A Study of APN Functions in Dimension 7 using Antiderivatives

Lukas Kölsch

University of South Florida

(joint work with Alexandr Polujan)

Block ciphers and their round functions

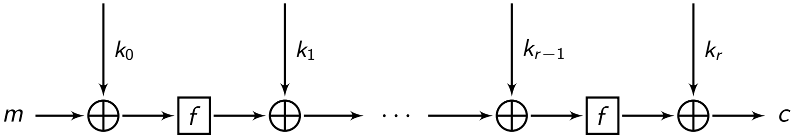

Figure: An iterated (key-alternating) block cipher with r rounds and subkeys k_i that encrypts a plaintext m into a ciphertext c

The round function of a substitution permuation network (SPN)

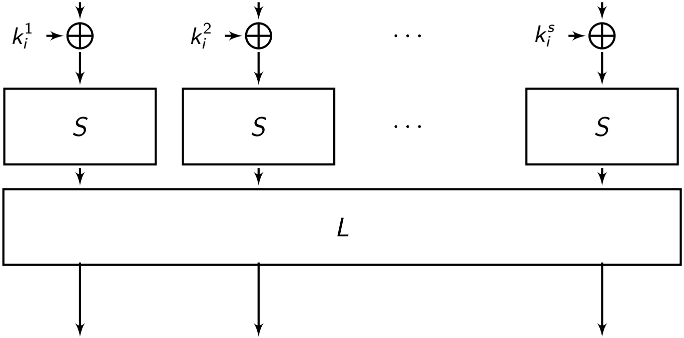

Figure: A high-level view of one round of an SPN with an S-box S, linear layer L and round key k_i

Differential attacks on SPNs

So an SPN consists of three steps that are repeated:

1. Key addition
2. S-box
3. Linear layer

Important: Differences are invariant under key addition and differences can be tracked through the linear layer:

$L(x+a) - L(x) = L(x+a-x) = L(a).$

So analysis can be broken down to the S-box level!

S-boxes in SPNs need to be bijective to allow decryption.

Differential uniformity

Definition (Differential Uniformity)

The differential uniformity δ_F of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as:

$$\delta_F = \max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^n \colon F(x+a)+F(x)=b\}|.$$

The differential uniformity tells us if there are statistical biases in how differences propagate through a function.

The S-box should have low differential uniformity!

It is easy to see that $F(x+a)+F(x) = F((x+a)+a)+F(x)$, so solutions always come in pairs.

APN functions

Definition

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called Almost Perfect Nonlinear (APN) if its differential uniformity δ_F is 2 (the lowest possible).

To defend optimally against differential attacks in an SPN one is thus interested in bijective APN functions/APN permutations.

Goal

Construct APN permutations $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$.

APN permutations

Constructing infinite families of APN functions is quite difficult. Thousands of examples have been constructed by computer in low dimensions $n = 7, n = 8, \ldots$.

All known APN functions are equivalent to either monomials $F(x) = x^d$ for some d or *quadratic*, i.e., $F(x + a) + F(x)$ is $\mathbb{F}_2$-affine for all $a \neq 0$... except one sporadic counterexample!

If n is even then neither monomials nor quadratic functions can be permutations.

Edel-Pott function

Goal

Construct APN functions that are inequivalent to quadratic functions and monomials.

The only known such APN function is the Edel-Pott function defined in 6 variables, found using the switching construction and computer searches (Edel, Pott, 2008).

So far, this function has not been generalized.

Degree of a (vectorial) Boolean function

Boolean functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$:

$f(x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n + 1$

Degree 1 function, or *affine* function

Degree of a (vectorial) Boolean function

Boolean functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$:

$f(x_1,\ldots,x_n) = x_1 + x_2 + \cdots + x_n + 1$

Degree 1 function, or *affine* function

$f(x_1,\ldots,x_n) = x_1 + x_1x_2 + x_3 + \cdots + x_n$

Degree 2 function, or *quadratic* function

Degree of a (vectorial) Boolean function

Boolean functions $f: \mathbb{F}_2^n \to \mathbb{F}_2$:

$f(x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n + 1$

Degree 1 function, or *affine* function

$f(x_1, \ldots, x_n) = x_1 + x_1 x_2 + x_3 + \cdots + x_n$

Degree 2 function, or *quadratic* function

$f(x_1, \ldots, x_n) = x_1 x_2 x_4 + x_1 x_2 + x_3 + \cdots + x_n + 1$

Degree 3 function, or *cubic* function

Degree of a (vectorial) Boolean function

Boolean functions $f\colon \mathbb{F}_2^n \to \mathbb{F}_2$:

$f(x_1, \ldots, x_n) = x_1 + x_2 + \cdots + x_n + 1$

Degree 1 function, or *affine* function

$f(x_1, \ldots, x_n) = x_1 + x_1x_2 + x_3 + \cdots + x_n$

Degree 2 function, or *quadratic* function

$f(x_1, \ldots, x_n) = x_1x_2x_4 + x_1x_2 + x_3 + \cdots + x_n + 1$

Degree 3 function, or *cubic* function

Degree of $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is maximum degree of its coordinate functions.

Discrete derivatives

Definition

Let $F \colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ be a function. Then, the mapping $\Delta_v F(x) = F(x) + F(x+v)$ is called the *derivative* of F in direction $v \in \mathbb{F}_2^n$. For for a set $S = \{v_1, \dots, v_n\}$, we also define $\Delta_S F(x) = \Delta_{v_1}(\Delta_{v_2}, \dots, (\Delta_{v_n} F(x)), \dots,)$.

The degree of the derivative is always smaller than the degree of the original function.

Differential uniformity via discrete derivative

Definition (Differential Uniformity)

The differential uniformity δ_F of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as:

$$\delta_F = \max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^n \colon F(x+a) + F(x) = b\}|.$$

Definition (Differential Uniformity, equivalent formulation)

The differential uniformity δ_F of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is defined as:

$$\delta_F = \max_{a \in \mathbb{F}_2^{n*}, b \in \mathbb{F}_2^n} |\{x \in \mathbb{F}_2^n \colon \Delta_a F(x) = b\}|.$$

Fast points

Sometimes (though rarely) the degree of a (vectorial) Boolean function decreases by *more than one* when taking the derivative in a specific direction.

Definition (Fast points)

We say that $v \in \mathbb{F}_2^n$ is a fast point of a function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ if $\deg(\Delta_v F(x)) < \deg(F(x)) - 1$.

Peculiar properties of the Edel-Pott function

The Edel-Pott function is *cubic*.

It is however *almost quadratic* in the sense that many discrete derivatives are *linear*.

In other words: It has many fast points!

This was not a goal of the original construction by Edel and Pott! It was observed by Suder in 2019.

Cubic APN functions via fast points

Goal

Construct other cubic APN functions with many fast points.

Theorem

The set of all fast points of $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ forms an $\mathbb{F}_2$-vector space.

Edel-Pott function: $F\colon \mathbb{F}_2^6 \to \mathbb{F}_2^6$, three dimensional fast point space.

Construction idea

We want to construct a cubic APN function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Decompose $\mathbb{F}_2^n = V \oplus W$.

Set $F = G + H$, where G is cubic but $\Delta_v G = 0$ for all $v \in V$ and H is a quadratic APN function.

Then F has fast point space V.

We need conditions on G such that F remains APN.

The condition

Theorem (Kölsch, Polujan, Suder)

Let $\mathbb{F}_2^n = V \oplus W$ and $F = G + H$ be a function on $\mathbb{F}_2^n$ where G is such that $\Delta_v G(x) = 0$ for any $v \in V$ and H is an APN function. Then F is APN if and only if

$$\{\Delta_{w,w'} G(x) \colon x \in \mathbb{F}_2^n\} \cap$$
$$\{\Delta_{w+v,w'+v'} H(x) \colon v, v' \in V, x \in \mathbb{F}_2^n\} = \varnothing$$

for any $w, w' \in W$.

Using the theorem

$\mathbb{F}_2^n = V \oplus W$.

G cubic with $\Delta_v G(x) = 0$ for $v \in V$.

H quadratic APN.

Condition: For all $w, w' \in W$:

$$\{\Delta_{w,w'} G(x) \colon x \in \mathbb{F}_2^n\} \cap \{\Delta_{w+v,w'+v'} H(x) \colon v, v' \in V, x \in \mathbb{F}_2^n\} = \varnothing.$$

Fix n, V, W, H. Compute admissible values for $\Delta_{w,w'} G(x)$ and reconstruct G from the second derivatives.

Integrating vectorial Boolean functions

Compute admissible values for $\Delta_{w,w'}G(x)$ and reconstruct G from the second derivatives.

This is not always possible, and also not easy. An algorithm to construct these "integrals" had to be found, based on previous work by Suder (2017).

Results

For $n = 6$ we were able to do successfully do this process for 9 "starting" APN functions, where $\dim(V) = 3$ — all equivalent to Edel-Pott.

For $n = 7$, $\dim(V) = 3$, this process does not yield any solutions, for any starting APN function, and any choice of V, W.

Current and future work

For $n = 7$, $\dim(V) = 4$,

$n = 8$ is the big interesting case! $\dim(V) = 3$, $\dim(V) = 4$?

There are thousands of quadratic APN functions known in dimension 8...
Computational difficulties.

Theoretical work to examine when this approach can/cannot work.

Thank you for your attention!