Permutation groups and security of block ciphers

Marco Calderini

June 7, 2021

Block ciphers

Let $V = (\mathbb{F}_2)^n$ be the set of messages.

Block cipher

A block cipher $\mathcal{C}$ is a set of (bijective) encryption functions.

$$\{\varphi_k\}_{k \in \mathcal{K}} \subseteq \mathrm{Sym}(V),$$

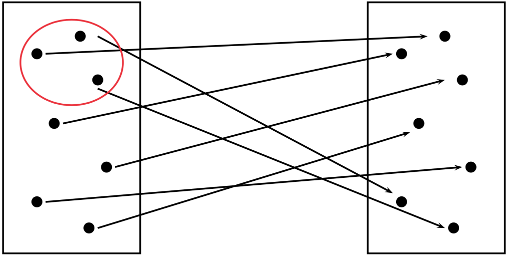
each of which is individuated by a key k in the space $\mathcal{K} = (\mathbb{F}_2)^\kappa$.

Most block ciphers are iterated block ciphers, where φ_k is the composition of many key-dependent permutations, known as round functions

A Block Cipher is considered secure if an attacker cannot understand φ_k (or k) from

$$\{(P, \varphi_k(P))\}_{P \in X}$$

with X small subset of V, even if X is chosen by the attacker.

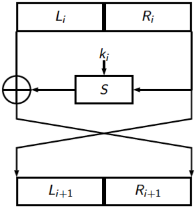


We would like that the most efficient attack is equivalent to trying all the possible keys (**brute force attack**).

Iterated Block Cipher

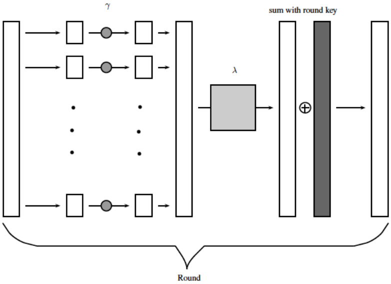
Round of Feistel Network

$$\begin{pmatrix} 0 & 1 \\ 1 & S \end{pmatrix} \sigma_{(0,k_i)}$$



Round of Translation Based (TB) Cipher
(more commonly called SPN)

$$\gamma\lambda\sigma_{k_i}$$



Translation Based Cipher

Let $\mathcal{C} = \{\varphi_k \mid k \in \mathcal{K}\}$ 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 $\gamma \in \mathrm{Sym}(V)$ is called a **parallel S-box** of V if there exist some γ_i's in $\mathrm{Sym}(V_i)$ (called S-boxes) s.t. for all $v = (v_1 \oplus \cdots \oplus v_s) \in V$

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

Definition

A block cipher $\mathcal{C} = \{\varphi_k \mid k \in \mathcal{K}\}$ is called **translation based (TB)** if each φ_k is the composition of r round functions $\varphi_{k,h}$, for $k \in \mathcal{K}$, and $h = 1, \ldots, r$, where in turn each round function can be written as a composition $\gamma_h \lambda_h \sigma_{k_h}$ of three permutations of V, with

- γ_h is a parallel S-box depending on the round
- λ_h is a linear permutation depending on the round
- σ_{k_h} is the translation by k_h depending on the key k and the round

Weaknesses based on properties of permutation groups

Let $\mathcal{C}$ be an r-round iterated block cipher acting on V.
The group generated by the encryption functions

$$\Gamma(\mathcal{C}) \stackrel{\text{def}}{=} \langle \varphi_k \in \mathrm{Sym}(V) \mid k \in \mathcal{K} \rangle$$

can reveal dangerous weaknesses of the cipher:

- the group is too small (Kaliski, Rivest and Sherman, 1998)
- the group acts imprimitively on the message space (Paterson, 1999)
- the group is of affine type (Calderini and Sala, 2015)

Weaknesses based on properties of permutation groups

Let $\mathcal{C}$ be an r-round iterated block cipher acting on V.
The group generated by the encryption functions

$$\Gamma(\mathcal{C}) \overset{\text{def}}{=} \langle \varphi_k \in \mathrm{Sym}(V) \mid k \in \mathcal{K} \rangle$$

can reveal dangerous weaknesses of the cipher:

- the group is too small (Kaliski, Rivest and Sherman, 1998)
- the group acts imprimitively on the message space (Paterson, 1999)
- the group is of affine type (Calderini and Sala, 2015)

Since $\Gamma(\mathcal{C})$ depends on the key-schedule algorithm it is hard to study this, in general.
So, usually, we study the group generated by the round functions

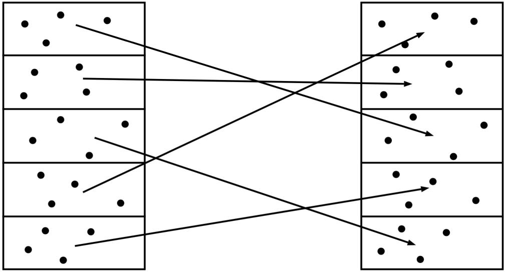
$$\Gamma_\infty(\mathcal{C}) \overset{\text{def}}{=} \langle \varphi_{k,h} \in \mathrm{Sym}(V) \mid k \in \mathcal{K}, h = 1, \dots, r \rangle$$

Imprimitive action

A finite group G is called *imprimitive* in its action on V if there exists a non-trivial partition of V, $\mathcal{B}$, such that $Bg \in \mathcal{B}$, for every $B \in \mathcal{B}$ and $g \in G$.

If $\Gamma_\infty(\mathcal{C})$ acts imprimitively on V then it is possible to introduce a trapdoor on $\mathcal{C}$. There exists a (non-trivial) partition $\mathcal{B}$ of V such that for any encryption function $\varphi_k \in \Gamma_\infty$ $B\varphi_k \in \mathcal{B}$ for all $B \in \mathcal{B}$.

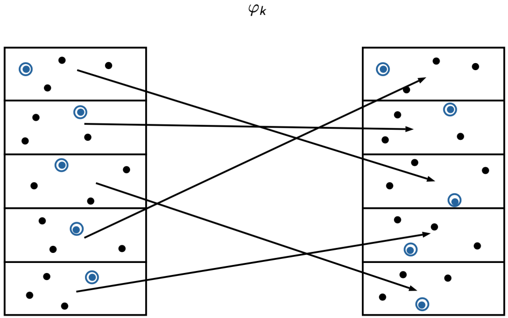
φ_k



Imprimitive action

A finite group G is called *imprimitive* in its action on V if there exists a non-trivial partition of V, $\mathcal{B}$, such that $Bg \in \mathcal{B}$, for every $B \in \mathcal{B}$ and $g \in G$.

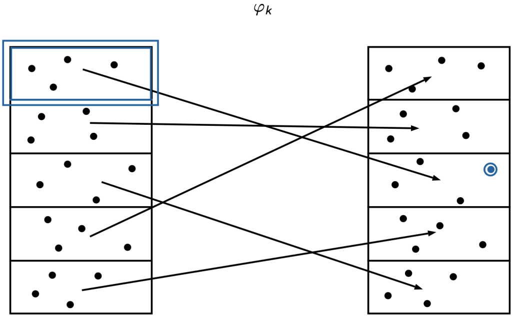
If $\Gamma_\infty(\mathcal{C})$ acts imprimitively on V then it is possible to introduce a trapdoor on $\mathcal{C}$. There exists a (non-trivial) partition $\mathcal{B}$ of V such that for any encryption function $\varphi_k \in \Gamma_\infty$ $B\varphi_k \in \mathcal{B}$ for all $B \in \mathcal{B}$.



Imprimitive action

A finite group G is called *imprimitive* in its action on V if there exists a non-trivial partition of V, $\mathcal{B}$, such that $Bg \in \mathcal{B}$, for every $B \in \mathcal{B}$ and $g \in G$.

If $\Gamma_\infty(\mathcal{C})$ acts imprimitively on V then it is possible to introduce a trapdoor on $\mathcal{C}$. There exists a (non-trivial) partition $\mathcal{B}$ of V such that for any encryption function $\varphi_k \in \Gamma_\infty$ $B\varphi_k \in \mathcal{B}$ for all $B \in \mathcal{B}$.



Imprimitive action

A finite group G is called *imprimitive* in its action on V if there exists a non-trivial partition of V, $\mathcal{B}$, such that $Bg \in \mathcal{B}$, for every $B \in \mathcal{B}$ and $g \in G$.

If $\Gamma_\infty(\mathcal{C})$ acts imprimitively on V then it is possible to introduce a trapdoor on $\mathcal{C}$. There exists a (non-trivial) partition $\mathcal{B}$ of V such that for any encryption function $\varphi_k \in \Gamma_\infty$ $B\varphi_k \in \mathcal{B}$ for all $B \in \mathcal{B}$.

`Attack cost`

The preprocessing costs ℓ encryptions. For any intercepted ciphertext, the search for the corresponding plaintext is limited to a block, whose size is $\frac{|V|}{\ell}$, requiring at most $\frac{|V|}{\ell}$ encryptions.

Affine type

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

$(V, \circ)$ is a vector space and $\varphi_k \in \mathrm{AGL}(V, \circ)$

Affine type

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

$(V,\circ)$ is a vector space and $\varphi_k \in \mathrm{AGL}(V,\circ)$

Let us focus on round functions. Then the question is:

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

$$\Gamma(\mathcal{C}) \subseteq \Gamma_\infty(\mathcal{C}) \subseteq \mathrm{AGL}(V,\circ)?$$

Let $T_+ \subset \mathrm{Sym}(V)$ be the usual translation group. Let T be an elementary abelian regular group, then T is a translation group with respect to some operation $\circ$. Indeed,

- $T = \{\tau_a \mid a \in V\}$ where τ_a is the unique map in T such that $0 \mapsto a$.
- define $x \circ a := x\tau_a$,

so $(V, \circ)$ is an additive group and it is an $\mathbb{F}_2$-vector space.

$T_\circ = T_+^g$ for some $g \in \mathrm{Sym}(V)$, and $\mathrm{AGL}(V, \circ) = \mathrm{AGL}(V, +)^g$.

Properties that $\circ$ should satisfy

We would like to understand which types of sums $\circ$ could produce an efficient attack.

Remark

$T_+ < \Gamma_\infty(\mathcal{C})$.

- $T_+ < \mathrm{AGL}(V, \circ)$
- we want to compute $x \circ y$ in an efficient way

We focused on $T_\circ < \mathrm{AGL}(V, +)$.

Let $T_\circ < \mathrm{AGL}(V,+)$, then $T_\circ \cap T_+ \neq \{1_V\}$.
We can define the (non trivial) vector space

$$U(T_\circ) = \{v \mid \sigma_v \in T_\circ \cap T_+\}$$

where $\sigma_v : x \mapsto x + v$.
Not all the dimensions are possible for the space U:

Proposition

Let $T_\circ \subseteq \mathrm{AGL}(V,+)$. If $T_\circ \neq T_+$, then $1 \leq \dim(U(T_\circ)) \leq n-2$.

Wlog, $U(T_\circ)$ is spanned by the last elements of the canonical basis. In that case we obtain:

Theorem

Let $V = \mathbb{F}_2^{n+k}$, with $n \geq 2$, $k \geq 1$, and $T_\circ \subseteq \mathrm{AGL}(V,+)$ be such that $U(T_\circ) = \mathrm{Span}\{e_{n+1}, \ldots, e_{n+k}\}$. Then,

$T_+ \subseteq \mathrm{AGL}(V,\circ)$ $\iff$ *for all $\tau_v = \kappa_v \cdot \sigma_v \in T_\circ$ there exists an $n \times k$ matrix B_v s.t.*

$$\kappa_v = \begin{bmatrix} I_{n\times n} & B_v \\ 0 & I_{k\times k} \end{bmatrix}.$$

Attack with hidden sum

Theorem

If $T_\circ \subseteq AGL(V,+)$ and $T_+ \subseteq \mathrm{AGL}(V,\circ)$, then there exists a procedure of polynomial time complexity that for all $v \in V$ returns

$$[\alpha_1, \ldots, \alpha_n],$$

where $\alpha_i \in \mathbb{F}_2$ s.t. $v = \alpha_1 v_1 \circ \cdots \circ \alpha_n v_n$ for a fixed basis of $(V,\circ)$.

Remark

We are able to compute efficiently $\phi : (V,\circ) \to (V,+)$ isomorphism of vector spaces.

Suppose $\Gamma_\infty \subseteq \mathrm{AGL}(V,\circ)$, then for all $k \in \mathcal{K}$ $\varphi_k \in \mathrm{AGL}(V,\circ)$.

- choose the vector $v_1,\dots,v_n$ of the basis as in the previous Theorem,
- compute $[0\varphi_k],[v_1\varphi_k],\dots,[v_n\varphi_k]$,
- consider the affinity $M\cdot\sigma_t$ s.t. $M_i=[v_i\varphi_k]$ and $t=[0\varphi_k]$
- for all $v\in V$ we have $[v\varphi_k]=[v]M+t$ and $[v\varphi_k^{-1}]=([v]+t)M^{-1}$.

We can reconstruct the encryption/decryption function using only $n+1$ ciphertexts

$$\begin{tikzcd}
(V,\circ) \arrow[r, "\varphi_k"] \arrow[d, "\phi"'] & (V,\circ) \\
(V,+) \arrow[r, "M\cdot\sigma_t"] & (V,+) \arrow[u, "\phi^{-1}"']
\end{tikzcd}$$

Suppose $\Gamma_\infty \subseteq \mathrm{AGL}(V, \circ)$, then for all $k \in \mathcal{K}$ $\varphi_k \in \mathrm{AGL}(V, \circ)$.

- choose the vector $v_1, \dots, v_n$ of the basis as in the previous Theorem,
- compute $[0\varphi_k], [v_1\varphi_k], \dots, [v_n\varphi_k]$,
- consider the affinity $M \cdot \sigma_t$ s.t. $M_i = [v_i\varphi_k]$ and $t = [0\varphi_k]$
- for all $v \in V$ we have $[v\varphi_k] = [v]M + t$ and $[v\varphi_k^{-1}] = ([v] + t)M^{-1}$.

We can reconstruct the encryption/decryption function using only $n+1$ ciphertexts

$$\begin{tikzcd}
(V, \circ) \arrow[r, "\varphi_k"] \arrow[d, "\phi"'] & (V, \circ) \\
(V, +) \arrow[r, "M \cdot \sigma_t"] & (V, +) \arrow[u, "\phi^{-1}"']
\end{tikzcd}$$

Question: Can we identify properties on the components of a cipher so that the groups associated to them is secure with respect to these attacks?

Some security notions of vectorial Boolean functions

Let $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^s$. Given $u, v \in (\mathbb{F}_2)^s$ we define

$$\delta(f)_{u,v} \overset{\text{def}}{=} |\{x \in (\mathbb{F}_2)^s \mid x\hat{f}_u = xf + (x+u)f = v\}|$$

Some security notions of vectorial Boolean functions

Let $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^s$. Given $u, v \in (\mathbb{F}_2)^s$ we define

$$\delta(f)_{u,v} \stackrel{\text{def}}{=} |\{x \in (\mathbb{F}_2)^s \mid x\hat{f}_u = xf + (x+u)f = v\}|$$

- The differential uniformity of f is

$$\delta(f) \stackrel{\text{def}}{=} \max_{u,v \in (\mathbb{F}_2)^s, u \neq 0} \delta(f)_{u,v},$$

  and f is said differentially δ-uniform if $\delta(f) = \delta$ ($\delta = 1$: PN; $\delta = 2$: APN).

Some security notions of vectorial Boolean functions

Let $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^s$. Given $u, v \in (\mathbb{F}_2)^s$ we define

$$\delta(f)_{u,v} \overset{\text{def}}{=} |\{x \in (\mathbb{F}_2)^s \mid x\hat{f}_u = xf + (x+u)f = v\}|$$

- The differential uniformity of f is

$$\delta(f) \overset{\text{def}}{=} \max_{u,v \in (\mathbb{F}_2)^s, u \neq 0} \delta(f)_{u,v},$$

  and f is said differentially δ-uniform if $\delta(f) = \delta$ ($\delta = 1$: PN; $\delta = 2$: APN).

- A function f satisfying

$$|\operatorname{Im}(\hat{f}_u)| > \frac{2^{s-1}}{\delta}$$

  for each $u \in (\mathbb{F}_2)^s \setminus \{0\}$ is called weakly differentially δ-uniform ($\delta = 2$: weakly-APN).

Some security notions of vectorial Boolean functions

- $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^s$ is strongly l-anti-invariant, with $0 \leq l \leq s-1$, if, for any two subspaces U and W of $(\mathbb{F}_2)^s$ such that $Uf = W$, then either $\dim(U) = \dim(W) < s - l$ or $U = W = (\mathbb{F}_2)^s$.

Proposition

Let $f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^s$ be a permutation. f is strongly 1-anti-invariant iff is the nonlinearity of f is not zero.

Properties of the mixing layer

Let $V = V_1 \oplus \cdots \oplus V_b$, $V_i \simeq (\mathbb{F}_2)^s$ called *bricks*.

- $\lambda \in \mathrm{GL}(V)$ is a proper mixing layer if no direct sum of bricks properly contained in V (called wall) is λ-invariant.
- λ is a strongly proper mixing layer if there are no walls W and W' such that $W\lambda = W'$.

Avoiding the imprimitive attack

Theorem (Caranti, Dalla Volta, Sala)

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^n$ such that λ is proper and, for some $1 \leq l < s$, each S-Box is

(*i*) *weakly differentially 2^l-uniform, and*

(*ii*) *strongly l-anti-invariant.*

Then $\Gamma_\infty(\mathcal{C})$ is primitive.

From the O'Nan-Scott classification of finite primitive groups we have:

If G is a primitive permutation group of degree 2^d, with $d \geq 1$, containing an abelian regular subgroup T, then:

1. G is of affine type, that is, $G \leq \mathrm{AGL}(d, 2)$;
2. G is a wreath product;
3. $G \simeq \mathrm{Alt}(2^d)$ or $\mathrm{Sym}(2^d)$.

Note that $T_+ < \Gamma_\infty(\mathcal{C})$.

Avoiding the affine type

$f : (\mathbb{F}_2)^s \to (\mathbb{F}_2)^s$ is anti-crooked (AC, for short) if, for any $u \in (\mathbb{F}_2)^s \setminus \{0\}$, $\mathrm{Im}(\hat{f}_u)$ is not an affine subspace of $(\mathbb{F}_2)^s$.

Theorem (Caranti, Dalla Volta, Sala)

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^n$ such that λ is strongly proper and, for some $1 \leq l < s$, each S-Box is AC and satisfies (i) and (ii). Then $\Gamma_\infty(\mathcal{C})$ is $\mathrm{Alt}(V)$ or $\mathrm{Sym}(V)$.

The S-Boxes of AES and $\mathrm{SERPENT}$ satisfy the hypotheses of previous theorems. Hence, $\Gamma_\infty(\mathrm{AES})$ and $\Gamma_\infty(\mathrm{SERPENT})$ are $\mathrm{Alt}((\mathbb{F}_2)^{128})$.

Some lightweight ciphers (i.e., ciphers designed to run on devices with very low computing power), such as $\mathrm{PRESENT}$, do not satisfy the hypotheses of previous theorems.

The S-Boxes of AES and $\mathrm{SERPENT}$ satisfy the hypotheses of previous theorems. Hence, $\Gamma_\infty(\mathrm{AES})$ and $\Gamma_\infty(\mathrm{SERPENT})$ are $\mathrm{Alt}((\mathbb{F}_2)^{128})$.

Some lightweight ciphers (i.e., ciphers designed to run on devices with very low computing power), such as $\mathrm{PRESENT}$, do not satisfy the hypotheses of previous theorems.

Is $\Gamma_\infty(\mathrm{PRESENT})$ primitive?

Is $\Gamma_\infty(\mathrm{PRESENT})$ the alternating group?

Avoinding the imprimitive attack

PRESENT and Lightweight TB Ciphers

Theorem

Let $\mathcal{C}$ be a TB cipher over $(\mathbb{F}_2)^{bs}$ with a proper mixing layer. Suppose that, for some $1 < l < s$, each S-Box is

(i) *differentially 2^l-uniform, and*

(ii) *strongly $(l-1)$-anti-invariant.*

Then $\Gamma_\infty(\mathcal{C})$ is primitive.

Corollary

The group generated by the round functions of the lightweight ciphers PRESENT, RECTANGLE *and* PRINTcipher *are primitive.*

Avoiding the affine type with AC

Theorem

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^{bs}$, with a strongly proper mixing layer such that the corresponding S-Boxes are AC and satisfy the hypotheses of the previous theorem. Then $\Gamma_\infty(\mathcal{C}) = \mathrm{Alt}(V)$.

Avoiding the affine type with AC

Theorem

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^{bs}$, with a strongly proper mixing layer such that the corresponding S-Boxes are AC and satisfy the hypotheses of the previous theorem. Then $\Gamma_\infty(\mathcal{C}) = \mathrm{Alt}(V)$.

The AC condition has been introduced to avoid that $\Gamma_\infty(\mathcal{C})$ is affine.

Avoiding the affine type with AC

Theorem

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^{bs}$, with a strongly proper mixing layer such that the corresponding S-Boxes are AC and satisfy the hypotheses of the previous theorem. Then $\Gamma_\infty(\mathcal{C}) = \mathrm{Alt}(V)$.

The AC condition has been introduced to avoid that $\Gamma_\infty(\mathcal{C})$ is affine.

PRESENT S-Box does not satisfy AC condition

Avoiding the affine type with AC

Proposition

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^{bs}$, with $s \geq 3$ and $b \geq 2$. Suppose that there exists an S-Box γ_i such that

$$\mathrm{Alt}(V_i) \subseteq \langle T(V_i), \gamma_i T(V_i) \gamma_i^{-1} \rangle.$$

If $\Gamma_\infty(\mathcal{C})$ is primitive, then it is not of affine type.

Theorem

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^{bs}$, with a strongly proper mixing layer such that the corresponding S-Boxes are

(i) *differentially 2^l-uniform, and*

(ii) *strongly $(l-1)$-anti-invariant.*

Suppose that there exists an S-Box γ_i such that

$$\mathrm{Alt}(V_i) \subseteq \langle T(V_i), \gamma_i T(V_i) \gamma_i^{-1} \rangle.$$

Then $\Gamma_\infty(\mathcal{C}) = \mathrm{Alt}(V)$.

Theorem

Let $\mathcal{C}$ be a TB cipher over $V = (\mathbb{F}_2)^{bs}$, with a strongly proper mixing layer such that the corresponding S-Boxes are

(i) *differentially 2^l-uniform, and*

(ii) *strongly $(l-1)$-anti-invariant.*

Suppose $s = 3, 4$ or 5, and $b \geq 2$. Then $\Gamma_\infty(\mathcal{C}) = \mathrm{Alt}(V)$.

Corollary

The round functions of PRESENT, RECTANGLE *and* PRINTcipher *generate the alternating group ($l = 2$).*

Starting to consider the key-schedule

We can consider another group associate to a cipher $\mathcal{C}$, the group of encryption functions with independent round keys (long-key scenario):

$$\Gamma_{ind} = \langle \gamma_1 \lambda_1 \sigma_{k_1} \cdot \ldots \cdot \gamma_r \lambda_r \sigma_{k_r} \mid k_i \in V \rangle.$$

Note that $\Gamma \subset \Gamma_{ind} \subset \Gamma_\infty$.

Why study Γ_{ind}?
It could happen that Γ_∞ seems secure but Γ_{ind} is not.

Remark

If $\gamma_i \lambda_i$ are the same for all rounds then $\Gamma_{ind} \lhd \Gamma_\infty$. So if $\Gamma_\infty \simeq \mathrm{Alt}(V)$ then $\Gamma_{ind} = \Gamma_\infty$.

Group generated by encryptions with independent round keys

A partition $\mathcal{L}(U) = \{U + v \,:\, v \in V\}$ with U subspace of V is called *linear*

Theorem

If all encryption functions $\gamma_1\lambda_1\sigma_{k_1} \cdot \ldots \cdot \gamma_r\lambda_r\sigma_{k_r}$ *map a partition* $\mathcal{P}$ *into* $\mathcal{P}'$ *(for all round-keys* k_i*'s), then* $\mathcal{P}$ *and* $\mathcal{P}'$ *are linear. Moreover* $\mathcal{A}_i = (\mathcal{A}_{i-1})\gamma_i\lambda_i$ *is linear for all* i *(*$\mathcal{A}_0 = \mathcal{P}$*).*

Theorem

Let $\mathcal{C}$ be a TB and there exists at least two consecutive round h and $h+1$ with λ_h strongly proper and the parallel S-boxes γ_h and γ_{h+1} are s.t.:

- *γ_i 2^l-uniform,*
- *strongly $(l-1)$-anti-invariant*

Where $1 \leq t \leq m-1$.

$\Rightarrow$

There do not exist $\mathcal{P}$ and $\mathcal{P}'$ (non-trivial) partitions such that $\mathcal{P}\varphi_k = \mathcal{P}'$ for all k. In particular, $\Gamma_{ind}(\mathcal{C})$ is primitive.

Group generated by encryptions with independent round keys

Theorem

Let $\mathcal{C}$ be a TB cipher over V. Suppose that there exists a brick γ_i (S-box) corresponding to the first round ($h = 1$) such that

$$Alt(V_i) = \langle T_+(V_i), \gamma_i \left(T_+(V_i)\right) \gamma_i^{-1} \rangle$$

If $\Gamma_{ind}(\mathcal{C})$ is primitive, then it is not of affine type.

Group generated by encryptions with independent round keys

Theorem

Let $\mathcal{C}$ be a TB cipher over V. Suppose that there exists a brick γ_i (S-box) corresponding to the first round ($h = 1$) such that

$$Alt(V_i) = \langle T_+(V_i), \gamma_i \left(T_+(V_i)\right) \gamma_i^{-1} \rangle$$

If $\Gamma_{ind}(\mathcal{C})$ is primitive, then it is not of affine type.

Open question: Is $\Gamma_{ind} \simeq \mathrm{Alt}(V)$?

The Feistel case

Group generated by encryptions with independent round keys

Let $\bar{\rho}_i = \begin{pmatrix} 0 & 1 \\ 1 & \rho_i \end{pmatrix}$.

$$\Gamma_{ind}(\mathcal{F}) = \langle \bar{\rho}_1 \sigma_{(0,k_1)} \cdot \ldots \cdot \bar{\rho}_r \sigma_{(0,k_r)} \mid k_i \in V \rangle.$$

Theorem

$T_+(V \times V) < \Gamma_{ind}(\mathcal{F})$. Moreover,
$\langle \bar{\rho}_1 \sigma_{(k_{1,1},k_{1,2})} \cdot \ldots \cdot \bar{\rho}_r \sigma_{(k_{r,1},k_{r,2})} \mid (k_{i,1}, k_{i,2}) \in V^2 \rangle < \Gamma_{ind}(\mathcal{F})$.

Corollary

Let $\mathcal{F}$ be a Feistel network on $V \times V$. If all encryption functions $\bar{\rho}_1 \sigma_{(0,k_1)} \cdot \ldots \cdot \bar{\rho}_r \sigma_{(0,k_r)}$ map a partition $\mathcal{P}$ into $\mathcal{P}'$, then $\mathcal{P}$ and $\mathcal{P}'$ are linear. Moreover $\mathcal{A}_i = (\mathcal{A}_{i-1})\bar{\rho}_i$ is linear for all i ($\mathcal{A}_0 = \mathcal{P}$).

Remark (Goursat's Lemma)

Let U be a subspace of $V \times V$. Then, there exist $A, D < V$ and ϕ morphism such that $U = \{(a, a\phi + d) \mid a \in A, d \in D\}$.

Theorem

Let $\rho_1, \rho_2 \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$. If $\langle \bar{\rho}_1 \sigma_{(0,k_1)} \bar{\rho}_2 \sigma_{(0,k_2)} \mid k_1, k_2 \in V \rangle$ is imprimitive, then there exist $U_1, W_1, U_2, W_2 < V$ such that $\mathcal{L}(U_1)\rho_1 = \mathcal{L}(W_1)$ and $\mathcal{L}(U_2)\rho_2 = \mathcal{L}(W_2)$.

Corollary

$\Gamma_\infty(\mathcal{F})$ is primitive iff for some round i, $\langle \rho_i, T_+(V) \rangle$ is primitive.

Excluding some partitions

Theorem

Let $\mathcal{F}$ be a Feistel network, with $\rho_1, \ldots, \rho_r \in \mathrm{Sym}(V)$. Let us assume that $0\rho_i = 0$ and $\rho_i = \gamma_i \lambda_i$, where

a) *γ_i is a parallel map which applies 2^δ-differentially uniform and $(\delta - 1)$-strongly anti-invariant S-boxes, for some $\delta < s$, where s denotes the dimension of each brick,*

b) *λ_i a linear strongly-proper mixing layer.*

Suppose that there exists a sequence of $r + 1$ non-trivial linear partitions $\mathcal{L}(\mathcal{U}_1), \ldots, \mathcal{L}(\mathcal{U}_{r+1})$, where $\mathcal{U}_i$ is a proper and non-trivial subgroup of $V \times V$ and $\mathcal{L}(\mathcal{U}_i)\bar{\rho}_i = \mathcal{L}(\mathcal{U}_{i+1})$ for all $1 \leq i \leq r$. Then, none of the following condition is satisfied:

1. *there exists $1 \leq i \leq r - 1$ such that $\mathcal{L}(\mathcal{U}_{i+1})\bar{\rho}_{i+1} = \mathcal{L}(\mathcal{U}_i)$,*
2. *there exists $1 \leq i \leq r - 1$ such that $\mathcal{U}_i = A_i \times D_i$, $\mathcal{U}_{i+1} = A_{i+1} \times D_{i+1}$ and $\mathcal{U}_{i+2} = A_{i+2} \times D_{i+2}$,*
3. *there exists $1 \leq i \leq r$ such that $D_i = \{0\}$ and $D_{i+1} = \{0\}$,*
4. *there exists $1 \leq i \leq r$ such that $A_i = \{0\}$ and $A_{i+1} = \{0\}$.*

Open questions:

- Prove that $\Gamma_{ind}(\mathcal{F})$ is primitive.
- Prove that we can avoid affine type for $\Gamma_{ind}(\mathcal{F})$ or $\Gamma_{\infty}(\mathcal{F})$
- Prove that $\Gamma_{ind}(\mathcal{F})$ or $\Gamma_{\infty}(\mathcal{F})$ are $\mathrm{Alt}(V \times V)$.

Thanks for your attention!