G. Leander
.
.

Lehrstuhl für
Informationssicherheit und Kryptologie
Ruhr-Universität Bochum

Kryptographie I
Übungsblatt 5

Aufgabe 1 *FFT*
Berechnen Sie mit der Hilfe des FFT die Walshkoeffizienten der folgenden Funktion

$$f : \mathbb{F}_2^3 \to \mathbb{F}_2$$

mit

x	000	001	010	011	100	101	110	111
$f(x)$	0	1	1	0	0	0	1	0

Aufgabe 2 *Walsh-Transformation*

1. Im Folgenden sind 10 Spektren g_i angegeben. Welche 4 dieser Spektren können keine Walsh-Spektren $g_i = f_i^W$ einer Funktion $f_i : GF(2)^4 \to GF(2)$ sein?
   Begründen Sie jede einzelne Auswahl!

$a_1a_2a_3a_4$	$g_1(a)$	$g_2(a)$	$g_3(a)$	$g_4(a)$	$g_5(a)$	$g_6(a)$	$g_7(a)$	$g_8(a)$	$g_9(a)$	$g_{10}(a)$
0000	0	−6	−6	4	0	0	0	−2	0	−2
0001	−8	−6	−2	−4	0	8	4	2	0	6
0010	8	2	−2	−4	0	0	4	2	0	−6
0011	0	2	2	−4	0	0	0	−2	0	2
0100	4	−2	−2	4	−4	8	0	2	−16	−6
0101	4	6	10	−4	4	0	4	−2	0	−6
0110	4	−2	2	−4	−4	0	4	−2	0	−2
0111	4	6	−2	−4	4	0	0	2	0	−2
1000	4	2	2	4	−8	0	−4	−2	0	−6
1001	−4	−6	6	−4	−4	8	0	2	0	2
1010	−4	−6	−2	4	8	0	0	2	0	6
1011	4	2	2	4	4	0	12	−2	0	−2
1100	0	−2	6	−4	−4	−8	−4	2	0	−2
1101	0	2	2	4	−4	0	0	14	0	−2
1110	0	−2	2	−4	−4	0	1	−2	0	0
1111	0	−2	−2	−4	−4	0	−4	2	0	4

2. Bestimmen Sie die Funktion f_9, also die zu dem 9.ten Spektrum gehörende Funktion.

Hausaufgabe 1 *Inverse Walshtransformation*
Wenden Sie das FFT Verfahren auf die Walshkoeffizienten der Funktion aus Aufgabe 1 an. Was fällt auf? Beweisen Sie Ihre Vermutung.

Hausaufgabe 2 *FFT*
Implementieren Sie den FFT für beliebige Boolsche Funktionen

$$f : \mathbb{F}_2^n \to \mathbb{F}_2 \,.$$