Permutation group methods for block cipher security

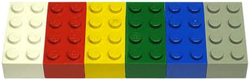
Riccardo Aragona

DISIM, University of L'Aquila

CrypTO Conference 2021
27/5/2021

Block cipher

Parameters



block size n $\leq$ key size κ

Spaces

- $V \stackrel{\text{def}}{=} (\mathbb{F}_2)^n$ the message space
- $K \approx (\mathbb{F}_2)^\kappa$ the key space

Block ciphers

Block cipher

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

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

Block ciphers

Block cipher

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

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

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.

Key-schedule

Once the key $k \in \mathcal{K}$ to be used has been chosen for the encryption, the encryption function is obtained by composing the r round functions induced by the corresponding round keys, which are derived by a key-schedule.

Key-schedule

Once the key $k \in \mathcal{K}$ to be used has been chosen for the encryption, the encryption function is obtained by composing the r round functions induced by the corresponding round keys, which are derived by a key-schedule.

The key-schedule is a public function

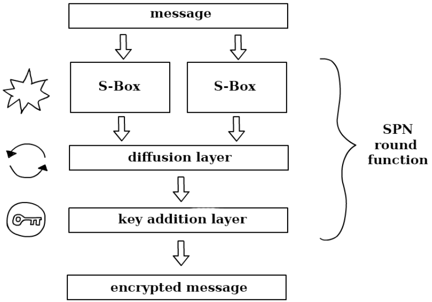
$$\mathcal{K}S : \mathcal{K} \to V^r$$

such that $\mathcal{K}S(k) \stackrel{\text{def}}{=} (k_1, \ldots, k_r)$ for any $k \in \mathcal{K}$, where $\mathcal{K}S(k)_i \stackrel{\text{def}}{=} k_i$ is the i-th round key derived from the user-provided key k.

Iterated Block Cipher: Substitution Permutation Network

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

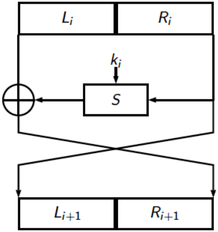
- $\gamma \in \mathrm{Sym}(V)$ is a non-linear transformation, called parallel S-Box, which acts in parallel way by $\gamma' \in \mathrm{Sym}(V_j)$, for each V_j
- $\lambda \in \mathrm{GL}(V)$, called diffusion layer
- $\sigma_k : V \to V, x \mapsto x + k$ represents the key addition, where $+$ is the usual bitwise XOR on $\mathbb{F}_2$



Iterated Block Cipher: Feistel Network

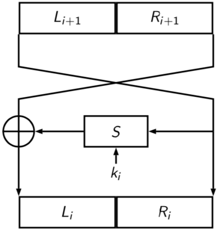
i-th Round Encryption

$$L_{i+1} = R_i$$
$$R_{i+1} = L_i \oplus S(R_i, k_i)$$



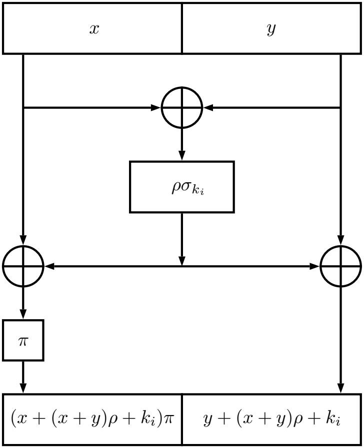
i-th Round Decryption

$$R_i = L_{i+1}$$
$$L_i = R_{i+1} \oplus S(L_{i+1}, k_i)$$



The Feistel-function S may have the structure of an SPN-round ε_{k_i}.
The invertibility of the whole Feistel round transformation does not depend on the invertibility of S.

Iterated Block Cipher: Lai-Massey Scheme



i-th Round Encryption

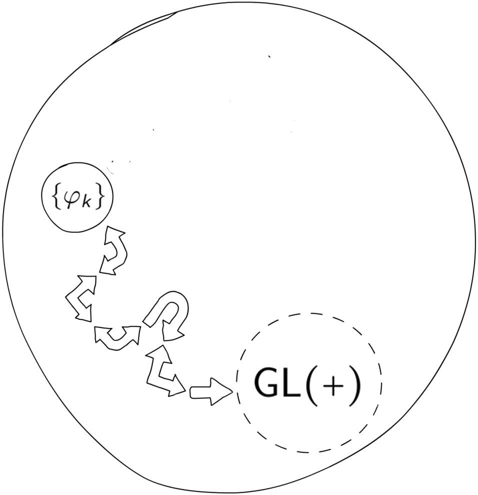
$$(x,y)\overline{\varepsilon_{i,K}} =$$

$$\big((x+(x+y)\rho+k_i)\pi, y+(x+y)\rho+k_i\big)$$

As in the Feistel Network case, it is possible to prove that the inverse $\overline{\varepsilon_{i,K}}^{\,-1}$ of the round function $\overline{\varepsilon_{i,K}}$ of a Lai-Massey cipher does not involve the inverse of ρ

Security parameters for block ciphers

Non-linearity



Security parameters for block ciphers

Non-linearity for vectorial Boolean functions (vBf)

Let $f \in \mathrm{Sym}\left((\mathbb{F}_2)^s\right)$ and let $u \in (\mathbb{F}_2)^s \setminus \{0\}$. Let us define

$$x\hat{f}_u = xf + (x+u)f.$$

Given $v \in (\mathbb{F}_2)^s$ we define

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

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

Security parameters for block ciphers

Non-linearity for vectorial Boolean functions (vBf)

Let $f \in \mathrm{Sym}((\mathbb{F}_2)^s)$ and let $u \in (\mathbb{F}_2)^s \setminus \{0\}$. Let us define

$$x\hat{f}_u = xf + (x+u)f.$$

Given $v \in (\mathbb{F}_2)^s$ we define

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

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

Notice that δ-differentially uniform functions with small δ are "farther" from being linear compared to functions with a larger differential uniformity value (when f is linear, then $\delta = 2^s$).

Security parameters for block ciphers

Some security (non-linearity) notions for vBfs

- $f \in \mathrm{Sym}\left((\mathbb{F}_2)^s\right)$ is strongly l-anti-invariant, with $0 \le l \le s-1$, if, for any two subspaces U and W of $(\mathbb{F}_2)^s$ such that $Uf = W$, then either $\mathrm{codim}(U) = \mathrm{codim}(W) > l$ or $U = W = (\mathbb{F}_2)^s$.

Security parameters for block ciphers

Some security (non-linearity) notions for vBfs

- $f \in \mathrm{Sym}((\mathbb{F}_2)^s)$ is strongly l-anti-invariant, with $0 \le l \le s-1$, if, for any two subspaces U and W of $(\mathbb{F}_2)^s$ such that $Uf = W$, then either $\mathrm{codim}(U) = \mathrm{codim}(W) > l$ or $U = W = (\mathbb{F}_2)^s$.

- $f \in \mathrm{Sym}((\mathbb{F}_2)^s)$ 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 $(\mathbb{F}_2)^s$.

Security parameters for block cipher

Security notions for the linear component of a block cipher

- $\lambda \in \mathrm{GL}(V)$ is a proper diffusion layer if no direct sum of bricks properly contained in V (called wall) is λ-invariant.

- λ is a strongly proper diffusion layer if there are no walls W and W' such that $W\lambda = W'$.

Security parameters for block cipher

Security notions for the linear component of a block cipher

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

The previous properties are standard requests for the linear component of a block cipher to spread the input bits as much as possible within the ciphertext.

Group Theoretical Security for Block Ciphers

Weaknesses based on group theoretical properties

Let $\mathcal{C}$ be an r-round iterated block cipher on V.
We define (Coppersmith and Grossman 1975) the group generated by the encryption functions of $\mathcal{C}$

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

Group Theoretical Security for Block Ciphers

Weaknesses based on group theoretical properties

Let $\mathcal{C}$ be an r-round iterated block cipher on V.
We define (Coppersmith and Grossman 1975) the group generated by the encryption functions of $\mathcal{C}$

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

This group can reveal dangerous weaknesses of the cipher which could be exploited to recover from a ciphertext the corresponding message or the encryption key:

- the group is too small (Kaliski, Rivest and Sherman, 1988)
- the group is of affine type (Calderini, Civino and Sala, 2020)
- the group acts imprimitively on the message space (Paterson, 1999; Leander, Minaud, and Ronjom, 2015)

Group Theoretical Security for Block Ciphers

Weaknesses based on group theoretical properties

Let $\mathcal{C}$ be an r-round iterated block cipher on V.
We define (Coppersmith and Grossman 1975) the group generated by the encryption functions of $\mathcal{C}$

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

This group can reveal dangerous weaknesses of the cipher which could be exploited to recover from a ciphertext the corresponding message or the encryption key:

- the group is too small (Kaliski, Rivest and Sherman, 1988)
- the group is of affine type (Calderini, Civino and Sala, 2020)
- the group acts imprimitively on the message space (Paterson, 1999; Leander, Minaud, and Ronjom, 2015)

TO AVOID THESE WEAKNESSES

THE BEST IS WHEN $\Gamma(\mathcal{C})$ EQUALS $\mathrm{Alt}(V)$ OR $\mathrm{Sym}(V)$

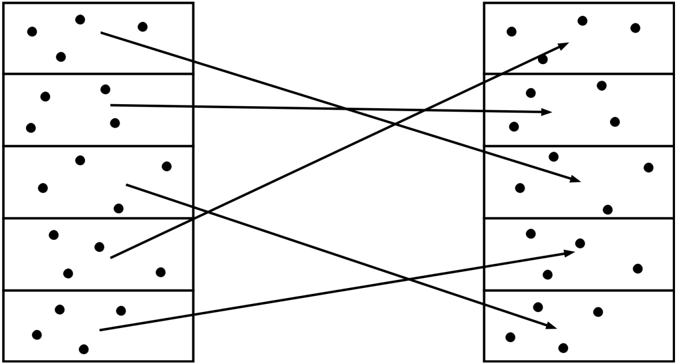
Primitive groups

Let G be a finite group.

- A partition $\mathcal{B}$ of V is said to be G-invariant if $Bg \in \mathcal{B}$, for every $B \in \mathcal{B}$ and $g \in G$.
- A partition $\mathcal{B}$ is trivial if $\mathcal{B} = \{V\}$ or $\mathcal{B} = \{\{v\} \mid v \in V\}$.
- We will say that G is *imprimitive* in its action on V if it admits a non-trivial G-invariant partition of V. Otherwise it is called *primitive*.

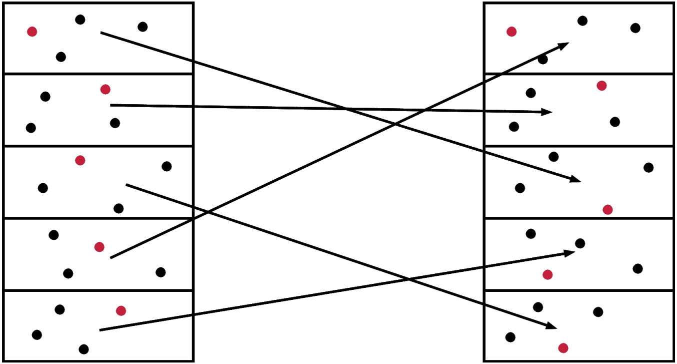
Imprimitive attack

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



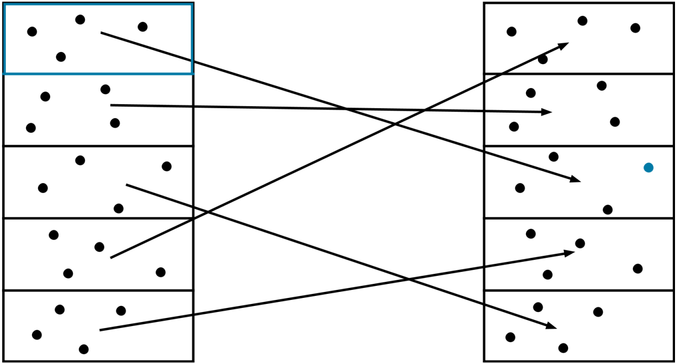
Imprimitive attack

Preprocessing performed ones per key:



Imprimitive attack

Real-time processing:



Group Theoretical Security for Block Ciphers

Notice that the study of $\Gamma(\mathcal{C})$ is a hard task in general, since the dependence on the key-schedule is not easily turned into algebraic conditions.

Group Theoretical Security for Block Ciphers

Notice that the study of $\Gamma(\mathcal{C})$ is a hard task in general, since the dependence on the key-schedule is not easily turned into algebraic conditions.

In literature there are only partial results for block ciphers with very particular types of key schedules (Calderini, 2018; –, Calderini and Civino, 2020)

Group Theoretical Security for Block Ciphers

Notice that the study of $\Gamma(\mathcal{C})$ is a hard task in general, since the dependence on the key-schedule is not easily turned into algebraic conditions.

In literature there are only partial results for block ciphers with very particular types of key schedules (Calderini, 2018; –, Calderini and Civino, 2020)

We have much more results in the case when we consider a group containing $\Gamma(\mathcal{C})$, the so-called group generated by the round functions of $\mathcal{C}$

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

Group Theoretical Security for Block Ciphers

Notice that the study of $\Gamma(\mathcal{C})$ is a hard task in general, since the dependence on the key-schedule is not easily turned into algebraic conditions.

In literature there are only partial results for block ciphers with very particular types of key schedules (Calderini, 2018; –, Calderini and Civino, 2020)

We have much more results in the case when we consider a group containing $\Gamma(\mathcal{C})$, the so-called group generated by the round functions of $\mathcal{C}$

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

WHEN IS $\Gamma_\infty(\mathcal{C})$ PRIMITIVE?

WHEN IS $\Gamma_\infty(\mathcal{C})$ THE ALTERNATING GROUP?

Some Results

The groups of the following ciphers are the alternating group (in particular primitive)

- DES (Wernsdorf, 1993)
- SERPENT (Wernsdorf, 2000)
- AES (Sparr and Wernsdorf, 2008)
- KASUMI (Sparr and Wernsdorf, 2015)
- SPNs, under some cryptographic assumptions (Caranti, Dalla Volta and Sala for $p = 2$, 2009; –, Caranti, Dalla Volta and Sala for $p > 2$, 2014)
- GOST-like cipher (–, Caranti and Sala, 2017)

Group Theoretical Security for SPNs

Primitivity

Theorem (–, Calderini, Tortora and Tota, 2018)

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

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

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

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

Corollary

The group generated by the round functions of AES, SERPENT *and* PRESENT *are primitive ($l = 2$).*

The O'Nan-Scott classification

Once proved the primitivity, we exploit a special case of the O'Nan-Scott classification of the finite primitive permutation groups to prove when $\Gamma_\infty(\mathrm{SPN})$ is the alternating group.
We denote by $G = N.K$ an extension G of N by K.

Theorem

Let G be a primitive permutation group of degree 2^d, with $d \geq 1$. Assume that G contains an elementary abelian regular subgroup T. Then one of the following holds

(1) *G is of affine type, that is, $G \leq \mathrm{AGL}(d, 2)$;*

(2) *$G \simeq \mathrm{Alt}(2^d)$ or $\mathrm{Sym}(2^d)$;*

(3) *G is a wreath product, that is,*

$$G = (S_1 \times \ldots \times S_c).O.P \quad \text{and} \quad T = T_1 \times \ldots \times T_c,$$

where $c \geq 1$ divides d, each T_i is an abelian subgroup of S_i of order $2^{d/c}$ with $S_i \simeq \mathrm{Alt}(2^{d/c})$ or $\mathrm{Sym}(2^{d/c})$, the S_i are all conjugate, $O \leq \mathrm{Out}(S_1) \times \ldots \times \mathrm{Out}(S_c)$, and P permutes transitively the S_i.

Group Theoretical Security for SPNs

Translation group

Let $T(V) \stackrel{\text{def}}{=} \{\sigma_k \mid x \mapsto x + k\} \leq \mathrm{Sym}(V)$ be the translation group of V and let $\rho = \gamma\lambda$.

Lemma (Caranti, Dalla Volta and Sala, 2014)

Let $\mathcal{C}$ be an SPN over V. Then

$$\Gamma_\infty(\mathcal{C}) = \langle T(V), \rho \rangle$$

In particular $\Gamma_\infty(\mathcal{C})$ contains an elementary abelian regular subgroup

Group Theoretical Security for SPNs
The alternating group

Lemma (–, Calderini, Tortora and Tota, 2018)

Let $\mathcal{C}$ be a SPN cipher over V. Then $\Gamma_\infty(\mathcal{C}) \leq \mathrm{Alt}(V)$.

Group Theoretical Security for SPNs
The alternating group

Lemma (–, Calderini, Tortora and Tota, 2018)

Let $\mathcal{C}$ be a SPN cipher over V. Then $\Gamma_\infty(\mathcal{C}) \leq \mathrm{Alt}(V)$.

Theorem (–, Calderini, Tortora and Tota, 2018)

Let $\mathcal{C}$ be an SPN over $V = (\mathbb{F}_2)^{bs}$ such that λ is strongly proper and, for some $1 \leq l < s$, each S-Box is AC and satisfies

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

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

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

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

Group Theoretical Security for SPNs

Some applications to real-life Cryptography

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

Group Theoretical Security for SPNs

Some applications to real-life Cryptography

The S-Boxes of AES and $\mathrm{SERPENT}$ satisfy the hypotheses of the previous theorem.
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 AC condition for the S-Boxes.

Group Theoretical Security for SPNs
Some applications to real-life Cryptography

The S-Boxes of AES and $\mathrm{SERPENT}$ satisfy the hypotheses of the previous theorem.
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 AC condition for the S-Boxes.

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

Theorem (–, Calderini, Tortora and Tota, 2018)

Let $\mathcal{C}$ be a SPN cipher over $V = (\mathbb{F}_2)^{bs}$, with a strongly proper mixing layer such that for $1 < l < s$ the corresponding S-Boxes are

(i) *2^l-differentially 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

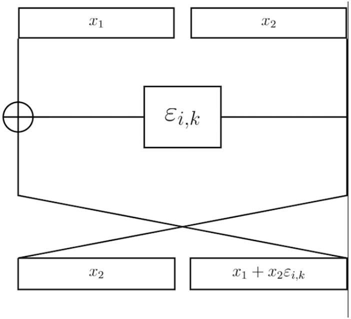
The round functions of PRESENT, RECTANGLE *and* PRINTcipher *generate the alternating group ($l = 2$).*

Group Theoretical Security for Feistel Networks

Round functions

Let us define an r-round Feistel Network $\mathcal{C}$ as a family of encryption functions $\{\varepsilon_k \mid k \in \mathcal{K}\} \subseteq \mathrm{Sym}(V \times V)$ such that for each $k \in \mathcal{K}$ $\varepsilon_k = \overline{\varepsilon_{1,k}\varepsilon_{2,k}} \dots \overline{\varepsilon_{r,k}}$, 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 $\varepsilon_{i,k} = \rho\sigma_{k_i}$, with $\rho \in \mathrm{Sym}(V)$.

Group Theoretical Security for Feistel Networks
Group generated by the round functions

We define

$$\Gamma_\infty(\mathcal{C}) \stackrel{\text{def}}{=} \langle \overline{\varepsilon_{i,k}} \mid k \in \mathcal{K}, 1 \le i \le r \rangle.$$

We define

$$\Gamma_\infty(\mathcal{C}) \stackrel{\text{def}}{=} \langle \overline{\varepsilon_{i,k}} \mid k \in \mathcal{K}, 1 \le i \le r \rangle.$$

Let $T_{(0,n)} \stackrel{\text{def}}{=} \{\sigma_{(0,k)} : (x_1, x_2) \mapsto (x_1, x_2 + k) \mid k \in V\} \le \mathrm{Sym}(V \times V)$.

Note that $T_{(0,n)} \cong T(V)$.

Lemma

Let $\overline{\rho}$ be the formal operator $\begin{pmatrix} \mathbb{0} & \mathbb{1} \\ \mathbb{1} & \rho \end{pmatrix}$. Then

$$\Gamma_\infty(\mathcal{C}) = \langle T_{(0,n)}, \overline{\rho} \rangle.$$

Group Theoretical Security for Feistel Networks

Security Reduction

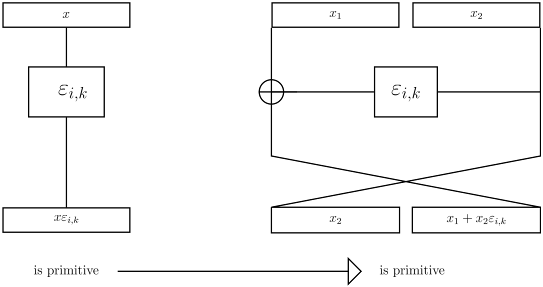
Let $\varepsilon_{i,k} = \rho\sigma_{k_i} \in \mathrm{Sym}(V)$ and $\Gamma \stackrel{\text{def}}{=} \langle \varepsilon_{i,k} \mid k \in \mathcal{K}, 1 \leq i \leq r \rangle$.

Then

$$\Gamma_\infty(\mathcal{C}) = \langle\, T_{(0,n)}, \overline{\rho}\,\rangle \quad \text{and} \quad \Gamma = \langle\, T(V), \rho\,\rangle$$

Theorem (–, Calderini, Civino, Sala and Zappatore, 2019)

If $\rho \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$ and Γ is primitive, then $\Gamma_\infty(\mathcal{C})$ is primitive.

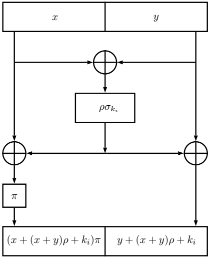


Group Theoretical Security for Lai-Massey Schemes

Round functions

Let us define an r-round Lai-Massey Scheme $\mathcal{C}$ as a family of encryption functions $\{\varepsilon_k \mid k \in \mathcal{K}\} \subseteq \mathrm{Sym}(V \times V)$ such that for each $k \in \mathcal{K}$ $\varepsilon_k = \overline{\varepsilon_{1,k}}\,\overline{\varepsilon_{2,k}} \dots \overline{\varepsilon_{r,k}}$, where the i-th round function $\overline{\varepsilon_{i,k}}$ is defined as

$$\overline{\varepsilon_{i,k}} \stackrel{\text{def}}{=} \overline{\rho}\,\overline{\pi}\sigma_{(k_i\pi, k_i)},$$



where

- $\overline{\rho}$ denotes the formal operator $\begin{pmatrix} \mathbb{1} & \mathbb{1} \\ \mathbb{1} & \mathbb{0} \end{pmatrix}\begin{pmatrix} \mathbb{1} & \mathbb{1}+\rho \\ \mathbb{0} & \mathbb{1} \end{pmatrix} \in \mathrm{Sym}(V \times V)$;
- $\overline{\pi}$ denotes the formal operator $\begin{pmatrix} \pi & \mathbb{0} \\ \pi & \mathbb{1} \end{pmatrix} \in \mathrm{GL}(V \times V)$;

Let us coinsider an *r-round generalized Lai-Massey cipher* when the key addition in the round function $\sigma_{(k_i\pi, k_i)}$ is replaced by the more general $\sigma_{(k_i,k_j)}$, for $(k_i, k_j) \in V \times V$.

Given $\rho \in \mathrm{Sym}(V) \setminus \mathrm{AGL}(V)$ and $\pi \in \mathrm{GL}(V)$, we define

$$\Gamma(\mathrm{GLM}(\rho, \pi)) \overset{\text{def}}{=} \langle T_{2n}, \overline{\rho}, \overline{\pi} \rangle;$$

where

$$T_{2n} \overset{\text{def}}{=} \{\sigma_{(k_1,k_2)} : (x_1, x_2) \mapsto (x_1+k_1, x_2+k_2) \mid (k_1, k_2) \in V \times V\} \leq \mathrm{Sym}(V \times V).$$

Let $\varepsilon_{i,k} = \rho\sigma_{k_i} \in \mathrm{Sym}(V)$ and $\Gamma \stackrel{\text{def}}{=} \langle \varepsilon_{i,k} \mid k \in \mathcal{K}, 1 \leq i \leq r \rangle$.
Then

$$\Gamma = \langle T(V), \rho \rangle.$$

Theorem (– and Civino, 2021)

If $\langle T(V), \rho \rangle$ is primitive, then $\Gamma(\mathrm{GLM}(\rho, \pi))$ is primitive.

Group Theoretical Security for Lai-Massey Schemes

…"Viceversa"

Lemma (– and Civino, 2021)

If $\langle T(V), \rho, \pi \rangle$ is imprimitive, then $\Gamma(\mathrm{GLM}(\rho, \pi))$ is imprimitive.

Proof.

Let us assume that $U \leq V$ is an invariant subspace for ρ and for π. Then, for $(u_1, u_2) \in U \times U$,

$$\begin{aligned} (u_1, u_2)\overline{\rho} &= (u_1, u_2) \begin{pmatrix} \mathbb{1} & \mathbb{1} \\ \mathbb{1} & \mathbb{0} \end{pmatrix} \begin{pmatrix} \mathbb{1} & \mathbb{1} + \rho \\ \mathbb{0} & \mathbb{1} \end{pmatrix} \\ &= (u_1 + u_2, u_2 + (u_1 + u_2)\rho) \in U \times U, \end{aligned}$$

and analogously

$$(u_1, u_2)\overline{\pi} = (u_1, u_2) \begin{pmatrix} \pi & \mathbb{0} \\ \pi & \mathbb{1} \end{pmatrix} = ((u_1 + u_2)\pi, u_2) \in U \times U.$$

Therefore $U \times U \leq V \times V$ is an invariant subspace for $\overline{\rho}$ and $\overline{\pi}$. $\square$

Thanks for your attention!

- R. Aragona and R. Civino, On invariant subspaces in the Lai-Massey scheme and a primitivity reduction, to appear in *Mediterranean Journal of Mathematics*, 2021.
- R. Aragona, M. Calderini, R. Civino, M. Sala, I. Zappatore, Wave-Shaped Round Functions and Primitive Groups, *Advances in Mathematics of Communications*, **13** (2019), 67–88.
- R. Aragona, M. Calderini, A. Tortora and M. Tota, On the primitivity of PRESENT and other lightweight ciphers, *J. Algebra Appl.*, **17** (2017), 1850115 (16 pages).
- R. Aragona, A. Caranti and M. Sala, The group generated by the round functions of a GOST-like cipher, Ann. Mat. Pura Appl., **196** (2016), 1–17.
- R. Aragona, A. Caranti, F. Dalla Volta and M. Sala, On the group generated by the round functions of translation based ciphers over arbitrary fields, *Finite Fields Appl.*, **25** (2014), 293–305.
- M. Calderini, A note on some algebraic trapdoors for block ciphers, *Advances in Mathematics of Communications*, **12** (2018), 515–524.

- M. Calderini, R. Civino and M. Sala, On properties of translation groups in the affine general linear group with applications to cryptography, *Journal of Algebra*, **569** (2021), 658–680.
- A. Caranti, F. Dalla Volta and M. Sala, On some block ciphers and imprimitive groups, *Appl. Algebra Engrg. Comm. Comput.*, **20** (2009), 339–350.
- A. Caranti, F. Dalla Volta and M. Sala, An application of the O'Nan-Scott theorem to the group generated by the round functions of an AES-like cipher, *Des. Codes Cryptogr.*, **52** (2009), 293–301.
- D. Coppersmith and E. Grossman, Generators for certain alternating groups with applications to cryptography, *SIAM J. Appl. Math.*, **29** (1975), 624–627.
- Jr. B. S. Kaliski, R. L. Rivest and A. T. Sherman, Is the Data Encryption Standard a group? (Results of cycling experiments on DES), *J. Cryptology*, **1** (1988), 3–36.
- G. Leander, B. Minaud, and S. Ronjom. A generic approach to invariant subspace attacks: Cryptanalysis of Robin, iSCREAM and

Zorro. In *Advances in cryptology–EUROCRYPT 2015*. Lecture Notes in Comput. Sci., **9056** (2015), 254–283.

K. G. Paterson, Imprimitive permutation groups and trapdoors in iterated block ciphers, *Fast Software Encryption*, Lecture Notes in Comput. Sci., **1636** (1999), 201–214.

C. E. Shannon, Communication theory of secrecy systems, *Bell System Tech.*, **28** (1949), 656–715.

R. Sparr and R. Wernsdorf, The round functions of KASUMI generate the alternating group, *Journal of Mathematical Cryptology*, **9**(1) (2015), 23–32.

R. Sparr and R. Wernsdorf, Group theoretic properties of Rijndael-like ciphers, *Discrete Appl. Math.*, **156** (2008), 3139–3149.

R. Wernsdorf, The round functions of RIJNDAEL generate the alternating group, Fast Software Encryption, Lecture Notes in Comput. Sci., **2365** (2002), 143–148.

R. Wernsdorf, The round functions of SERPENT generate the alternating group, 2000. Available from: `http://csrc.nist.gov/archive/aes/round2/comments/20000512-rwernsdorf.pdf`.

R. Wernsdorf, The one-round functions of the DES generate the alternating group, *Advances in Cryptology-EUROCRYPT '92*, Lecture Notes in Comput. Sci., **658** (1993), 99–112.