Unicyclic strong permutations

Claude Gravel (Université de Montréal)
Daniel Panario (Carleton University)
David Thomson (Carleton University)

Tuesday, June 19th, and Wednesday, 20th, 2018

The 3rd International Workshop
on **B**oolean **F**unctions and their **A**pplications
BFA 2018

Loen (Norway)

Some properties of permutations

By unicyclic strong permutations, we mean permutations that satisfy:

(1) Unicyclic (contains only one cycle of maximal length),

(2) Number of terms per output bits is about 2^{d-1}, where d is the degree of the irreducible polynomial,

(3) Maximal algebraic degree,

(4) Easy to describe,

(5) Small values of the first-order differences (differential cryptanalysis),

(6) Small values of Walsh sums (Walsh spectrum cryptanalysis),

(7) On-the-fly generation.

We shall refer to above properties later when necessary.

Finding unicyclic permutation

For large $n > 0$, listing all of the $n!$ permutations, and retaining only the unicyclic ones is infeasible.

The are exactly $(n-1)!$ unicyclic permutations over a finite set of n distinct elements.

Finding unicyclic permutation

For large $n > 0$, listing all of the $n!$ permutations, and retaining only the unicyclic ones is infeasible.

The are exactly $(n-1)!$ unicyclic permutations over a finite set of n distinct elements.

QUESTION: Is it possible to construct efficiently a subset of the set of all permutations which are easy to describe, permutations there have only one cycle (and eventually other strong properties)?

Polynomial & permutation–example

We construct a permutation over the set $\{0,1\}^d$ of binary words, hence $n = 2^d$. To fit here, $d = 3$. The construction uses operations over polynomials.

Polynomial & permutation–example

We construct a permutation over the set $\{0,1\}^d$ of binary words, hence $n = 2^d$. To fit here, $d = 3$. The construction uses operations over polynomials.

NOTATION: $P_a(X) = a_0 + a_1 X + \ldots + a_{d-1} X^{d-1}$ where $a = (a_0, \ldots, a_{d-1}) \in \{0,1\}^d$.

FACT: For all *nonzero* $a \in \{0,1\}^3$, functions over $\{0,1\}^3$ defined through $P_a(X) \mapsto P_a^\ell(X)$ for $\ell = 1, 2, 3, 4, 5, 6$ are permutations. For example, we compute $P_a^6(X) = P_a^{2^d-2}(X)$.

Polynomial & permutation–example cont'd

For example, choosing the irreducible polynomial $Q(X) = 1 + X^2 + X^3$, compute X^j mod $Q(X)$ for $j = 0, \ldots, 6$.

Polynomial & permutation–example cont'd

For example, choosing the irreducible polynomial $Q(X) = 1 + X^2 + X^3$, compute X^j mod $Q(X)$ for $j = 0, \ldots, 6$.

For $a = a_0 a_1 a_2 \in \{0,1\}^3$, focus on $P_a^{2^k}(X)$.

$$
\begin{aligned}
P_a^{2^0}(X) &= P_a(X), \\
P_a^{2^1}(X) &= \big(a_0 + a_2\big) + a_2 X + \big(a_1 + a_2\big) X^2, \\
P_a^{2^2}(X) &= \big(P_a^2(X)\big)^2 \\
&= \big(a_0 + a_1\big) + \big(a_1 + a_2\big) X + a_1 X^2.
\end{aligned}
$$

Polynomial & permutation–example cont'd

Finally,

$$
\begin{aligned}
P_a^6(X) &= P_a^{2^1}(X) P_a^{2^2}(X) \\
&= \big(a_0 + a_2 + a_0 a_1 + a_0 a_2 + a_1 a_2\big) + \\
&\quad \big(a_1 + a_2 + a_0 a_1 + a_1 a_2\big) X + \\
&\quad \big(a_1 + a_0 a_2 + a_1 a_2\big) X^2 \\
&\stackrel{\text{def}}{=} P_b(X),
\end{aligned}
$$

and

Polynomial & permutation–example cont'd

Finally,

$$\begin{aligned} P_a^6(X) &= P_a^{2^1}(X) P_a^{2^2}(X) \\ &= \big(a_0 + a_2 + a_0 a_1 + a_0 a_2 + a_1 a_2\big) + \\ &\quad \big(a_1 + a_2 + a_0 a_1 + a_1 a_2\big) X + \\ &\quad \big(a_1 + a_0 a_2 + a_1 a_2\big) X^2 \\ &\stackrel{\text{def}}{=} P_b(X), \end{aligned}$$

and

a_0	a_1	a_2	b_0	b_1	b_2
0	0	0	0	0	0
0	0	1	1	1	0
0	1	0	0	1	1
0	1	1	0	1	0
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	0	0	1
1	1	1	1	0	1

Polynomial & permutation–example cont'd

Finally,

$$\begin{aligned} P_a^6(X) &= P_a^{2^1}(X) P_a^{2^2}(X) \\ &= \big(a_0 + a_2 + a_0a_1 + a_0a_2 + a_1a_2\big) + \\ &\quad \big(a_1 + a_2 + a_0a_1 + a_1a_2\big)X + \\ &\quad \big(a_1 + a_0a_2 + a_1a_2\big)X^2 \\ &\stackrel{\text{def}}{=} P_b(X), \end{aligned}$$

and

a_0	a_1	a_2	b_0	b_1	b_2
0	0	0	0	0	0
0	0	1	1	1	0
0	1	0	0	1	1
0	1	1	0	1	0
1	0	0	1	0	0
1	0	1	1	1	1
1	1	0	0	0	1
1	1	1	1	0	1

FACT: For all d and irreducible polynomial $Q(X)$ of degree d, the permutation obtained by considering $P_a^{2^d-2}(X)$ mod Q has fixed points and cycles of length two.

NOTE: Another example with fixed points and cycle of length two is the non-linear part of AES for which $d = 8$.

Polynomial & permutation–example cont'd

Three binary coordinate functions, one for each power of X.

Bits b_0, b_1, b_2 are themselves polynomials of the bits a_0, a_1, a_2 modulo 2.

$$b_0(a_0, a_1, a_2) = a_0 + a_2 + a_0a_1 + a_0a_2 + a_1a_2,$$
$$b_1(a_0, a_1, a_2) = a_1 + a_2 + a_0a_1 + a_1a_2,$$
$$b_2(a_0, a_1, a_2) = a_1 + a_0a_2 + a_1a_2.$$

Polynomial & permutation–example cont'd

Three binary coordinate functions, one for each power of X.

Bits b_0, b_1, b_2 are themselves polynomials of the bits a_0, a_1, a_2 modulo 2.

$$b_0(a_0, a_1, a_2) = a_0 + a_2 + a_0a_1 + a_0a_2 + a_1a_2,$$
$$b_1(a_0, a_1, a_2) = a_1 + a_2 + a_0a_1 + a_1a_2,$$
$$b_2(a_0, a_1, a_2) = a_1 + a_0a_2 + a_1a_2.$$

Like for polynomials with real coefficients, differential calculus can be used to approximate, and get information on the polynomials b_0, b_1, and b_2; this is differential cryptanalysis. Another cryptanalytic method is based the Walsh spectrum, and can translate easily into a quantum cryptanalytic method by using the quantum Fourier transform.

Polynomial & permutation–example cont'd

Three binary coordinate functions, one for each power of X.

Bits b_0, b_1, b_2 are themselves polynomials of the bits a_0, a_1, a_2 modulo 2.

$$b_0(a_0, a_1, a_2) = a_0 + a_2 + a_0a_1 + a_0a_2 + a_1a_2,$$
$$b_1(a_0, a_1, a_2) = a_1 + a_2 + a_0a_1 + a_1a_2,$$
$$b_2(a_0, a_1, a_2) = a_1 + a_0a_2 + a_1a_2.$$

Like for polynomials with real coefficients, differential calculus can be used to approximate, and get information on the polynomials b_0, b_1, and b_2; this is differential cryptanalysis. Another cryptanalytic method is based the Walsh spectrum, and can translate easily into a quantum cryptanalytic method by using the quantum Fourier transform.

FACT: The degree of the functions $b_j(a)$'s is $d - 1 = 2$. However, all the functions involved in $P_a^{2^k}(X)$ are linear in the a_j's...

Unicyclic strong permutations–Definition I

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is a permutation over $\{0,1\}^d$ constructed by composing d permutations σ_k for $k = 0, \ldots, d-1$ such that σ_k is defined by the map:

Unicyclic strong permutations–Definition I

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is a permutation over $\{0,1\}^d$ constructed by composing d permutations σ_k for $k = 0, \ldots, d-1$ such that σ_k is defined by the map:

$$P_{\sigma_k(a)}(X) = \left(P_a(X) + \mathbf{P}(X)\right)^{2^d - 2^k - 1} \pmod{Q} \text{ for } k = 0, \ldots, d-1$$

Unicyclic strong permutations–Definition I

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is a permutation over $\{0,1\}^d$ constructed by composing d permutations σ_k for $k = 0, \ldots, d-1$ such that σ_k is defined by the map:

$$P_{\sigma_k(a)}(X) = \left(P_a(X) + \mathbf{P}(X)\right)^{2^d - 2^k - 1} \pmod{Q} \text{ for } k = 0, \ldots, d-1$$
$$a \mapsto \sigma_k(a)$$

Unicyclic strong permutations–Definition I

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is a permutation over $\{0,1\}^d$ constructed by composing d permutations σ_k for $k = 0, \ldots, d-1$ such that σ_k is defined by the map:

$$P_{\sigma_k(a)}(X) = \left(P_a(X) + \mathbf{P}(X)\right)^{2^d - 2^k - 1} \pmod{Q} \text{ for } k = 0, \ldots, d-1$$
$$a \mapsto \sigma_k(a)$$

And then

$$\sigma = \sigma_{d-1} \circ \sigma_{d-2} \circ \cdots \circ \sigma_0$$

Unicyclic strong permutations–Definition II

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is permutation over $\{0,1\}^d$ constructed by recurrence. A word $a \in \{0,1\}^d$ is mapped to $b \in \{0,1\}^d$ through a sequence of steps $a = a^{(0)} \to \ldots \to a^{(i)} \to \ldots \to a^{(d)} = \sigma(a) = b$ defined by

Unicyclic strong permutations–Definition II

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is permutation over $\{0,1\}^d$ constructed by recurrence. A word $a \in \{0,1\}^d$ is mapped to $b \in \{0,1\}^d$ through a sequence of steps $a = a^{(0)} \to \ldots \to a^{(i)} \to \ldots \to a^{(d)} = \sigma(a) = b$ defined by

$$P_{a^{(0)}}(X) = P_a(X)$$

$$P_{a^{(j)}}(X) = \left(P_{a^{(j-1)}}(X) + \mathbf{P}(X)\right)^{2^d - 2^{j-1} - 1} \pmod{Q} \text{ for } j = 1, \ldots, d$$

Unicyclic strong permutations–Definition II

Let $\mathbf{P}(X)$ be a fixed non-constant perturbation polynomial.

Here σ is permutation over $\{0,1\}^d$ constructed by recurrence. A word $a \in \{0,1\}^d$ is mapped to $b \in \{0,1\}^d$ through a sequence of steps $a = a^{(0)} \to \ldots \to a^{(i)} \to \ldots \to a^{(d)} = \sigma(a) = b$ defined by

$$P_{a^{(0)}}(X) = P_a(X)$$

$$P_{a^{(j)}}(X) = \left(P_{a^{(j-1)}}(X) + \mathbf{P}(X)\right)^{2^d - 2^{j-1} - 1} \pmod{Q} \text{ for } j = 1, \ldots, d$$

$$a \mapsto b$$

$$= (b_0(a), \ldots, b_{d-1}(a)).$$

An example without a giant cycle

$a = a^{(0)}$
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31

$a = a^{(0)}$
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

An example without a giant cycle

$a = a^{(0)}$	$a^{(1)}$
0	10
1	13
2	46
3	38
4	48
5	18
6	47
7	34
8	43
9	21
10	41
11	20
12	59
13	3
14	39
15	35
16	19
17	37
18	23
19	7
20	60
21	8
22	5
23	28
24	17
25	27
26	45
27	2
28	9
29	53
30	24
31	15

$a = a^{(0)}$	$a^{(1)}$
32	1
33	0
34	44
35	58
36	55
37	29
38	50
39	22
40	61
41	52
42	12
43	33
44	32
45	11
46	62
47	25
48	57
49	26
50	49
51	36
52	40
53	42
54	51
55	6
56	14
57	63
58	56
59	16
60	4
61	54
62	30
63	31

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

An example without a giant cycle

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$
0	10	38
1	13	5
2	46	13
3	38	40
4	48	24
5	18	43
6	47	10
7	34	55
8	43	19
9	21	53
10	41	60
11	20	9
12	59	62
13	3	6
14	39	42
15	35	29
16	19	21
17	37	26
18	23	27
19	7	22
20	60	16
21	8	34
22	5	58
23	28	52
24	17	3
25	27	4
26	45	48
27	2	51
28	9	47
29	53	35
30	24	63
31	15	23

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$
32	1	36
33	0	49
34	44	18
35	58	25
36	55	20
37	29	61
38	50	45
39	22	17
40	61	56
41	52	39
42	12	28
43	33	0
44	32	1
45	11	46
46	62	31
47	25	14
48	57	12
49	26	54
50	49	15
51	36	57
52	40	8
53	42	37
54	51	2
55	6	50
56	14	7
57	63	30
58	56	33
59	16	**59**
60	4	44
61	54	41
62	30	11
63	31	32

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

An example without a giant cycle

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$
0	10	38	39
1	13	5	29
2	46	13	17
3	38	40	53
4	48	24	12
5	18	43	59
6	47	10	**6**
7	34	55	46
8	43	19	47
9	21	53	23
10	41	60	62
11	20	9	50
12	59	62	30
13	3	6	40
14	39	42	3
15	35	29	8
16	19	21	61
17	37	26	56
18	23	27	16
19	7	22	63
20	60	16	28
21	8	34	57
22	5	58	10
23	28	52	7
24	17	3	20
25	27	4	55
26	45	48	11
27	2	51	4
28	9	47	49
29	53	35	26
30	24	63	31
31	15	23	14

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$
32	1	36	24
33	0	49	32
34	44	18	34
35	58	25	33
36	55	20	52
37	29	61	25
38	50	45	44
39	22	17	5
40	61	56	19
41	52	39	35
42	12	28	60
43	33	0	45
44	32	1	2
45	11	46	36
46	62	31	18
47	25	14	21
48	57	12	27
49	26	54	38
50	49	15	43
51	36	57	37
52	40	8	22
53	42	37	15
54	51	2	41
55	6	50	54
56	14	7	42
57	63	30	48
58	56	33	0
59	16	**59**	13
60	4	44	58
61	54	41	9
62	30	11	51
63	31	32	1

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

An example without a giant cycle

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$	$a^{(4)}$
0	10	38	39	**23**
1	13	5	29	53
2	46	13	17	17
3	38	40	53	43
4	48	24	12	14
5	18	43	59	36
6	47	10	**6**	39
7	34	55	46	2
8	43	19	47	45
9	21	53	23	33
10	41	60	62	31
11	20	9	50	56
12	59	62	30	44
13	3	6	40	61
14	39	42	3	46
15	35	29	8	42
16	19	21	61	10
17	37	26	56	59
18	23	27	16	27
19	7	22	63	30
20	60	16	28	9
21	8	34	57	3
22	5	58	10	20
23	28	52	7	**35**
24	17	3	20	60
25	27	4	55	51
26	45	48	11	41
27	2	51	4	57
28	9	47	49	18
29	53	35	26	25
30	24	63	31	58
31	15	23	14	47

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$	$a^{(4)}$
32	1	36	24	37
33	0	49	32	1
34	44	18	34	24
35	58	25	33	**0**
36	55	20	52	21
37	29	61	25	19
38	50	45	44	29
39	22	17	5	26
40	61	56	19	50
41	52	39	35	15
42	12	28	60	13
43	33	0	45	55
44	32	1	2	38
45	11	46	36	11
46	62	31	18	22
47	25	14	21	8
48	57	12	27	62
49	26	54	38	7
50	49	15	43	28
51	36	57	37	32
52	40	8	22	12
53	42	37	15	34
54	51	2	41	52
55	6	50	54	6
56	14	7	42	5
57	63	30	48	48
58	56	33	0	54
59	16	**59**	13	63
60	4	44	58	49
61	54	41	9	40
62	30	11	51	16
63	31	32	1	4

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

An example without a giant cycle

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$	$a^{(4)}$	$a^{(5)}$
0	10	38	39	**23**	19
1	13	5	29	53	34
2	46	13	17	17	63
3	38	40	53	43	27
4	48	24	12	14	50
5	18	43	59	36	48
6	47	10	**6**	39	43
7	34	55	46	2	6
8	43	19	47	45	57
9	21	53	23	33	0
10	41	60	62	31	29
11	20	9	50	56	28
12	59	62	30	44	26
13	3	6	40	61	**49**
14	39	42	3	46	4
15	35	29	8	42	17
16	19	21	61	10	46
17	37	26	56	59	2
18	23	27	16	27	**13**
19	7	22	63	30	55
20	60	16	28	9	39
21	8	34	57	3	51
22	5	58	10	20	9
23	28	52	7	**35**	**32**
24	17	3	20	60	36
25	27	4	55	51	62
26	45	48	11	41	60
27	2	51	4	57	5
28	9	47	49	18	42
29	53	35	26	25	59
30	24	63	31	58	45
31	15	23	14	47	54

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$	$a^{(4)}$	$a^{(5)}$
32	1	36	24	37	**18**
33	0	49	32	1	16
34	44	18	34	24	3
35	58	25	33	**0**	56
36	55	20	52	21	53
37	29	61	25	19	40
38	50	45	44	29	61
39	22	17	5	26	10
40	61	56	19	50	25
41	52	39	35	15	22
42	12	28	60	13	12
43	33	0	45	55	41
44	32	1	2	38	21
45	11	46	36	11	38
46	62	31	18	22	37
47	25	14	21	8	35
48	57	12	27	62	30
49	26	54	38	7	**23**
50	49	15	43	28	52
51	36	57	37	32	1
52	40	8	22	12	33
53	42	37	15	34	11
54	51	2	41	52	47
55	6	50	54	6	7
56	14	7	42	5	15
57	63	30	48	48	44
58	56	33	0	54	20
59	16	**59**	13	63	31
60	4	44	58	49	58
61	54	41	9	40	8
62	30	11	51	16	14
63	31	32	1	4	24

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

An example without a giant cycle

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$	$a^{(4)}$	$a^{(5)}$	$a^{(6)}$
0	10	38	39	**23**	19	39
1	13	5	29	53	34	48
2	46	13	17	17	63	30
3	38	40	53	43	27	36
4	48	24	12	14	50	10
5	18	43	59	36	48	55
6	47	10	**6**	39	43	14
7	34	55	46	2	6	21
8	43	19	47	45	57	17
9	21	53	23	33	0	25
10	41	60	62	31	29	8
11	20	9	50	56	28	60
12	59	62	30	44	26	49
13	3	6	40	61	**49**	29
14	39	42	3	46	4	11
15	35	29	8	42	17	12
16	19	21	61	10	46	**16**
17	37	26	56	59	2	20
18	23	27	16	27	**13**	37
19	7	22	63	30	55	38
20	60	16	28	9	39	34
21	8	34	57	3	51	13
22	5	58	10	20	9	7
23	28	52	7	**35**	**32**	1
24	17	3	20	60	36	44
25	27	4	55	51	62	31
26	45	48	11	41	60	2
27	2	51	4	57	5	32
28	9	47	49	18	42	63
29	53	35	26	25	59	4
30	24	63	31	58	45	24
31	15	23	14	47	54	46

$a = a^{(0)}$	$a^{(1)}$	$a^{(2)}$	$a^{(3)}$	$a^{(4)}$	$a^{(5)}$	$a^{(6)}$
32	1	36	24	37	**18**	35
33	0	49	32	1	16	**33**
34	44	18	34	24	3	41
35	58	25	33	**0**	56	27
36	55	20	52	21	53	22
37	29	61	25	19	40	53
38	50	45	44	29	61	45
39	22	17	5	26	10	51
40	61	56	19	50	25	28
41	52	39	35	15	22	3
42	12	28	60	13	12	19
43	33	0	45	55	41	9
44	32	1	2	38	21	61
45	11	46	36	11	38	47
46	62	31	18	22	37	58
47	25	14	21	8	35	18
48	57	12	27	62	30	57
49	26	54	38	7	**23**	59
50	49	15	43	28	52	50
51	36	57	37	32	1	62
52	40	8	22	12	33	0
53	42	37	15	34	11	6
54	51	2	41	52	47	56
55	6	50	54	6	7	43
56	14	7	42	5	15	42
57	63	30	48	48	44	15
58	56	33	0	54	20	52
59	16	**59**	13	63	31	26
60	4	44	58	49	58	54
61	54	41	9	40	8	23
62	30	11	51	16	14	40
63	31	32	1	4	24	5

$$P(X) = X^5 + 1,\ Q(X) = 1 + X + X^4 + X^5 + X^6$$

Table I of proportions for a specific $P(X)$

For the table below specifically, $\mathbf{X^{d-1}+1}$ is the perturbation polynomial. Here $\mathcal{I}_d$ denotes the set of irreducible polynomials of degree d, and $\mathcal{J}_d$ denotes the set of polynomials of degrees d that lead to unicyclic strong permutations with $\mathbf{P(X)=X^{d-1}+1}$.

d	$\lvert\mathcal{J}_d\rvert$	$\lvert\mathcal{I}_d\rvert$	$\lvert\mathcal{J}_d\rvert/\lvert\mathcal{I}_d\rvert$
3	1	2	0.5
5	2	6	0.333333
7	6	18	0.333333
9	10	56	0.178571
11	30	186	0.16129
13	87	630	0.138095
15	259	2182	0.118698
17	1130	7710	0.146563
19	3805	27594	0.137892
21	12551	99858	0.125688
23	46290	364722	0.126919
25	153976	1342176	0.114721

Table II of proportions

NOTATION: $[a_0 \quad a_1 \quad \dots \quad a_\ell] :=: \sum_{j=0}^{\ell} a_j X^j$

d	**P(X)**	$\lvert\mathcal{J}_d\rvert$	$\lvert\mathcal{I}_d\rvert$	$\lvert\mathcal{J}_d\rvert/\lvert\mathcal{I}_d\rvert$
15	[0100100000001]	334	2182	0.153071
15	[1101000100101]	275	2182	0.126031
15	[101011001110111]	358	2182	0.16407
15	[1001111000111]	367	2182	0.168194
17	[00111011101000001]	1111	7710	0.144099
17	[11110111111101]	1186	7710	0.153826
17	[11010110100010111]	1116	7710	0.144747
17	[0010011000101]	1179	7710	0.152918

Matrix of first-order differences

Define the (a, b)-entry of the matrix by

$$\frac{1}{2^d} \sum_{x \in \mathbb{F}_2^d} \mathbb{1}\{\sigma(x \oplus a) \oplus \sigma(x) = b\} \stackrel{\text{def}}{=} d_{a,b},$$

where σ is a permutation over $\{0,1\}^d$, a is a "direction vector", and b is a possible value for the derivative of σ in the direction of a for a given input $x \in \{0,1\}^d$.

Matrix of first-order differences

Define the (a, b)-entry of the matrix by

$$\frac{1}{2^d} \sum_{x \in \mathbb{F}_2^d} \mathbb{1}\{\sigma(x \oplus a) \oplus \sigma(x) = b\} \stackrel{\text{def}}{=} d_{a,b},$$

where σ is a permutation over $\{0,1\}^d$, a is a "direction vector", and b is a possible value for the derivative of σ in the direction of a for a given input $x \in \{0,1\}^d$.

NOTE: For random plaintexts, want to find a sequence $(a_0, a_1, \ldots, a_\ell)$ (Markov chain) for which the probability $\prod_{i=0}^{\ell-1} d_{a_i,a_{i+1}}$ is as high as possible. We look at counts as on the next slide (second level statistics).

Matrix of first-order differences–example

NOTATION: $[a_0 \quad a_1 \quad \ldots \quad a_\ell] :=: \sum_{j=0}^{\ell} a_j X^j$

$d = 19 =$ degree of irreducible polynomial

Irreducible polynomial = [1 0 0 0 0 1 0 1 1 1 0 1 0 1 0 0 1 1 1 1]

Perturbation polynomial = [1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1]

Entry value[1]	Number of entries
0	137444193323
2	137428735987
4	4977558
6	75

Note that
$137444193323 + 137428735987 + 4977558 + 75 = \left(2^{19}\right)^2 - 1.$

[1] Before normalization by 2^{19}

Walsh spectrum analysis

Define the (a, b)-entry of the matrix by

$$\begin{aligned}\frac{1}{2^d}\sum_{x\in\mathbb{F}_2^d}(-1)^{a\cdot x+b\cdot\sigma(x)} &= \frac{1}{2^d}\sum_{x\in\mathbb{F}_2^d}\Big(1-2\Big(\big(a\cdot x+b\cdot\sigma(x)\big)\bmod 2\Big)\Big)\\ &= 1-\frac{1}{2^{d-1}}\sum_{x\in\mathbb{F}_2^d}\Big(\big(a\cdot x+b\cdot\sigma(x)\big)\bmod 2\Big)\\ &\stackrel{\text{def}}{=} w_{a,b}\end{aligned}$$

where σ is a permutation over $\{0,1\}^d$, a is combiner for x (identity permutation), and b is the combiner for response σ. The matrix defined by $w_{a,b}$'s is a correlation matrix.

Walsh spectrum analysis

Define the (a, b)-entry of the matrix by

$$\frac{1}{2^d}\sum_{x\in\mathbb{F}_2^d}(-1)^{a\cdot x+b\cdot\sigma(x)} = \frac{1}{2^d}\sum_{x\in\mathbb{F}_2^d}\Big(1-2\Big(\big(a\cdot x+b\cdot\sigma(x)\big)\bmod 2\Big)\Big)$$

$$= 1-\frac{1}{2^{d-1}}\sum_{x\in\mathbb{F}_2^d}\Big(\big(a\cdot x+b\cdot\sigma(x)\big)\bmod 2\Big)$$

$$\stackrel{\text{def}}{=} w_{a,b}$$

where σ is a permutation over $\{0,1\}^d$, a is combiner for x (identity permutation), and b is the combiner for response σ. The matrix defined by $w_{a,b}$'s is a correlation matrix.

NOTE: Instead of the identity (linear boolean functions) permutation, one can also look at permutations that lead to quadratic or higher degree boolean functions, like those from arising from $P_x^{2^{k_1}}(X)P_x^{2^{k_2}}(X)$ for $k_1 \neq k_2$; this lead to something of the form $a\cdot\rho(x)+b\cdot\sigma(x)$ with ρ not the identity.

Walsh spectrum analysis example – slide I

NOTATION: $[a_0 \quad a_1 \quad \ldots \quad a_\ell] :=: \sum_{j=0}^{\ell} a_j X^j$

$d = 15 =$ degree of irreducible polynomial

Irreducible polynomial = [1 0 0 1 1 1 0 1 0 0 0 0 0 0 1 1]

Perturbation polynomial = [1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1]

In the following table, the entry values are given before normalization by 2^{15}.

NOTE: As expected, the weighted average of the entry values is 0.

(**Table is on next slide, followed by a slide for a random permutation on the same number of elements as a comparison for expected extreme values.**)

Walsh spectrum analysis example – slide II

Entry value	Number of entries
-384	6 (extreme)
-380	146
⋮	⋮
12	7748469
-8	7519934
-4	7416332
0	7486434
4	7419616
8	7521798
12	7751075
⋮	⋮
380	148
384	4 (extreme)
32768	1 (trivial)

Walsh spectrum analysis example – slide III

The Walsh-sums on a random permutation:

Entry value	Number of entries
-1088	1 (extreme)
-1072	1
⋮	⋮
-384	998280 (extreme of previous slide)
-380	1044401
⋮	⋮
-4	9465140
0	9525299
4	9464656
⋮	⋮
380	1046219
384	997790 (extreme of previous slide)
⋮	⋮
1196	1
1252	1 (extreme)
32768	1 (trivial)

Results, facts and intuitions – I

For $k = 0, \ldots, d-1$, recall that $\sigma_k(a)$ is defined through $\left(P_a(X) + \mathbf{P(X)}\right)^{2^d - 2^k - 1}$ where **P(X)** is a non-constant polynomial.

✠ Because σ_k are bijections, composing them in any order or just some of them ends up in a permutation with algebraic degree which is equal to the smallest among all retained for the composition. For all k, σ_k has algebraic degree $d-1$ and so for σ.

✠ Also $2^d - 2^k - 1 \equiv -2^k \equiv (2^d - 2)2^k \pmod{2^d - 1}$. Shift by power of 2 and inversion in finite field. Only numbers strictly between 0 and $2^d - 1$ having Hamming weight $d-1$ are $2^d - 2^k - 1$.

✠ For all k, the average number of terms in the polynomial expressions of the output bits of $\sigma_k(a)$ for an arbitrary a is 2^{d-1}. Term $\prod_{i=0}^{d-1} a_i$ is always absent.

Results, facts and intuitions – II

✠ Generally, if the space of binary plaintexts doubles, i.e., the length of a plaintext increases by 1, then one more "operation" must be to completed to maintain statistical properties. Here there are exactly $d = \log_2(2^d)$ numbers with exactly Hamming weight $d - 1$, and these numbers are $2^d - 2^d - 1$. An "operation" here *means* shift-by-power-of-two-AND-inverse.

✠ Analogy with continued fractions over finite fields.

✠ The secret key is the irreducible polynomial. Possibility to have both a public key system (Matsumoto) and a symmetric key system. The key is not something added or something multiplied; the key is something divided (irreducible polynomial).

✠ Given a perturbation polynomial, sample randomly the key, i.e., the irreducible polynomials. The sampling is efficient, i.e., the expected number of bits requires to draw randomly a unicyclic

Results, facts and intuitions – III

strong permutation is much smaller than it would be for a generic random permutation over sets of the same size.

✠ Efficiently on-the-fly produce the output for a given input. There is no need to store the entire permutation.

✠ The linear functions $\lambda_{j,k}(a)$ such that $\left(P_a(X) + P(X)\right)^{2^d - 2^k - 1} = \sum_{j=0}^{d-1} \lambda_{j,k}(a)$ are central in the algebraic degree as well as the number of terms properties; these two properties are important to shield against attacks such as linearization, hidden substructures (probabilistic, quantum, or deterministic), sat-type solver/optimization/hamiltonian type solver etc., differential calculus, and Walsh/Fourier, etc.

✠ There is at least one way to linearly extend over vector spaces with characteristic larger than two a hash or a permutation and obtained a group (non-commutative) of permutations (block

Results, facts and intuitions – IV

ciphers) so that all the differential cryptanalysis, characters (Walsh) cryptanalysis, and as well as the order of the group *reduces* respectively to the differential cryptanalysis, characters (Walsh) cryptanalysis, and period the non-linear part. This is why we are interesting in permutation with one cycle, and hence the period equals to the length of the cycle. Prevent quantum attacks in the case one founds an efficient quantum algorithm for the hidden subgroup problem for the symmetric group.

Results, facts and intuitions – V

If $\nu_2(x)$ denotes the number of times the prime number 2 appears in the factorization of some positive integer x, then

$$\nu_2\big((2^d-2)!\big) = \sum_{j=1}^{d-1} \nu_2\big((2^j)!\big),$$

and therefore the multinomial coefficient is odd. Hence one must have that the degree of the output bits with w.r.t. to the input bits a is $d-1$.

Results, facts and intuitions – VI

Lemma

For an even integer $m \geq 2$ and integers k_i such that $0 \leq k_i \leq n-1$ for $0 \leq i \leq m$, let ℓ be defined by

$$\ell = \left(\sum_{j=0}^{m} k_j (-1)^{j \bmod 2} \right) \bmod n,$$

then

$$\sigma_{k_m} \sigma_{k_{m-1}}^{-1} \sigma_{k_{m-2}} \cdots \sigma_{2i+2} \sigma_{2i+1}^{-1} \sigma_{2i} \cdots \sigma_{k_2} \sigma_{k_1}^{-1} \sigma_{k_0} = \sigma_\ell$$

Results, facts and intuitions – VII

Let $q = {}^{(2^n-2)}/_n$, $b = 10^{n-1} \oplus b$, i.e., $P_{b'}(X) = 1 + P_b(X)$, and respectively defined $\overline{a}_i, \overline{a}'_i \in V$ by

$$P_{\overline{a}_i}(X) \stackrel{\text{def}}{=} X^i P_b(X) \pmod{Q} \text{ for } i = 0, \ldots, q, \tag{1}$$

$$P_{\overline{a}'_i}(X) \stackrel{\text{def}}{=} X^i P_{b'}(X) \pmod{Q} \text{ for } i = 0, \ldots, q. \tag{2}$$

Since $P_b(X)$ is non-constant, then $P_{\overline{a}_i}(X) \neq 0$, and $P_{\overline{a}'_i}(X) \neq 0$ as well. Note also that $\overline{a}_0 = b$, and $\overline{a}'_0 = b'$. Define the set A_i and A'_i respectively by

$$A_i = \left\{ a \in \mathbb{F}_2^n \mid a = \sigma_j\left(\overline{a}_i\right) \text{ for } j = 0, \ldots, n-1 \right\}, \tag{3}$$

$$A'_i = \left\{ a \in \mathbb{F}_2^n \mid a = \sigma_j\left(\overline{a}'_i\right) \text{ for } j = 0, \ldots, n-1 \right\}. \tag{4}$$

Then clearly $A_0 = \{0\}$, and $A'_0 = \{1\}$, and for all $i \neq 0$, $|A_i| = |A'_i| = n$.

Theorem

For a fixed k, the sets $\sigma_k^{-1}\left(A_i\right)$ partition $\mathbb{F}_2^n$.

Results, facts and intuitions – VIII

Lemma

Vectors of positive integers of length d, say $(\ell_0, \ldots, \ell_{d-1})$, such that: (1) $2^d - 2 = \sum_{i=0}^{d-1} \ell_i$ (2) have k non-zero coordinates for $k \in \{1, \ldots, d\}$, and (3) $\nu_2\Big(\big(2^d-2\big)!\Big) = \sum_{i=0}^{d-1} \nu_2\big(\ell_i!\big)$ are the $\frac{n!}{(n-k)!}$ arrangements of the canonical vector

$$\left((2^d-2) - \sum_{j=1}^{k-1} 2^{i_j}, 2^{i_1}, \ldots, 2^{i_{k-1}}, 0, 0, \ldots, 0\right),$$

where i_j are distinct integers such that $1 \leq i_j \leq d-1$. In other words, the only vectors that lead to odd multinomial coefficients must be those with $k-1$ distinct coordinates of powers of 2 (powers between 2 and 2^{d-1}), and a remaining non-zero coordinate that is the difference between (2^d-2) and the former $k-1$ powers of 2, up to ordering.

Results, facts and intuitions – IX

Lemma

Consider the set of vectors of positive integers of length n as in Lemma from previous slide with k non-zero coordinates for $k \in \{1, \ldots d-1\}$. There are ✠ (need to be found explicitly) possible values for the sum

$$\sum_{i=0}^{d-1} i\ell_i \pmod{2^d - 1}.$$

CYCLE STRUCTURE

Line format for an excerpt:
[irreducible poly.] [perturbation poly.] * decimal value of perturbation * list of pairs (n_i, ℓ_i)

The index i ranges from 1 to L, where L is the number of distinct lengths. L is the length of the list of pairs as well, and depends on the perturbation and representation polynomials.

A pair (n_i, ℓ_i) indicates that there are n_i cycles of length ℓ_i.

The period is the least common multiple (lcm) of the ℓ_i's.

Next slides: Excerpts of concentration / distributions of cycles for some degrees.

Results, facts and intuitions – XI

EXCERPT CYCLE STRUCTURE FOR DEGREE 26

[11011000000000000000000001][01000101011100001010001111] * 63245986 * (1, 2) (3, 2731) (1, 3844) (1, 5289) (12264, 5462) (1, 13438) (1, 14040) (1, 18118) (1, 59972)

[11100010000000000000000001][01000101011100001010001111] * 63245986 * (2, 1) (1, 1701) (1, 8024) (1, 8191) (1, 8314) (1, 10922) (1, 11172) (1, 14192) (1, 15280) (1, 15554) (4083, 16382) (1, 17272) (1, 18994) (1, 21822) (1, 22370) (1, 23618) (1, 23730)

EXCERPT CYCLE STRUCTURE FOR DEGREE 24

[11011000000000000000000001][00001101100010101111000111] * 14930352 * (1, 2) (17, 241) (34775, 482) (1, 11567)

[11110110000000000000000001][00001101100010101111000111] * 14930352 * (2, 1) (1, 804) (1, 1424) (1, 1832) (1, 3106) (1, 4095) (1, 6647) (1, 7112) (2036, 8190) (1, 8694) (1, 8944) (1, 10248) (1, 11766) (1, 11770) (1, 12658) (1, 13274)

[11100001000000000000000001][00001101100010101111000111] * 14930352 * (1, 2) (1, 3220) (1, 3488) (1, 4097) (1, 5167) (1, 5870) (1, 6098) (1, 7274) (1, 7852) (2036, 8194) (1, 8432) (1, 8602) (1, 9350) (1, 11772) (1, 13008)

EXCERPT CYCLE STRUCTURE FOR DEGREE 22

[11000000000000000000001][01000111111000110101011] * 3524578 * (2, 1) (1, 434) (1, 1692) (1, 1937) (1, 2047) (1, 2698) (1, 2724) (1013, 4094) (1, 4148) (1, 4244) (1, 4460) (1, 4504) (1, 5854) (1, 5946) (1, 6392)

[11100100000000000000001][01000111111000110101011] * 3524578 * (2, 1) (1, 536) (1, 648) (1, 1290) (1, 2047) (1, 2203) (1, 2370) (1, 3226) (1, 3594) (1013, 4094) (1, 4188) (1, 5358) (1, 6874) (1, 7084) (1, 7662)

[11010100000000000000001][01000111111000110101011] * 3524578 * (2, 1) (1, 558) (1, 1909) (1, 2047) (1, 3100) (1, 3206) (1, 3714) (1, 3860) (1, 3976) (1013, 4094) (1, 4206) (1, 4230) (1, 4876) (1, 5116) (1, 6282)

[10011100000000000000001][01000111111000110101011] * 3524578 * (1, 2) (1, 1089) (1, 1576) (1, 1808) (1, 2049) (1, 3108) (1, 3470) (1, 3954) (1012, 4098) (1, 4326) (1, 4428) (1, 4528) (1, 4596) (1, 5716) (1, 6478)

EXCERPT CYCLE STRUCTURE FOR DEGREE 18

[1001110111110000101][0000010010101101] * 46368 * (2, 1) (7, 73) (1775, 146) (1, 928) (1, 1553)

Results, facts and intuitions – XII

[1010101111110000101][0000010010101101] * 46368 * (2, 1) (7, 73) (1775, 146) (1, 964) (1, 1517)

[1111011111110000101][0000010010101101] * 46368 * (2, 1) (1, 468) (1, 510) (1, 511) (1, 516) (1, 655) (1, 680) (1, 814) (1, 958) (247, 1022) (1, 1310) (1, 1610) (1, 1676)

[1000111111110000101][0000010010101101] * 46368 * (1, 2) (1, 284) (1, 303) (1, 472) (1, 513) (1, 856) (1, 980) (246, 1026) (1, 1148) (1, 1156) (1, 1286) (1, 1324) (1, 1424)

[1100000000001000101][0000010010101101] * 46368 * (1, 2) (1, 346) (1, 378) (1, 433) (1, 513) (1, 650) (1, 664) (1, 920) (1, 974) (246, 1026) (1, 1388) (1, 1466) (1, 2014)

[1011100000001000101][0000010010101101] * 46368 * (1, 2) (1, 30) (1, 398) (1, 430) (1, 513) (1, 699) (1, 794) (1, 898) (246, 1026) (1, 1126) (1, 1586) (1, 1618) (1, 1654)

[1110010000001000101][0000010010101101] * 46368 * (2, 1) (1, 352) (1, 483) (1, 511) (1, 654) (1, 714) (1, 858) (1, 930) (1, 1008) (247, 1022) (1, 1038) (1, 1484) (1, 1676)

[1101010000001000101][0000010010101101] * 46368 * (1, 2) (1, 332) (1, 513) (1, 550) (1, 566) (1, 592) (1, 690) (1, 709) (246, 1026) (1, 1086) (1, 1464) (1, 1466) (1, 1778)

[1010110000001000101][0000010010101101] * 46368 * (1, 2) (1, 134) (1, 298) (1, 513) (1, 549) (1, 802) (1, 818) (1, 926) (247, 1026) (1, 1258) (1, 1570) (1, 1852)

[1100011000001000101][0000010010101101] * 46368 * (2, 1) (7, 73) (1775, 146) (1, 914) (1, 1567)

[1011111000001000101][0000010010101101] * 46368 * (2, 1) (7, 73) (1775, 146) (1, 338) (1, 2143)

EXCERPT CYCLE STRUCTURE FOR DEGREE 17

[11111000010001011][101]* 5 * (1, 131072)

[11000100010001011][101] * 5 * (2, 1) (2, 1558) (2, 18990) (2, 22959) (1, 44056)

[10100100010001011][101 * 5 * (2, 22005) (1, 87062)

[10010100010001011][101] * 5 * (2, 1) (1, 131070)

[10001100010001011][101] * 5 * (1, 3386) (2, 15736) (2, 48107)

[11011100010001011][101] * 5 * (2, 6020) (2, 20431) (1, 20498) (2, 28836)

Results, facts and intuitions – XIII

[10010010010010011][101] * 5 * (1, 131072)
[11110010010010011][101] * 5 * (2, 1) (1, 131070)
[11101010010010011][101] * 5 * (1, 27462) (2, 51805)
[11011010010010011][101] * 5 * (2, 16173) (1, 98726)
[11111110010010011][101] * 5 * (1, 131072)
[11000010010010011][101] * 5 * (1, 131072)
[11101001010010011][101] * 5 * (2, 1) (2, 15004) (1, 17462) (2, 41800)
[10111001010010011][101] * 5 * (2, 1) (2, 23208) (1, 84654)
[11100101010010011][101] * 5 * (1, 131072)
[10011101010010011][101] * 5 * (2, 1) (2, 21467) (1, 26762) (2, 30687)

CONJECTURE: Even degrees lead to many cycles with length mostly concentrated around $2^{n/2+1}$. Odd degrees lead to few long cycles, with a good proportion of them having only a giant.

Future work – I

(1) Clarifying the relation between the choice perturbation and irreducible modulus. This is to design (efficient) ciphers that could be useful not only for low-latent data. Also a better understanding of this relation is likely to give us insights on possible algebraic attacks.

(2) Characterizing the set $\mathcal{J}_d$ for a given $P(X) \in \mathbb{F}_2[X]$ with $1 \leq \deg P \leq d-1$. Have an algorithm to construct it, and then from which we could sample randomly. Connected to (1).

Future work – II

(**3**) Are the entries of the matrix for the first-order differences bounded by $4 \cdot 2^{-d}$ as $d \to \infty$? Markov chain stochastic analysis.

(**4**) Walsh spectra analysis with function approximation other identity, i.e., replace $a \cdot x$ in the previous formula by $a \cdot \rho(x)$, with ρ a permutation with quadratic boolean coordinate functions for instance. The coordinate boolean functions of ρ, i.e. $\rho = (\rho_0, \cdots, \rho_{d-1})$ could be obtained by considering $P_a(X)^{2^{k_1}} P_a(X)^{2^{k_2}} \pmod{Q}$ for some irreducible polynomial Q.

(**5**) Statistical analysis (local and global, mid-round and full-round) for different choices of metrics and measures of concentration. Different metrics can be used to assess different statistical properties over general random permutations, and often only asymptotic expressions for the null distributions are available. Some metrics on S_N are (next slide):

Future work – III

1. $\ell_1(\rho_1, \rho_2) = \sum_{j=0}^{N-1} |\sigma_1(j) - \sigma_2(j)|$ (Spearman footrule statistic)
2. $\ell_2(\rho_1, \rho_2) = \sum_{j=0}^{N-1} |\sigma_1(j) - \sigma_2(j)|^2$ (Spearman correlation statistic)
3. $\ell_\infty(\rho_1, \rho_2) = \max_{j \in \{0,\ldots,N-1\}} |\sigma_1(j) - \sigma_2(j)|$
4. $H(\rho_1, \rho_2) = |\{i \mid i \in \{0, \ldots, N-1\}, \sigma_1(i) \neq \sigma_2(i)\}|$ (Hamming distance)
5. $C(\rho_1, \rho_2) \stackrel{\text{def}}{=}$ the minimum number of transpositions needed to obtain ρ_2 from ρ_1 (Cayley distance)
6. $K(\rho_1, \rho_2) = |\{(i,j) \mid 0 \leq i, j \leq N-1, \sigma_1(i) < \sigma_2(j), \text{ and } \sigma_1(i) > \sigma_2(j)\}|$ (Kendall statistic)

Future work – IV

(**6**) Characterizing the structure of cycles for all degrees. Why for even degrees, are there many small cycles, and why for odd degrees, are there few very long cycles? Studying the distributions of cycles through mid-rounds or for a simpler start by studying linear extension for a given power of the form $2^d - 2^k - 1$.

(**7**) More important is to show that

$$\liminf_{d\to\infty} \frac{|\mathcal{J}_d|}{|\mathcal{I}_d|} > 0.$$

We recall that

$$|\mathcal{I}_d| = \frac{1}{d}\sum_{a|d} 2^a \mu(d/a).$$

The importance is such that we are not working on negligible subset of the symmetric group.

Future work – V

(**8**) The same as (**7**) restated for even degrees, i.e., with cycles's length concentrated around $2^{\frac{n}{2}+1}$.

NOTE: Showing (**7** or **8**) may be done possibly without a full characterization (**6**) using asymptotic complex analysis.

Remerciements–Acknowledgements

Thanks to the organizers to allow me to speak here. Thanks to Gilles Brassard (the crypt side) and Luc Devroye (cycle and statistical properties) for the discussions we had during my Ph.D.

mutation

Bibliography I

Bacher, Axel and Bodini, Olivier and Hwang, Hsien-Kuei and Tsai, Tsung-Hsi.
Generating random permutations by coin tossing: Classical algorithms, new analysis, and modern implementation.
ACM Trans. Algorithms, 13(2):24:1–24:43, February 2017.
ISSN 1549-6325.
doi: 10.1145/3009909.
URL http://doi.acm.org/10.1145/3009909.

Brassard, Gilles and Kannan, Sampath.
The generation of random permutations on the fly.
Inf. Process. Lett., 28(4):207–212, July 1988.
ISSN 0020-0190.
doi: 10.1016/0020-0190(88)90210-4.
URL
http://dx.doi.org/10.1016/0020-0190(88)90210-4.

Bibliography II


Carlet, Claude.
Boolean functions for cryptography and error correcting codes.
Technical report, Universités Paris 8 et Paris 13, CNRS, a.


Carlet, Claude.
Vectorial boolean functions for cryptography.
Technical report, Universités Paris 8 et Paris 13, CNRS, b.


Flajolet, Philippe and Odlyzko, Andrew M.
Random mapping statistics.
In Jean-Jacques Quisquater and Joos Vandewalle, editors, *Advances in Cryptology — EUROCRYPT '89: Workshop on the Theory and Application of Cryptographic Techniques Houthalen, Belgium, April 10–13, 1989 Proceedings*, pages 329–354, Berlin, Heidelberg, 1990. Springer Berlin Heidelberg. ISBN 978-3-540-46885-1.

Bibliography III

doi: 10.1007/3-540-46885-4_34.
URL https://doi.org/10.1007/3-540-46885-4_34.

Flajolet, Philippe and Sedgewick, Robert.
Analytic Combinatorics.
Cambridge University Press, New York, NY, USA, 1 edition, 2009.
ISBN 0521898064, 9780521898065.

Lidl, Rudolf and Niederreiter, Harold.
Finite Fields.
Number v. 20, pt. 1 in EBL-Schweitzer. Cambridge University Press, 1997.
ISBN 9780521392310.

Bibliography IV


Mullen, Gary L. and Panario, Daniel.
Handbook of Finite Fields.
Chapman & Hall/CRC, 1st edition, 2013.
ISBN 143987378X, 9781439873786.


Szpankowski, Wojciech.
Average Case Analysis of Algorithms on Sequences.
John Wiley & Sons, Inc., New York, NY, USA, 2001.
ISBN 047124063X.