UNIVERSITÀ DEGLI STUDI DI TRENTO
LABORATORIO DI MATEMATICA INDUSTRIALE E CRITTOGRAFIA

# On weakly APN functions and 4-bit S-Boxes

Claudio Fontanari, Valentina Pulice, Anna Rimoldi, Massimiliano Sala

arXiv:1102.3882v2

10 marzo 2011

This work is in my Master's thesis, supervised by M. Sala.

We thank TELSY SPA for they graceful support.

# Cryptosystems

*"A secrecy system is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are supposed reversible (non-singular) so that unique deciphering is possible when the key is known."*[1]

**Formally**

A cryptosystem is a tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \Phi, \Psi)$, where

$$\mathcal{M} = \{plaintext\} \quad \mathcal{C} = \{ciphertext\} \quad \mathcal{K} = \{key\}$$
$$\Phi = \{\phi_K : \mathcal{M} \to \mathcal{C}\} \quad \Psi = \{\psi_K = (\phi_K)^{-1} : \mathcal{C} \to \mathcal{M}\}$$

[1] Shannon, C.E., "Communication Theory of Secrecy System"

# Cryptosystems

*"A secrecy system is defined abstractly as a set of transformations of one space (the set of possible messages) into a second space (the set of possible cryptograms). Each particular transformation of the set corresponds to enciphering with a particular key. The transformations are supposed reversible (non-singular) so that unique deciphering is possible when the key is known."*[1]

**Formally**

A cryptosystem is a tuple $(\mathcal{M}, \mathcal{C}, \mathcal{K}, \Phi, \Psi)$, where

$$\mathcal{M} = \{plaintext\} \quad \mathcal{C} = \{ciphertext\} \quad \mathcal{K} = \{key\}$$
$$\Phi = \{\phi_k : \mathcal{M} \to \mathcal{C}\} \quad \Psi = \{\psi_k = (\phi_k)^{-1} : \mathcal{C} \to \mathcal{M}\}$$

[1] Shannon, C.E., "Communication Theory of Secrecy System"

# Block ciphers

Let $\mathcal{C} = \mathcal{M} = (\mathbb{F}_q)^n$ and $\mathcal{K} = (\mathbb{F}_q)^r$ for some $n, r \in \mathbb{N}$

**Algebraic block cipher**

$$\phi : (\mathbb{F}_q)^n \times (\mathbb{F}_q)^r \rightarrow (\mathbb{F}_q)^n$$

is an *algebraic block cipher* if $\forall k \in (\mathbb{F}_q)^r$,

$$\phi_k : (\mathbb{F}_q)^n \rightarrow (\mathbb{F}_q)^n, \quad \text{such that} \quad \phi_k(x) = \phi(x, k)$$

is a permutation of $(\mathbb{F}_q)^n$.

Here we focus on the binary case $q = 2$.

Let $\mathcal{M} = V = V_1 \oplus \cdots \oplus V_s$, $\dim(V_i) = m$, $\mathcal{S}_V = \mathrm{Sym}(V)$

If $\gamma \in \mathcal{S}_V$ is such that $v\gamma = v_1\gamma_1 \oplus \cdots \oplus v_s\gamma_s \ \forall v \in V$ then

- $\gamma$ is a bricklayer transformation or a *parallel S-box*
- $\gamma_i$ is a *brick* or a S-box

**$\lambda$ proper**

$\lambda \in GL(V)$ is proper if no vector subspace $W = \bigoplus_{i \in I}(V_i) \subset V$, with $I \neq \emptyset, \{1, \ldots, s\}$, is invariant under the action of $\lambda$.

**Translation Based Block Cipher**

An algebraic block cipher $\phi$ is *translation based* if:

- $\phi_k = \tau_k^1 \circ \cdots \circ \tau_k^N$, and every round $\tau_k^h = \gamma\lambda\sigma_{\bar{k}}$;
- for at least one round we have that $\lambda$ is proper and the function $\mathcal{K} \to V$, $k \mapsto \bar{k}$, is surjective.

# Translation Based Ciphers

Let $\mathcal{M} = V = V_1 \oplus \cdots \oplus V_s$, $\dim(V_i) = m$, $\mathcal{S}_V = \mathrm{Sym}(V)$

If $\gamma \in \mathcal{S}_V$ is such that $v\gamma = v_1\gamma_1 \oplus \cdots \oplus v_s\gamma_s \ \forall v \in V$ then

- $\gamma$ is a bricklayer transformation or a *parallel S-box*
- $\gamma_i$ is a *brick* or a S-box

**$\lambda$ proper**

$\lambda \in GL(V)$ is proper if no vector subspace $W = \bigoplus_{i \in I}(V_i) \subset V$, with $I \neq \emptyset, \{1, \ldots, s\}$, is invariant under the action of $\lambda$.

**Translation Based Block Cipher**

An algebraic block cipher $\phi$ is *translation based* if:

- $\phi_K = \tau_k^1 \circ \cdots \circ \tau_k^N$, and every round $\tau_k^h = \gamma\lambda\sigma_{\bar{k}}$;
- for at least one round we have that $\lambda$ is proper and the function $\mathcal{K} \to V$, $k \mapsto \bar{k}$, is surjective.

# Translation Based Ciphers

Let $\mathcal{M} = V = V_1 \oplus \cdots \oplus V_s$, $\dim(V_i) = m$, $\mathcal{S}_V = \mathrm{Sym}(V)$

If $\gamma \in \mathcal{S}_V$ is such that $v\gamma = v_1\gamma_1 \oplus \cdots \oplus v_s\gamma_s \ \forall v \in V$ then

- $\gamma$ is a bricklayer transformation or a *parallel S-box*
- $\gamma_i$ is a *brick* or a S-box

**$\lambda$ proper**

$\lambda \in GL(V)$ is proper if no vector subspace $W = \bigoplus_{i \in I}(V_i) \subset V$, with $I \neq \emptyset, \{1, \ldots, s\}$, is invariant under the action of $\lambda$.

**Translation Based Block Cipher**

An algebraic block cipher $\phi$ is *translation based* if:

- $\phi_k = \tau_k^1 \circ \cdots \circ \tau_k^N$, and every round $\tau_k^h = \gamma\lambda\sigma_{\bar{k}}$;
- for at least one round we have that $\lambda$ is proper and the function $\mathcal{K} \to V$, $k \mapsto \bar{k}$, is surjective.

# Primitivity of the permutation group

$$\Pi = \{\phi_k\}_{k \in \mathcal{K}}\,, \quad \Gamma = \Gamma(\phi) = \langle \phi_k \rangle_{k \in \mathcal{K}} = \langle \tau_k^{(1)} \circ \cdots \circ \tau_k^{(N)} \rangle_{k \in \mathcal{K}}\,, \quad \Gamma < \mathcal{S}_V$$

In order to avoid weakness of a given cipher it is desiderable that the permutation group is primitive.

### Block System

Let $H$ be a subgroup of $\mathcal{S}_V$, $H < \mathcal{S}_V$, and $\mathcal{B} = \{X_1, \dots, X_N\} \subset 2^V$ a partition of $V$. We say that $\mathcal{B}$ is a (non-trivial) *block system* for $H$ if

$$\forall f \in H,\ \forall i\, \exists j \text{ t.c. } f(X_i) = X_j\,.$$

### Primitive action

Let $\mathcal{B} = \{X_1, \dots, X_N\} \subset 2^V$, $H < \mathcal{S}_V$. We say that $H$ is *primitive* in its action on $V$ if

1. there are no non-trivial block systems;
2. the action of $H$ is *transitive*, i.e. $\forall (x, y) \in V^2$ exists $f \in H$ such that $f(x) = y$.

# Primitivity of the permutation group

$$\Pi = \{\phi_k\}_{k\in\mathcal{K}}\,, \quad \Gamma = \Gamma(\phi) = \langle \phi_k \rangle_{k\in\mathcal{K}} = \langle \tau_k^{(1)} \circ \cdots \circ \tau_k^{(N)} \rangle_{k\in\mathcal{K}}\,, \quad \Gamma < \mathcal{S}_V$$

In order to avoid weakness of a given cipher it is desiderable that the permutation group is primitive.

**Block System**

Let $H$ be a subgroup of $\mathcal{S}_V$, $H < \mathcal{S}_V$, and $\mathcal{B} = \{X_1, \ldots, X_N\} \subset 2^V$ a partition of $V$. We say that $\mathcal{B}$ is a (non-trivial) *block system* for $H$ if

$$\forall f \in H,\ \forall i\, \exists j \text{ t.c. } f(X_i) = X_j\,.$$

**Primitive action**

Let $\mathcal{B} = \{X_1, \ldots, X_N\} \subset 2^V$, $H < \mathcal{S}_V$. We say that $H$ is *primitive* in its action on $V$ if

1. there are no non-trivial block systems;
2. the action of $H$ is *transitive*, i.e. $\forall (x, y) \in V^2$ exists $f \in H$ such that $f(x) = y$.

# Primitivity of the permutation group

$$\Pi = \{\phi_k\}_{k\in\mathcal{K}}\,, \quad \Gamma = \Gamma(\phi) = \langle\phi_k\rangle_{k\in\mathcal{K}} = \langle\tau_k^{(1)}\circ\cdots\circ\tau_k^{(N)}\rangle_{k\in\mathcal{K}}\,, \quad \Gamma < \mathcal{S}_V$$

In order to avoid weakness of a given cipher it is desiderable that the permutation group is primitive.

**Block System**

Let $H$ be a subgroup of $\mathcal{S}_V$, $H < \mathcal{S}_V$, and $\mathcal{B} = \{X_1, \ldots, X_N\} \subset 2^V$ a partition of $V$. We say that $\mathcal{B}$ is a (non-trivial) *block system* for $H$ if

$$\forall f \in H,\ \forall i\, \exists j\, \text{t.c.}\ \ f(X_i) = X_j\,.$$

**Primitive action**

Let $\mathcal{B} = \{X_1, \ldots, X_N\} \subset 2^V$, $H < \mathcal{S}_V$. We say that $H$ is *primitive* in its action on $V$ if

1. there are no non-trivial block systems;
2. the action of $H$ is *transitive*, i.e. $\forall (x, y) \in V^2$ exists $f \in H$ such that $f(x) = y$.

# Primitivity of the permutation group

$$\Pi = \{\phi_k\}_{k \in \mathcal{K}}\,, \quad \Gamma = \Gamma(\phi) = \langle \phi_k \rangle_{k \in \mathcal{K}} = \langle \tau_k^{(1)} \circ \cdots \circ \tau_k^{(N)} \rangle_{k \in \mathcal{K}}\,, \quad \Gamma < \mathcal{S}_V$$

In order to avoid weakness of a given cipher it is desiderable that the permutation group is primitive.

## Block System

Let $H$ be a subgroup of $\mathcal{S}_V$, $H < \mathcal{S}_V$, and $\mathcal{B} = \{X_1, \ldots, X_N\} \subset 2^V$ a partition of $V$. We say that $\mathcal{B}$ is a (non-trivial) *block system* for $H$ if

$$\forall f \in H,\ \forall i \, \exists j \,\text{t.c.}\ \ f(X_i) = X_j\,.$$

## Primitive action

Let $\mathcal{B} = \{X_1, \ldots, X_N\} \subset 2^V$, $H < \mathcal{S}_V$. We say that $H$ is *primitive* in its action on $V$ if

1. there are no non-trivial block systems;
2. the action of $H$ is *transitive*, i.e. $\forall (x, y) \in V^2$ exists $f \in H$ such that $f(x) = y$.

# Primitivity of the group generated by the round functions

Unfortunately, the knowledge of $\Gamma(\phi)$ is out of reach for the most important ciphers, so we consider a larger group:

**Group generated by the round functions**

$$\Gamma_\infty = \langle \Gamma_h \rangle_{1 \le h \le N} = \langle \tau_{k_1}^{(1)}, \ldots, \tau_{k_N}^{(N)} \rangle_{k_1,\ldots,k_N \in \mathcal{K}}$$

where for every round $h$ we set $\Gamma_h = \langle \tau_k^{(h)} \rangle_{k \in \mathcal{K}}$ , $\quad \Gamma_h < \mathcal{S}_V$.

We have $\Gamma \le \Gamma_\infty$ and $\Gamma_h \le \Gamma_\infty$, hence

| $\Gamma_\infty$ | $\Longrightarrow$ | $\Gamma$ |
|---|---|---|
| imprimitive | | imprimitive |
| primitive | | primitive<br>imprimitive |

# Primitivity of the group generated by the round functions

Unfortunately, the knowledge of $\Gamma(\phi)$ is out of reach for the most important ciphers, so we consider a larger group:

**Group generated by the round functions**

$$\Gamma_\infty = \langle \Gamma_h \rangle_{1 \le h \le N} = \langle \tau_{k_1}^{(1)}, \ldots, \tau_{k_N}^{(N)} \rangle_{k_1, \ldots, k_N \in \mathcal{K}}$$

where for every round $h$ we set $\Gamma_h = \langle \tau_k^{(h)} \rangle_{k \in \mathcal{K}}$ , $\quad \Gamma_h < \mathcal{S}_V$.

We have $\Gamma \le \Gamma_\infty$ and $\Gamma_h \le \Gamma_\infty$, hence

| $\Gamma_\infty$ | $\Longrightarrow$ | $\Gamma$ |
|---|---|---|
| imprimitive | | imprimitive |
| primitive | | primitive<br>imprimitive |

# Differential uniformity

The primitivity of $\Gamma_\infty$ depends on the properties of the S-boxes $\gamma_i$ and $\lambda$. Since each S-box $\gamma_i$ can be seen as vectorial Boolean function $f : (\mathbb{F}_2)^m \rightarrow (\mathbb{F}_2)^m$, we introduce some properties of the v.B.f.'s

$\forall u \in (\mathbb{F}_2)^m$

$$\hat{f}_u : \begin{array}{ccc} (\mathbb{F}_2)^m & \longrightarrow & (\mathbb{F}_2)^m \\ x & \longmapsto & f(x) + f(x+u) \end{array}$$

**$\delta$ uniformity of $f$**

$f$ is $\delta$*-uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$ and $\forall v \in (\mathbb{F}_2)^m$

$$|\{x \in (\mathbb{F}_2)^m : \hat{f}_u(x) = v\}| \leq \delta\,.$$

- $\downarrow \delta \uparrow$ security
- $\delta \geq 2$
- If $\delta = 2$ then $f$ is an APN function
- There are no APN functions for $m = 4$

The primitivity of $\Gamma_\infty$ depends on the properties of the S-boxes $\gamma_i$ and $\lambda$. Since each S-box $\gamma_i$ can be seen as vectorial Boolean function $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$, we introduce some properties of the v.B.f.'s

$\forall u \in (\mathbb{F}_2)^m$

$$\hat{f}_u : \begin{array}{ccc} (\mathbb{F}_2)^m & \longrightarrow & (\mathbb{F}_2)^m \\ x & \longmapsto & f(x) + f(x+u) \end{array}$$

**$\delta$ uniformity of $f$**

$f$ is *$\delta$-uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$ and $\forall v \in (\mathbb{F}_2)^m$

$$|\{x \in (\mathbb{F}_2)^m : \hat{f}_u(x) = v\}| \leq \delta\,.$$

- $\downarrow \delta \uparrow$ security
- $\delta \geq 2$
- If $\delta = 2$ then $f$ is an APN function
- There are no APN functions for $m = 4$

# Differential uniformity

The primitivity of $\Gamma_\infty$ depends on the properties of the S-boxes $\gamma_i$ and $\lambda$. Since each S-box $\gamma_i$ can be seen as vectorial Boolean function $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$, we introduce some properties of the v.B.f.'s

$\forall u \in (\mathbb{F}_2)^m$

$$\hat{f}_u : \begin{array}{ccc} (\mathbb{F}_2)^m & \longrightarrow & (\mathbb{F}_2)^m \\ x & \longmapsto & f(x) + f(x+u) \end{array}$$

**$\delta$ uniformity of $f$**

$f$ is $\delta$-*uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$ and $\forall v \in (\mathbb{F}_2)^m$

$$|\{x \in (\mathbb{F}_2)^m : \hat{f}_u(x) = v\}| \leq \delta\,.$$

- $\downarrow \delta \uparrow$ security
- $\delta \geq 2$
- If $\delta = 2$ then $f$ is an APN function
- There are no APN functions for $m = 4$

# Weakly $\delta$-uniformity and strongly $l$-invariant

W.l.o.g., we consider B.f. $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ such that $f(0) = 0$.

**weakly $\delta$-uniform**

$\forall m \geq 2$, $\delta \geq 2$, $f$ is *weakly $\delta$-uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$,

$$|\mathrm{Im}(\hat{f}_u)| > \frac{2^{m-1}}{\delta}.$$

- $\downarrow \delta \implies \uparrow$ security
- If $\delta = 2$ then $f$ is a weakly APN function.

If $f$ is differential $\delta$-uniform, then it is weakly $\delta$-uniform.

**strongly $l$-anti-invariant**

$f$ is *strongly $l$-anti-invariant*, if $\forall V, W \leq (\mathbb{F}_2)^m$ such that $f(V) = W$ we have

- either $\dim(V) = \dim(W) < m - l$,
- or $V = W = (\mathbb{F}_2)^m$.

The largest subspace invariant under $f$ has codimension strictly greater than $l$.

# Weakly $\delta$-uniformity and strongly $l$-invariant

W.l.o.g., we consider B.f. $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ such that $f(0) = 0$.

**weakly $\delta$-uniform**

$\forall m \geq 2$, $\delta \geq 2$, $f$ is *weakly $\delta$-uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$,

$$|\mathrm{Im}(\hat{f}_u)| > \frac{2^{m-1}}{\delta}.$$

- $\downarrow \delta \implies \uparrow$ security
- If $\delta = 2$ then $f$ is a weakly APN function.

If $f$ is differential $\delta$-uniform, then it is weakly $\delta$-uniform.

**strongly $l$-anti-invariant**

$f$ is *strongly $l$-anti-invariant*, if $\forall V, W \leq (\mathbb{F}_2)^m$ such that $f(V) = W$ we have

- either $\dim(V) = \dim(W) < m - l$,
- or $V = W = (\mathbb{F}_2)^m$.

The largest subspace invariant under $f$ has codimension strictly greater than $l$.

# Weakly $\delta$-uniformity and strongly $l$-invariant

W.l.o.g., we consider B.f. $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ such that $f(0) = 0$.

**weakly $\delta$-uniform**

$\forall m \geq 2$, $\delta \geq 2$, $f$ is *weakly $\delta$-uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$,

$$|\text{Im}(\hat{f}_u)| > \frac{2^{m-1}}{\delta}.$$

- $\downarrow \delta \implies \uparrow$ security
- If $\delta = 2$ then $f$ is a weakly APN function.

If $f$ is differential $\delta$-uniform, then it is weakly $\delta$-uniform.

**strongly $l$-anti-invariant**

$f$ is *strongly $l$-anti-invariant*, if $\forall V, W \leq (\mathbb{F}_2)^m$ such that $f(V) = W$ we have

- either $\dim(V) = \dim(W) < m - l$,
- or $V = W = (\mathbb{F}_2)^m$.

The largest subspace invariant under $f$ has codimension strictly greater than $l$.

# Weakly $\delta$-uniformity and strongly $l$-invariant

W.l.o.g., we consider B.f. $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ such that $f(0) = 0$.

**weakly $\delta$-uniform**

$\forall m \geq 2$, $\delta \geq 2$, $f$ is *weakly $\delta$-uniform* if $\forall u \in (\mathbb{F}_2)^m \setminus \{0\}$,

$$|\mathrm{Im}(\hat{f}_u)| > \frac{2^{m-1}}{\delta}.$$

- $\downarrow \delta \implies \uparrow$ security
- If $\delta = 2$ then $f$ is a weakly APN function.

If $f$ is differential $\delta$-uniform, then it is weakly $\delta$-uniform.

**strongly $l$-anti-invariant**

$f$ is *strongly $l$-anti-invariant*, if $\forall V, W \leq (\mathbb{F}_2)^m$ such that $f(V) = W$ we have

- either $\dim(V) = \dim(W) < m - l$,
- or $V = W = (\mathbb{F}_2)^m$.

The largest subspace invariant under $f$ has codimension strictly greater than $l$.

**Theorem**

Let $\phi$ be a tb cipher, $h$ a proper round, $G = \Gamma_h(\phi)$ and $1 \leq r \leq m/2$. If every brick (i.e. every S-box) of $\gamma$ is:

1. weakly $2^r$-uniform *and*
2. strongly $r$-anti-invariant,

then $G$ is primitive and hence $\Gamma_\infty(\phi)$ is primitive.

In the case $m = 4$ we have only two possibilities:

a. $r = 1 \implies f$ *weakly APN* and *strongly* 1*-anti invariant*,

b. $r = 2 \implies f$ *weakly* 4*-uniform* and *strongly* 2*-anti invariant*

Actually, we will show that for 4-uniform functions case *b.* is a sub-case of *a.*

**Theorem**

Let $\phi$ be a tb cipher, $h$ a proper round, $G = \Gamma_h(\phi)$ and $1 \leq r \leq m/2$. If every brick (i.e. every S-box) of $\gamma$ is:

1. weakly $2^r$-uniform *and*
2. strongly $r$-anti-invariant,

then $G$ is primitive and hence $\Gamma_\infty(\phi)$ is primitive.

In the case $m = 4$ we have only two possibilities:

a. $r = 1 \implies f$ *weakly APN* and *strongly* 1*-anti invariant*,

b. $r = 2 \implies f$ *weakly* 4*-uniform* and *strongly* 2*-anti invariant*

Actually, we will show that for 4-uniform functions case *b.* is a sub-case of *a.*

**Theorem**

Let $\phi$ be a tb cipher, $h$ a proper round, $G = \Gamma_h(\phi)$ and $1 \leq r \leq m/2$. If every brick (i.e. every S-box) of $\gamma$ is:

1. weakly $2^r$-uniform *and*
2. strongly $r$-anti-invariant,

then $G$ is primitive and hence $\Gamma_\infty(\phi)$ is primitive.

In the case $m = 4$ we have only two possibilities:

a. $r = 1 \implies f$ *weakly APN* and *strongly* 1*-anti invariant*,

b. $r = 2 \implies f$ *weakly* 4*-uniform* and *strongly* 2*-anti invariant*

Actually, we will show that for 4-uniform functions case *b.* is a sub-case of *a*.

# Case *b.* implies case *a.*

**Proposition**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\overset{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \ \ \forall y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u + x\}$ for some $x$

$\Longrightarrow$
- $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*
- $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x + u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u + x\})$ is a 2-*dimensional vector subspace.*

But this contradicts (ii)!

# Case *b.* implies case *a.*

**Proposition**

Let $f : (\mathbb{F}_2)^4 \rightarrow (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\stackrel{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \;\; \forall\, y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u+x\}$ for some $x$

$\Longrightarrow$ ▶ $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*

▶ $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x+u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u+x\})$ is a 2-*dimensional vector subspace.*

But this contradicts (ii)!

# Case *b.* implies case *a.*

**Proposition**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\overset{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \ \ \forall\, y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u + x\}$ for some $x$

$\Longrightarrow$
- $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*
- $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x + u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u + x\})$ is a 2-*dimensional vector subspace.*

But this contradicts (ii)! □

**Proposition**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\stackrel{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \ \forall y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u + x\}$ for some $x$

$\Longrightarrow$
- $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*
- $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x + u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u + x\})$ is a 2-*dimensional vector subspace.*

But this contradicts (ii)!

# Case *b.* implies case *a.*

**Proposition**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\overset{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \;\; \forall\, y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u + x\}$ for some $x$

$\Longrightarrow$
- $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*
- $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x + u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u + x\})$ is a 2-*dimensional vector subspace.*

But this contradicts (ii)! □

# Case *b.* implies case *a.*

**Proposition**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\overset{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \ \ \forall y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u + x\}$ for some $x$

$\Longrightarrow$
- $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*
- $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x + u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u + x\})$ is a 2-*dimensional vector subspace*.

But this contradicts (ii)! □

# Case *b.* implies case *a.*

**Proposition**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ be a Boolean function such that

(i) $f$ is 4-uniform

(ii) $f$ is strongly 2-anti-invariant.

Then $f$ is weakly APN.

By contradiction, assume $|\mathrm{Im}(\hat{f}_u)| \leq 4$

$\overset{(i)}{\Longrightarrow} |\hat{f}_u^{-1}(y)| = 4 \ \forall y \in \mathrm{Im}(\hat{f}_u)$

$\Longrightarrow \hat{f}_u^{-1}(f(u)) = \{0, u, x, u + x\}$ for some $x$

$\Longrightarrow$
- $\hat{f}_u^{-1}(f(u))$ is a 2-*dimensional vector subspace*
- $\hat{f}_u(x) = \hat{f}_u(u)$

$\Longrightarrow f(x + u) = f(u) - f(x)$

$\Longrightarrow f(\{0, u, x, u + x\})$ is a 2-*dimensional vector subspace*.

But this contradicts (ii)! □

# Notation

We relate weakly APN functions $f : (\mathbb{F}_2)^m \rightarrow (\mathbb{F}_2)^m$ to the following values:

**Number of degree $i$ components of $f$**

$$n_i(f) = |\{v \in (\mathbb{F}_2)^m \setminus \{0\} : \deg(< f, v >) = i\}|$$

**Number of degree 0 components of $\hat{f}_u$**

$$\hat{n}(f) = \max_{u \in (\mathbb{F}_2)^m \setminus \{0\}} |\{v \in (\mathbb{F}_2)^m \setminus \{0\} : \deg(< \hat{f}_u, v >) = 0\}|$$

# Notation

We relate weakly APN functions $f : (\mathbb{F}_2)^m \to (\mathbb{F}_2)^m$ to the following values:

**Number of degree $i$ components of $f$**

$$n_i(f) = |\{v \in (\mathbb{F}_2)^m \setminus \{0\} : \deg(< f, v >) = i\}|$$

**Number of degree 0 components of $\hat{f}_u$**

$$\hat{n}(f) = \max_{u \in (\mathbb{F}_2)^m \setminus \{0\}} |\{v \in (\mathbb{F}_2)^m \setminus \{0\} : \deg(< \hat{f}_u, v >) = 0\}|$$

# Main result

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

**Remark: The converse does not hold**

Indeed, we have explicit counterexamples to the converse of both statement 1 and statement 2.

# Main result

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

**Remark: The converse does not hold**

Indeed, we have explicit counterexamples to the converse of both statement 1 and statement 2.

# Proof

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

Let $f = (f_1, f_2, f_3, f_4)$ with $f_i : (\mathbb{F}_2)^4 \to \mathbb{F}_2$.

By contradiction, assume that $< \hat{f}_u, v_1 >$ and $< \hat{f}_u, v_2 >$ are constant for some $u, v_1 \neq v_2 \in (\mathbb{F}_2)^4 \setminus \{0\}$.

linear transformation
$v_1 \to (1,0,0,0)$
$v_2 \to (0,1,0,0)$

$\Longrightarrow$

w.l.o.g.
$(\hat{f}_u)_1 = (\hat{f}_1)_u$ constant
$(\hat{f}_u)_2 = (\hat{f}_2)_u$ constant

It follows that $|\mathrm{Im}(\hat{f}_u)| \leq 4$ and $f$ is not weakly APN, contradiction.

# Proof

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

Let $f = (f_1, f_2, f_3, f_4)$ with $f_i : (\mathbb{F}_2)^4 \to \mathbb{F}_2$.

By contradiction, assume that $< \hat{f}_u, v_1 >$ and $< \hat{f}_u, v_2 >$ are constant for some $u, v_1 \neq v_2 \in (\mathbb{F}_2)^4 \setminus \{0\}$.

linear transformation $v_1 \to (1,0,0,0)$ $v_2 \to (0,1,0,0)$ $\Longrightarrow$ w.l.o.g. $(\hat{f}_u)_1 = (\hat{f}_1)_u$ constant $(\hat{f}_u)_2 = (\hat{f}_2)_u$ constant

It follows that $|\mathrm{Im}(\hat{f}_u)| \leq 4$ and $f$ is not weakly APN, contradiction.

# Proof

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

Let $f = (f_1, f_2, f_3, f_4)$ with $f_i : (\mathbb{F}_2)^4 \to \mathbb{F}_2$.

By contradiction, assume that $< \hat{f}_u, v_1 >$ and $< \hat{f}_u, v_2 >$ are constant for some $u, v_1 \neq v_2 \in (\mathbb{F}_2)^4 \setminus \{0\}$.

| linear transformation | | w.l.o.g. |
|---|---|---|
| $v_1 \to (1,0,0,0)$ | $\Longrightarrow$ | $(\hat{f}_u)_1 = (\hat{f}_1)_u$ constant |
| $v_2 \to (0,1,0,0)$ | | $(\hat{f}_u)_2 = (\hat{f}_2)_u$ constant |

It follows that $|\mathrm{Im}(\hat{f}_u)| \leq 4$ and $f$ is not weakly APN, contradiction.

# Proof

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

Let $f = (f_1, f_2, f_3, f_4)$ with $f_i : (\mathbb{F}_2)^4 \to \mathbb{F}_2$.

By contradiction, assume that $< \hat{f}_u, v_1 >$ and $< \hat{f}_u, v_2 >$ are constant for some $u, v_1 \neq v_2 \in (\mathbb{F}_2)^4 \setminus \{0\}$.

| linear transformation | | w.l.o.g. |
|---|---|---|
| $v_1 \to (1,0,0,0)$ | $\Longrightarrow$ | $(\hat{f}_u)_1 = (\hat{f}_1)_u$ constant |
| $v_2 \to (0,1,0,0)$ | | $(\hat{f}_u)_2 = (\hat{f}_2)_u$ constant |

It follows that $|\mathrm{Im}(\hat{f}_u)| \leq 4$ and $f$ is not weakly APN, contradiction.

□

# Proof

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

Let $(\mathbb{F}_2)^4 = \{x_1, \ldots, x_{16}\}$ and let $M = (m_{ij}) \in (\mathbb{F}_2)^{4\times 16}$ with $m_{ij} := (\hat{f}_u)_i(x_j)$

$$M = \begin{pmatrix} (\hat{f}_u)_1(x_1) & (\hat{f}_u)_1(x_2) & \ldots & (\hat{f}_u)_1(x_{16}) \\ (\hat{f}_u)_2(x_1) & (\hat{f}_u)_2(x_2) & \ldots & (\hat{f}_u)_2(x_{16}) \\ (\hat{f}_u)_3(x_1) & (\hat{f}_u)_3(x_2) & \ldots & (\hat{f}_u)_3(x_{16}) \\ (\hat{f}_u)_4(x_1) & (\hat{f}_u)_4(x_2) & \ldots & (\hat{f}_u)_4(x_{16}) \end{pmatrix}$$

**Theorem**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ a v.B.f.

1. if $f$ is weakly APN, then $\hat{n}(f) \leq 1$
2. if $\hat{n}(f) = 0$, then $f$ is weakly APN.

Let $(\mathbb{F}_2)^4 = \{x_1, \dots, x_{16}\}$ and let $M = (m_{ij}) \in (\mathbb{F}_2)^{4\times 16}$ with $m_{ij} := (\hat{f}_u)_i(x_j)$

$$M = \begin{pmatrix} (\hat{f}_u)_1(x_1) & (\hat{f}_u)_1(x_2) & \dots & (\hat{f}_u)_1(x_{16}) \\ (\hat{f}_u)_2(x_1) & (\hat{f}_u)_2(x_2) & \dots & (\hat{f}_u)_2(x_{16}) \\ (\hat{f}_u)_3(x_1) & (\hat{f}_u)_3(x_2) & \dots & (\hat{f}_u)_3(x_{16}) \\ (\hat{f}_u)_4(x_1) & (\hat{f}_u)_4(x_2) & \dots & (\hat{f}_u)_4(x_{16}) \end{pmatrix}$$

# Proof

By contradiction, assume that $M$ has only $n = 4$ distinct columns (the case $n \leq 3$ is easier!), say the first 4 columns, and let $M' \in (\mathbb{F}_2)^{4\times 4}$ be the corresponding submatrix:

$$M' = \begin{pmatrix} (\hat{f}_u)_1(x_1) & (\hat{f}_u)_1(x_2) & (\hat{f}_u)_1(x_3) & (\hat{f}_u)_1(x_4) \\ (\hat{f}_u)_2(x_1) & (\hat{f}_u)_2(x_2) & (\hat{f}_u)_2(x_3) & (\hat{f}_u)_2(x_4) \\ (\hat{f}_u)_3(x_1) & (\hat{f}_u)_3(x_2) & (\hat{f}_u)_3(x_3) & (\hat{f}_u)_3(x_4) \\ (\hat{f}_u)_4(x_1) & (\hat{f}_u)_4(x_2) & (\hat{f}_u)_4(x_3) & (\hat{f}_u)_4(x_4) \end{pmatrix}$$

If $M'$ has rank $\rho = 4$ (the case $\rho \leq 3$ is easier!), then

$$\begin{aligned} (1,1,1,1) \quad = \quad & a\left((\hat{f}_u)_1(x_1), (\hat{f}_u)_1(x_2), (\hat{f}_u)_1(x_3), (\hat{f}_u)_1(x_4)\right) + \\ & b\left((\hat{f}_u)_2(x_1), (\hat{f}_u)_2(x_2), (\hat{f}_u)_2(x_3), (\hat{f}_u)_2(x_4)\right) + \\ & c\left((\hat{f}_u)_3(x_1), (\hat{f}_u)_3(x_2), (\hat{f}_u)_3(x_3), (\hat{f}_u)_3(x_4)\right) + \\ & d\left((\hat{f}_u)_4(x_1), (\hat{f}_u)_4(x_2), (\hat{f}_u)_4(x_3), (\hat{f}_u)_4(x_4)\right) \end{aligned}$$

# Proof

By contradiction, assume that $M$ has only $n = 4$ distinct columns (the case $n \leq 3$ is easier!), say the first 4 columns, and let $M' \in (\mathbb{F}_2)^{4\times 4}$ be the corresponding submatrix:

$$M' = \begin{pmatrix} (\hat{f}_u)_1(x_1) & (\hat{f}_u)_1(x_2) & (\hat{f}_u)_1(x_3) & (\hat{f}_u)_1(x_4) \\ (\hat{f}_u)_2(x_1) & (\hat{f}_u)_2(x_2) & (\hat{f}_u)_2(x_3) & (\hat{f}_u)_2(x_4) \\ (\hat{f}_u)_3(x_1) & (\hat{f}_u)_3(x_2) & (\hat{f}_u)_3(x_3) & (\hat{f}_u)_3(x_4) \\ (\hat{f}_u)_4(x_1) & (\hat{f}_u)_4(x_2) & (\hat{f}_u)_4(x_3) & (\hat{f}_u)_4(x_4) \end{pmatrix}$$

If $M'$ has rank $\rho = 4$ (the case $\rho \leq 3$ is easier!), then

$$\begin{aligned}(1,1,1,1) &= a\Big((\hat{f}_u)_1(x_1),(\hat{f}_u)_1(x_2),(\hat{f}_u)_1(x_3),(\hat{f}_u)_1(x_4)\Big) + \\ & \quad b\Big((\hat{f}_u)_2(x_1),(\hat{f}_u)_2(x_2),(\hat{f}_u)_2(x_3),(\hat{f}_u)_2(x_4)\Big) + \\ & \quad c\Big((\hat{f}_u)_3(x_1),(\hat{f}_u)_3(x_2),(\hat{f}_u)_3(x_3),(\hat{f}_u)_3(x_4)\Big) + \\ & \quad d\Big((\hat{f}_u)_4(x_1),(\hat{f}_u)_4(x_2),(\hat{f}_u)_4(x_3),(\hat{f}_u)_4(x_4)\Big)\end{aligned}$$

# Proof

Since all the other columns of $M$ are equal to the columns of $M'$,

$$
\begin{aligned}
(1,1,\ldots,1) \quad = \quad & a\left((\hat{f}_u)_1(x_1),(\hat{f}_u)_1(x_2),\ldots,(\hat{f}_u)_1(x_{16})\right)+\\
& b\left((\hat{f}_u)_2(x_1),(\hat{f}_u)_2(x_2),\ldots,(\hat{f}_u)_2(x_{16})\right)+\\
& c\left((\hat{f}_u)_3(x_1),(\hat{f}_u)_3(x_2),\ldots,(\hat{f}_u)_3(x_{16})\right)+\\
& d\left((\hat{f}_u)_4(x_1),(\hat{f}_u)_4(x_2),\ldots,(\hat{f}_u)_4(x_{16})\right)
\end{aligned}
$$

Hence the function $<\hat{f}_u,(a,b,c,d)>$ is the constant 1, contradiction. □

# Proof

Since all the other columns of $M$ are equal to the columns of $M'$,

$$\begin{aligned}(1,1,\ldots,1) \quad = \quad & a\Big((\hat{f}_u)_1(x_1),(\hat{f}_u)_1(x_2),\ldots,(\hat{f}_u)_1(x_{16})\Big) + \\ & b\Big((\hat{f}_u)_2(x_1),(\hat{f}_u)_2(x_2),\ldots,(\hat{f}_u)_2(x_{16})\Big) + \\ & c\Big((\hat{f}_u)_3(x_1),(\hat{f}_u)_3(x_2),\ldots,(\hat{f}_u)_3(x_{16})\Big) + \\ & d\Big((\hat{f}_u)_4(x_1),(\hat{f}_u)_4(x_2),\ldots,(\hat{f}_u)_4(x_{16})\Big)\end{aligned}$$

Hence the function $< \hat{f}_u, (a,b,c,d) >$ is the constant 1, contradiction. □

# Security criteria

## linearity

$$\mathrm{Lin}(f) = \max_{a\in(\mathbb{F}_2)^m,\ b\in(\mathbb{F}_2)^m\setminus\{0\}} |< f, b >^{\mathcal{W}} (a)|$$

## 1-linearity

$$\mathrm{Lin}_1(f) = \max_{\substack{a,b\in(\mathbb{F}_2)^m \\ \mathrm{w}(a)=\mathrm{w}(b)=1}} \{|< f, b >^{\mathcal{W}} (a)|\}$$

## 1-differentiability

$$\mathrm{Diff}_1(S) = \max_{\substack{a,b\in(\mathbb{F}_2)^m \\ \mathrm{w}(a)=\mathrm{w}(b)=1}} \{|\hat{f}_a^{-1}(b)|\}$$

# Security criteria

## linearity

$$\mathrm{Lin}(f) = \max_{a\in(\mathbb{F}_2)^m,\ b\in(\mathbb{F}_2)^m\setminus\{0\}} |< f, b >^{\mathcal{W}} (a)|$$

## 1-linearity

$$\mathrm{Lin}_1(f) = \max_{\substack{a,b\in(\mathbb{F}_2)^m \\ \mathrm{w}(a)=\mathrm{w}(b)=1}} \{|< f, b >^{\mathcal{W}} (a)|\}$$

## 1-differentiability

$$\mathrm{Diff}_1(S) = \max_{\substack{a,b\in(\mathbb{F}_2)^m \\ \mathrm{w}(a)=\mathrm{w}(b)=1}} \{|\hat{f}_a^{-1}(b)|\}$$

# Security criteria

## linearity

$$\mathrm{Lin}(f) = \max_{a \in (\mathbb{F}_2)^m,\ b \in (\mathbb{F}_2)^m \setminus \{0\}} | < f, b >^{\mathcal{W}} (a)|$$

## 1-linearity

$$\mathrm{Lin}_1(f) = \max_{\substack{a,b \in (\mathbb{F}_2)^m \\ \mathrm{w}(a)=\mathrm{w}(b)=1}} \{| < f, b >^{\mathcal{W}} (a)|\}$$

## 1-differentiability

$$\mathrm{Diff}_1(S) = \max_{\substack{a,b \in (\mathbb{F}_2)^m \\ \mathrm{w}(a)=\mathrm{w}(b)=1}} \{|\hat{f}_a^{-1}(b)|\}$$

## G. Leander and A. Poschmann:

On the classification of 4 bit S-boxes. LNCS 4547, 159–176.

**Optimal S-box**

A Boolean permutation $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is an *optimal* S-Box if it has minimal linearity and minimal $\delta$-uniformity, namely, $\mathrm{Lin}(f) = 8$ and $f$ is 4-uniform.

**Serpent-type S-box**

A Boolean permutation $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is a *Serpent-type* S-Box if it is optimal and $\mathrm{Diff}_1(f) = 0$.

### Optimal S-box

A Boolean permutation $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is an *optimal* S-Box if it has minimal linearity and minimal $\delta$-uniformity, namely, $\mathrm{Lin}(f) = 8$ and $f$ is 4-uniform.

### Serpent-type S-box

A Boolean permutation $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is a *Serpent-type* S-Box if it is optimal and $\mathrm{Diff}_1(f) = 0$.

# Our contribution

**Strong S-box**

A Boolean permutation $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is a *strong* S-Box if $f$ is weakly APN and

$$\mathrm{Lin}(f) = 8, \quad f \text{ is } 4-\text{uniform}, \quad \mathrm{Diff}_1(f) = 0 \quad \mathrm{Lin}_1(f) = 4, \quad n_3(f) \geq 14\,.$$

**Very strong S-box**

A Boolean permutation $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is *very strong* if it is strong and strongly 2-anti-invariant.

# Our contribution

## Strong S-box

A Boolean permutation $f : (\mathbb{F}_2)^4 \rightarrow (\mathbb{F}_2)^4$ is a *strong* S-Box if $f$ is weakly APN and

$$\mathrm{Lin}(f) = 8, \quad f \text{ is } 4-\text{uniform}, \quad \mathrm{Diff}_1(f) = 0 \quad \mathrm{Lin}_1(f) = 4, \quad n_3(f) \geq 14\,.$$

## Very strong S-box

A Boolean permutation $f : (\mathbb{F}_2)^4 \rightarrow (\mathbb{F}_2)^4$ is *very strong* if it is strong and strongly 2-anti-invariant.

# Computational results

**Fact**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is a Boolean permutation such that

$$(i)\ \mathrm{Lin}(f) = 8, \quad (ii)\ 4 - \text{uniform}, \quad (iii) \quad n_3(f) \geq 14\,.$$

Then $f$ is weakly APN.

**Remark**

The assumptions of this Fact cannot be weakened: counterexamples are provided by the permutations

$$(i)\ (0, 1, 2, 12, 4, 6, 14, 5, 8, 3, 13, 10, 9, 7, 15, 11)$$

$$(ii)\ (0, 1, 2, 12, 4, 13, 11, 10, 8, 15, 5, 9, 6, 14, 7, 3)$$

$$(iii)\ (0, 1, 2, 7, 4, 12, 10, 3, 8, 6, 5, 14, 15, 9, 11, 13)\,.$$

# Computational results

**Fact**

Let $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ is a Boolean permutation such that

$$(i)\ \mathrm{Lin}(f) = 8, \quad (ii)\ 4 - \text{uniform}, \quad (iii) \quad n_3(f) \geq 14\,.$$

Then $f$ is weakly APN.

**Remark**

The assumptions of this Fact cannot be weakened: counterexamples are provided by the permutations

$$(i)\ (0, 1, 2, 12, 4, 6, 14, 5, 8, 3, 13, 10, 9, 7, 15, 11)$$

$$(ii)\ (0, 1, 2, 12, 4, 13, 11, 10, 8, 15, 5, 9, 6, 14, 7, 3)$$

$$(iii)\ (0, 1, 2, 7, 4, 12, 10, 3, 8, 6, 5, 14, 15, 9, 11, 13)\,.$$

# Computational results

The 4-bit S-boxes $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ such that $f(0) = 0$ are $15! \sim 10^{12}$

**Fact**

There are 55296 strong S-boxes and 2304 very strong ones.

**Fact**

Let $S_0, S_1, \ldots, S_7$ the S-boxes used in SERPENT.
The S-boxes $S_3, S_4, S_5, S_7$ are strong. None of the $S_i$'s is very strong.

# Computational results

The 4-bit S-boxes $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ such that $f(0) = 0$ are $15! \sim 10^{12}$

**Fact**

There are 55296 strong S-boxes and 2304 very strong ones.

**Fact**

Let $S_0, S_1, \ldots, S_7$ the S-boxes used in SERPENT.
The S-boxes $S_3, S_4, S_5, S_7$ are strong. None of the $S_i$'s is very strong.

# Computational results

The 4-bit S-boxes $f : (\mathbb{F}_2)^4 \to (\mathbb{F}_2)^4$ such that $f(0) = 0$ are $15! \sim 10^{12}$

**Fact**

There are 55296 strong S-boxes and 2304 very strong ones.

**Fact**

Let $S_0, S_1, \ldots, S_7$ the S-boxes used in SERPENT.
The S-boxes $S_3, S_4, S_5, S_7$ are strong. None of the $S_i$'s is very strong.

*Thank you for your attention.*