Equivalences of S-boxes

Lukas Kölsch

University of Rostock, Germany

17.08.2021

Intro: Block ciphers

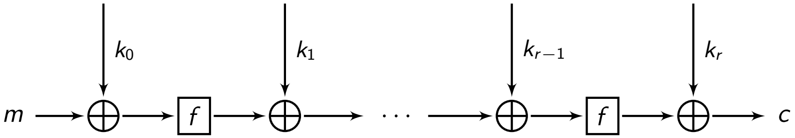
Block ciphers: Message $m \in \mathbb{F}_2^m$ is divided into blocks of the same size n.

Most block ciphers are iterated:

Key: k divided into subkeys k_i.

A simple round function $f : \mathbb{F}_2^n \to \mathbb{F}_2^n$.

The message m is turned into a cipher text c by repeated applications of the round function.

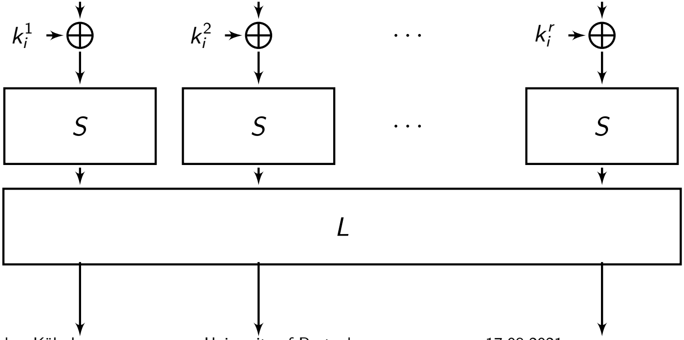


How do we choose the round function?

Common choice is: *Substitution-Permutation Network (SPN)*:

An SPN consists of a S(ubsitution)-box $S\colon \mathbb{F}_2^r \to \mathbb{F}_2^r$ and a linear permutation L.

The choice of the bijective S-box is mainly responsible for "nonlinearity" of the cipher!



Differential Attack

A differential attack on a cipher exploits the propagation of differences in an encryption function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$:

$$m_1 + m_2 = a \quad \text{and} \quad F(m_1) + F(m_2) = b$$

The number of solutions should be uniform (i.e. low) for all $(a, b) \in \mathbb{F}_2^n \setminus \{0\} \times \mathbb{F}_2^n$.

Differential Uniformity

Definition (Differential Uniformity)

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ has differential uniformity d, if

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

An S-box should have low differential uniformity.

Since $F(x+a) + F(x) = b$ if and only if $F((x+a)+a) + F(x+a) = b$, the differential uniformity is always even.

Definition (Almost Perfect Nonlinear functions)

A function $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ is called Almost Perfect Nonlinear (APN) if it has differential uniformity 2.

APN functions

APN functions are *very* rare.

All theoretical constructions use finite fields: $\mathbb{F}_{2^n} \cong \mathbb{F}_2^n$.

Example

The function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by $x \mapsto x^3$ is APN.

Proof.

$$F(x) + F(x+a) = x^3 + (x+a)^3 = ax^2 + a^2x + a^3 = b$$

is a quadratic equation and has thus at most 2 solutions for $(a, b) \in \mathbb{F}_{2^n}^* \times \mathbb{F}_{2^n}$. □

Problem: The cube function is bijective only if n is odd.

The AES S-box

The S-box that AES uses is the inverse function.

Example (The AES S-box: The inverse function)

The AES S-box on n bits is $\mathrm{Inv}\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ defined by

$$\mathrm{Inv}(x) = x^{-1}.$$

(Notation: $0^{-1} = 0$).

The inverse function is bijective, *but* it is APN only if n is odd.

AES uses the S-box on 8 bits: It is not APN (but has differential uniformity 4).

The AES S-box

Question

Why does AES not use a bijective APN function on $\mathbb{F}_2^8$?

The AES S-box

Question

Why does AES not use a bijective APN function on $\mathbb{F}_2^8$?

There are no known bijective APN functions on $\mathbb{F}_2^8$.

Question (The big APN question)

Are there bijective APN functions on $\mathbb{F}_2^n$ for n even and n>6.

$n = 4$: There are no bijective APN functions (Hou, 2004)

$n = 6$: An NSA research group headed by Dillon presented a bijective APN function (2009).

Equivalences of functions

CCZ-equivalence is the most general notion of equivalence that leaves the differential uniformity invariant.

Definition (CCZ-equivalence)

Two functions $F_1, F_2\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called CCZ-equivalent if there is an linear, bijective function $\mathcal{L}\colon \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}^2$ such that

$$\mathcal{L}(G_{F_1}) = G_{F_2},$$

where $G_F = \{(x, F(x)) \subseteq \mathbb{F}_{2^n}^2 \colon x \in \mathbb{F}_{2^n}\}$ is the graph of F.

Dillon's idea: Take a known APN function that is not bijective, and find a bijective function in its CCZ-equivalence class.

Led to the first example of a bijective APN function on $\mathbb{F}_2^6$.

Equivalences of functions

There are two interesting questions:

Question

Find all bijective functions inside the equivalence class of APN functions (or, more generally, of functions with good cryptographic properties).

Question

How can we decide if different APN functions are equivalent or not? Can we count the (known) APN functions up to equivalence?

Equivalences of functions

Question

Find all bijective functions inside the equivalence class of functions with good cryptographic properties.

Equivalences of functions

Question

Find all bijective functions inside the equivalence class of functions with good cryptographic properties.

Question

Find all bijective functions inside the equivalence class of the inverse function $\mathrm{Inv}(x) = x^{-1}$*!*

These functions are good candidates for S-boxes.

A criterion

Notation: $L_1(x), L_2(x)$ are $\mathbb{F}_2$-linear functions.

Result (Göloğlu, K., Kyureghyan, Perrin, 2020)

A complete classification of all bijective functions $L_1(F(x)) + L_2(x)$ is in many cases enough to find all bijective mappings that are CCZ-equivalent to $F(x)$.

Inverse function: Need to classify bijective functions of the form $L_1(x^{-1}) + L_2(x)$ over $\mathbb{F}_{2^n}$!

A criterion

Theorem (K., 2021)

$F(x) = L_1(x^{-1}) + L_2(x)$ is bijective on $\mathbb{F}_{2^n}$ for $n \geq 5$ if and only if $L_1 = 0$ and L_2 is a bijection or $L_2 = 0$ and L_1 is a bijection.

What made this problem difficult:

Linear functions preserve additive structure but destroy multiplicative structure.

The function $x \mapsto x^{-1}$ preserves multiplicative structure but destroys additive structure.

High level view of the proof

Assume $L_1(x^{-1}) + L_2(x)$ is bijective on $\mathbb{F}_{2^n}$

$\Downarrow$

Then $K_n(L_1^*(x)L_2^*(x)) = 0$ for all $x \in \mathbb{F}_{2^n}$,

where L_1^*, L_2^* are the adjoint functions of L_1, L_2 and K_n is the

Kloosterman sum $K_n(a) = \sum_{x\in\mathbb{F}_{2^n}}(-1)^{\mathrm{Tr}(x^{-1}+ax)}$

$\Downarrow$

Exploit a dyadic approximation of Kloosterman sums using quadratic forms

Details: Kölsch, L. On CCZ-Equivalence of the inverse function. *IEEE Transactions on Information Theory*, 2021. Or on the arxiv.

The result

Question

Find all bijections inside the equivalence class of the inverse function $\mathrm{Inv}(x)$.

Theorem (K., 2021)

The bijections that are CCZ-equivalent to the inverse function $\mathrm{Inv}(x)$ *are precisely the functions* $F = L_1 \circ \mathrm{Inv} \circ L_2$ *where* L_1, L_2 *are bijective linear functions.*

Counting APN functions

Question

How can we decide if different APN functions are equivalent or not? Can we count the (known) APN functions up to equivalence?

Theorem (Göloğlu, K., 2021+)

Let $F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ *be defined as*

$$F_{i,a,B}(x,y) = (x^{2^i+1} + By^{2^i+1}, x^{2^{i+n}}y + (a/B)xy^{2^{i+n}}),$$

where $n \equiv 2 \pmod 4$, $\gcd(i,n) = 1$, $a \in \mathbb{F}_{2^{n/2}}^*$, $B \in \mathbb{F}_{2^n}^*$ *is a non-cube,* $B^{2^i+2^{i+n}} \neq a^{2^i+1}$. *Then* F *is APN.*

Which choices of i, a, B yield equivalent APN functions?

How large is the family?

The automorphism group

Definition (CCZ-equivalence)

Two functions $F_1, F_2\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ are called CCZ-equivalent if there is an linear, bijective function $\mathcal{L}\colon \mathbb{F}_{2^n}^2 \to \mathbb{F}_{2^n}^2$ such that

$$\mathcal{L}(G_{F_1}) = G_{F_2},$$

where $G_F = \{(x, F(x)) \subseteq \mathbb{F}_{2^n}^2 : x \in \mathbb{F}_{2^n}\}$ is the graph of F.

Definition (Automorphism group)

The automorphism group $\mathrm{Aut}(F)$ of a function $F\colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ is defined by

$$\mathrm{Aut}(F) = \{\mathcal{L} \in \mathrm{GL}(\mathbb{F}_{2^n}^2)\colon \mathcal{L}(G_F) = G_F\}.$$

Lemma

Assume $F_1, F_2 \colon \mathbb{F}_{2^n} \to \mathbb{F}_{2^n}$ *are CCZ-equivalent. Then* $\mathrm{Aut}(F_1)$ *and* $\mathrm{Aut}(F_2)$ *are conjugate in* $\mathrm{GL}(\mathbb{F}_{2^n}^2)$.

Problem: Determining the automorphism group is also very hard!

There is often a way to use the lemma without knowing the automorphism group!

Show that F_1, F_2 are CCZ-inequivalent - in five simple steps!

- Find subgroups $G_1 \leq \mathrm{Aut}(F_1)$, $G_2 \leq \mathrm{Aut}(F_2)$ with $|G_1| = |G_2|$.
- Choose a suitable prime p and Sylow p-groups $S_1 \leq G_1$, $S_2 \leq G_2$.
- Prove that S_1, S_2 are also Sylow p-groups of $\mathrm{Aut}(F_1), \mathrm{Aut}(F_2)$ (might be hard)
- Show that S_1, S_2 are not conjugate in $\mathrm{GL}(\mathbb{F}_{2^n}^2)$.
- Then $\mathrm{Aut}(F_1)$ and $\mathrm{Aut}(F_2)$ are also not conjugate in $\mathrm{GL}(\mathbb{F}_{2^n}^2)$.

Technique first used by Yoshiara (2015), Dempwolff (2016) just for power functions.

Generalization to more general classes of functions (Göloğlu, K., 2021+)

soon to be found on the arxiv...

Counting..

Theorem (Göloğlu, K., 2021+)

Let $F : \mathbb{F}_{2^n} \times \mathbb{F}_{2^n} \to \mathbb{F}_{2^n} \times \mathbb{F}_{2^n}$ *be defined as*

$$F_{i,a,B}(x, y) = (x^{2^i+1} + By^{2^i+1}, x^{2^{i+n}} y + (a/B)xy^{2^{i+n}}),$$

where $n \equiv 2 \pmod 4$, $\gcd(i, n) = 1$, $a \in \mathbb{F}^*_{2^{n/2}}$, $B \in \mathbb{F}^*_{2^n}$ *is a non-cube,* $B^{2^i+2^{i+n}} \neq a^{2^i+1}$*. Then F is APN.*

The number of inequivalent APN functions in this family is $\approx 2^{n/2}$*.*

Only the second family which (provably) contains exponentially (in n) many inequivalent functions!

Other applications

CCZ-equivalence of functions is structurally similar to:

- Equivalence of certain codes
- Isomorphisms of certain projective planes
- Isotopisms of semifields (see Göloğlu, K. 2021+ on the arxiv soon)
- ...

The technique might generalize!

Thank you for your attention!