New classes of 8-bit permutations based on a butterfly structure

Denis Fomin

May 28, 2018

- Let $\mathbb{F}_{2^n}$ be a finite field of size 2^n.
- S-Box S is any nonlinear function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$.
- In this work we will build a nonlinear bijective S-Box $\mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$.
- Properties of nonlinear function is a set of measures of resistance against known methods of cryptanalysis.

Definition

The Walsh-Hadamard Transform (WHT) of an S-Box S $W_S(a,b)$ and fixed values $a \in \mathbb{F}_{2^n}$, $b \in \mathbb{F}_{2^m}$ is defined as:

$$W_S(a,b) = \sum_{x \in \mathbb{F}_{2^n}} (-1)^{\langle a,x \rangle + \langle b,S(x) \rangle}.$$

Definition

The nonlinearity N_S of an S-Box S is a measure that is defined as follows:

$$N_S = 2^{n-1} - \frac{1}{2} \max_{a,b \neq 0} |W_S(a,b)|.$$

Definition

The algebraic degree $\deg(S)$ *of the S-Box* S *is the minimum among all maximum numbers of variables of the terms in the algebraic normal form (ANF) of* $\langle a, S(x)\rangle$ *for all possible values* x *and* $a \neq 0$*:*

$$\deg(S) = \min_{a \in \mathbb{F}_{2^m}/0} \deg\left(\langle a, S(x)\rangle\right).$$

Definition

For a given $a \in \mathbb{F}_{2^m}/0, b \in \mathbb{F}_{2^m}$ *we consider*

$$\delta_S(a,b) = \#\left\{x \in \mathbb{F}_{2_n} | S(x+a) + S(x) = b\right\}.$$

The differential uniformity of an S-Box S *is*

$$\delta_S = \max_{a \in \mathbb{F}_{2^m}/0, b} \delta_S(a,b).$$

There are several well known ways of building S-Boxes $S : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$:

- Pseudorandom generation. Differential uniformity and nonlinearity $\delta_S \leq 8$, $N_S \leq 100$. But complex interpolation polynomial and a huge amount of such a permutation.

There are several well known ways of building S-Boxes
$S : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$:

- Pseudorandom generation. Differential uniformity and nonlinearity $\delta_S \leq 8$, $N_S \leq 100$. But complex interpolation polynomial and a huge amount of such a permutation.
- Heuristic methods. Differential uniformity and nonlinearity up to $\delta_S = 6$, $N_S = 104$. Complex interpolation polynomial, huge amount of such a permutation but hard to find.

There are several well known ways of building S-Boxes $S : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$:

- Pseudorandom generation. Differential uniformity and nonlinearity $\delta_S \leq 8$, $N_S \leq 100$. But complex interpolation polynomial and a huge amount of such a permutation.
- Heuristic methods. Differential uniformity and nonlinearity up to $\delta_S = 6$, $N_S = 104$. Complex interpolation polynomial, huge amount of such a permutation but hard to find.
- Monomial permutations. As example – finite field inversion with best known differential uniformity and nonlinearity: $\delta_S = 4$, $N_S \leq 112$. Simple interpolation polynomial, not many permutations. But finite inversion has a weakens: there exists systems of quadratic equations (graph algebraic immunity is equal to 2).

There is one more way of building S-Boxes $S : \mathbb{F}_{2^n} \mapsto \mathbb{F}_{2^n}$: build it from smaller ones. There are a lot of reasons to build S-Box from smaller ones:

- good software implementation with precomputed tables,
- better bit-sliced implementation,
- implementation for lightweight cryptography with smaller tables or lower gate count,
- efficient masking in hardware,
- secure against cache timing attacks than those relying on general 8-bit S-boxes, which require table lookups in memory,
- generally has cryptographic properties like random permutation has

There are known a lot of ways to build large S-Box from smaller one. Several block ciphers that used the idea:

- Feistel network (CRYPTON v0.5, Zorro)
- Misty network (Mysty, Kasumi, Fantomas)
- SPN network (Iceberg, Khazard, Crypton v1.0)
- other constructions (Whirpool, BelT).

In this work we will study how to build 8-bit S-box using a *butterfly structure* that was suggested in [1]. Let $x_i, y_i, x_o, y_o \in \mathbb{F}_{2^m}$.

1. y_o depends on x_i, y_i according to the equation: $y_o = F_1(x_i, y_i)$,
2. y_i depends on x_o, y_o according to the equation: $y_i = F_2(x_o, y_o)$.

Proposition

Function $F : \mathbb{F}_{2^{2m}} \mapsto \mathbb{F}_{2^{2m}}$ with input $x_i \| y_i$ and output $x_o \| y_o$ is a permutation if and only if for every fixed value $y \in \mathbb{F}_{2^m}$ functions $F_1(x, y)$ and $F_2(x, y)$ are permutations. We will call F as a generalized butterfly structure.

[1] Lo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem

Definition

A nonlinear function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called a bent function when its nonlinearity is equal to $2^{n-1} - 2^{n/2-1}$.

Let $n = 2m$, $x, y \in \mathbb{F}_{2^m}$. The MaioranaMcFarland bent function:

$$f(x, y) = \pi(x) \cdot l(y) + f(x),$$

where $\pi : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a permutation, $l : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a linear permutation and $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a function.

[2] Lo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem

Definition

A nonlinear function $S : \mathbb{F}_2^n \mapsto \mathbb{F}_2^m$ is called a bent function when its nonlinearity is equal to $2^{n-1} - 2^{n/2-1}$.

Let $n = 2m$, $x, y \in \mathbb{F}_{2^m}$. The MaioranaMcFarland bent function:

$$f(x, y) = \pi(x) \cdot l(y) + f(x),$$

where $\pi : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a permutation, $l : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a linear permutation and $f : \mathbb{F}_{2^m} \mapsto \mathbb{F}_{2^m}$ is a function.

In [[2]] there was revealed that only one known 6-bit APN permutation is CCZ equivalent to the butterfly structure and that in our terms F_1, F_2 are bent functions.

[2] Lo Perrin, Aleksei Udovenko, and Alex Biryukov. Cryptanalysis of a theorem: Decomposing the only known solution to the big APN problem

These functions can be based on MaioranaMcFarland construction:

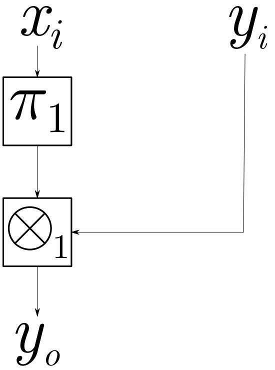
$$F'_i(x,y) = \begin{cases} \pi_i(x)\cdot l_i(y) + f_i(x), \; l_i(y) \neq 0; \\ \widehat{\pi}_i(x), \; l_i(y) = 0. \end{cases}, \qquad (1)$$

$$F''_i(x,y) = \begin{cases} \pi_i(y)\cdot l_i(x) + f_i(y), \; \pi_i(y) \neq 0; \\ \widehat{\pi}_i(x), \; \pi_i(y) = 0. \end{cases}, \qquad (2)$$

where $\pi_i, \widehat{\pi}_i$ are m-bit permutations, l_i is an m-bit linear permutation and f_i is an m-bit function.

Proposition

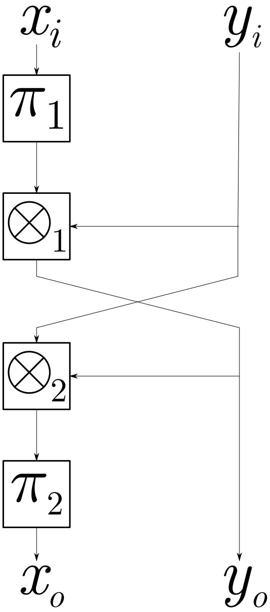
The function $F_i'(x,y)$ from equation 1 is a bijective function for any fixed value y if and only if $f(x)$ is a constant function.



$$F_i'(x,y) = \begin{cases} \pi_i(x)\cdot y, & y \neq 0; \\ \widehat{\pi}_i(x), & y = 0. \end{cases} .$$

Let us denote

$$x \otimes_i y = \begin{cases} x\cdot y, & y \neq 0; \\ \widehat{\pi}_i'(x), & y = 0. \end{cases}$$



1. We've found 32 constructions that provide us the way to construct permutations with semi-optimal cryptographic properties $N_S = 108$, $\delta_S = 6$, $deg(S) = 7$;
2. There are all these constructions: $\pi_1(x)$ is any monomial function, $\pi_2(x) = x^\alpha$, $\alpha \in \{7, 11, 13, 14\}$.
3. Semi-optimal cryptographic properties could be obtained even for non monomial permutation $\pi_1(x)$ and $\pi_2(x)$.

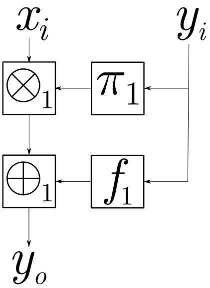


Fig.: Construction "B"

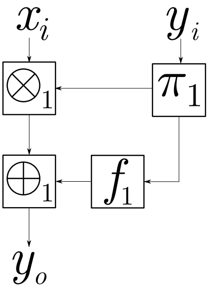


Fig.: Construction "C"

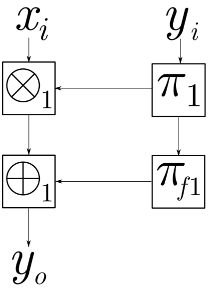
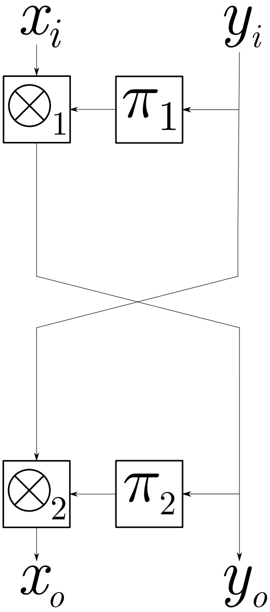


Fig.: Construction "D"



1. We've found 4 constructions that provide us the way to construct permutations with semi-optimal cryptographic properties $N_S = 108$, $\delta_S = 6$, $deg(S) = 7$:
    1. $\pi_1(x) = x$, $\pi_2(x) = x^{13}$,
    2. $\pi_1(x) = x^2$, $\pi_2(x) = x^{14}$,
    3. $\pi_1(x) = x^4$, $\pi_2(x) = x^7$,
    4. $\pi_1(x) = x^8$, $\pi_2(x) = x^{11}$.

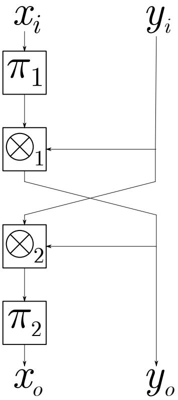


Fig.: Permutation based on two "A" constructions

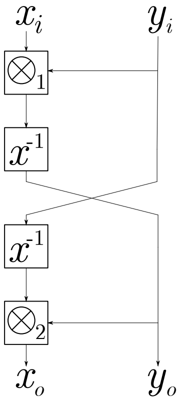


Fig.: Permutation published in [3]

[3] Reynier Antonio de la Cruz Jiménez. Generation of 8-bit s-boxes having almost optimal cryptographic properties using smaller 4-bit s-boxes and finite field multiplication.

We've generalized that construction on fig. 5 and replace x^{-1} by monomial function π_1 and π_2.

- for the following 12 constructions almost optimal cryptographic properties are obtained: differential uniformity is up to 6 and the nonlinearity is up to 108;
- for 4 constructions the differential uniformity is up to 8 and the nonlinearity is up to 104;
- for 8 constructions the differential uniformity is up to 8 and the nonlinearity is up to 100.

[4] Reynier Antonio de la Cruz Jiménez. Generation of 8-bit s-boxes having almost optimal cryptographic properties using smaller 4-bit s-boxes and finite field multiplication.

- How many possibilities to choose F_1 and F_2 to construct a permutation with good cryptographic properties?
- How many possibilities to choose π_i and f_i in all these constructions?
- Can we choose permutations $\widehat{\pi}_i$ for our constructions to obtain good cryptographic properties without a search algorithm?
- Can we find a construction that will be an involution?
- Can we use mixed construction for butterfly structure (as example permutation based on "A" and "B" constructions) to find a permutation with rather good cryptographic properties?
- How to find permutations with good hardware, FPGA or bit-sliced implementations?

- This work has presented some new constructions to build permutation $\mathbb{F}_{2^{2m}} \mapsto \mathbb{F}_{2^{2m}}$, $m = 4$ based on butterfly structure.
- There are at least 36 new constructions for permutations that have the nonlinearity 108, differential uniformity 6, algebraic degree 7 and the value of graph algebraic immunity 3.
- Some other constructions based on butterfly structure have been found recently.
- There are a lot of open questions

Thank you for your attention

Questions?