Wave-shaped round functions and primitive groups

Joint work with M. Calderini, R. Civino, M. Sala and I. Zappatore[1]

Riccardo Aragona

DISIM, University of L'Aquila

SandGAL 2019

[1] R. Aragona, M. Calderini, R. Civino, M. Sala, I. Zappatore, *Wave-Shaped Round Functions and Primitive Groups*, Advances in Mathematics of Communications 13(1), 67-88 (2019).

Block ciphers

Let $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ be the message space

Block cipher

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

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

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

Block ciphers

Let $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ be the message space

Block cipher

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

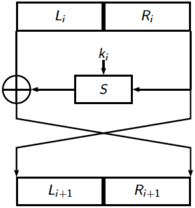
$$\{\varepsilon_k\}_{k \in \mathcal{K}} \subseteq \mathrm{Sym}(V),$$

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

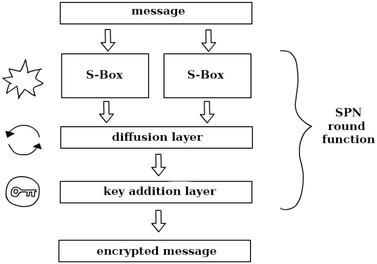
Most block ciphers are iterated block ciphers, where $\varepsilon_k = \varepsilon_{k_1} \cdots \varepsilon_{k_r}$, with $k_i \in V$, is the composition of many key-dependent permutations, known as round functions.

Iterated Block Cipher

Round of Feistel Network



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



Classical round function in a TB cipher

Let $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$ where each V_j is an s-dimensional brick. For each $c \in V$, the classical round function induced by c is a map $\varepsilon_c : V \to V$ where $\varepsilon_c = \gamma\lambda\sigma_c$ and

- $\gamma \in \mathrm{Sym}(V)$ is a non-linear bricklayer transformation which acts in parallel way on each V_j

  $$\gamma \qquad \boxed{\gamma'}\boxed{\gamma'}\boxed{\quad\cdots\quad}\boxed{\gamma'}$$

  The map $\gamma' : V_j \to V_j$ is traditionally called an S-box
- $\lambda \in \mathrm{Sym}(V)$ is a linear map, called mixing layer
- $\sigma_c : V \to V, x \mapsto x + c$ represents the key addition, where $+$ is the usual bitwise XOR on $\mathbb{F}_2$

Non-linearity

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

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

and f is said δ-differentially uniform if $\delta(f) = \delta$.

Non-linearity

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

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

and f is said δ-differentially uniform if $\delta(f) = \delta$.

Note that δ-differentially uniform functions with small δ are "farther" from being linear (when f is linear $\delta = 2^s$).

Almost Perfect Non-linearity

2-differentially uniform S-Boxes are called Almost Perfect Non-linear (APN)

Almost Perfect Non-linearity

2-differentially uniform S-Boxes are called Almost Perfect Non-linear (APN)

APN S-Boxes are optimal against some statistical attacks

Almost Perfect Non-linearity

2-differentially uniform S-Boxes are called Almost Perfect Non-linear (APN)

APN S-Boxes are optimal against some statistical attacks

Unfortunately NO APN permutation of even dimension has yet been found except one of dimension 6.

- when $s = 4$ no permutation is APN (Calderini, Sala and Villa, 2017)
- when $s = 6$, only one is known (Dillon APN permutation, 2009)

Almost Perfect Non-linearity

2-differentially uniform S-Boxes are called Almost Perfect Non-linear (APN)

APN S-Boxes are optimal against some statistical attacks

Unfortunately NO APN permutation of even dimension has yet been found except one of dimension 6.

- when $s = 4$ no permutation is APN (Calderini, Sala and Villa, 2017)
- when $s = 6$, only one is known (Dillon APN permutation, 2009)

If $s < t$, there exist $s \times t$ APN injective S-Boxes

Almost Perfect Non-linearity

2-differentially uniform S-Boxes are called Almost Perfect Non-linear (APN)

APN S-Boxes are optimal against some statistical attacks

Unfortunately NO APN permutation of even dimension has yet been found except one of dimension 6.

- when $s = 4$ no permutation is APN (Calderini, Sala and Villa, 2017)
- when $s = 6$, only one is known (Dillon APN permutation, 2009)

If $s < t$, there exist $s \times t$ APN injective S-Boxes

Is it possible to define an iterated block cipher with such APN S-Boxes?

Generalisation of Round Functions: Wave functions

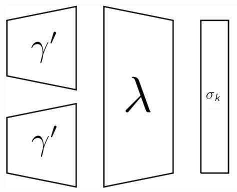
Let $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$,
$\dim_{\mathbb{F}_2}(V) = n$ and $\dim_{\mathbb{F}_2}(V_i) = s$.

Let $W = W_1 \oplus W_2 \oplus \ldots \oplus W_b$,
$\dim_{\mathbb{F}_2}(W) = m \geq n$ and $\dim_{\mathbb{F}_2}(W_i) = t$.

Generalisation of Round Functions: Wave functions

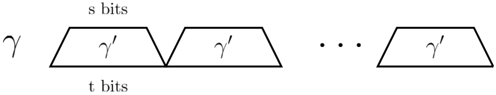
Let $V = V_1 \oplus V_2 \oplus \ldots \oplus V_b$,
$\dim_{\mathbb{F}_2}(V) = n$ and $\dim_{\mathbb{F}_2}(V_i) = s$.

Let $W = W_1 \oplus W_2 \oplus \ldots \oplus W_b$,
$\dim_{\mathbb{F}_2}(W) = m \geq n$ and $\dim_{\mathbb{F}_2}(W_i) = t$.



For each $c \in V$, we define a Wave function induced by c as a map $\varepsilon_c : V \to V$, where $\varepsilon_c = \gamma\lambda\sigma_c$ and

- $\gamma : V \to W$ is an injective non-linear bricklayer transformation which acts independently on each V_j



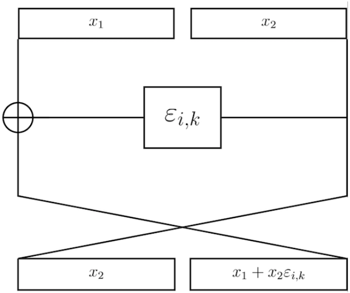
  The map $\gamma' : V_j \to W_j$ is an injective S-box
- $\lambda : W \to V$ is a surjective mixing linear
- $\sigma_c : V \to V$ is the key addition

Wave ciphers

In order to guarantee an efficient decryption, we propose to use Wave functions inside a Feistel Network

An r-round Wave block cipher $\mathcal{C}$ is a family of encryption functions $\{\varepsilon_k \mid k \in \mathcal{K}\} \subseteq \mathrm{Sym}(V \times V)$ such that for each $k \in \mathcal{K}$ $\varepsilon_k = \overline{\varepsilon_{1,k}\varepsilon_{2,k}} \ldots \overline{\varepsilon_{r,k}}$, where $\overline{\varepsilon_{i,k}}$ is the formal operator

$$\overline{\varepsilon_{i,k}} = \begin{pmatrix} 0_n & 1_n \\ 1_n & \varepsilon_{i,k} \end{pmatrix}$$



and $\varepsilon_{i,k} = \gamma\lambda\sigma_{k_i}$ is an n-bit Wave function.

Group Theoretical Security of Block ciphers

Weaknesses based on group theoretical properties

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

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

can reveal dangerous weaknesses of the cipher:

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

Group Theoretical Security of Block ciphers

Weaknesses based on group theoretical properties

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

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

can reveal dangerous weaknesses of the cipher:

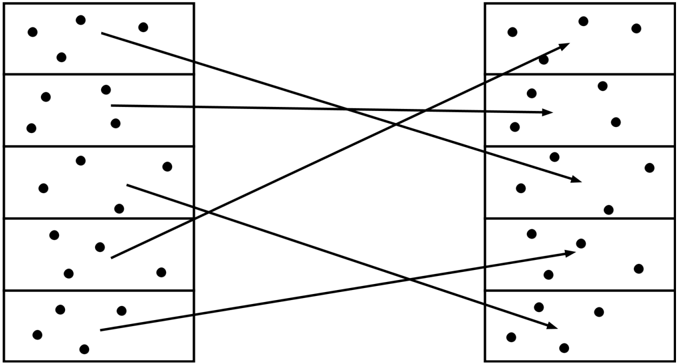
- the group is too small (Kaliski, Rivest and Sherman, 1998)
- the group is of affine type (Calderini and Sala, 2015)
- the group acts imprimitively on the message space (Paterson, 1999)

Under some cryptographic assumptions for a Wave cipher $\mathcal{C}$

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

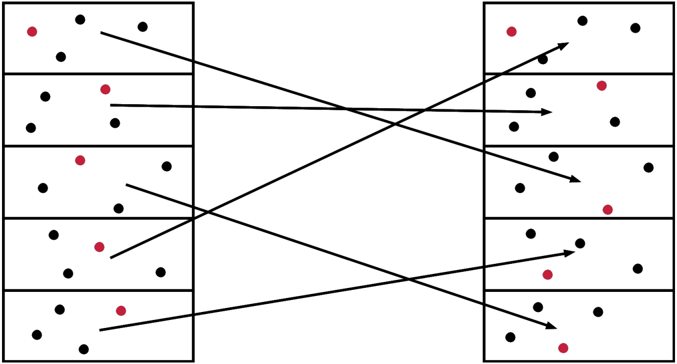
Imprimitive attack

Let $\mathcal{C}$ be an r-round iterated block cipher.
Suppose that $\Gamma_\infty(\mathcal{C})$ is imprimitive, then there exists a partition $\mathcal{B}$ of V such that for any encryption function $\varepsilon_k \in \Gamma_\infty$, we have $B\varepsilon_k \in \mathcal{B}$ for all $B \in \mathcal{B}$.



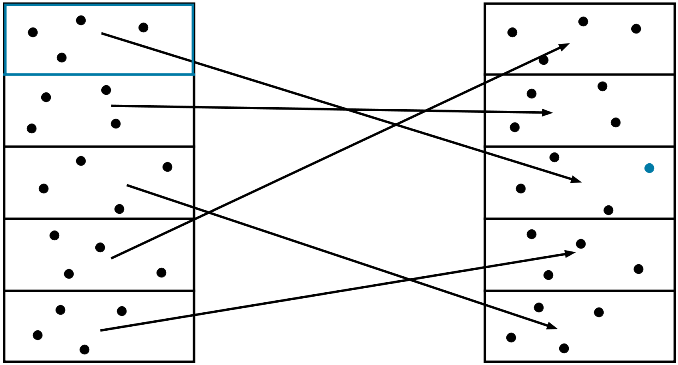
Imprimitive attack

Preprocessing performed ones per key:



Imprimitive attack

Real-time processing:



Group generated by the round functions of a Wave cipher

Let $\varepsilon_{i,k} = \gamma\lambda\sigma_{k_i} \in \mathrm{Sym}(V)$ be an n-bit Wave function. We define

$$\Gamma_i \overset{\text{def}}{=} \langle \varepsilon_{i,k} \mid k \in \mathcal{K} \rangle \quad \text{and} \quad \overline{\Gamma}_i \overset{\text{def}}{=} \langle \overline{\varepsilon_{i,k}} \mid k \in \mathcal{K} \rangle,$$

where

$$\overline{\varepsilon_{i,k}} = \begin{pmatrix} 0_n & 1_n \\ 1_n & \varepsilon_{i,k} \end{pmatrix}.$$

Hence

$$\Gamma_\infty(\mathcal{C}) \overset{\text{def}}{=} \langle \overline{\Gamma}_i \mid 1 \leq i \leq r \rangle.$$

Our goal

Show that $\Gamma_\infty(\mathcal{C})$ is primitive

Group generated by the round functions of a Wave cipher

Let us denote with

- $T_n \stackrel{\text{def}}{=} \{\sigma_k \mid x \mapsto x + k\} \leq \mathrm{Sym}(V)$
- $T_{(0,n)} \stackrel{\text{def}}{=} \{\sigma_{(0,k)} \mid (x_1, x_2) \mapsto (x_1, x_2 + k)\} \leq \mathrm{Sym}(V^2)$

Being $\rho \stackrel{\text{def}}{=} \gamma\lambda$ and denoting with $\overline{\rho}$ the formal operator $\begin{pmatrix} 0_n & 1_n \\ 1_n & \rho \end{pmatrix}$ one has

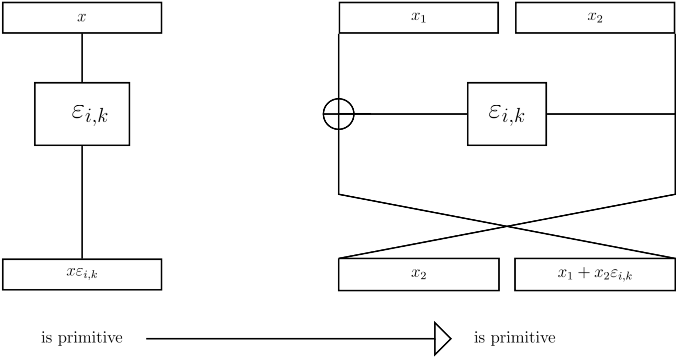
$$\Gamma_i = \langle T_n, \rho \rangle \quad \text{and} \quad \overline{\Gamma}_i(\mathcal{C}) = \langle T_{(0,n)}, \overline{\rho} \rangle,$$

for any $1 \leq i \leq r$.

Security Reduction

Theorem (A., Calderini, Civino, Sala, Zappatore)

If $\gamma\lambda \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$ and $\Gamma_i = \langle T_n, \rho \rangle$ is primitive on V, then $\overline{\Gamma}_i(\mathcal{C}) = \langle T_{(0,n)}, \overline{\rho} \rangle$ is primitive on $V \times V$.



Two other security assumptions for the components of a Wave function

Definition

A wall of V (resp. W) is any nontrivial sum of proper bricks of V (resp. W). A linear transformation $\lambda : W \longrightarrow V$ is a proper mixing layer if for any nontrivial wall $W' = \bigoplus_{i \in I} W_i$ of W and $V' = \bigoplus_{i \in I} V_i$ of V, where $I \subset \{1, \ldots, m\}$, then

$$V'\lambda^{-1} \not\subset W' + \operatorname{Ker} \lambda.$$

Definition

Let $j \in \{1, 2, \ldots, b\}$, $\gamma_j : V_j \to W_j$ be an S-box such that $0\gamma_j = 0$, and $\lambda : W \to V$ be a surjective linear map. Given $0 \le l < s$, γ_j is l-non-invariant with respect to λ if for any proper subspaces $V' < V_j$ and $W' < W_j$ such that $V'\gamma_j + (\operatorname{Ker} \lambda \cap W_j) = W'$, then $\dim(W') < s - l$.

Primitivity of a Wave cipher

Theorem (A., Calderini, Civino, Sala, Zappatore)

Let $\mathcal{C}$ *be Wave cipher with a proper mixing layer* λ. *If there exists* $1 \leq l < s$ *such that each S-box* γ_j *is*

- 2^l*- differentially uniform,*
- $(l-1)$*-non-invariant with respect to* λ*,*

and if $\operatorname{Ker}\lambda = \bigoplus_{j=1}^{b} \operatorname{Ker}\lambda \cap W_j$, *then* Γ_i *is primitive (and so it is* $\Gamma_\infty(\mathcal{C})$*).*

Works in progress and future works

Several problems arise from the new construction regarding Wave functions and Wave ciphers $\mathcal{C}$, such as:

- Determining conditions on the Wave functions to ensure that $\Gamma_\infty(\mathcal{C})$ is the alternating group.

Works in progress and future works

Several problems arise from the new construction regarding Wave functions and Wave ciphers $\mathcal{C}$, such as:

- Determining conditions on the Wave functions to ensure that $\Gamma_\infty(\mathcal{C})$ is the alternating group.
- Studying the group generated by the round functions of a Wave cipher for which the function $\gamma\lambda$ is not invertible. Note that in this case, we cannot use the result Γ_i primitive implies Γ_∞ primitive unless we consider in some way the transformation monoid generated by the wave functions.

Works in progress and future works

Several problems arise from the new construction regarding Wave functions and Wave ciphers $\mathcal{C}$, such as:

- Determining conditions on the Wave functions to ensure that $\Gamma_\infty(\mathcal{C})$ is the alternating group.
- Studying the group generated by the round functions of a Wave cipher for which the function $\gamma\lambda$ is not invertible. Note that in this case, we cannot use the result Γ_i primitive implies Γ_∞ primitive unless we consider in some way the transformation monoid generated by the wave functions.
- Studying the resistance of a Wave cipher with respect to other statistical attacks, for example studying the impact of differential and linear cryptanalysis on the Wave-shaped structure.

Works in progress and future works

Several problems arise from the new construction regarding Wave functions and Wave ciphers $\mathcal{C}$, such as:

- Determining conditions on the Wave functions to ensure that $\Gamma_\infty(\mathcal{C})$ is the alternating group.
- Studying the group generated by the round functions of a Wave cipher for which the function $\gamma\lambda$ is not invertible. Note that in this case, we cannot use the result Γ_i primitive implies Γ_∞ primitive unless we consider in some way the transformation monoid generated by the wave functions.
- Studying the resistance of a Wave cipher with respect to other statistical attacks, for example studying the impact of differential and linear cryptanalysis on the Wave-shaped structure.

Finally, to the best of our knowledge, $s \times t$ APN functions with $s < t$ are not very much investigated in literature.

Thanks for your attention!