Numerical Results on Boolean Functions with Applications in Cryptography

G. Leander

GRIM,
Universite Toulon, France.

leander@itsc.rub.de

2007

Outline

What is this about?

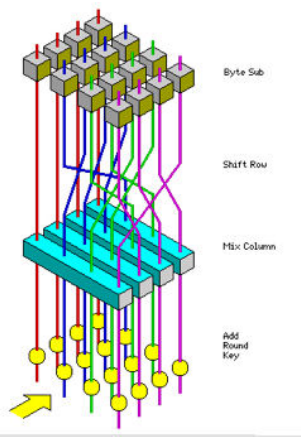
- Boolean functions play an important role in symmetric crypto.
- Many fundamental questions still open
  - What is the best nonlinearity for a balanced Boolean function in even dimension?
  - What is the best nonlinearity for an Sbox in even dimension?
  - Are there APN permutations?
- It is often a key tool to start with numerical experiments
- In this talk we focus on APN/AB functions.

Block Cipher

$$\begin{aligned} B : \mathbb{F}_2^{tn} \times \mathbb{F}_2^{tn} &\rightarrow \mathbb{F}_2^{tn} \\ B(M, K) &= C \end{aligned}$$

- A Block cipher encrypts a fixed number of bits.
- Usually iterated design
- A round consists of
  - A "substitution" part.
  - A linear "permutation" part.
  - Adding the round key.
- The only nonlinear part is the substitution part.
- The substitution part consists of Sboxes $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$:

Advanced Encryption Standard



Criteria for good Sboxes

- The Sbox is usually the only non-linear part of a Block cipher.
- It has to fulfil several conditions to make the cipher resistant against known attacks.
- In general it is not easy to find good Sboxes.
- No classification of good Sboxes is known.

In particular the Sbox should be chosen such that the cipher resists

- Linear Cryptanalysis
- Differential Cryptanalysis

Differential Cryptanalysis

- tries to trace the differences of message pairs through the encryption process.
- this should be difficult
- a measure for this is given by

Definition (Uniformity)

The uniformity of an Sbox is defined by

$$\mathrm{Diff}(S) = \max_{a \neq 0, b} |\{x \mid S(x) + S(x+a) = b\}|$$

APN Functions

Definition (APN Functions)

A function $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called almost perfect nonlinear (APN) if

$$\mathrm{Diff}(F) = 2$$

This means that for any $a \neq 0, b \in \mathbb{F}_2^n$ the equation

$$F(x) + F(x + a) = b$$

has either 2 or 0 solutions.

Remark

APN functions provide an optimal resistance against differential attacks.

APN functions

Until recently all APN known functions where equivalent to power functions

APN Power Functions

$$\begin{aligned} F : \mathbb{F}_{2^n} &\rightarrow \mathbb{F}_{2^n} \\ F(x) &= x^d \end{aligned}$$

for suitable exponents d.

This is strange: APN is an additive property only!

Task

Find other APN functions!

APN functions

Task

Find other APN functions!

This can be approached in two ways:

- Classify all APN functions for small dimensions.
- Find new infinite families of APN functions.

Both approaches have there own right.

Are there other APN functions

What does "other" mean?

Definition

Two functions F, G are called CCZ-equivalent if there exist an affine permutation L such that

$$L(\mathcal{G}_F) = \mathcal{G}_G$$

where $\mathcal{G}_F = \{(x, F(x)) \ : \ x \in F_2^n\}$ is the graph of a function.

Theorem

Let F, G be two CCZ-equivalent functions. F is APN iff G is APN.

So "other" means APN functions which are not equivalent to power functions.

Are there other APN functions

Edel, Kyureghyan and Pott found two APN functions that are CCZ-inequivalent to power functions

- $n = 10 : F(x) = x^3 + ux^{36}$
- $n = 12 : F(x) = x^3 + ux^{528}$

New Task

Can this idea be generalized?

The functions are:

- Binomials
- Quadratics

Infinite families

By generalizing the idea of quadratic binomials many classes where found:

- A family of APN functions when n is divisible by 3 but not by 9, Budagyan, Carlet, Felke, L.
- A family of APN functions when n is divisible by 4 but not by 8, Budagyan, Carlet, L.
- A family of APN functions when n is divisible by 2 but not by 4 by Bracken, Byrne, Markin, McGuire
- $x^3 + Tr(x^9)$, Budagyan, Carlet, L.

Infinite families

Remark

- This was conjectured after computer search.
- All these classes give quadratic APN functions only.
- The proof of the non-equivalence to power functions is not so nice.
- A nicer prove would be: These functions are CCZ not equivalent to any power function.

New Task

Find APN functions that are not equivalent to power functions and quadratic functions

This is a necessary condition for APN permutations in even dimension!

Classify APN functions in small dimension

Problem

Classify all APN functions in some fixed (small) dimension.

Example

For permutations in dimension $n = 5$ there are:

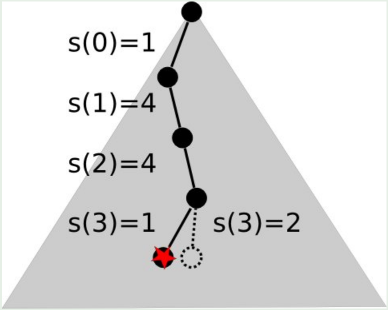
- $2^5! \approx 2.6 \cdot 10^{35}$ permutations
- $2.6 \cdot 10^{18}$ affine equivalence classes (Lorens 1964, dong Hou 2003)
- 5 classes of APN permutations

The results are due to Marcus Brinkmann.

APN Backtrack Search Example

First approach: use backtracking strategy.

Example



$$S(0) + S(0+1) = 5$$
$$S(2) + S(2+1) = 5$$

This is not efficient enough. There are 11082367891040769146880 $\approx 2^{76}$ APN functions in dim. 5.

Affine equivalence

Definition

Two functions F and G are affine equivalent if there exist two affine permutations L_1, L_2 such that $L_2 \circ F \circ L_1 = G$

Lemma

Let $F \sim_{af} G$ then F is APN iff G is APN. Furthermore $F \sim_{ccz} G$.

Idea

Search only for "smallest" APN functions up to affine equivalence

Affine equivalence

Key observation

It is possible to check if there exist an equivalent function which is smaller during backtracking!

Example

L_1	0	1	2	3	4	5	6	7
F	0	1	2	5	_	_	_	_
L_2	0	1	2	3	5	4	7	6
$L_2 \circ F \circ L_1$	0	1	2	4	_	_	_	_

Using this idea the classification of APN functions in dimension 4 and 5 can be computed.

Classification of APN functions for Dimension 4 and 5

Dimension 4

#	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	d°	EA	CCZ
1	0	0	0	1	0	2	4	7	0	4	6	3	8	14	10	13	2	x^3	can.
2	0	0	0	1	0	2	4	7	0	4	6	3	8	14	11	12	3	[1]	1

Dimension 5

#	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	$^\circ$	EA	CCZ
1	0	0	0	1	0	2	4	7	0	4	8	13	16	22	28	27	0	8	16	25	5	15	17	26	22	26	14	3	3	13	31	16	2	x^5	can.
2	0	0	0	1	0	2	4	7	0	4	8	13	16	22	28	27	0	8	16	25	5	15	17	26	27	23	3	14	14	0	18	29	2	x^3	can.
3	0	0	0	1	0	2	4	7	0	4	8	13	16	22	29	26	0	8	16	25	5	15	19	24	7	11	27	22	26	20	1	14	3	[1]	1
4	0	0	0	1	0	2	4	7	0	4	8	13	16	22	29	26	0	8	16	25	5	15	19	24	10	6	22	27	23	25	12	3	3	[1]	2
5	0	0	0	1	0	2	4	8	0	3	6	12	7	16	25	23	0	7	3	22	28	19	9	0	19	8	15	28	21	9	29	2	4	x^{15}	can.
6	0	0	0	1	0	2	4	8	0	3	6	16	8	21	26	29	0	5	12	27	20	6	31	16	7	31	8	22	9	26	17	11	3	x^{11}	2
7	0	0	0	1	0	2	4	8	0	3	6	16	8	21	26	29	0	6	15	24	18	3	17	30	2	29	14	20	25	13	9	23	3	x^7	1

[1] Budagyan, Carlet, Pott 2006.

More numerical results

Remarks and Further Results

- All APN functions are members of previously known infinite classes.
- For $n = 5$ this computation took about three weeks on one PC.
- For $n = 6$ this would take far too long.
- For $n = 6$ not every APN function is equivalent to power functions (Dillon).
- For $n = 6$ every APN function that can be represented as a polynomial with coefficients in $\mathbb{F}_2$ is equivalent to a power function.
- This is wrong in dimension 7: $x^3 + \mathrm{tr}(x^9)$. (Budaghyan, Carlet, L)

The optimal Sbox

Remember: An Sbox has to provide resistance against differential and linear attacks.

Linear Cryptanalysis

- tries to approximate the function by linear function
- this should be difficult
- a measure for this is given by

Definition (Linearity I)

The Linearity of an Sbox is defined by

$$\mathrm{Lin}(S) = \max_{a,b \neq 0} \left| \sum_x (-1)^{\langle b,S(x)\rangle + \langle a,x\rangle} \right|$$

The optimal Sbox

An Sbox has to provide resistance against differential and linear attacks.

Bounds

- It is known that $\mathrm{Lin}(F) \geq 2^{(n+1)/2}$.

Definition

Functions achieving these bounds are called Almost Bent.

AB functions also provide optimal resistance against differential attack

Theorem

If F is AB then F is APN.

Almost Bent functions

These functions exist when n is odd only.

- Now and for the rest of this talk n is odd.
- Which means that they do not play an important role as Sboxes in block ciphers.

Theorem

A function F is Almost Bent iff

$$\mathrm{spec}(F) = \{0, \pm 2^{(n+1)/2}\}$$

where

$$\mathrm{spec}(F) = \{\widehat{F}_b(a) \mid a, b \neq 0\}$$

and

$$\widehat{F}_b(a) = \sum_x (-1)^{\langle b, S(x)\rangle + \langle a, x\rangle}.$$

Known AB Power functions

Theorem

Let $F(x) = x^d$. Then F is AB if

- $d = 2^i + 1$, *where* $\gcd(i, n) = 1$ *(Gold)*
- $d = 4^i - 2^i + 1$, *where* $\gcd(i, n) = 1$ *(Kasami)*
- $d = 2^{2t} + 2^t - 1$ *where* $4t = -1 \bmod n$ *(Niho)*
- $d = 2^{(n-1)/2} + 3$ *(Welch)*

Conjecture (Dobbertin)

This list is complete.

What to do?

- As we do not see any chance to proof the Conjecture, we do not believe in it.
- Therefore we started to search for counterexamples.
- The Conjecture has been verified up to dimension 23.
- Dobbertin said he knows that it is true up to dimension 29.

Question

How did he check this???

Joint work with Philippe Langevin.

What is known?

Up to dimension 25 it is possible (but not easy) to compute the fourier transformation of all exponents.

- It seems impossible to do this up to dimension 29.
- So is there a better way?

Divisibility of Fourier Coefficients

Definition

Let d be an exponent with $\gcd(d, 2^n - 1) = 1$. Then we define the valuation of d as the largest power of 2 dividing all Fourier coefficients of $x \mapsto x^d$. I.e.

$$2^{\mathrm{val}(d)} | \widehat{F}(a),$$

and there exist an a such that

$$2^{\mathrm{val}(d)+1} \nmid \widehat{F}(a).$$

- If an exponent d is AB then $\mathrm{val}(d) = \frac{n+1}{2}$.
- The converse is false.

Divisibility of Fourier Coefficients

Using Stickelberger's congruences on Gauss sums it can be proved that

Theorem

$$\mathrm{val}(d) = \min_{1 \le j \le q-1} \mathrm{wt}(j) + \mathrm{wt}(-jd)$$

where $\mathrm{wt}(j)$ *is the* 2*-weight of the smallest non negative residue of* j *modulo* $2^n - 1$.

Does this help? Yes!

Divisibility of Fourier Coefficients

Does this help? Yes!

Corollary

All the exponents of the form $d = \frac{-r}{s}$ *where* $\mathrm{wt}(r) + \mathrm{wt}(s) \leq \frac{n-1}{2}$ *are no AB exponents.*

Proof.

For such a d, we have $\mathrm{wt}(s) + \mathrm{wt}(-sd) = \mathrm{wt}(s) + \mathrm{wt}(r) < \frac{n+1}{2}$. Therefore

$$\mathrm{val}(d) < \frac{n+1}{2}$$

□

Sieving Algorithm

Sieving Algorithm

For (r, s) with

$$\mathrm{wt}(s) \leq \mathrm{wt}(r), \quad \mathrm{wt}(s) + \mathrm{wt}(r) \leq \frac{n-1}{2}.$$

mark $d = \frac{-r}{s}$ as a bad exponent.

- All exponents which are not marked have valuation greater then $\frac{n-1}{2}$.
- Only the exponents which are not marked as bad are candidates for AB exponents.
- The work factor of sieving is about $2^{1.2n}$.
- This is very small compared to $n2^{2n}$.

Sieving Algorithm

There where only a very few exponents with valuation greater or equal $(n+1)/2$. Indeed

Sieving Results

Only a few invertible exponents with valuation greater or equal $\frac{n+1}{2}$ are found.

- 69 for dimension 27.
- 80 for dimension 29.
- 93 for dimension 31.

Step II

Compute the spectra of these few exponents. This is easy

Results

This is what we get after approximately one week of computation:

Fact

Dobbertin's conjecture is correct up to $n \leq 33$.

Generalized Kasami-Welch Exponents

Nearly all the invertible d of valuation greater or equal to $\frac{n+1}{2}$ have the form $\frac{2^{tk}+1}{2^k+1}$.

Three exceptional cases

There are three exponents for each odd n that we conjecture to have the following spectra $S = \{0, \pm 2^{(m+1)/2}, \pm 2^{(m+3)/2}\}$

Master Plan

A way to prove the conjecture:

- Prove that Generalized Kasami-Welch Exponents are never AB
- Prove that the three sporadic cases are never AB
- Compute the size of the set

$$\left\{ \frac{A}{B} \mid \mathrm{wt}(A) + \mathrm{wt}(B) \leq \frac{n-1}{2} \right\}$$

Master Plan

A way to prove the conjecture:

- Prove the conjecture stated above Difficult!
- Prove that the three sporadic cases are never AB Difficult!
- Compute the size of the set

$$\left\{ \frac{A}{B} \mid \mathrm{wt}(A) + \mathrm{wt}(B) \leq \frac{n-1}{2} \right\}$$

VERY Difficult!

Further Research

- Find new non-quadratic APN functions.
- Proof the conjecture about Generalized Kasami-Welch Exponents
- Get more numerical results for APN power functions.