A new criterion for avoiding the propagation of linear relations through an Sbox

Christina Boura and **Anne Canteaut**

INRIA Paris-Rocquencourt
DTU Compute

March 13, 2013

Outline

Outline

Introduction

Investigate SPN primitives using small Sboxes.

Ideally, after several rounds, **all output bits** should be expessed as non-linear functions of **all input bits.**

Introduction

Investigate SPN primitives using small Sboxes.

Ideally, after several rounds, **all output bits** should be expessed as non-linear functions of **all input bits.**

This is not always so.

The need for a new linearity measure

Some **output bits** can be expressed as affine functions of some **input bits** (when the other input bits are fixed to a constant).

- The sizes of the **input** and **output** sets are important.
- Large sets can lead to a big number of affine relations between **input** and **output bits**.
- Possibly lead to cryptanalysis (Attack against Hamsi 2010, cube-like attacks).

We show that the number of affine relations depends on a **new** linearity measure of the Sbox, that we call (v, w)-**linearity**.

An example

ANF of the Hamsi Sbox

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

An example

ANF of the Hamsi Sbox

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

If we fix all-but-one variables to a **constant** value then all the coordinates of the Sbox are affine with respect to the input variable.

An example

ANF of the Hamsi Sbox

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

If we fix two variables to a **constant** value then two coordinates of the Sbox are affine with respect to the input variables.

An example

ANF of the Hamsi Sbox

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3\\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2\\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3\\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

If we fix one variable to a **constant** value then one coordinate of the Sbox is affine with respect to the input variables.

Outline

Definition of (v, w)-linearity

Definition. Let S be a function from $\mathbf{F}_2^n$ into $\mathbf{F}_2^m$. Then,

S is $\boldsymbol{(v, w)}$**-linear**

if there exist two linear subspaces $V \subset \mathbf{F}_2^n$ and $W \subset \mathbf{F}_2^m$ with $\dim V = v$ and $\dim W = w$ such that, for all $\lambda \in W$,

$$S_\lambda : x \mapsto \lambda \cdot S(x)$$

has **degree at most 1** on all cosets of V.

Example

$$
\begin{aligned}
y_0 &= x_0 x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0 x_1 x_2 + x_0 x_1 x_3 + x_0 x_2 x_3 + x_1 x_2 + x_0 x_3 + x_2 x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0 x_1 x_3 + x_0 x_2 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0 x_1 x_2 + x_1 x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

S is $(2, 2)$-**linear** for $V = \langle 1, 8 \rangle$ and $W = \langle 1, 8 \rangle$.

Example

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

S is $(3, 1)$-**linear** for $V = \langle 1, 2, 8 \rangle$ and $W = \langle 1 \rangle$.

Link with the Maiorana-McFarland Construction

An Example: Let $f : \mathbf{F}_2^4 \to \mathbf{F}_2$ with

$$f(x_1, x_2, x_3, x_4) = x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4.$$

Let $V = \langle 1, 2 \rangle$. Then f is $(2, 1)$-linear w.r.t. V.

Link with the Maiorana-McFarland Construction

An Example: Let $f : \mathbf{F}_2^4 \to \mathbf{F}_2$ with

$$f(x_1, x_2, x_3, x_4) = x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4.$$

Let $V = \langle 1, 2\rangle$. Then f is $(2, 1)$-linear w.r.t. V.

Link with the Maiorana-McFarland Construction

An Example: Let $f : \mathbf{F}_2^4 \to \mathbf{F}_2$ with

$$f(x_1, x_2, x_3, x_4) = x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4.$$

Let $V = \langle 1, 2 \rangle$. Then f is $(2, 1)$-linear w.r.t. V.

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4 \\ &= (x_3x_4 + x_4)x_1 + (x_3 + 1)x_2 + x_3x_4 + x_4 \\ &= (x_3x_4 + x_4, x_3 + 1) \cdot (x_1, x_2) + x_3x_4 + x_4 \end{aligned}$$

Link with the Maiorana-McFarland Construction

An Example: Let $f : \mathbf{F}_2^4 \to \mathbf{F}_2$ with

$$f(x_1, x_2, x_3, x_4) = x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4.$$

Let $V = \langle 1, 2\rangle$. Then f is $(2, 1)$-linear w.r.t. V.

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4 \\ &= (x_3x_4 + x_4)x_1 + (x_3 + 1)x_2 + x_3x_4 + x_4 \\ &= (x_3x_4 + x_4, x_3 + 1) \cdot (x_1, x_2) + x_3x_4 + x_4 \end{aligned}$$

In general, any $f : \mathbf{F}_2^n \to \mathbf{F}_2$ that is $(v, 1)$-linear w.r.t. V can be written as

$$f(x, y) = \pi(x) \cdot y + h(x), \text{ with } (x, y) \in U \times V.$$

Link with the Maiorana-McFarland Construction

An Example: Let $f : \mathbf{F}_2^4 \to \mathbf{F}_2$ with

$$f(x_1, x_2, x_3, x_4) = x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4.$$

Let $V = \langle 1, 2 \rangle$. Then f is $(2, 1)$-linear w.r.t. V.

$$\begin{aligned} f(x_1, x_2, x_3, x_4) &= x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4 + x_2 + x_4 \\ &= (x_3x_4 + x_4)x_1 + (x_3 + 1)x_2 + x_3x_4 + x_4 \\ &= (x_3x_4 + x_4, x_3 + 1) \cdot (x_1, x_2) + x_3x_4 + x_4 \end{aligned}$$

In general, any $f : \mathbf{F}_2^n \to \mathbf{F}_2$ that is $(v, 1)$-linear w.r.t. V can be written as

$$f(x, y) = \pi(x) \cdot y + h(x), \text{ with } (x, y) \in U \times V.$$

Generalisation of the Maiorana-McFarland construction for bent functions.

Link with the Maiorana-McFarland Construction

Proposition. S is **(v, w)-linear** w.r.t. (V, W) **if and only if** its components $S_\lambda, \lambda \in W$, can be written as

$$\begin{array}{rcl} S_W : U \oplus V & \to & \mathbf{F}_2^w \\ (u, v) & \mapsto & M(u)v + G(u) \end{array}$$

where $M(u)$ is a $w \times v$ binary matrix.

Equivalently, all second-order derivatives $D_\alpha D_\beta S_W$, with $\alpha, \beta \in V$, vanish.

General Properties

Proposition. If S is $\boldsymbol{(v, w)}$**-linear** w.r.t. (V, W), then all its components S_λ, $\lambda \in W$ have degree at most $\boldsymbol{n + 1 - v}$ and $\boldsymbol{\mathcal{L}(S) \geq 2^v}$.

Equivalence holds for $v = n - 1$ and $w = 1$.

Outline

4-bit optimal Sboxes

Many symmetric primitives are based on 4-bit balanced Sboxes.

Optimal Sbox: Sbox with optimal resistance against **differential** and **linear** cryptanalysis

[Leander-Poschmann07]: **16 classes** of optimal 4-bit balanced Sboxes upon affine equivalence.

4-bit optimal Sboxes

Many symmetric primitives are based on 4-bit balanced Sboxes.

Optimal Sbox: Sbox with optimal resistance against **differential** and **linear** cryptanalysis

[Leander-Poschmann07]: **16 classes** of optimal 4-bit balanced Sboxes upon affine equivalence.

Study these **16 classes** under the spectrum of (v, w)**-linearity**.

$\#\ (V, W)$ such that an Sbox is (v, w)-linear w.r.t. (V, W)
$\rightarrow$ invariant under affine equivalence.

Analysis of 4-bit optimal Sboxes

Number of V such that S is (v, w)-linear w.r.t. (V, W) for some W.

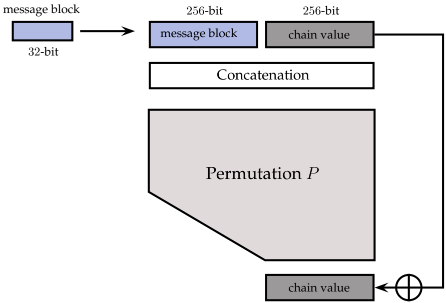
		(v, w)							
	Q	(2,1)	(2,2)	(2,3)	(2,4)	(3,1)	(3,2)	(3,3)	(3,4)
G_0	3	35	19	5	0	7	1	0	0
G_1	3	35	23	3	0	7	1	0	0
G_2	3	35	23	3	0	7	1	0	0
G_3	0	35	5	0	0	0	0	0	0
G_4	0	35	5	0	0	0	0	0	0
G_5	0	35	5	0	0	0	0	0	0
G_6	0	35	5	0	0	0	0	0	0
G_7	0	35	5	0	0	0	0	0	0
G_8	3	35	19	5	0	7	1	0	0
G_9	1	35	13	0	0	3	0	0	0
G_{10}	1	35	13	0	0	3	0	0	0
G_{11}	0	35	5	0	0	0	0	0	0
G_{12}	0	35	5	0	0	0	0	0	0
G_{13}	0	35	5	0	0	0	0	0	0
G_{14}	1	35	13	0	0	3	0	0	0
G_{15}	1	35	11	1	0	3	0	0	0

Outline

Hamsi Hash Function

Designed by Özgül Küçük in 2008 for the SHA-3 competition.

Compression function of Hamsi-256



Permutation P: 3 SPN rounds based on a 4-bit Sbox.

Second-preimage attack for Hamsi-256

Presented by Thomas Fuhr in Asiacrypt 2010.

> **Idea of the attack:** Find **affine relations** between some input bits and some output bits of the compression function when the other input bits are **fixed** to a well chosen value.

→ Preimages for the compression function.
→ Second-preimages for the hash function.

Finding affine relations

Choose the variables to go **linearly** through the first round.

For the second and the third round:

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

- y_0 is of degree at most 1 if x_0x_2 is of degree at most 1.
- y_3 is of degree at most 1 if x_1x_3 and $x_0x_1x_2$ are of degree at most 1.

Finding affine relations

Choose the variables to go **linearly** through the first round.

For the second and the third round:

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

- y_0 is of degree at most 1 if x_0x_2 is of degree at most 1.
- y_3 is of degree at most 1 if x_1x_3 and $x_0x_1x_2$ are of degree at most 1.

Finding affine relations

Choose the variables to go **linearly** through the first round.

For the second and the third round:

$$
\begin{aligned}
y_0 &= x_0x_2 + x_1 + x_2 + x_3 \\
y_1 &= x_0x_1x_2 + x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_0x_3 + x_2x_3 + x_0 + x_1 + x_2 \\
y_2 &= x_0x_1x_3 + x_0x_2x_3 + x_1x_2 + x_1x_3 + x_2x_3 + x_0 + x_1 + x_3 \\
y_3 &= x_0x_1x_2 + x_1x_3 + x_0 + x_1 + x_2 + 1.
\end{aligned}
$$

- y_0 is $(3, 1)$-linear for three hyperplanes.
- y_3 is $(2, 1)$-linear for three 2-dimensional subspaces V.

Automatic search for affine relations

- There are 23 subspaces V, with $\dim V = 2$ for which the Sbox of Hamsi is $(2, 2)$-linear.
- There are 3 subspaces V, with $\dim V = 2$ for which the Sbox of Hamsi is $(2, 3)$-linear.

Exploit this to **propagate more relations** through the second and the third round.

Results:

- $\boldsymbol{N_{var} = 9}$: **13** affine relations (two more than in [Fuhr '10])
- $\boldsymbol{N_{var} = 10}$: **11** affine relations (two more than in [Fuhr '10])

What if replacing the Sbox?

Replace the Hamsi Sbox by some other 4-bit Sbox

- JH Sboxes
- Sboxes in the classes G_3-G_7, G_{11}-G_{13}.

Keep the other parameters unchanged and **repeat** the attack.

What if replacing the Sbox?

Replace the Hamsi Sbox by some other 4-bit Sbox

- JH Sboxes
- Sboxes in the classes G_3-G_7, G_{11}-G_{13}.

Keep the other parameters unchanged and **repeat** the attack.

The attack does not work anymore!

Outline

Conclusion and Open Questions

- We have introduced a new cryptographic property for vectorial Boolean functions.
- Leads to a new measure of linearity for Sboxes.
- We have showed that the success of Fuhr's attack against Hamsi depends on the choice of the Sbox.
- **Open question**: "Are such attacks related to other recently proposed attacks (e.g. invariant subspace attack)"?

Conclusion and Open Questions

- We have introduced a new cryptographic property for vectorial Boolean functions.
- Leads to a new measure of linearity for Sboxes.
- We have showed that the success of Fuhr's attack against Hamsi depends on the choice of the Sbox.
- **Open question**: "Are such attacks related to other recently proposed attacks (e.g. invariant subspace attack)"?

Thanks for your attention!