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

Léo Perrin[1], Aleksei Udovenko[1]

[1]SnT, University of Luxembourg

https://www.cryptolux.org

March 6, 2017

Fast Software Encryption 2017

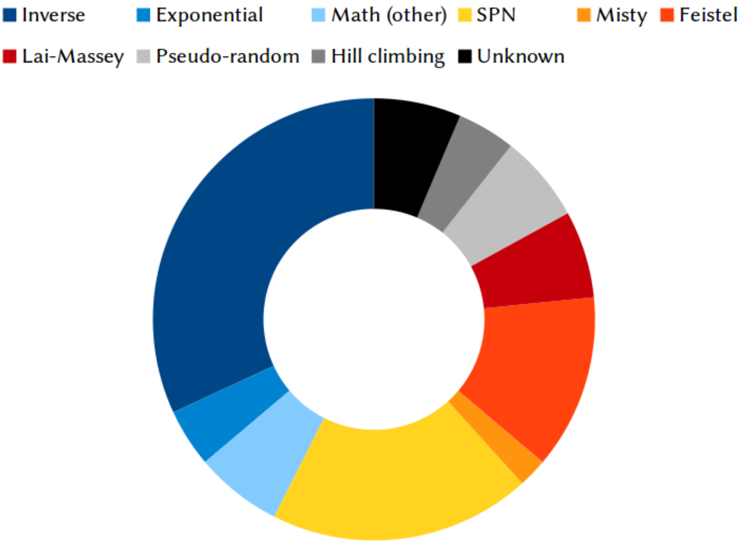
UNIVERSITÉ DU LUXEMBOURG

securityandtrust.lu

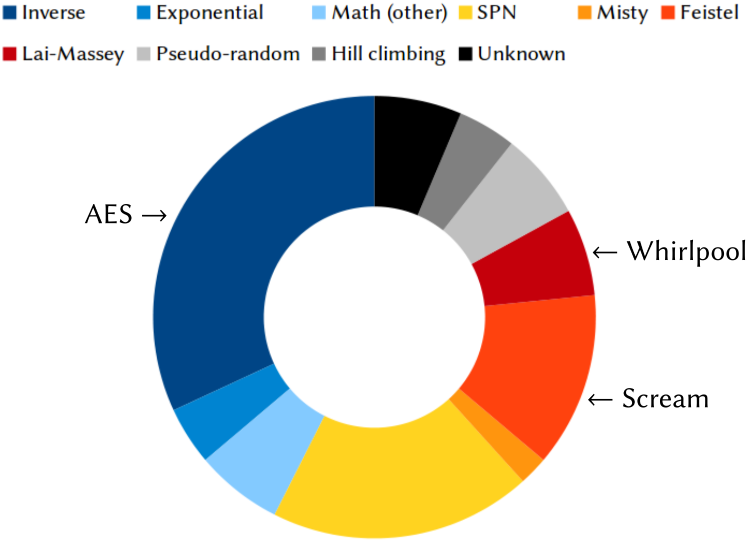
S-Box Design

■ Inverse ■ Exponential ■ Math (other) ■ SPN ■ Misty ■ Feistel
■ Lai-Massey ■ Pseudo-random ■ Hill climbing ■ Unknown

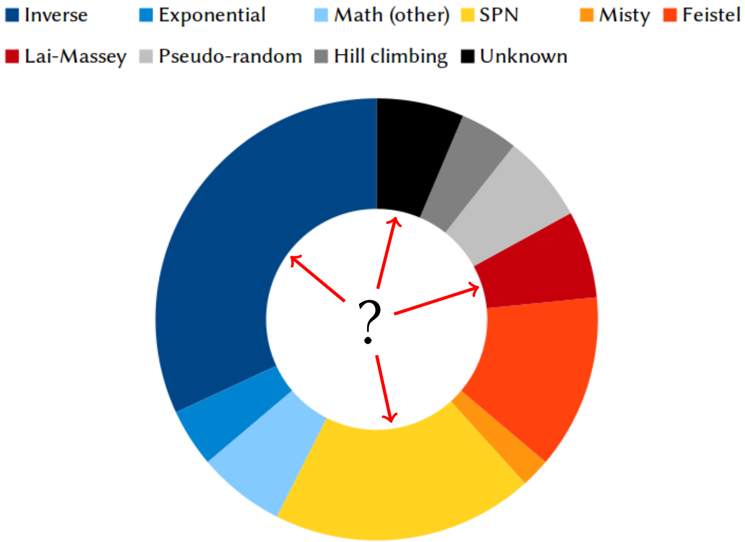
S-Box Design


Inverse
Exponential
Math (other)
SPN
Misty
Feistel
Lai-Massey
Pseudo-random
Hill climbing
Unknown

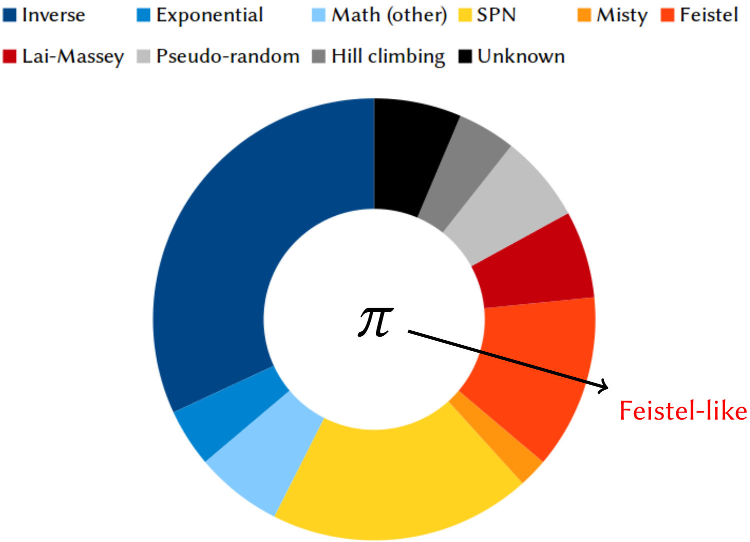
S-Box Design


Inverse
Exponential
Math (other)
SPN
Misty
Feistel
Lai-Massey
Pseudo-random
Hill climbing
Unknown
AES →
← Whirlpool
← Scream

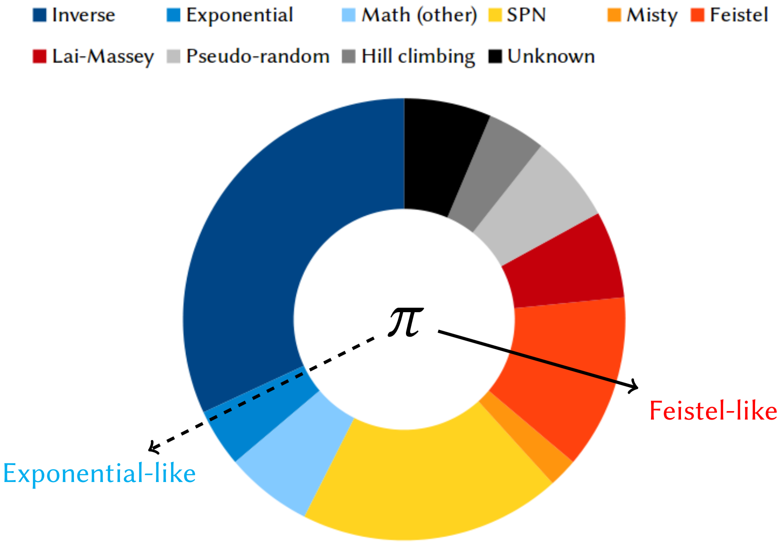
S-Box Reverse-Engineering



Results on Kuznyechik/Streebog



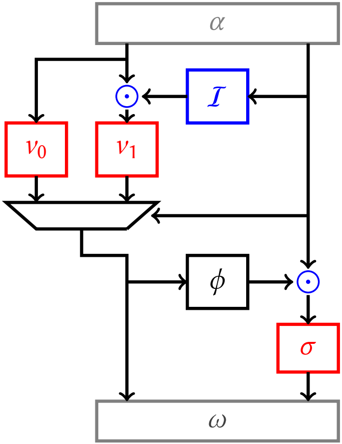
Results on Kuznyechik/Streebog



Outline

Plan

A First Decomposition of π



- From Eurocrypt'16
- α, ω: linear 8-bit permutations
- ν_0, ν_1, σ: 4-bit permutations
- ϕ: 4-bit function ($\phi(x) \neq 0$)
- $\mathcal{I}$ multiplicative inverse in $\mathbb{F}_{16}$
- $\odot$ multiplication in $\mathbb{F}_{16}$

How was it found?

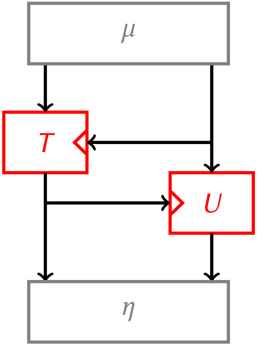
Decomposition Procedure Overview

1. Identify patterns in LAT;

How was it found?

Decomposition Procedure Overview

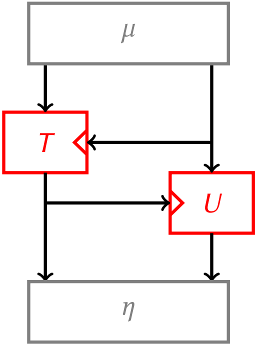
1. Identify patterns in LAT;
2. Deduce linear layers μ, η such that π is decomposed as in right picture;



How was it found?

Decomposition Procedure Overview

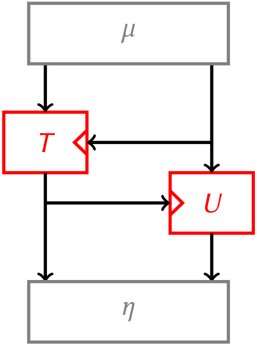
1. Identify patterns in LAT;
2. Deduce linear layers μ, η such that π is decomposed as in right picture;
3. Decompose U, T;



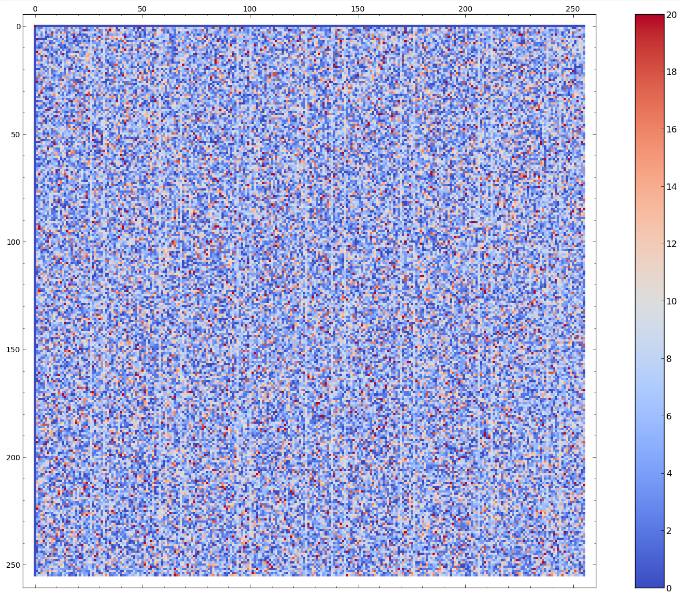
How was it found?

Decomposition Procedure Overview

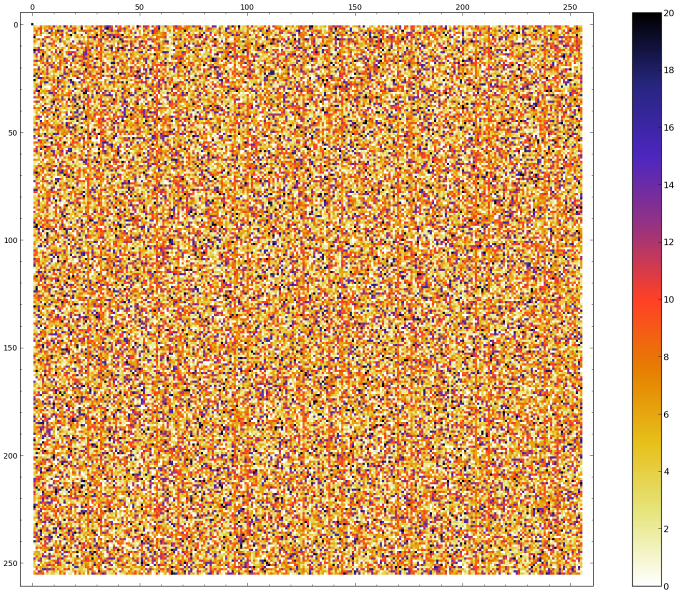
1. Identify patterns in LAT;
2. Deduce linear layers μ, η such that π is decomposed as in right picture;
3. Decompose U, T;
4. Put it all together.



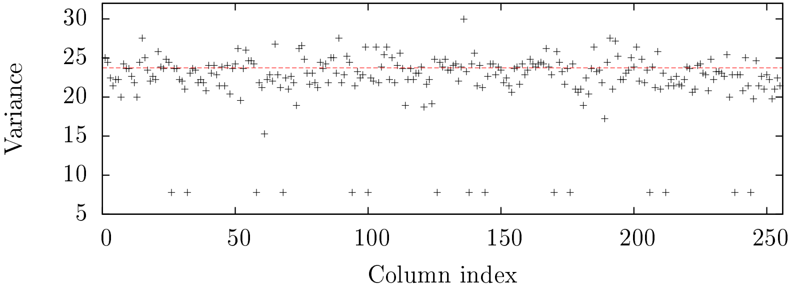
Pollock to the Rescue



Pollock to the Rescue



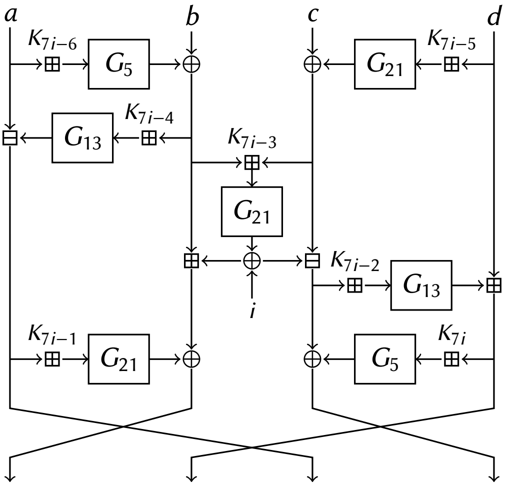
What the Lines Mean



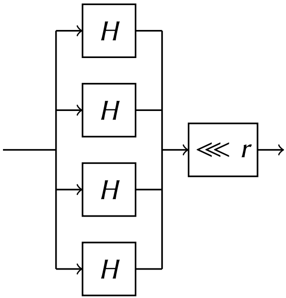
Variance of the absolute value of the coefficients in each column of the LAT of π.

Plan

Round Function of BelT

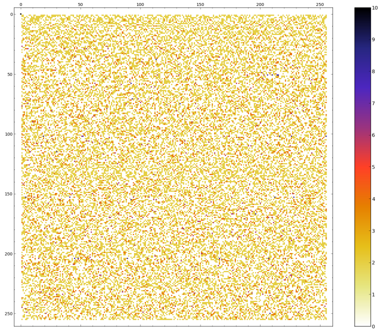


The round function of BelT.

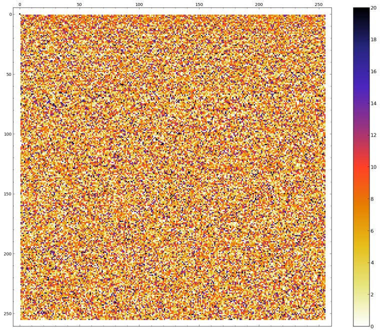


The 32-bit function G_r.

Properties of H



DDT



LAT

- max(DDT) = 8
- max(LAT) = 26
- $P[random] \leq 2^{-122}$

- Algebraic degree 7 (all coordinates)

Structure of H (1/3)

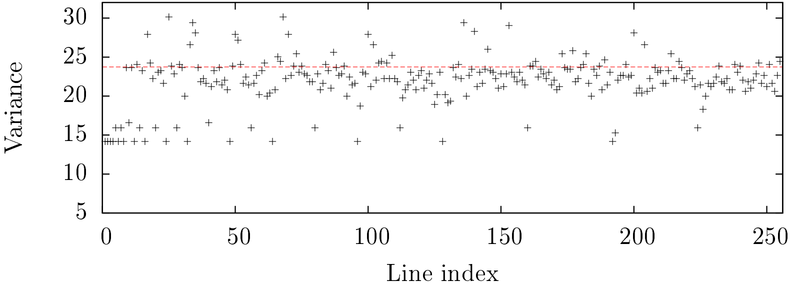
Is H structured?

Structure of H (1/3)

Is H structured?

Yes!

LAT Row Variance



Variance of the absolute value of the coefficients in each row of the LAT of H.

The Actual Structure

The BelT S-Box Construction (translated)

The look-up tables of the S-Box coordinate functions were chosen as different segments of length 255 of different linear recurrences defined by the irreducible polynomial $p(\lambda)$:

$$p(\lambda) = \lambda^8 + \lambda^6 + \lambda^5 + \lambda^2 + 1.$$

Additionally, a zero element was inserted in a fixed position of each segment.

[1] `http://eprint.iacr.org/2004/024`

The Actual Structure

The BelT S-Box Construction (translated)

The look-up tables of the S-Box coordinate functions were chosen as different segments of length 255 of different linear recurrences defined by the irreducible polynomial $p(\lambda)$:

$$p(\lambda) = \lambda^8 + \lambda^6 + \lambda^5 + \lambda^2 + 1.$$

Additionally, a zero element was inserted in a fixed position of each segment.

Equivalent Pseudo-Exponential Representation

$$S \;:=\; [w^i, i < z] \;+\; [0] \;+\; [w^i, z \leq i]$$

Exponential (case $z = 0$) studied in [AA04][1]

[1] http://eprint.iacr.org/2004/024

Properties of (Pseudo-)Exponentials

Exponential ($z = 0$) $\neq$ Pseudo-Exponential ($z \neq 0$)

Properties of (Pseudo-)Exponentials

Exponential ($z = 0$) $\neq$ Pseudo-Exponential ($z \neq 0$)

- "Exponential" definition inconsistent in literature...
- $z = 0$? $z = 255$?

Properties of (Pseudo-)Exponentials

Exponential ($z = 0$) $\neq$ Pseudo-Exponential ($z \neq 0$)

- "Exponential" definition inconsistent in literature...
- $z = 0$? $z = 255$?
- For exponentials, for all $a \in \mathbb{F}_2^n, r \in \mathbb{N}$:

$$\left\{\mathrm{LAT}[a, b],\ \forall b\right\} = \left\{\mathrm{LAT}[(a \lll r), b],\ \forall b\right\}$$

Properties of (Pseudo-)Exponentials

Exponential ($z = 0$) $\neq$ Pseudo-Exponential ($z \neq 0$)

- "Exponential" definition inconsistent in literature...
- $z = 0$? $z = 255$?
- For exponentials, for all $a \in \mathbb{F}_2^n, r \in \mathbb{N}$:

$$\left\{\text{LAT}[a, b],\ \forall b\right\} = \left\{\text{LAT}[(a \lll r), b],\ \forall b\right\}$$

- For pseudo-exponentials, for all ℓ, for $r < \log_2(z)$:

$$\left\{\text{LAT}[a, b],\ \forall b\right\} = \left\{\text{LAT}[(a \lll r), b],\ \forall b\right\}$$

Paper in Управление защитой информации *[Information Security Management]* discloses design criteria:

- good nonlinearity,
- $\Pr\left[H(x \boxplus a) \oplus H(x) = b\right]$ and $\Pr\left[H(x \oplus a) \boxminus H(x) = b\right]$ are low
- no quadratic equations relating inputs/outputs

Paper in Управление защитой информации *[Information Security Management]* discloses design criteria:

- good nonlinearity,
- $\Pr\left[H(x \boxplus a) \oplus H(x) = b\right]$ and $\Pr\left[H(x \oplus a) \boxminus H(x) = b\right]$ are low
- no quadratic equations relating inputs/outputs

Fair enough...

Paper in Управление защитой информации *[Information Security Management]* discloses design criteria:

- good nonlinearity,
- $\Pr\left[H(x \boxplus a) \oplus H(x) = b\right]$ and $\Pr\left[H(x \oplus a) \boxminus H(x) = b\right]$ are low
- no quadratic equations relating inputs/outputs

Fair enough...

... but then what of π?

Plan

Exponential-Like Pattern

Observation

- $x \oplus 2^j = x \boxplus 2^j$ if $x_j = 0$ and $x \oplus 2^j = x \boxminus 2^j$ if $x_j = 1$
- $w^{x \boxplus 1} = w \odot w^x$

Exponential-Like Pattern

Observation

- $x \oplus 2^j = x \boxplus 2^j$ if $x_j = 0$ and $x \oplus 2^j = x \boxminus 2^j$ if $x_j = 1$
- $w^{x \boxplus 1} = w \odot w^x$

$$\Longrightarrow \quad \Pr\left[w^{x \oplus 1}/w^x = w\right] = 1/2 \quad \text{and} \quad \Pr\left[w^{x \oplus 1}/w^x = w^{-1}\right] = 1/2$$

Exponential-Like Pattern

Observation

- $x \oplus 2^j = x \boxplus 2^j$ if $x_j = 0$ and $x \oplus 2^j = x \boxminus 2^j$ if $x_j = 1$
- $w^{x \boxplus 1} = w \odot w^x$

$\Longrightarrow$ $\Pr\left[w^{x \oplus 1} / w^x = w\right] = 1/2$ and $\Pr\left[w^{x \oplus 1} / w^x = w^{-1}\right] = 1/2$

In the case of π

Let $C = [\texttt{0x12}, \texttt{0x26}, \texttt{0x24}, \texttt{0x30}]$. Then:

$$\Pr\left[\begin{cases} \pi^{-1}(x \oplus C[i]) \ / \ \pi^{-1}(x) = w^{2^i}, \text{ or} \\ \pi^{-1}(x \oplus C[i]) \ / \ \pi^{-1}(x) = w^{-2^i} \end{cases}\right] = \frac{240}{256} .$$

Obtaining a First Decomposition

1. Assume that $\pi = \tau \circ \log$ for some simple τ;

Obtaining a First Decomposition

1. Assume that $\pi = \tau \circ \log$ for some simple τ;
2. Study $\tau = \log \circ \pi^{-1}$;

Obtaining a First Decomposition

1. Assume that $\pi = \tau \circ \log$ for some simple τ;
2. Study $\tau = \log \circ \pi^{-1}$;
3. Let α be such that $\alpha(2^{i}) = C[i]$ for $i < 4$;

Obtaining a First Decomposition

1. Assume that $\pi = \tau \circ \log$ for some simple τ;
2. Study $\tau = \log \circ \pi^{-1}$;
3. Let α be such that $\alpha(2^i) = C[i]$ for $i < 4$;
4. Use random values for $\alpha(2^i)$ for $i \geq 4$ such that α is 1-to-1;

Obtaining a First Decomposition

1. Assume that $\pi = \tau \circ \log$ for some simple τ;
2. Study $\tau = \log \circ \pi^{-1}$;
3. Let α be such that $\alpha(2^i) = C[i]$ for $i < 4$;
4. Use random values for $\alpha(2^i)$ for $i \geq 4$ such that α is 1-to-1;
5. Find linear patterns in $\tau \circ \alpha^{-1}$;

Obtaining a First Decomposition

1. Assume that $\pi = \tau \circ \log$ for some simple τ;
2. Study $\tau = \log \circ \pi^{-1}$;
3. Let α be such that $\alpha(2^i) = C[i]$ for $i < 4$;
4. Use random values for $\alpha(2^i)$ for $i \geq 4$ such that α is 1-to-1;
5. Find linear patterns in $\tau \circ \alpha^{-1}$;
6. Deduce better linear layer β such that $\tau \circ \beta^{-1}$ is even more structured

Structure of π^{-1}

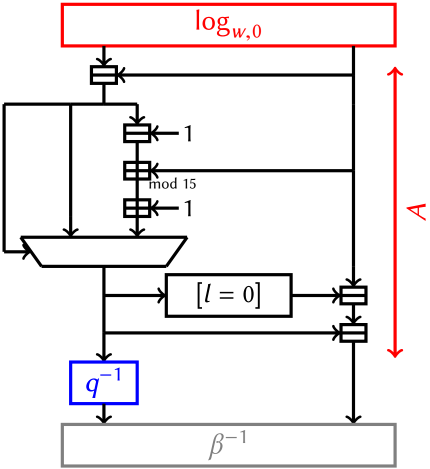
Algorithm 1 Computing the inverse of π: $y = \pi^{-1}(x)$.

$(l||r) \leftarrow \beta(x)$
$l \leftarrow q(l)$
if $l = 0$ **then**
  $z \leftarrow 17 \times ((r+1) \mod 16)$
else
  $z \leftarrow 17 \times l + r - 16$
end if
$y \leftarrow \exp_{w,0}(z)$
return y

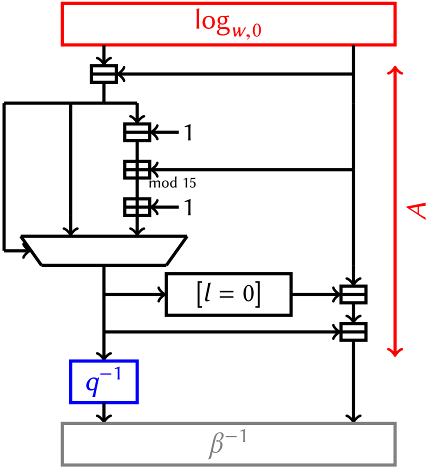
β: 8-bit linear permutation ; q: 4-bit S-Box

$\exp_{w,0}(z) = w^z$, but $\exp_{w,0}(0) = 0$

First Decomposition of π

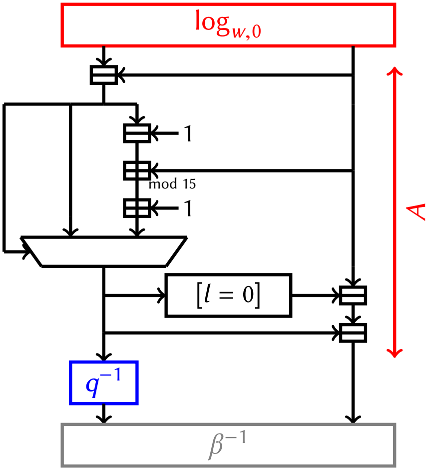


First Decomposition of π



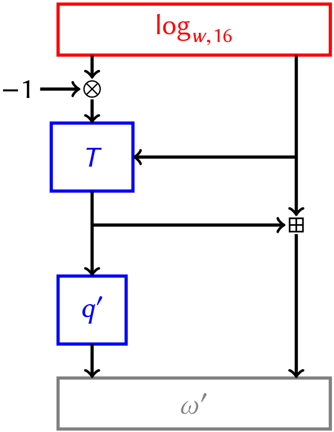
A is extremely weak...

First Decomposition of π



A is extremely weak... Can we simplify it even further using a pseudo-exponential?

A Second Decomposition of π



	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
T_0	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
T_1	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
T_2	0	1	2	3	4	5	6	7	8	9	a	b	c	d	f	e
T_3	0	1	2	3	4	5	6	7	8	9	a	b	c	f	d	e
T_4	0	1	2	3	4	5	6	7	8	9	a	b	f	c	d	e
T_5	0	1	2	3	4	5	6	7	8	9	a	f	b	c	d	e
T_6	0	1	2	3	4	5	6	7	8	9	f	a	b	c	d	e
T_7	0	1	2	3	4	5	6	7	8	f	9	a	b	c	d	e
T_8	0	1	2	3	4	5	6	7	f	8	9	a	b	c	d	e
T_9	0	1	2	3	4	5	6	f	7	8	9	a	b	c	d	e
T_a	0	1	2	3	4	5	f	6	7	8	9	a	b	c	d	e
T_b	0	1	2	3	4	f	5	6	7	8	9	a	b	c	d	e
T_c	0	1	2	3	f	4	5	6	7	8	9	a	b	c	d	e
T_d	0	1	2	f	3	4	5	6	7	8	9	a	b	c	d	e
T_e	0	1	f	2	3	4	5	6	7	8	9	a	b	c	d	e
T_f	0	f	1	2	3	4	5	6	7	8	9	a	b	c	d	e

What now?

The structure inside π is stronger than expected

- One 4-bit S-Box instead of 5

What now?

The structure inside π is stronger than expected

- One 4-bit S-Box instead of 5
- One linear layer instead of 2

What now?

The structure inside π is stronger than expected

- One 4-bit S-Box instead of 5
- One linear layer instead of 2
- Two parameters needed to describe main component (field representation + position of 0)

What now?

The structure inside π is stronger than expected

- One 4-bit S-Box instead of 5
- One linear layer instead of 2
- Two parameters needed to describe main component (field representation + position of 0)
- ... But doesn't make a lot of sense.

What now?

The structure inside π is stronger than expected

- One 4-bit S-Box instead of 5
- One linear layer instead of 2
- Two parameters needed to describe main component (field representation + position of 0)
- ... But doesn't make a lot of sense.

Still, $\pi^{-1} \circ \log_{w,16}$ is **differentially 128-uniform!**

What now?

The structure inside π is stronger than expected

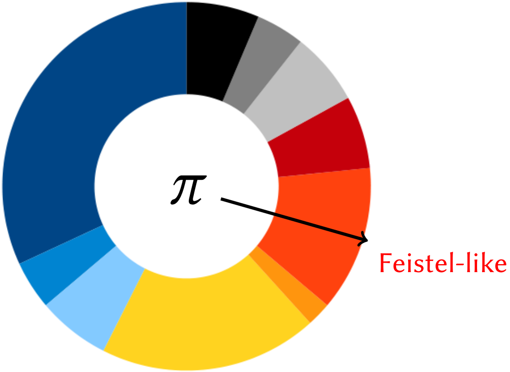
- One 4-bit S-Box instead of 5
- One linear layer instead of 2
- Two parameters needed to describe main component (field representation + position of 0)
- ... But doesn't make a lot of sense.

Still, $\pi^{-1} \circ \log_{w,16}$ is **differentially 128-uniform!**

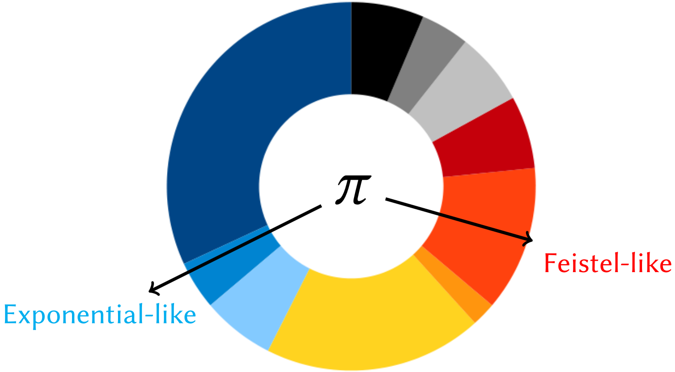
- For random 8-bit permutation, $Pr[\max(\text{DDT})] = 128 \approx 2^{-346}$
- $\implies$ π is related to an exponential.

Plan

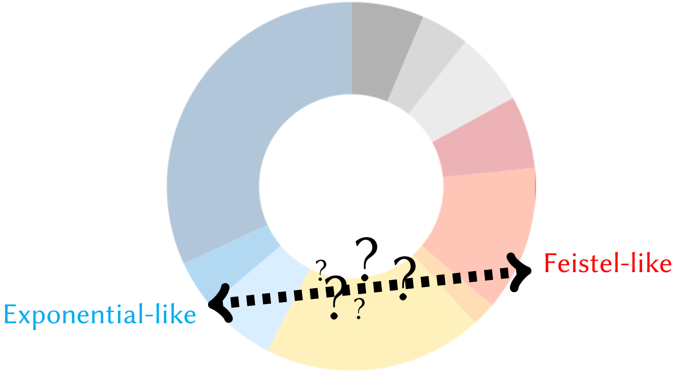
Conclusion



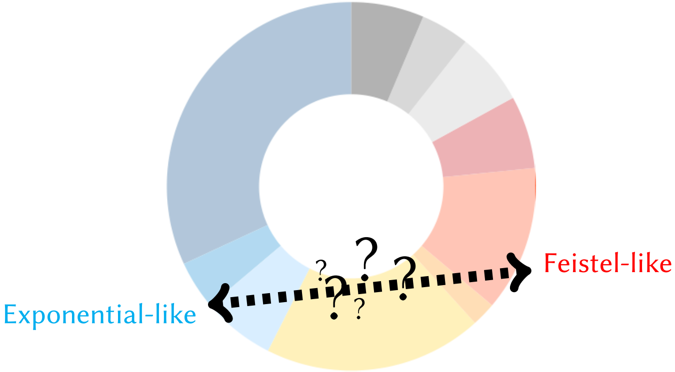
Conclusion



Conclusion



Conclusion



Thank you!