Boolean Functions and Trapdoors on Block Cipher

Prof. Massimiliano Sala
University of Trento

International Workshop on
Boolean Functions and Their Applications
Rosendal, September 2-7

Trapdoors Project (2005–)

A. Caranti
F. Dalla Volta
I. Simonetti
I. Toli
A. Rimoldi
R. Aragona
E. Bellini
Especially on properties of Boolean functions
M. Calderini

Block Cipher

Let $\mathcal{C} = \{\phi_k | k \in \mathcal{K}\}$ be a block cipher acting on $V = V_1 \oplus \cdots \oplus V_s$, with $V_i = \mathbb{F}_2^m$ for $i = 1, \ldots, s$.

Definition

An element $\gamma \in Sym(V)$ is called a bricklayer transformation (or parallel S-box) of V if for any $v = (v_1 \oplus \cdots \oplus v_s) \in V$

$$v\gamma = v_1\gamma_1 \oplus \cdots \oplus v_s\gamma_s,$$

for some $\gamma_i \in Sym(V_i)$.

Definition

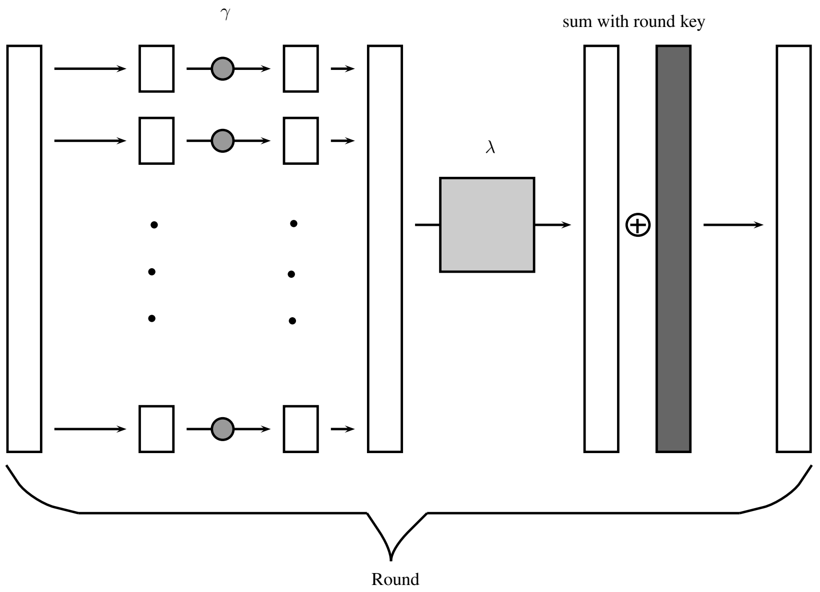
A linear map $\lambda \in GL(V)$ is called a proper mixing layer if no sum of the V_i, except $\{0\}$ and V, is λ-invariant.

Definition

A block cipher $\mathcal{C} = \{\phi_k | k \in \mathcal{K}\}$ is called translation based (TB) if

(1) each ϕ_k is the composition of ℓ round functions $\phi_{k,h}$, for $k \in \mathcal{K}$, and $h = 1, \ldots, \ell$, where in turn each round function can be written as a composition $\gamma_h \lambda_h \sigma_{\bar{k},h}$ of three permutations of V, with
   - γ_h is a bricklayer transformation depending on the round
   - λ_h is a linear permutation depending on the round
   - $\sigma_{\bar{k},h}$ is the translation by $\bar{k}$ depending on the key k and the round

(2) for at least one round the mixing layer is proper and the map $\mathcal{K} \to V$, $k \mapsto \bar{k}$ is surjective.


γ
sum with round key
λ
Round

Linear Trapdoors

Cryptographers construct $\mathcal{C}$ s.t. $\phi_k \notin AGL(V,+)$ for any key k, but there could be a hidden sum $\circ$ s.t.:

$(V,\circ)$ is a vector space and $\phi_k \in AGL(V,\circ)$

On a single round

Let us focus on a sigle round. Then the question is:

Is there any operation $\circ$ s.t. $(V, \circ)$ is a vector space and

$$\gamma_h \lambda_h \sigma_{k,h} \in AGL(V, \circ)?$$

Proposition

If $\gamma_h \lambda_h \sigma_{k,h} \in AGL(V, \circ)$ for all $k \in V$, then $\gamma_h \lambda_h \in AGL(V, \circ)$ and $T_+ = \{\text{translations with respect to } +\} \subseteq AGL(V, \circ)$.

Problems

(a) Find $\circ$ s.t. $T_+ \subseteq AGL(V, \circ)$.

(b) When γ, λ or $\gamma\lambda \in AGL(V, \circ)$?

Problem (a)

In [1], Caranti *et al.* characterized the abelian regular subgroups of $AGL(V,+)$ in terms of algebras. Let $T_\circ$ be the translation group with respect to $\circ$, we have:

Theorem

There is a one-to-one correspondence between

$$T_\circ \subseteq AGL(V,+)$$

$$\updownarrow$$

elementary abelian regular subgroups of $AGL(V,+)$

$$\updownarrow$$

commutative, associative $\mathbb{F}_2$*-algebra structures* $(V,+,\cdot)$*, with* $x\cdot x = 0$ *for all* $x \in V$ *and such that the resulting ring is radical* $(x+y+x\cdot y = x\circ y)$*.*

Problem (a)

Theorem

Let $V = \mathbb{F}_2^n$. *For* $n \leq 6$

$$T_\circ \subseteq AGL(V,+) \Leftrightarrow T_+ \subseteq AGL(V,\circ)$$

For $n \geq 7$

$$\exists T_\circ \subseteq AGL(V,+) \text{ s.t. } T_+ \nsubseteq AGL(V,\circ)$$

Problem (a)

How many $T_\circ \subseteq AGL(V,+)$

- $n = 2$ only T_+
- $n = 3$ there are 8 groups, of which 1 is T_+ and the others 7 are conjugated.
- $n = 4$ there are 106 groups, of which 1 is T_+ and the others 105 are conjugated.
- $n = 5$ there are 1954 groups, of which 1 is T_+ and the others form 2 classes of cardinality 1085 and 868.
- there are complex formulae for $n \geq 6$.

Problem (b)

Let $f : V \to V$, we denote by $\hat{f}_a : x \mapsto f(x) + f(x+a)$

Definition

f is called weakly δ-uniform if for every $a \in V \setminus \{0\}$

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

Definition

f is called strongly r-anti-invariant if for any two subspace U and W s.t. $f(U) = W$, we have $\dim(U) = \dim(W) < m - r$ or $U = W = V$.

Problem (b)

Definition

f is called anti-crooked (AC) if for every $a \in V \setminus \{0\}$ $\mathrm{Im}(\hat{f}_a)$ is not an affine subspace of V.

Theorem

Let f be a power function (i.e. x^d). If f is weakly-APN and not APN then f is AC.

Corollary

x^{-1} in even dimension is AC.

Problem (b)

Lemma

Let f be a power function. If there exists $a \neq 0$ s.t. $\mathrm{Im}(\hat{f}_a)$ is not an affine subspace of V, then $\mathrm{Im}(\hat{f}_{a'})$ is not an affine subspace of V for all $a' \in V \setminus \{0\}$.

Recalling that f is called crooked if f is APN and $\mathrm{Im}(\hat{f}_a)$ is an hyperplane for all $a \in V \setminus \{0\}$.

Corollary

Let f be an APN power function not crooked, then f is AC.

Problem (b)

[3] gives sufficient conditions on γ and λ in order to have $\gamma\lambda$ non linear

Theorem

Let $\mathcal{C}$ be a TB and there exists at least 1 round with S-box $\gamma = (\gamma_1, \ldots, \gamma_s)$ and mixing layer λ s.t.:

- γ_i *weakly-APN, strongly 1-AI and AC for all* $i = 1, \ldots, s$
- λ *proper*

$\Rightarrow$ $\gamma\lambda \notin AGL(V, \circ)$ *for any* $\circ$

Some differential properties of $AGL(V, \circ)$

Let

$$\delta(f) = \max_{a \neq 0, b \in V} |\hat{f}_a^{-1}(b)|.$$

Theorem

$T_+ \subseteq AGL(V, \circ) \Rightarrow$ for any $f \in AGL(V, \circ)$

$$\delta(f) \geq 2^{\frac{n}{2}}.$$

Theorem

For $n = 3, 4, 5$, if $T_+ \subseteq AGL(V, \circ)$ then $\delta(f) \geq 2^{n-1}$ for any $f \in AGL(V, \circ)$.

Remark

$n = 6$: $\delta(f)$?
For $n = 7$: *there exists* f *s.t.* $\delta(f) = 2^{n-2}$.

Remark

Let $V = (\mathbb{F}_2^m)^s$ *and* γ_i *be APN, then* $\delta(\gamma) = 2^{m(s-1)+1}$.
E.g. $s = 2$ *and* $m = 5$ *we have that if all the* γ_i *are APN then* $\delta(\gamma) = 2^6 > 2^5$.

Conclusions

(1) If γ is not in our class (i.e. weakly-APN, strongly AI, and AC) maybe there exists a hidden sum $\circ$ s.t. for any round and key-schedule $\mathcal{C}$ is linear.

(2) Even if γ is in our class maybe there exists a hidden sum $\circ$ s.t. ϕ_k is linear depending on the key-schedule.

(3) Only APN's will not be enough!

A. Caranti, F. Dalla Volta, M. Sala, "Abelian regular subgroups of the affine group and radical rings", Publicationes Mathematicae Debrecen, 2006, vol. 69, no. 3, p. 297-308.

A. Caranti, F. Dalla Volta, M. Sala,"On some block ciphers and imprimitive groups", Appl. Algebra Engrg. Comm. Comput., 2009, vol. 20, no. 5, p. 339-350.

A. Caranti, F. Dalla Volta, M. Sala, "An application of the O'Nan-Scott theorem to the group generated by the round function of an AES-like cipher", Design, Codes and Cryptography, 2009, vol. 52, no. 3, p. 293-301.

R. Aragona, A. Caranti, F. Dalla Volta, M. Sala,"On the group generated by the round encryptions of translation based ciphers over arbitrary finite fields", Finite Fields and Their Applications, 2014, vol. 25, p. 293-305.

R. Aragona, M. Calderini, D. Maccauro, M. Sala, "On some differential properties of Boolean functions", 2014, http://arxiv.org/abs/1403.7922