoplus_{i=1}^{n}(\bar{x}_i \wedge \bar{\Lambda}_{(n,c)_i})}
\end{aligned} $$

Ponieważ, dla $0 \leqslant i < g_n/2$ $wt(\Lambda_{m,i})$ jest parzyste, to na mocy lematu 4.1 mamy

$$ {}_nA^{\pi}_{r,c} = {}_n A^{\pi}_{r,c+g_n/2} = {}_n A^{\pi}_{r+g_n/2,c} = -{}_nA^{\pi}_{r+g_n/2,c+g_n/2}. $$

Stwierdzenie 4.1. *Pierwsza kolumna macierzy ${}_nA$ zawiera dokładnie $d_{n,t}$ wartości t, dla $t = 1, 2, \ldots, n$. Dodatkowo dla n nieparzystego $d_{n,t}$ jest parzyste.*

Dowód. Elementy pierwszej kolumny ${}_nA_{i,0}$ można przedstawić

$$ {}_nA_{i,0} = \sum_{x \in G_n(\Lambda_{m,i})} (-1)^{<x,0>} = |G_n(\Lambda_{m,i})|. $$

Stąd widać, że są $d_{n,t}$ klasy o liczności $|G_n(\Lambda_{m,i})|$.
W przypadku, gdy n jest nieparzysta, to macierz ${}_nA$ można skonstruować przy pomocy macierzy ${}_nH$, która musi zawierać $d_{n,t}/2$ wartości t w pierwszej kolumnie. Stąd $d_{n,t}$ musi być parzyste. □

Ze względu na fakt, że macierz ${}_nA^{\pi}$ ma specyficzną postać, możliwe jest szybsze wyznaczanie transformaty Walsha-Hadamarda dla funkcji RSBF. Tablicę prawdy funkcji RSBF (oznaczmy ją przez RSTT – Rotation Symmetric Truth Table) podzielmy na dwie części, to jest

$$ RSTT = \{0,1\}^{g_n} = \{0,1\}^{g_n/2} || \{0,1\}^{g_n/2} = \sigma_1 || \sigma_2 . $$

Wprowadźmy przekształcenie:

$$ \begin{aligned} \psi_\sigma \ : \ \sigma_1 || \sigma_2 = \{0,1\}^{g_n/2} || \{0,1\}^{g_n/2} &\mapsto \sigma_1^* || \sigma_2^* = \\ &= (-1)^{\{0,1\}^{g_n/2}} || (-1)^{\{0,1\}^{g_n/2}} \end{aligned} $$

Możemy zdefiniować

$$ \omega_1 = \sigma_1^* {}_nH, \quad \omega_2 = \sigma_2^* {}_nH. $$

Przy takich oznaczeniach możemy zapisać:

$$ \widehat{F} = ((\omega_1 + \omega_2) || (\omega_1 - \omega_2)). $$

Wektory ω_1, ω_2 nazywane są cząstkowymi transformatami Walsha-Hadamarda (partial Walsh-Hadamard Transform – pWHT).

Definicja 4.1. Mówimy, że funkcja boolowska n zmiennych, gdzie n jest nieparzyste, jest funkcją typu „plateaued", jeżeli jej transformata Walsha-Hadamarda przyjmuje tylko trzy wartości: 0 i $\pm\lambda$, gdzie λ jest liczbą naturalną.
Liczbę λ nazywamy amplitudą funkcji.

Korzystając z wcześniejszej notacji dla funkcji typu „plateaued", otrzymujemy zależności:

$$ \omega_{1_i} + \omega_{2_i} = 0 \text{ albo } \pm\lambda, \ \omega_{1_i} - \omega_{2_i} = 0 \text{ albo } \pm\lambda. $$

Tylko 9 par $(\omega_{1_i}, \omega_{2_i})$ spełnia powyższe warunki i są to:

$\omega_{1_i} + \omega_{2_i}$	$\omega_{1_i} - \omega_{2_i}$	ω_{1_i}	ω_{2_i}
0	0	0	0
0	λ	$\lambda/2$	$-\lambda/2$
0	$-\lambda$	$-\lambda/2$	$\lambda/2$
λ	0	$\lambda/2$	$\lambda/2$
λ	λ	λ	0
λ	$-\lambda$	0	$\lambda/2$
$-\lambda$	0	$-\lambda/2$	$-\lambda/2$
$-\lambda$	λ	0	$-\lambda/2$
$-\lambda$	$-\lambda$	$-\lambda/2$	0

Stwierdzenie 4.2. *Rozpatrzmy funkcję RSBF o nieparzystej liczbie zmiennych reprezentowaną przez RSTT* $(\sigma_1||\sigma_2)$.

— Jeżeli funkcja ta jest typu „plateaued", to funkcje o RSTT $(\sigma_2||\sigma_1)$, $(\overline{\sigma_1}||\overline{\sigma_2})$, $(\overline{\sigma_2}||\bar{\sigma_1})$, $(\sigma_1||\overline{\sigma_2})$, $(\overline{\sigma_1}||\sigma_2)$, $(\sigma_2||\overline{\sigma_1})$ i $(\overline{\sigma_2}||\sigma_1)$ są również funkcjami typu „plateaued".

— Jeżeli funkcja jest odporna korelacyjnie (względnie resilient), to funkcje o RSTT $(\sigma_2||\sigma_1)$, $(\overline{\sigma_1}||\overline{\sigma_2})$, $(\overline{\sigma_2}||\overline{\sigma_1})$ są także odporne korelacyjnie (względnie resilient).

Powyższe stwierdzenie pozwala na ograniczenie ilości wyznaczanych i przechowywanych cząstkowych transformat Walsha-Hadamarda w trakcie procesu przeszukiwania zbioru funkcji „plateaued" RSBF przy wyszukiwaniu funkcji o określonych własnościach kryptograficznych.

5. Strategia znajdowania „plateaued" RSBF o określonych parametrach kryptograficznych

W tym rozdziale przedstawimy własne podejście do strategii zaproponowanej przez Alexandra Maximova, Martina Hella i Subhamoya Maitrę, mającej na celu znajdowanie funkcji boolowskich o n nieparzystym, będących jednocześnie funkcjami symetrycznymi względem rotacji, jaki i funkcjami typu „plateaued" o określonych własnościach ktyptograficznych. Propozycja polega na wprowadzeniu zmian w tej strategii, pozwalających na znaczne przyspieszenie obliczeń.

Prezentowana strategia zostanie wykorzystana do znalezienia wszystkich funkcji „plateaued" RSBF o parametrach (n, m, d, δ), gdzie:

— n – ilość zmiennych funkcji;
— m – rząd odporoności korelacyjnej;
— d – stopień algebraiczny;
— δ – nieliniowość.

W algorytmie tym przeszukiwany jest pełny zbiór funkcji boolowskich symetrycznych względem rotacji.

Strategia

1. Wyznaczenie zbioru S_{σ_1} elementów σ_1, dla których cząstkowa transformata Walsha-Hadamarda $w_1 = \sigma_1^* \cdot_n H$ spełnia warunek $w_{1_i} \in \{0, \pm\lambda/2, \pm\lambda\}$.
Ze stwierdzenia 2.1 wynika, że aby funkcja posiadała rząd odporności korelacyjnej m większy od 0, to w transformata Walsha-Hadamarda tej funkcji musi przyjmować wartość 0 we wszystkich punktach w o $1 \leqslant wt(w) \leqslant m$. W związku z tym dla wszystkich $\Lambda_{n,i}$ spełniających $1 \leqslant wt(\Lambda_{n,i}) \leqslant m$ musi zajść:

$$w_{1_i} \in \{0, \pm\lambda/2\}.$$

Wyznaczenie zbioru S_{σ_1} polega na wyznaczeniu w_1 dla wszystkich $\sigma_1 \in Z_2^{g_n/2}$ i sprawdzeniu, czy wyznaczona cząstkowa transformata Walsha-Hadamarda spełnia powyższe warunki.
Dla σ_2 warunki dla cząstkowej transformaty Watsha-Hadamarda są identyczne, więc $S_{\sigma_1} = S_{\sigma_2}$.

Jeżeli jednak zauważymy, że dla dowolnej funkcji boolowskiej n zmiennych $f(x)$ o macierzy transformaty Walsha-Hadamarda $\hat{F}$ zachodzi poniższa własność, (niech $g(x) = f(x) \oplus 1$) wtedy mamy

$$\forall_{w \in \mathbb{Z}_2^n} \hat{G}(w) = \sum_x (-1)^{g(x) \oplus \langle x, w \rangle} = -\hat{F}(w).$$

Dzięki temu możemy ograniczyć się do wyznaczenia w_1 dla $\sigma_1 = (0, \gamma)$, gdzie $\gamma \in \mathbb{Z}_2^{g_n/2-1}$. Wartości cząstkowych transformat dla elementów $\sigma_1 = (1, \gamma)$ można wyznaczyć, wykorzystując powyższą uwagę. Ponadto, jeżeli cząstkowa transformata Walsha-Hadamarda w_1 elementu $\sigma_1 = (0, \gamma)$ spełnia założone warunki, to spełniać je także będzie transformata elementu $\bar{\sigma}_1 = (1, \bar{\gamma})$.

2. Wyznaczenie transformaty Walsha-Hadamarda dla funkcji o tablicach prawdy $(\sigma_1||\sigma_2)$.

Wyznaczane są transformaty dla $(\sigma_1||\sigma_2)$ z przestrzeni $S_{\sigma_1} \times S_{\sigma_2}$. Następnie na podstawie wyznaczonej transformaty określane są parametry kryptograficzne danej funkcji.

Dla przyspieszenia obliczeń dzielimy zbior S_{σ_1} na 3^t rozłącznych podzbiorów, gdzie liczba naturalna t jest wybierana arbitralnie i nie większa niż liczba pozycji, dla których wymagamy, aby częściowa transformata Walsha-Hadamarda przyjmowała wartość ze zbioru $\{0, \pm\lambda/2\}$. Niech więc

$$S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)} = \{w_1 \in S_{\sigma_1} : w_{1_{i_k}} = a_k,\ 1 \leqslant k \leqslant t\}$$

gdzie i_k oznacza różne pozycje w częściowej transformacie Walsha-Hadamarda, dla których $w_{i_k} = a_k \in \{0, \pm\lambda/2\}$. Możemy zbiór S_{σ_1} przedstawić w postaci sumy 3^t rozłącznych zbiorów:

$$\begin{aligned} S_{\sigma_1} = {} & S_{\sigma_1}^{(-\lambda/2,i_1,-\lambda/2,i_2,\ldots,-\lambda/2,i_t)} \cup S_{\sigma_1}^{(-\lambda/2,i_1,-\lambda/2,i_2,\ldots,0,i_t)} \\ & \cup S_{\sigma_1}^{(-\lambda/2,i_1,-\lambda/2,i_2,\ldots,\lambda/2,i_t)} \cup \ldots \cup S_{\sigma_1}^{(\lambda/2,i_1,\lambda/2,i_2,\ldots,\lambda/2,i_t)}. \end{aligned}$$

Przy wyznaczaniu transformat Walsha-Hadamarda funkcji RSBF zamiast obliczania jej dla dwóch dowolnych $\sigma_1, \sigma_2 \in S_{\sigma_1}$ można ograniczyć się do wyznaczania transformaty dla $\sigma_1 \in S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$ i $\sigma_2 \in \in S_{\sigma_1}^{(b_1,i_1,b_2,i_2,\ldots,b_t,i_t)}$, gdzie dla każdego i_k, $1 \leqslant k \leqslant t$ zachodzi:

$$a_{i_k} = -b_{i_k}, \quad \text{gdy wymagamy, aby} \quad w_{1_{i_k}} + w_{2_{i_k}} = 0,$$

albo

$$a_{i_k} = b_{i_k}, \quad \text{gdy wymagamy, aby} \quad w_{1_{i_k}} - w_{2_{i_k}} = 0.$$

Ponieważ dla każdego zbioru $S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$ istnieje dokładnie jeden zbiór $S_{\sigma_1}^{(b_1,i_1,b_2,i_2,\ldots,b_t,i_t)}$, taki że dla $\sigma_1 \in S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$ i $\sigma_2 \in \in S_{\sigma_1}^{(b_1,i_1,b_2,i_2,\ldots,b_t,i_t)}$ zachodzą powyższe warunki, to oznaczmy ten zbiór $S_{\sigma_1}^{(b_1,i_1,b_2,i_2,\ldots,b_t,i_t)}$ przez $\bar{S}_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$. dlatego też nie ma potrzeby wyznaczania transformaty Walsha-Hadamarda dla funkcji o RSTT równej $(\sigma_1||\sigma_2) \in S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)} \times S_{\sigma_1}^{(b_1,i_1,b_2,i_2,\ldots,b_t,i_t)}$ jeżeli $S_{\sigma_1}^{(b_1,i_1,b_2,i_2,\ldots,b_t,i_t)} \neq \neq \bar{S}_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$.

Złożoność obliczeniowa.

Złożoność obliczeniowa powyższej strategii przedstawiona została w tabeli poniżej. W porównaniu z wynikami autorów (patrz [8]) udało się zmniejszyć złożoność pierwszego etapu. W przypadku drugiego etapu złożoność

obliczeniowa się nie zmieniła. Jednak zastosowanie podziału zbioru S_{σ_1} na rozłączne podzbiory $S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$ pozwoliło na znaczne skrócenie czasu praktycznej realizacji etapu 2.

Wyznaczenie S_{σ_1}	$O(2^{g_n/2-1})$
Wyznaczenie WHT dla $(\sigma_1\|\|\sigma_2)$	$O(\|S_{\sigma_1}\|^2)$
Razem	$O(2^{g_n/2}) + O(\|S_{\sigma_1}\|^2)$

Zastosowanie strategii do znalezienia zrównoważonej funkcji o parametrach $(9, 3, 5, 240)$**.**

W przypadku $n = 9$ mamy:

Funkcje boolowskie 9 zmiennych	2^{512}
Funkcje RSBF 9 zmiennych	2^{60}

Etap 1. W etapie wyznaczony zostaje zbiór $S_{\sigma_1} = \cup S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$ dla wszystkich $\sigma_1 = (0, \gamma)$, gdzie $\gamma \in Z_2^{29}$, a $1 \leqslant t \leqslant 15$.

W celu przyspieszenia obliczeń można skatalogować cząstkowe transformaty w następujący sposób:

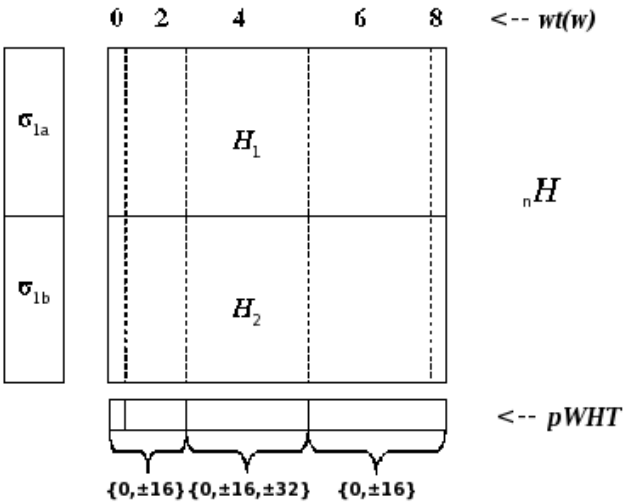
i Przedstawiamy σ_1 w postaci $(\sigma_{1a}||\sigma_{1b})$.
ii Wyznaczamy $\sigma_{1a}^* \cdot H_1$ i $\sigma_{1b}^* \cdot H_2$, gdzie:

$$_nH = \begin{pmatrix} H_1 \\ H_2 \end{pmatrix}.$$

iii Zapisujemy wyznaczone wartości w tablicy $H_{fast}[2][2^{15}][30]$.

W celu wyznaczenia cząstkowej transformaty wystarczy odczytanie wartości z tablicy H_{fast} i wykonanie maksymalnie 30 dodawań.
Liczność wyznaczonego zbioru S_{σ_1} wyniosła 173672.

Etap 2. Wyznaczenie wszystkich funkcji RSBF o tablicach prawdy RSTT $(\sigma_1||\sigma_2) \in S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)} \times \bar{S}_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$ dla wszystkich 3^t zbiorów $S_{\sigma_1}^{(a_1,i_1,a_2,i_2,\ldots,a_t,i_t)}$.



Rys. 1. Wyznaczanie cząstkowej trasformaty Hadamarda

Wyniki.
Aplikację realizującą powyższą strategię napisano w języku C++ i uruchomiono na komputerze z procesorem AMD Athlon 900 MHz, pamięcią 640 MB z systemem operacyjnym VectorLinux. W wyniku wykonania programu realizującego tę strategię otrzymano następujące rezultaty:

1. Nie istnieje zrównoważona funkcja "plateaued" RSBF o parametrach (9,3,5,240).
2. Znaleziono 2×8406 funkcji niezrównoważonych o parametrach (9,3,5,240).

W aplikacji ustalono wartość parametru t równą 4 oraz $i_1 = 2$, $i_2 = 3$, $i_3 = 4$ i $i_4 = 5$, co odpowiada numerom współrzędnych transformaty Walsha-Hadamarda dla argumentów o wadze Hamminga równej 2. Zbiór S_{σ_1} został więc podzielony na 81 rozłącznych podzbiorów. Znalezienie szukanych funkcji zajęło 182 sekundy (dla $t = 1$ i $i_1 = 5$ odpowiednio 1952 sekundy).

6. Podsumowanie

Zaproponowana w [8] metoda znajdowania symetrycznych względem cyklicznego przesunięcia funkcji boolowskich typu „plateaued" pozwala na zmniejszenie liczby „przetwarzanych" w algorytmie funkcji, zapewniając przez to skrócenie czasu obliczeń. Ograniczenie się jedynie do tego rodzaju

funkcji może spowodować, że dla wybranej liczby zmiennych szukanych funkcji n i dla ustalonych innych wymaganych parametrów kryptograficznych nie znajdziemy i nie otrzymamy żadnej takiej funkcji, chociaż funkcje o zadanych własnościach w całej przestrzeni funkcji n-zmiennych mogą istnieć.

Praca naukowa finansowana ze środków na naukę w latach 2008–2010 jako projekt rozwojowy Nr O R00 0031 06.

Artykuł wpłynął do redakcji w dniu 27.06.2008 r. Zweryfikowaną wersję po recenzji otrzymano w grudniu 2008 r.

LITERATURA

[1] J. Gawinecki, J. Szmidt, *Zastosowanie ciał skończonych i funkcji boolowskich w kryptografii*, wyd. II, WAT i BEL Studio, Warszawa, 2002.

[2] J. Szmidt, *Kryptograficzne własnoci funkcji boolowskich*, ENIGMA 2001, materiały konferencyjne, 2001.

[3] P. Sarkar, S. Maitra, *Construction of nonlinear Boolean functions with important cryptographic properties*, In Advances in Cryptology – EUROCRYPT 2000, number 1807 in Lecture Notes in Computer Science, 485–506, Springer Verlag, 2000.

[4] P. Sarkar, S. Maitra, *Nonlinearity bounds and construction of resilient Boolean functions*, ed. M. Bellare, Advances in Cryptology – Crypto 2000, s. 515–532, Lecture Notes in Computer Science vol. 1880, Berlin, 2000, Springer-Verlag.

[5] P. Stanica, S. Maitra, *Rotation Symmetric Boolean Functions – Count and Cryptographic Properties*, R. C. Bose Centenary Symposium on Discrete Mathematics and Applications, December 2002, Electronic Notes in Discrete Mathematics, vol. 15, Elsevier.

[6] P. Stanica, S. Maitra, J. Clark, *Results on Rotation Symmetric Bent and Correlation Immune Boolean Functions*, ed. B. Roy, W. Meier, Fast Software Encryption 2004. Pre-proceedings.

[7] M. Hell, A. Maximov, S. Maitra, *On efficient implementation of search strategy for rotation symmetric Boolean functions*, Ninth International Workshop on Algebraic and Combinatoral Coding Theory, ACCT 2004, Bułgaria, 2004.

[8] M. Hell, A. Maximov, S. Maitra, *Plateaued Rotation Symmetric Boolean Functions on Odd Number of Variables* BFCA 2005, Rouen, Francja, 2005.

[9] T. Siegenthaler, *Correlation immunity of non-linear combining functions for cryptographic applications*, IEEE trans. Inform. Theory, Tom IT-30, 1984, 766–780.

[10] G. Xiao, J. Massey, *A spectral characterization of correlation-immune combining functions*, IEEE trans. Inform. Theory, Tom IT-34, 1988, 569–571.

[11] S. Maitra, P. Sarkar, *New Directions in Design of Resilient Boolean Functions*, Technical Re-port No ASD/2000/04, Indian Statistic Institute, 2000.

T. KIJKO

Rotation Symmetric Boolean Functions on Odd Number of Variables

Abstract. This paper contains description of search strategy for rotation symmetric Boolean functions with certain cryptographic properties. There are also presented basic definitions and theorems connected to Boolean functions and the most important cryptographic parameters of the functions. Additionaly the practical results for searching for functions with parameters (9,3,5,240) are given.
Keywords: Boolean functions, rotation symmetric Boolean functions, cryptographic properties
2000 Mathematics Subject Classification: (primary) 94A60 (secondary) 06E30