Partitions in the S-Box of Streebog and Kuznyechik

Léo Perrin

@lpp_crypto

FSE'19, Paris

informatics mathematics

From Russia with Love (1963)

How does the *Lektor* work?

From Russia with Love? (2016-2019)

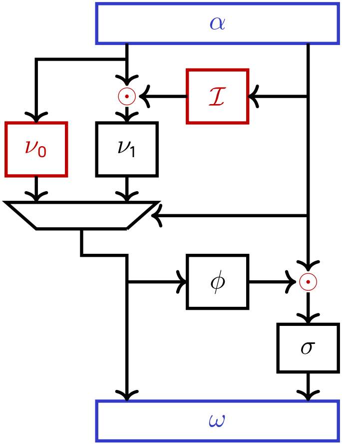
π' = (252, 238, 221, 17, 207, 110, 49, 22, 251, 196, 250, 218, 35, 197, 4, 77, 233, 119, 240, 219, 147, 46, 153, 186, 23, 54, 241. 187, 20, 205, 95, 193, 249, 24, 101, 90, 226, 92, 239, 33, 129, 28, 60, 66, 139, 1, 142, 79, 5, 132, 2, 174, 227, 106, 143, 160, 6, 11, 237, 152, 127, 212, 211, 31, 235, 52, 44, 81, 234, 200, 72, 171, 242, 42, 104, 162, 253, 58, 206, 204, 181, 112, 14, 86, 8, 12, 118, 18, 191, 114, 19, 71, 156, 183, 93, 135, 21, 161, 150, 41, 16, 123, 154, 199, 243, 145, 120, 111, 157, 158, 178, 177, 50, 117, 25, 61, 255, 53, 138, 126, 109, 84, 198, 128, 195, 189, 13, 87, 223, 245, 36, 169, 62, 168, 67, 201, 215, 121, 214, 246, 124, 34, 185, 3, 224, 15, 236, 222, 122, 148, 176, 188, 220, 232, 40, 80, 78, 51, 10, 74, 167, 151, 96, 115, 30, 0, 98, 68, 26, 184, 56, 130, 100, 159, 38, 65, 173, 69, 70, 146, 39, 94, 85, 47, 140, 163, 165, 125, 105, 213, 149, 59, 7, 88, 179, 64, 134, 172, 29, 247, 48, 55, 107, 228, 136, 217, 231, 137, 225, 27, 131, 73, 76, 63, 248, 254, 141, 83, 170, 144, 202, 216, 133, 97, 32, 113, 103, 164, 45, 43, 9, 91, 203, 155, 37, 208, 190, 229, 108, 82, 89, 166, 116, 210, 230, 244, 180, 192, 209, 102, 175, 194, 57, 75, 99, 182).

How does π work?

Outline

Outline

Previous decompositions: the TU-decomposition

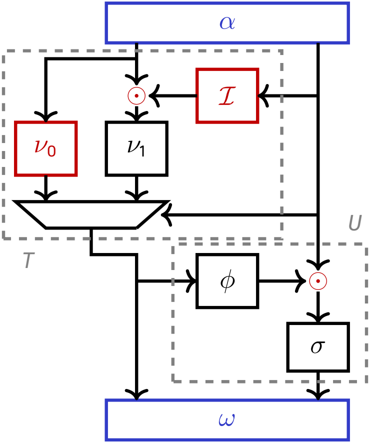


- $\odot$ Multiplication in $\mathbb{F}_{2^4}$
- $\mathcal{I}$ Inversion in $\mathbb{F}_{2^4}$
- ν_0 $\approx$ Discrete logarithm in $\mathbb{F}_{2^4}$
- ν_1, σ 4×4 permutations
- ϕ 4×4 function
- α, ω Linear permutations

Published in 2016[1].

[1] A. Biryukov, L. Perrin, A. Udovenko. *Reverse-engineering the S-box of streebog, kuznyechik and STRIBOBr1*. EUROCRYPT'16.

Previous decompositions: the TU-decomposition

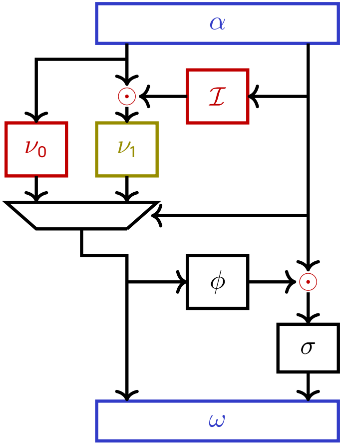


- $\odot$ Multiplication in $\mathbb{F}_{2^4}$
- $\mathcal{I}$ Inversion in $\mathbb{F}_{2^4}$
- ν_0 $\approx$ Discrete logarithm in $\mathbb{F}_{2^4}$
- ν_1, σ 4×4 permutations
- ϕ 4×4 function
- α, ω Linear permutations

Published in 2016[1].

[1] A. Biryukov, L. Perrin, A. Udovenko. *Reverse-engineering the S-box of streebog, kuznyechik and STRIBOBr1.* EUROCRYPT'16.

Previous decompositions: the TU-decomposition



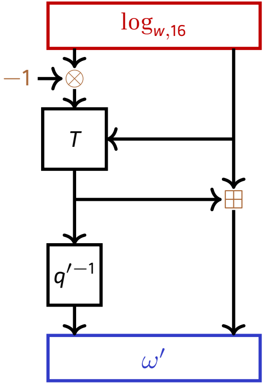
- $\odot$ Multiplication in $\mathbb{F}_{2^4}$
- $\mathcal{I}$ Inversion in $\mathbb{F}_{2^4}$
- ν_0 $\approx$ Discrete logarithm in $\mathbb{F}_{2^4}$
- ν_1, σ 4×4 permutations
- ϕ 4×4 function
- α, ω Linear permutations

Published in 2016[1].

ν_1 is differentially 16-uniform (the worst possible for differential cryptanalysis)!

[1] A. Biryukov, L. Perrin, A. Udovenko. *Reverse-engineering the S-box of streebog, kuznyechik and STRIBOBr1*. EUROCRYPT'16.

Previous decompositions: log-based



- Published in 2017[2]
- Completely different decomposition!
- Uses a $\approx$ discrete log. in $\mathbb{F}_{2^8}$.

[2] L. Perrin, A. Udovenko. *Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog*. ToSC vol. 16.

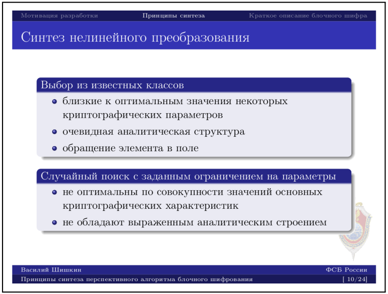
What then?

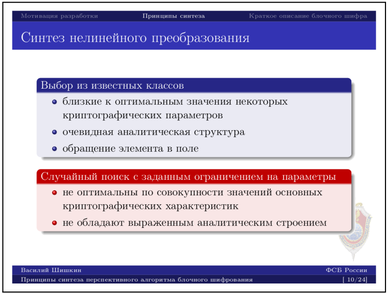
> Our results show that the algebraic structure, whose presence was known thanks to [PUB16], is stronger than hinted in this paper. The permutation π may have been built using one of the known decompositions. However, we think it more likely that each of these decompositions is a consequence of a strong algebraic structure used to design it, probably one related to a finite field exponential. Still this "master decomposition", from which the other would be consequences, remains elusive. Unfortunately, unless the Russian secret service release their design strategy, their exact process is likely to remain a mystery, if nothing else because of the existence of alternative decompositions: which exists by design and which is a mere side-effect of this design?

Exponential S-Boxes: a Link Between the S-Boxes of BelT and Kuznyechik/Streebog

Released by the designers

The following slides[3] are about **Kuznyechik**.





Selection from known classes

- close to optimal values of some cryptographic parameters
- obvious analytical structure
- finite field inversion

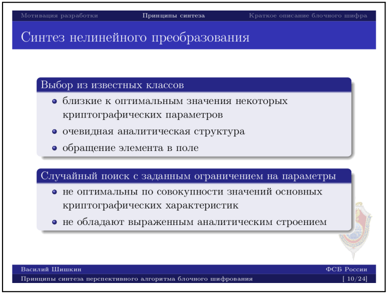
Random search with a given limit on the parameters

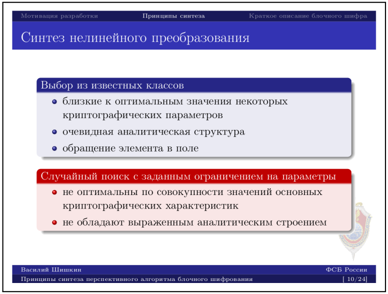
- are not optimal when considering the aggregate of the values of the basic cryptographic properties
- do not have a pronounced analytical structure

[3] Vassilij Shishkin. *Design principles of the perspective block encryption algorithm with a block length of 128 bits.* https://www.ruscrypto.ru/resource/archive/rc2013/files/03_shishkin.pdf

Released by the designers

The following slides[3] are about **Kuznyechik**.





Selection from known classes

- close to optimal values of some cryptographic parameters
- **obvious analytical structure**
- finite field inversion

Random search with a given limit on the parameters

- are not optimal when considering the aggregate of the values of the basic cryptographic properties
- **do not have a pronounced analytical structure**

[3] Vassilij Shishkin. *Design principles of the perspective block encryption algorithm with a block length of 128 bits.* https://www.ruscrypto.ru/resource/archive/rc2013/files/03_shishkin.pdf

Obtained from the designers

By Saarinen and Brumleyo[4] (2015)

" **Randomization** using various building blocks was simply iterated until a "good enough" permutation was found. This was seen as **an effective countermeasure against yet-unknown attacks**. "

[4] M. Saarinen, B. Brumleyo. *WHIRLBOB, the Whirlpool Based Variant of STRIBOB*. NordSec 2015.

Obtained from the designers

By Saarinen and Brumleyo[4] (2015)

" **Randomization** using various building blocks was simply iterated until a "good enough" permutation was found. This was seen as **an effective countermeasure against yet-unknown attacks**. "

At ISO/IEC (Jun. 2018)

- The designers **did not use the TU-decomposition**.
- Aim: best possible differential/linear properties from an **"optimized random search"**.
- Before the SHA-3 competition, the crypto community did not care about parameters origin and neither did the Streebog designers.

[4] M. Saarinen, B. Brumleyo. *WHIRLBOB, the Whirlpool Based Variant of STRIBOB*. NordSec 2015.

Obtained from the designers

By Saarinen and Brumleyo[4] (2015)

" **Randomization** using various building blocks was simply iterated until a "good enough" permutation was found. This was seen as **an effective countermeasure against yet-unknown attacks**. "

At ISO/IEC (Jun. 2018)

- The designers **did not use the TU-decomposition**.
- Aim: best possible differential/linear properties from an **"optimized random search"**.
- Before the SHA-3 competition, the crypto community did not care about parameters origin and neither did the Streebog designers. **(?)**

[4] M. Saarinen, B. Brumleyo. *WHIRLBOB, the Whirlpool Based Variant of STRIBOB*. NordSec 2015.

Obtained from the designers

By Saarinen and Brumleyo[4] (2015)

" **Randomization** using various building blocks was simply iterated until a "good enough" permutation was found. This was seen as **an effective countermeasure against yet-unknown attacks**. "

At ISO/IEC (Jun. 2018)

- The designers **did not use the TU-decomposition**.
- Aim: best possible differential/linear properties from an **"optimized random search"**.
- Before the SHA-3 competition, the crypto community did not care about parameters origin and neither did the Streebog designers. **(?)**

At CrossFyre 2018 (Sep. 2018)

During Q&A, a Russian cryptographer claimed the **TU-decomposition is correct**.

[4] M. Saarinen, B. Brumleyo. *WHIRLBOB, the Whirlpool Based Variant of STRIBOB*. NordSec 2015.

Outline

Partitions of $\mathbb{F}_{2^{2m}}$

Multiplicative cosets

Any element of $\mathbb{F}^*_{2^{2m}m}$ can be written $\alpha^{i+(2^m+1)j}$, so that

$$\mathbb{F}_{2^{2m}} = \{0\} \cup \left(\bigcup_{i=0}^{2^m} \alpha^i \odot \mathbb{F}^*_{2^m} \right) = \mathbb{F}_{2^m} \cup \left(\bigcup_{i=1}^{2^m} \alpha^i \odot \mathbb{F}^*_{2^m} \right) .$$

Partitions of $\mathbb{F}_{2^{2m}}$

Multiplicative cosets

Any element of $\mathbb{F}^*_{2^{2m}m}$ can be written $\alpha^{i+(2^m+1)j}$, so that

$$\mathbb{F}_{2^{2m}} = \{0\} \cup \left(\bigcup_{i=0}^{2^m} \alpha^i \odot \mathbb{F}^*_{2^m} \right) = \mathbb{F}_{2^m} \cup \left(\bigcup_{i=1}^{2^m} \alpha^i \odot \mathbb{F}^*_{2^m} \right) .$$

Additive cosets

$\mathbb{F}_{2^m}$ is a vector subspace of dimension m of $\mathbb{F}_{2^{2m}}$.
$\implies$ there exists a subspace W of $\mathbb{F}_{2^{2m}}$ such that $\dim(W) = m$ and

$$\mathbb{F}_{2^{2m}} = \bigcup_{w \in W} w \oplus \mathbb{F}_{2^m} = W \cup \left(\bigcup_{w \in W} w \oplus \mathbb{F}^*_{2^m} \right) .$$

Partitions of $\mathbb{F}_{2^{2m}}$

Multiplicative cosets

Any element of $\mathbb{F}^*_{2^{2mm}}$ can be written $\alpha^{i+(2^m+1)j}$, so that

$$\mathbb{F}_{2^{2m}} = \{0\} \cup \left(\bigcup_{i=0}^{2^m} \alpha^i \odot \mathbb{F}^*_{2^m} \right) = \mathbb{F}_{2^m} \cup \left(\bigcup_{i=1}^{2^m} \alpha^i \odot \mathbb{F}^*_{2^m} \right) .$$

Additive cosets

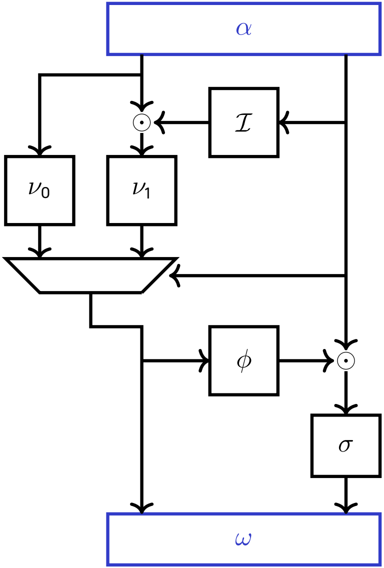
$\mathbb{F}_{2^m}$ is a vector subspace of dimension m of $\mathbb{F}_{2^{2m}}$.
$\implies$ there exists a subspace W of $\mathbb{F}_{2^{2m}}$ such that $\dim(W) = m$ and

$$\mathbb{F}_{2^{2m}} = \bigcup_{w \in W} w \oplus \mathbb{F}_{2^m} = W \cup \left(\bigcup_{w \in W} w \oplus \mathbb{F}^*_{2^m} \right) .$$

Both partitions involve one vector space of dimension m and 2^m "almost spaces" of size $2^m - 1$.

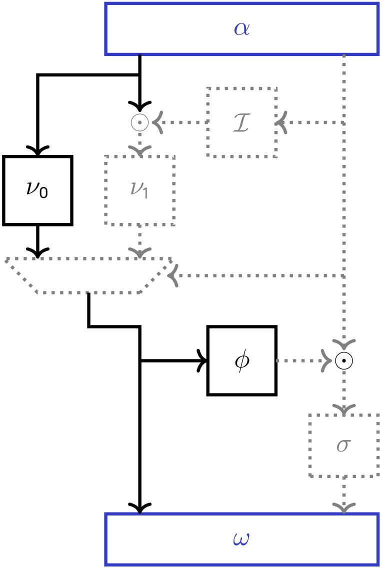
Here we go again!

- **New tool:** a vector space search algorithm!



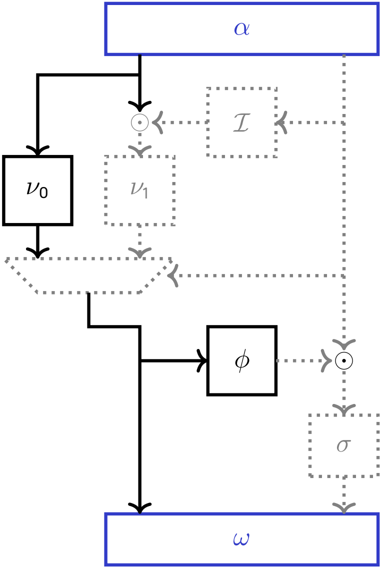
Here we go again!

- **New tool:** a vector space search algorithm!
- Expected: one space of dimension 4 mapped to another (when the right branch is 0).



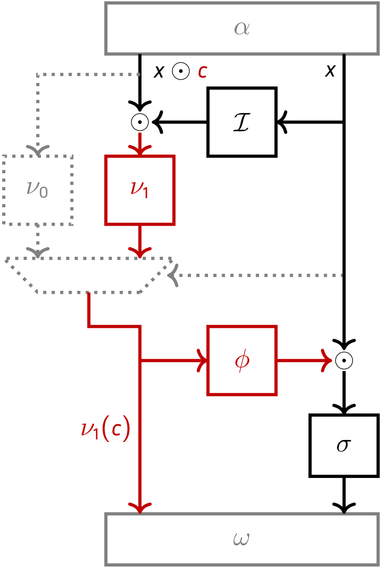
Here we go again!

- **New tool:** a vector space search algorithm!
- Expected: one space of dimension 4 mapped to another (when the right branch is 0).
- The tool found **2** such patterns!



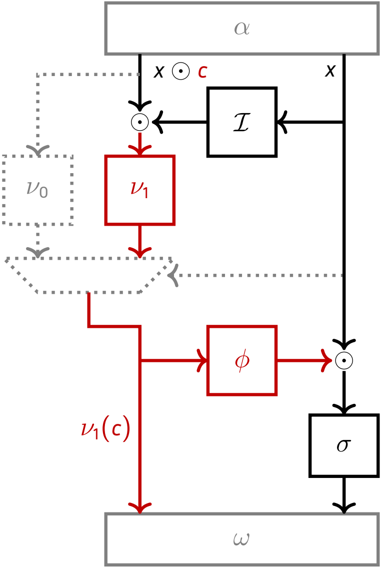
Here we go again!

- **New tool:** a vector space search algorithm!
- Expected: one space of dimension 4 mapped to another (when the right branch is 0).
- The tool found **2** such patterns!
- This transition can be generalized to “almost space” trails.

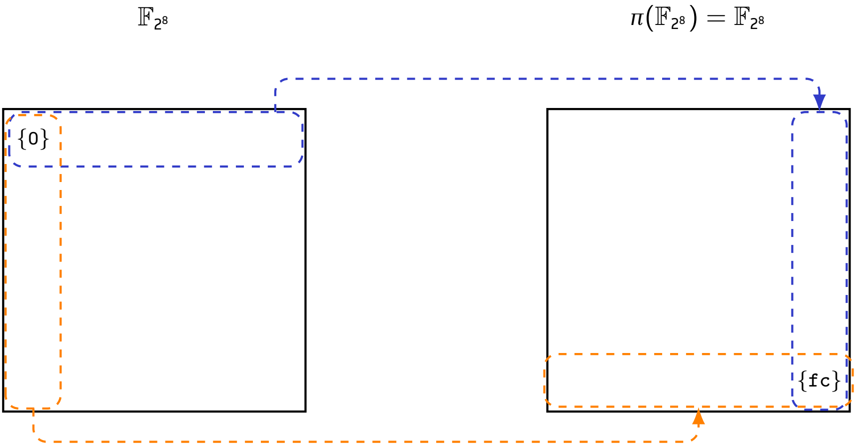


Here we go again!

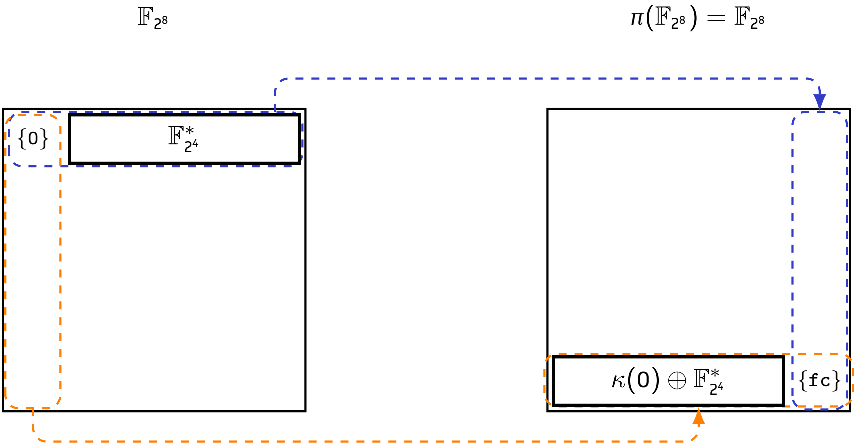
- **New tool:** a vector space search algorithm!
- Expected: one space of dimension 4 mapped to another (when the right branch is 0).
- The tool found **2** such patterns!
- This transition can be generalized to “almost space” trails.
- **16 of them!**



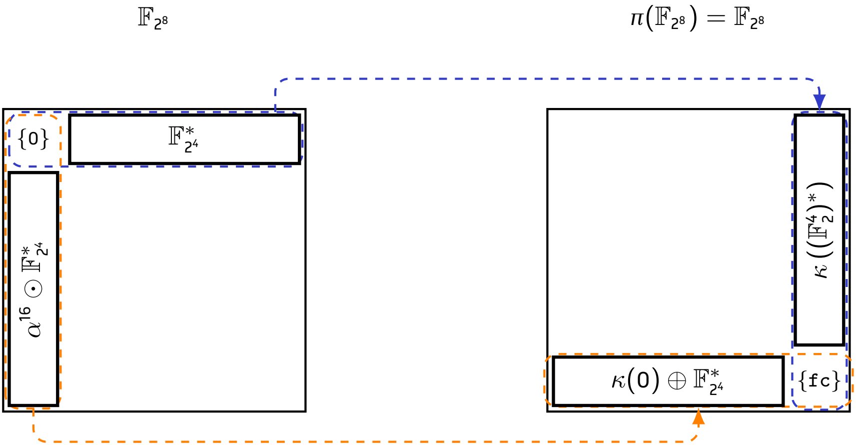
Cosets to cosets



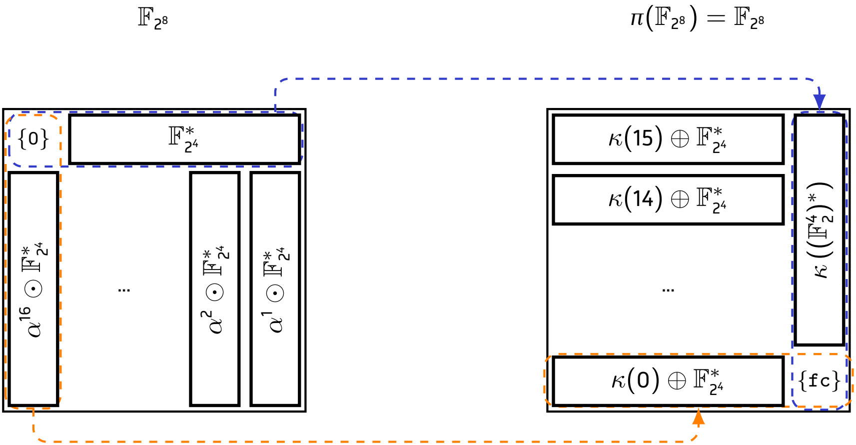
Cosets to cosets



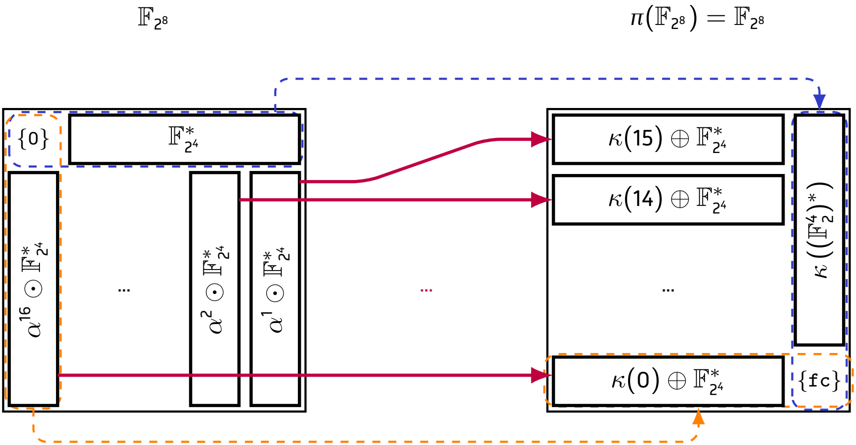
Cosets to cosets



Cosets to cosets



Cosets to cosets



π maps the partition of $\mathbb{F}_{2^8}$ into multiplicative cosets of $\mathbb{F}^*_{2^4}$ to its partition into additive cosets of $\mathbb{F}^*_{2^4}$!

The TKlog

A TKlog, denoted $\mathscr{T}_{\kappa,s}$, operates on $\mathbb{F}_{2^{2m}}$ and uses:

- α: a generator of $\mathbb{F}_{2^{2m}}$,
- κ: an affine function $\mathbb{F}_2^m \to \mathbb{F}_{2^{2m}}$ with $\langle \kappa(\mathbb{F}_2^m) \cup \mathbb{F}_{2^m} \rangle = \mathbb{F}_{2^{2m}}$,
- s: a permutation of $\mathbb{Z}/(2^m - 1)\mathbb{Z}$.

It works as follows:

$$\begin{cases} \mathscr{T}_{\kappa,s}(0) & = \kappa(0)\,, \\ \mathscr{T}_{\kappa,s}\left(\left(\alpha^{2^m+1}\right)^j\right) & = \kappa(2^m - j), \text{ for } 1 \leq j \leq 2^m - 1\,, \\ \mathscr{T}_{\kappa,s}\left(\alpha^{i+(2^m+1)j}\right) & = \kappa(2^m - i) \oplus \left(\alpha^{2^m+1}\right)^{s(j)}, \text{ for } 0 < i, 0 \leq j < 2^m - 1\,. \end{cases}$$

Some properties

Separation

π satisfies the following set equalities

$$\begin{cases} \pi\left(\mathbb{F}_{2^4}\right) & = \kappa(\mathbb{F}_2^4) \\ \pi\left(\alpha^i \odot \mathbb{F}_{2^4}^*\right) & = \kappa(16 - i) \oplus \mathbb{F}_{2^m}^* , \ \forall i \neq 0 \, . \end{cases}$$

Its restriction to each multiplicative coset is always the same:

$$\mathcal{T}_{\kappa,s}\left(\alpha^{i+(2^m+1)j}\right) = \underbrace{\kappa(2^m - i)}_{\in \kappa(\mathbb{F}_2^m)} \oplus \underbrace{\left(\alpha^{2^m+1}\right)^{s(j)}}_{\in \mathbb{F}_{2^m}^*} \, .$$

Some properties

Separation

π satisfies the following set equalities

$$\begin{cases} \pi\left(\mathbb{F}_{2^4}\right) & = \kappa(\mathbb{F}_2^4) \\ \pi\left(\alpha^i \odot \mathbb{F}_{2^4}^*\right) & = \kappa(16 - i) \oplus \mathbb{F}_{2^m}^* \text{ , } \forall i \neq 0 \text{ .} \end{cases}$$

Its restriction to each multiplicative coset is always the same:

$$\mathcal{T}_{\kappa,s}\left(\alpha^{i+(2^m+1)j}\right) = \underbrace{\kappa(2^m - i)}_{\in \kappa(\mathbb{F}_2^m)} \oplus \underbrace{\left(\alpha^{2^m+1}\right)^{s(j)}}_{\in \mathbb{F}_{2^m}^*} \text{ .}$$

If s depended on i then the coset-to-coset properties would still hold.

π is even simpler than that!

Some properties

Separation

π satisfies the following set equalities

$$\begin{cases} \pi\left(\mathbb{F}_{2^4}\right) & = \kappa(\mathbb{F}_2^4) \\ \pi\left(\alpha^i \odot \mathbb{F}_{2^4}^*\right) & = \kappa(16 - i) \oplus \mathbb{F}_{2^m}^* \ , \ \forall i \neq 0 \ . \end{cases}$$

Its restriction to each multiplicative coset is always the same:

$$\mathscr{T}_{\kappa,s}\left(\alpha^{i+(2^m+1)j}\right) = \underbrace{\kappa(2^m - i)}_{\in \kappa(\mathbb{F}_2^m)} \oplus \underbrace{\left(\alpha^{2^m+1}\right)^{s(j)}}_{\in \mathbb{F}_{2^m}^*} \ .$$

If s depended on i then the coset-to-coset properties would still hold.
π is even simpler than that!

The missing link

A TKlog instance **always** has a TU-decomposition identical to that in the EC'16 paper.

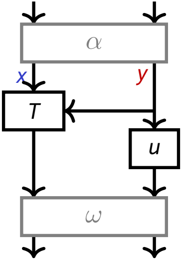
Outline

Partition-based backdoors (1/2)

In[5], Bannier introduced a backdoor such that, **regardless of the key schedule**:

$$x \in \mathcal{V}_i \Leftrightarrow E_k(x) \in \mathcal{W}_i$$

where the $\mathcal{V}_i$ and $\mathcal{W}_i$ are affine spaces of constant dimension.



Theorem (simplified)

In order to enable a partition-based backdoor, an S-box S of $\mathbb{F}_2^{2m}$ must be such that

$$(\omega^{-1} \circ S \circ \alpha^{-1})(x, y) = T_y(x) \oplus u(y)$$

for some linear permutations α, ω.

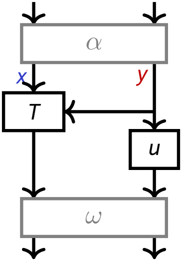
[5] Arnaud Bannier. *Combinatorial Analysis of Block Ciphers With Trapdoors*. PhD thesis ENSAM 2017.

Partition-based backdoors (1/2)

In[5], Bannier introduced a backdoor such that, **regardless of the key schedule**:

$$x \in \mathcal{V}_i \Leftrightarrow E_k(x) \in \mathcal{W}_i$$

where the $\mathcal{V}_i$ and $\mathcal{W}_i$ are affine spaces of constant dimension.



Theorem (simplified)

In order to enable a partition-based backdoor, an S-box S of $\mathbb{F}_2^{2m}$ must be such that

$$(\omega^{-1} \circ S \circ \alpha^{-1})(x, y) \ = \ T_y(x) \oplus u(y)$$

for some linear permutations α, ω.

In other words:

$$S(\alpha^{-1}(0, y) \oplus \mathcal{V}) \ = \ \omega(0, u(y)) \oplus \mathcal{W}, \text{ where } \begin{cases} \mathcal{V} & = \alpha^{-1}(\{(x, 0), x \in \mathbb{F}_2^m\}) \\ \mathcal{W} & = \omega(\{(x, 0), x \in \mathbb{F}_2^m\}) \end{cases}$$

[5] Arnaud Bannier. *Combinatorial Analysis of Block Ciphers With Trapdoors*. PhD thesis ENSAM 2017.

Partition-based backdoors (2/2)

What Bannier established is that, in order to have a partition-preserving backdoor, it is necessary to have **an S-box mapping additive cosets of a subspace to additive cosets of a subspace**.

Partition-based backdoors (2/2)

What Bannier established is that, in order to have a partition-preserving backdoor, it is necessary to have **an S-box mapping additive cosets of a subspace to additive cosets of a subspace**.

π does not.

Partition-based backdoors (2/2)

What Bannier established is that, in order to have a partition-preserving backdoor, it is necessary to have **an S-box mapping additive cosets of a subspace to additive cosets of a subspace**.

π does not.

But.

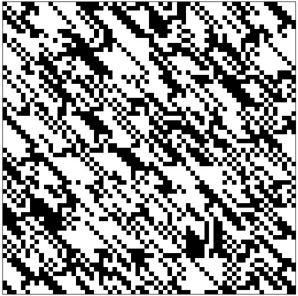
The linear layer of Streebog interacts with both additive and multiplicative cosets of $\mathbb{F}_{2^4}$!

The linear layer of Streebog

5.4 Линейное преобразование множества двоичных векторов

Линейное преобразование l множества двоичных векторов V_{64} задается умножением справа на матрицу A над полем $GF(2)$, строки которой записаны ниже последовательно в шестнадцатеричном виде. Строка матрицы с номером j, $j = 0,\dots,63$, записанная в виде $a_{j,15} \dots a_{j,0}$, где $a_{j,i} \in \mathbb{Z}_{16}$, $i = 0,\dots,15$, есть $\mathrm{Vec}_4(a_{j,15}) \| \dots \| \mathrm{Vec}_4(a_{j,0})$.

8e20faa72ba0b470	47107ddd9b505a38	ad08b0e0c3282d1c	d8045870ef14980e
6c022c38f90a4c07	3601161cf205268d	1b8e0b0e798c13c8	83478b07b2468764
a011d380818e8f40	5086e740ce47c920	2843fd2067adea10	14aff010bdd87508
0ad97808d06cb404	05e23c0468365a02	8c711e02341b2d01	46b60f011a83988e
90dab52a387ae76f	486dd4151c3dfdb9	24b86a840e90f0d2	125c354207487869
092e94218d243cba	8a174a9ec8121e5d	4585254f64090fa0	accc9ca9328a8950
9d4df05d5f661451	c0a878a0a1330aa6	60543c50de970553	302a1e286fc58ca7
18150f14b9ec46dd	0c84890ad27623e0	0642ca05693b9f70	0321658cba93c138
86275df09ce8aaa8	439da0784e745554	afc0503c273aa42a	d960281e9d1d5215
e230140fc0802984	71180a8960409a42	b60c05ca30204d21	5b068c651810a89e
456c34887a3805b9	ac361a443d1c8cd2	561b0d22900e4669	2b838811480723ba
9bcf4486248d9f5d	c3e9224312c8c1a0	effa11af0964ee50	f97d86d98a327728
e4fa2054a80b329c	727d102a548b194e	39b008152acb8227	9258048415eb419d
492c024284fbaec0	aa16012142f35760	550b8e9e21f7a530	a48b474f9ef5dc18
70a6a56e2440598e	3853dc371220a247	1ca76e95091051ad	0edd37c48a08a6d8
07e095624504536c	8d70c431ac02a736	c83862965601dd1b	641c314b2b8ee083

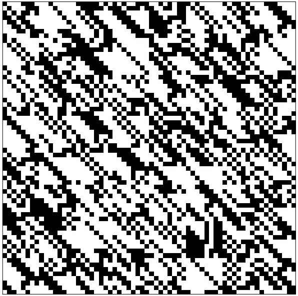


The linear layer of Streebog

5.4 Линейное преобразование множества двоичных векторов

Линейное преобразование l множества двоичных векторов V_{64} задается умножением справа на матрицу A над полем $GF(2)$, строки которой записаны ниже последовательно в шестнадцатеричном виде. Строка матрицы с номером j, $j = 0,\dots,63$, записанная в виде $a_{j,15} \dots a_{j,0}$, где $a_{j,i} \in \mathbb{Z}_{16}$, $i = 0, \dots, 15$, есть $\mathrm{Vec}_4(a_{j,15})\|\dots\|\mathrm{Vec}_4(a_{j,0})$.

8e20faa72ba0b470	47107ddd9b505a38	ad08b0e0c3282d1c	d8045870ef14980e
6c022c38f90a4c07	3601161cf205268d	1b8e0b0e798c13c8	83478b07b2468764
a011d380818e8f40	5086e740ce47c920	2843fd2067adea10	14aff010bdd87508
0ad97808d06cb404	05e23c0468365a02	8c711e02341b2d01	46b60f011a83988e
90dab52a387ae76f	486dd4151c3dfdb9	24b86a840e90f0d2	125c354207487869
092e94218d243cba	8a174a9ec8121e5d	4585254f64090fa0	accc9ca9328a8950
9d4df05d5f661451	c0a878a0a1330aa6	60543c50de970553	302a1e286fc58ca7
18150f14b9ec46dd	0c84890ad27623e0	0642ca05693b9f70	0321658cba93c138
86275df09ce8aaa8	439da0784e745554	afc0503c273aa42a	d960281e9d1d5215
e230140fc0802984	71180a8960409a42	b60c05ca30204d21	5b068c651810a89e
456c34887a3805b9	ac361a443d1c8cd2	561b0d22900e4669	2b838811480723ba
9bcf4486248d9f5d	c3e9224312c8c1a0	effa11af0964ee50	f97d86d98a327728
e4fa2054a80b329c	727d102a548b194e	39b008152acb8227	9258048415eb419d
492c024284fbaec0	aa16012142f35760	550b8e9e21f7a530	a48b474f9ef5dc18
70a6a56e2440598e	3853dc371220a247	1ca76e95091051ad	0edd37c48a08a6d8
07e095624504536c	8d70c431ac02a736	c83862965601dd1b	641c314b2b8ee083



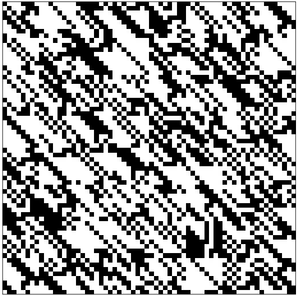
It is actually an 8×8 matrix of $\mathbb{F}_{2^8}$...

The linear layer of Streebog

5.4 Линейное преобразование множества двоичных векторов

Линейное преобразование l множества двоичных векторов V_{64} задается умножением справа на матрицу A над полем $GF(2)$, строки которой записаны ниже последовательно в шестнадцатеричном виде. Строка матрицы с номером j, $j = 0,\ldots,63$, записанная в виде $a_{j,15} \ldots a_{j,0}$, где $a_{j,i} \in \mathbb{Z}_{16}$, $i = 0, \ldots, 15$, есть $\mathrm{Vec}_4(a_{j,15})\|\ldots\|\mathrm{Vec}_4(a_{j,0})$.

8e20faa72ba0b470	47107ddd9b505a38	ad08b0e0c3282d1c	d8045870ef14980e
6c022c38f90a4c07	3601161cf205268d	1b8e0b0e798c13c8	83478b07b2468764
a011d380818e8f40	5086e740ce47c920	2843fd2067adea10	14aff010bdd87508
0ad97808d06cb404	05e23c0468365a02	8c711e02341b2d01	46b60f011a83988e
90dab52a387ae76f	486dd4151c3dfdb9	24b86a840e90f0d2	125c354207487869
092e94218d243cba	8a174a9ec8121e5d	4585254f64090fa0	accc9ca9328a8950
9d4df05d5f661451	c0a878a0a1330aa6	60543c50de970553	302a1e286fc58ca7
18150f14b9ec46dd	0c84890ad27623e0	0642ca05693b9f70	0321658cba93c138
86275df09ce8aaa8	439da0784e745554	afc0503c273aa42a	d960281e9d1d5215
e230140fc0802984	71180a8960409a42	b60c05ca30204d21	5b068c651810a89e
456c34887a3805b9	ac361a443d1c8cd2	561b0d22900e4669	2b838811480723ba
9bcf4486248d9f5d	c3e9224312c8c1a0	effa11af0964ee50	f97d86d98a327728
e4fa2054a80b329c	727d102a548b194e	39b008152acb8227	9258048415eb419d
492c024284fbaec0	aa16012142f35760	550b8e9e21f7a530	a48b474f9ef5dc18
70a6a56e2440598e	3853dc371220a247	1ca76e95091051ad	0edd37c48a08a6d8
07e095624504536c	8d70c431ac02a736	c83862965601dd1b	641c314b2b8ee083



It is actually an 8×8 matrix of $\mathbb{F}_{2^8}$... **defined in the same field as π**!

Subfield to multiplicative cosets

$$L = \begin{bmatrix} 83 & 47 & 8b & 07 & b2 & 46 & 87 & 64 \\ 46 & b6 & 0f & 01 & 1a & 83 & 98 & 8e \\ ac & cc & 9c & a9 & 32 & 8a & 89 & 50 \\ 03 & 21 & 65 & 8c & ba & 93 & c1 & 38 \\ 5b & 06 & 8c & 65 & 18 & 10 & a8 & 9e \\ f9 & 7d & 86 & d9 & 8a & 32 & 77 & 28 \\ a4 & 8b & 47 & 4f & 9e & f5 & dc & 18 \\ 64 & 1c & 31 & 4b & 2b & 8e & e0 & 83 \end{bmatrix} .$$

If $X = (x, 0, \ldots, 0)$, then

$$X \times L = \left(x \odot L_{0,0},\ x \odot L_{0,1}, \ldots, x \odot L_{0,7}\right) .$$

Subfield to multiplicative cosets

$$L = \begin{bmatrix} \texttt{83} & \texttt{47} & \texttt{8b} & \texttt{07} & \texttt{b2} & \texttt{46} & \texttt{87} & \texttt{64} \\ \texttt{46} & \texttt{b6} & \texttt{0f} & \texttt{01} & \texttt{1a} & \texttt{83} & \texttt{98} & \texttt{8e} \\ \texttt{ac} & \texttt{cc} & \texttt{9c} & \texttt{a9} & \texttt{32} & \texttt{8a} & \texttt{89} & \texttt{50} \\ \texttt{03} & \texttt{21} & \texttt{65} & \texttt{8c} & \texttt{ba} & \texttt{93} & \texttt{c1} & \texttt{38} \\ \texttt{5b} & \texttt{06} & \texttt{8c} & \texttt{65} & \texttt{18} & \texttt{10} & \texttt{a8} & \texttt{9e} \\ \texttt{f9} & \texttt{7d} & \texttt{86} & \texttt{d9} & \texttt{8a} & \texttt{32} & \texttt{77} & \texttt{28} \\ \texttt{a4} & \texttt{8b} & \texttt{47} & \texttt{4f} & \texttt{9e} & \texttt{f5} & \texttt{dc} & \texttt{18} \\ \texttt{64} & \texttt{1c} & \texttt{31} & \texttt{4b} & \texttt{2b} & \texttt{8e} & \texttt{e0} & \texttt{83} \end{bmatrix} .$$

If $X = (x, 0, \ldots, 0)$, then

$$X \times L = \left(x \odot L_{0,0},\ x \odot L_{0,1}, \ldots, x \odot L_{0,7} \right) .$$

Open problems

- Is there a stronger hidden structure in L?
- Can we leverage these properties to attack Streebog (or Kuznyechik)?

Some natural questions

- Isn't it possible to find a decomposition in any permutation?

- Others have used exponential/log-based S-boxes... why is it wrong this time?

- What is so special about this 3rd (!) decomposition? Why would this one be the one used by the designers?

Some natural questions

- Isn't it possible to find a decomposition in any permutation?

  No.

- Others have used exponential/log-based S-boxes... why is it wrong this time?

- What is so special about this 3rd (!) decomposition? Why would this one be the one used by the designers?

Some natural questions

- Isn't it possible to find a decomposition in any permutation?

  No.

- Others have used exponential/log-based S-boxes... why is it wrong this time?

  Because it's not a logarithm, it maps $\mathbb{F}_{2^8}$ to itself (and not $\mathbb{Z}/2^8\mathbb{Z}$). It also interacts in a very non-trivial way with the linear layer of Streebog.

- What is so special about this 3rd (!) decomposition? Why would this one be the one used by the designers?

The presence of the TKlog has to be deliberate

8-bit permutations

$$256! \approx 2^{1684}$$

8-bit TKlogs

$$\underbrace{16}_{\text{polynomial}} \times \underbrace{2^{30.3}}_{\text{lin. part of } \kappa} \times \underbrace{2^{8}}_{\kappa(0)} \times \underbrace{15!}_{s} \approx 2^{82.6}$$

8-bit affine permutations

$$\underbrace{\prod_{i=0}^{7}(2^8 - 2^i)}_{\text{linear part}} \underbrace{2^8}_{\text{cstt}} \times \approx 2^{70.2}$$

The presence of the TKlog has to be deliberate

8-bit permutations

$$256! \approx 2^{1684}$$

8-bit TKlogs

$$\underbrace{16}_{\text{polynomial}} \times \underbrace{2^{30.3}}_{\text{lin. part of } \kappa} \times \underbrace{2^{8}}_{\kappa(0)} \times \underbrace{15!}_{s} \approx 2^{82.6}$$

8-bit affine permutations

$$\underbrace{\prod_{i=0}^{7}(2^8 - 2^i)}_{\text{linear part}} \underbrace{2^{8}}_{\text{cstt}} \times \approx 2^{70.2}$$

If a "random permutation generator" returned an affine permutation, you would conclude that it did so on purpose. The situation is the same for TKlogs.

Possible generation algorithm

1. Generate a random TKlog
2. Are **both** linearity and diff. uniformity the best possible for a TKlog?
   - if not, go back to 1.
   - if yes, then output the TKlog

Possible generation algorithm

1. Generate a random TKlog
2. Are **both** linearity and diff. uniformity the best possible for a TKlog?
   - if not, go back to 1.
   - if yes, then output the TKlog

We only need to generate $\approx 2^{10.6}$ instances (experimental result).

The result closely resembles π and it is not better than a "regular" logarithm.

Outline

Conclusion

https://who.paris.inria.fr/Leo.Perrin/pi.html

Conclusion

`https://who.paris.inria.fr/Leo.Perrin/pi.html`

The TKlog structure in π...

... is a **deliberate** choice by its designers,

... is very reminiscent of a known backdoor structure.

Conclusion

`https://who.paris.inria.fr/Leo.Perrin/pi.html`

The TKlog structure in π...

... is a **deliberate** choice by its designers,
... is very reminiscent of a known backdoor structure.

Until the designers of Streebog and Kuznyechik explain how their "random generation process" could output an S-box mapping cosets of $\mathbb{F}_{2^4}^*$ to cosets of $\mathbb{F}_{2^4}^*$ in the same field as the one used for the linear layer of Streebog, and **why** that might be a good thing...

Conclusion

`https://who.paris.inria.fr/Leo.Perrin/pi.html`

The TKlog structure in π...

... is a **deliberate** choice by its designers,
... is very reminiscent of a known backdoor structure.

Until the designers of Streebog and Kuznyechik explain how their "random generation process" could output an S-box mapping cosets of $\mathbb{F}_{2^4}^*$ to cosets of $\mathbb{F}_{2^4}^*$ in the same field as the one used for the linear layer of Streebog, and **why** that might be a good thing...

... Do not use these algorithms.

Conclusion

`https://who.paris.inria.fr/Leo.Perrin/pi.html`

The TKlog structure in π...

... is a **deliberate** choice by its designers,
... is very reminiscent of a known backdoor structure.

Until the designers of Streebog and Kuznyechik explain how their "random generation process" could output an S-box mapping cosets of $\mathbb{F}_{2^4}^*$ to cosets of $\mathbb{F}_{2^4}^*$ in the same field as the one used for the linear layer of Streebog, and **why** that might be a good thing...

... Do not use these algorithms.

... Do not standardize them.

Components

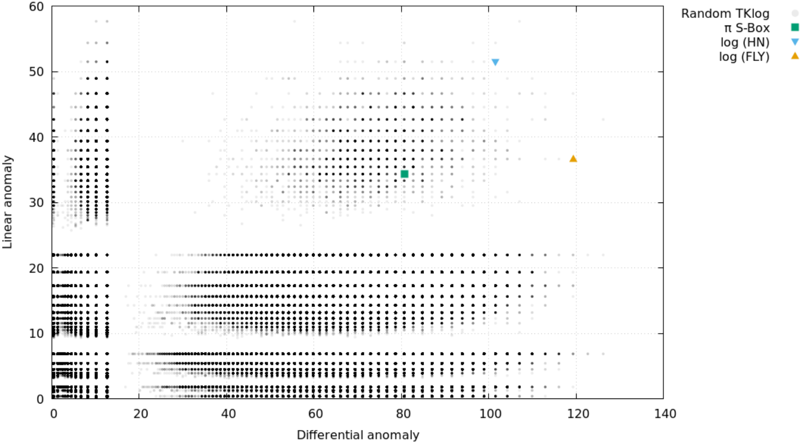
- `s = [0,12,9,8,7,4,14,6,5,10,2,11,1,3,13]`
- κ is such that $\kappa(x) = \kappa(0) \oplus \Lambda(x)$, where

$$\kappa(0) = \mathtt{FC}$$
$$\Lambda(1) = 1,\ \Lambda(2) = 26, \Lambda(4) = 24,\ \Lambda(8) = 30\ .$$

Λ only activates 4 output bits:

$$\Lambda(x)\ \&\ 36\ =\ \Lambda(x)\ .$$

Anomalies



Random TKlog
π S-Box
log (HN)
log (FLY)
Linear anomaly
Differential anomaly
0
10
20
30
40
50
60
0
20
40
60
80
100
120
140