



**HAL**  
open science

# S-Box Reverse-Engineering: Boolean Functions, American/Russian Standards, and Butterflies

Léo Perrin

► **To cite this version:**

Léo Perrin. S-Box Reverse-Engineering: Boolean Functions, American/Russian Standards, and Butterflies. CECC 2018 - Central European Conference on Cryptology, Jun 2018, Smolenice, Slovakia. pp.1-99. hal-01953348

**HAL Id: hal-01953348**

**<https://inria.hal.science/hal-01953348>**

Submitted on 12 Dec 2018

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

# S-Box Reverse-Engineering

Boolean Functions, American/Russian Standards, and Butterflies

Léo Perrin

Based on joint works with Biryukov, Canteaut, Duval and Udovenko

June 6, 2018

CECC'18



# Outline

- 1 Building Blocks for Symmetric Cryptography
- 2 Statistics and Skipjack
- 3 TU-Decomposition and Kuznyechik
- 4 The Butterfly Permutations and Functions
- 5 Conclusion

# Outline

- 1** Building Blocks for Symmetric Cryptography
- 2 Statistics and Skipjack
- 3 TU-Decomposition and Kuznyechik
- 4 The Butterfly Permutations and Functions
- 5 Conclusion

# Symmetric Cryptography

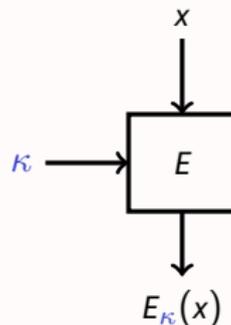
There are many **symmetric** algorithms! Hash functions, MACs...

# Symmetric Cryptography

There are many **symmetric** algorithms! Hash functions, MACs...

## Definition (Block Cipher)

- Input:  $n$ -bit block  $x$
- Parameter:  $k$ -bit key  $\kappa$
- Output:  $n$ -bit block  $E_{\kappa}(x)$
- Symmetry:  $E$  and  $E^{-1}$  use the same  $\kappa$

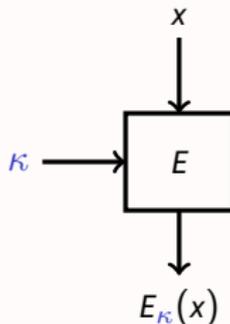


# Symmetric Cryptography

There are many **symmetric** algorithms! Hash functions, MACs...

## Definition (Block Cipher)

- Input:  $n$ -bit block  $x$
- Parameter:  $k$ -bit key  $\kappa$
- Output:  $n$ -bit block  $E_{\kappa}(x)$
- Symmetry:  $E$  and  $E^{-1}$  use the same  $\kappa$



### Properties needed:

Diffusion

Confusion

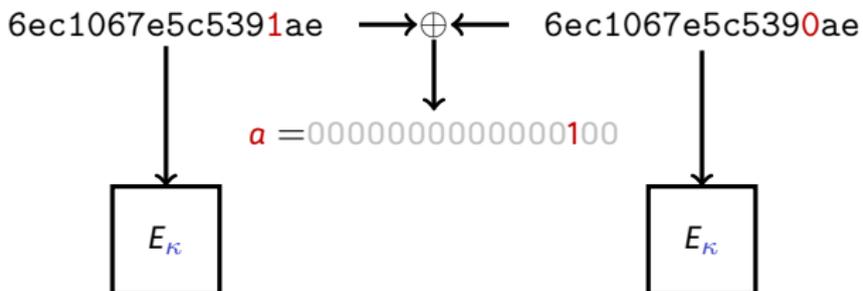
No cryptanalysis!

## No Cryptanalysis?

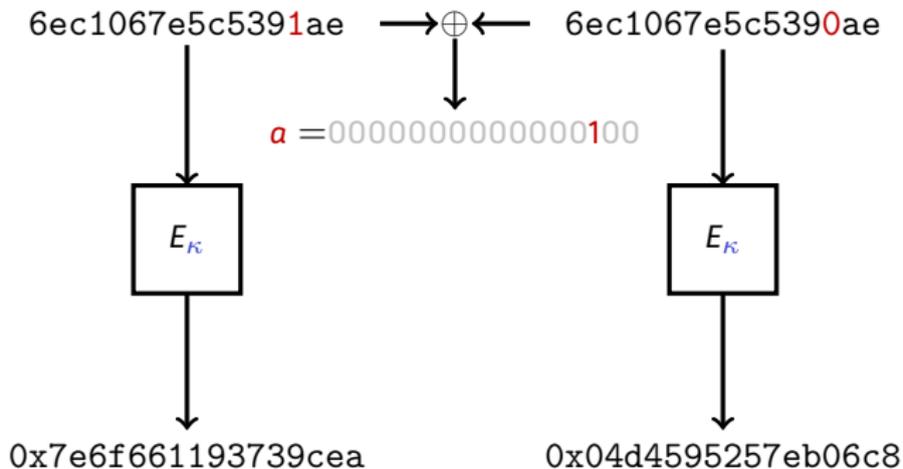
Let us look at a typical cryptanalysis technique: the **differential attack**.



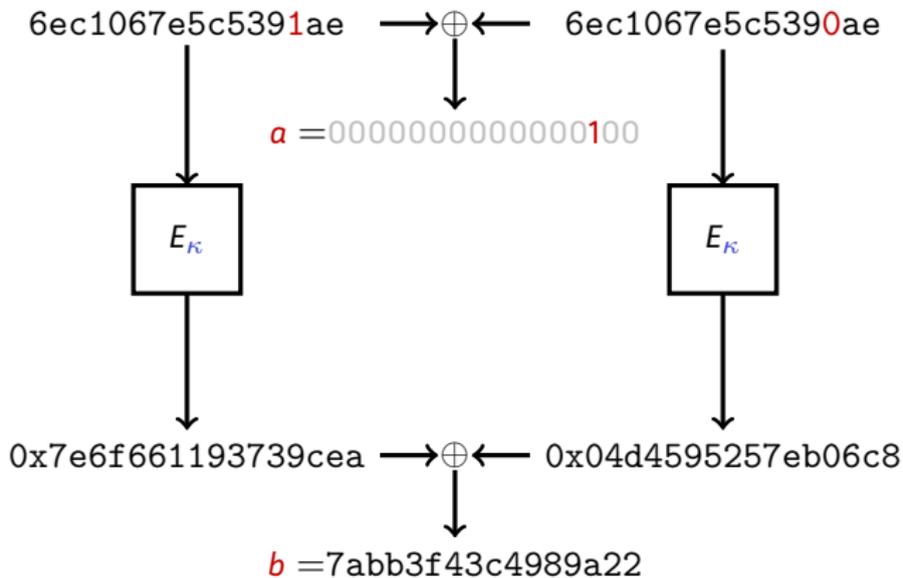
## Differential Attacks



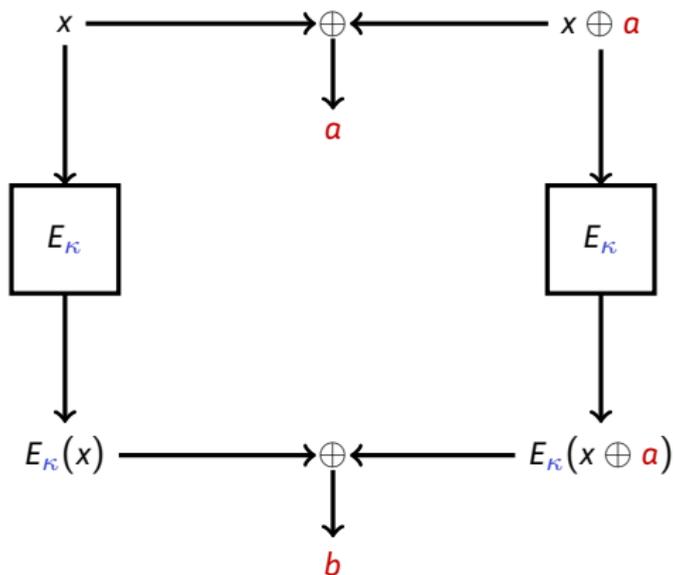
## Differential Attacks



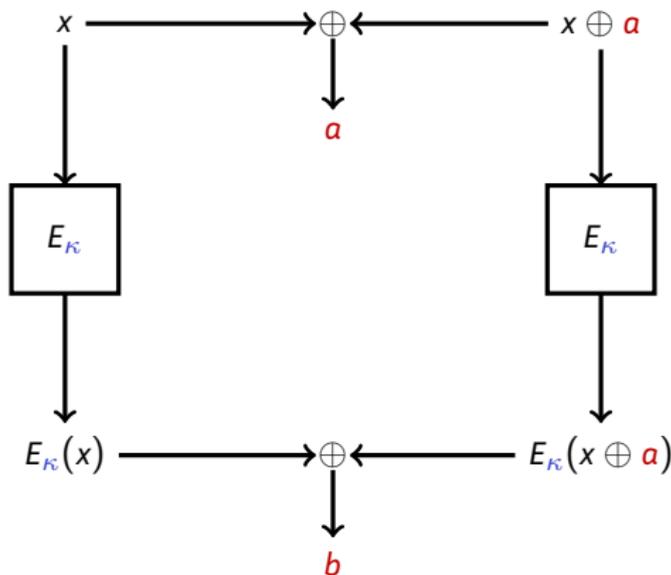
## Differential Attacks



## Differential Attacks



## Differential Attacks



### Differential Attack

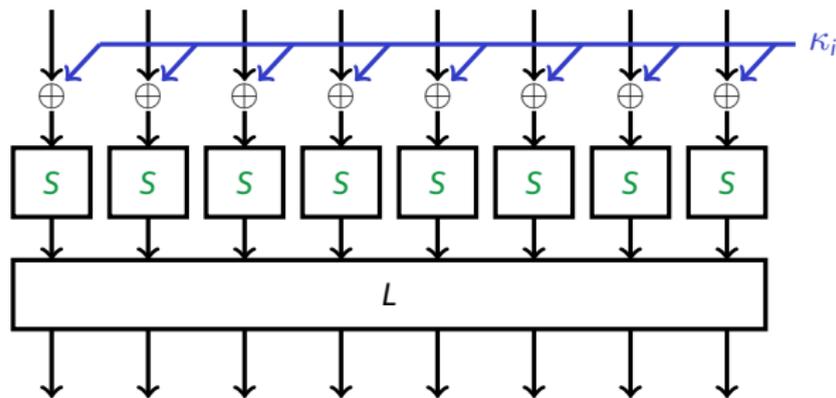
If there are many  $x$  such that  $E_{\kappa}(x) \oplus E_{\kappa}(x \oplus a) = b$ , then the cipher is **not secure**.

## Basic Block Cipher Structure

How do we build block ciphers that prevent such attacks (as well as others)?

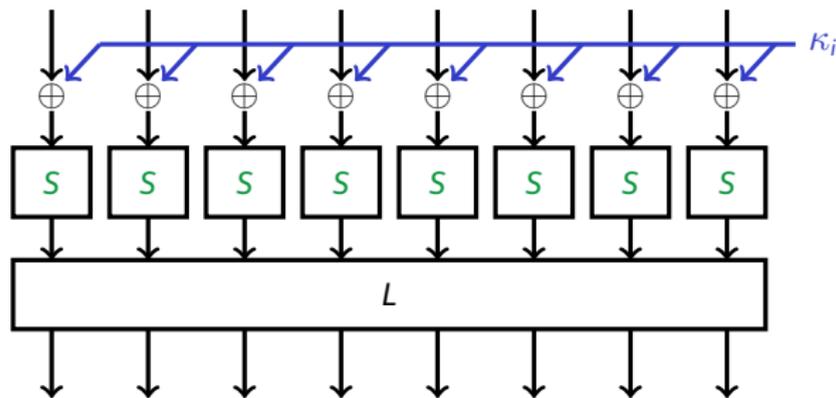
## Basic Block Cipher Structure

How do we build block ciphers that prevent such attacks (as well as others)?



## Basic Block Cipher Structure

How do we build block ciphers that prevent such attacks (as well as others)?



### Substitution-Permutation Network

Such a block cipher iterates the round function above several times. **S** is the Substitution Box (S-Box).

## The S-Box (1/2)

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

*The S-Box  $\pi$  of the latest Russian standards, Kuznyechik (BC) and Streebog (HF).*

## The S-Box (2/2)

### Importance of the S-Box

If  $S$  is such that

$$S(x) \oplus S(x \oplus a) = b$$

does not have many solutions  $x$  for all  $(a, b)$  then the cipher may be proved secure against differential attacks.

## The S-Box (2/2)

### Importance of the S-Box

If  $S$  is such that

$$S(x) \oplus S(x \oplus a) = b$$

does not have many solutions  $x$  for all  $(a, b)$  then the cipher may be proved secure against differential attacks.

In **academic** papers presenting new block ciphers, the choice of  $S$  is carefully explained.

## S-Box Design

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

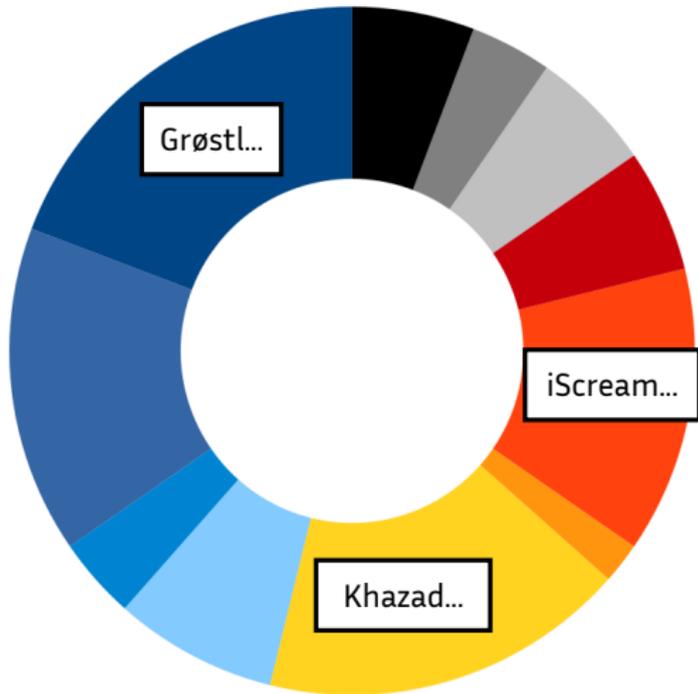
## S-Box Design

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



## S-Box Design

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



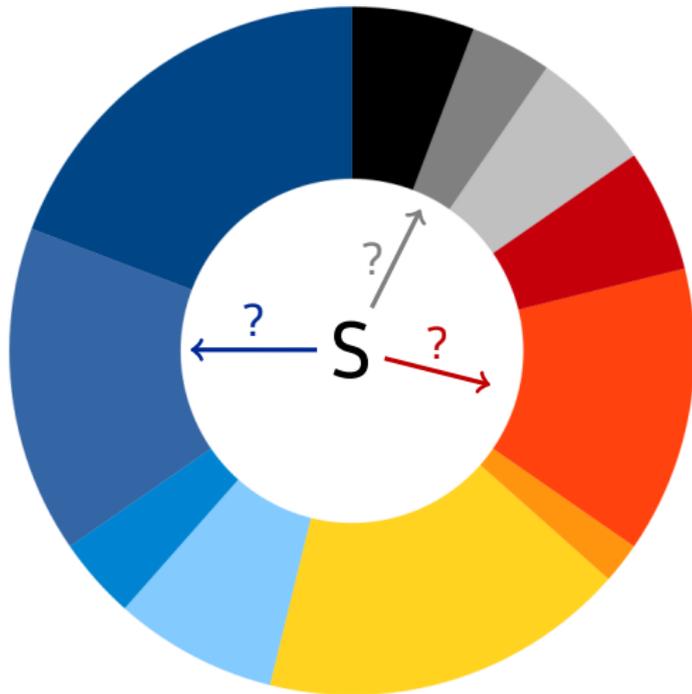
## S-Box Reverse-Engineering

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



## S-Box Reverse-Engineering

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



## Motivation (1/3)

A malicious designer can easily hide a structure in an S-Box.

## Motivation (1/3)

A malicious designer can easily hide a structure in an S-Box.

To keep an advantage in implementation (WB crypto)...

## Motivation (1/3)

**A malicious designer can easily hide a structure in an S-Box.**

To keep an advantage in implementation (WB crypto)...  
... or an advantage in cryptanalysis (backdoor).

## Motivation (2/3)

### Definition (Kleptography)

The study of trapdoored cryptography is called **kleptography** (term introduced by Jung and Young).

### S-Box based backdoors in the literature

- Rijmen, V., & Preneel, B. (1997). *A family of trapdoor ciphers*. FSE'97.
- Patterson, K. (1999). *Imprimitive Permutation Groups and Trapdoors in Iterated Block Ciphers*. FSE'99.
- Blondeau, C., Civino, R., & Sala, M. (2017). *Differential Attacks: Using Alternative Operations*. eprint report 2017/610.
- Bannier, A., & Filiol, E. (2017). *Partition-based trapdoor ciphers*. InTech'17.

## Motivation (3/3)

Even without malicious intent, an unexpected structure can be a problem.

⇒ We need tools to *reverse-engineer* S-Boxes!

# Outline

- 1 Building Blocks for Symmetric Cryptography
- 2 Statistics and Skipjack**
- 3 TU-Decomposition and Kuznyechik
- 4 The Butterfly Permutations and Functions
- 5 Conclusion

## Summary



We can recover parts of the design process of an S-Box using some statistics.

- 1 The two tables (basics of Boolean functions for cryptography)
- 2 A statistical tool based on the two tables
- 3 Application to NSA's Skipjack

# The Two Tables

Let  $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  be an S-Box.

## The Two Tables

Let  $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  be an S-Box.

### Definition (DDT)

The *Difference Distribution Table* of  $S$  is a matrix of size  $2^n \times 2^n$  such that

$$\text{DDT}[a, b] = \#\{x \in \mathbb{F}_2^n \mid S(x \oplus a) \oplus S(x) = b\}.$$

# The Two Tables

Let  $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  be an S-Box.

## Definition (DDT)

The *Difference Distribution Table* of  $S$  is a matrix of size  $2^n \times 2^n$  such that

$$\text{DDT}[a, b] = \#\{x \in \mathbb{F}_2^n \mid S(x \oplus a) \oplus S(x) = b\}.$$

## Definition (LAT)

The *Linear Approximations Table* of  $S$  is a matrix of size  $2^n \times 2^n$  such that

$$\text{LAT}[a, b] = \#\{x \in \mathbb{F}_2^n \mid x \cdot a = S(x) \cdot b\} - 2^{n-1}.$$

## Example

$$S = [4, 2, 1, 6, 0, 5, 7, 3]$$

The **DDT** of  $S$ .

$$\begin{bmatrix} 8 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 0 & 4 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \\ 0 & 4 & 4 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 0 & 4 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 2 & 2 & 2 \end{bmatrix}$$

The **LAT** of  $S$ .

$$\begin{bmatrix} 4 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 2 & 0 & 0 & 2 & -2 \\ 0 & 2 & 2 & 0 & 0 & 2 & -2 & 0 \\ 0 & 2 & 0 & 2 & 0 & -2 & 0 & 2 \\ 0 & 2 & 0 & -2 & 0 & -2 & 0 & -2 \\ 0 & -2 & 2 & 0 & 0 & -2 & -2 & 0 \\ 0 & 0 & -2 & 2 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 & -4 & 0 & 0 & 0 \end{bmatrix}$$

## Coefficient Distribution in the DDT

If an  $n$ -bit S-Box is bijective, then its DDT coefficients behave like **independent** and identically distributed random variables following a Poisson distribution:

$$\Pr [\text{DDT}[a, b] = 2z] = \frac{e^{-1/2}}{2^z} .$$

## Coefficient Distribution in the DDT

If an  $n$ -bit S-Box is bijective, then its **DDT** coefficients behave like **independent** and identically distributed random variables following a Poisson distribution:

$$\Pr [\text{DDT}[a, b] = 2z] = \frac{e^{-1/2}}{2^z} .$$

- Always even,  $\geq 0$
- Typically between 0 and 16.
- Lower is better.

## Coefficient Distribution in the LAT

If an  $n$ -bit S-Box is bijective, then its LAT coefficients behave like **independent** and identically distributed random variables following this distribution:

$$\Pr [\text{LAT}[a, b] = 2z] = \frac{\binom{2^{n-1}}{2^{n-2+z}}}{\binom{2^n}{2^{n-1}}}.$$

## Coefficient Distribution in the LAT

If an  $n$ -bit S-Box is bijective, then its LAT coefficients behave like **independent** and identically distributed random variables following this distribution:

$$\Pr [\text{LAT}[a, b] = 2z] = \frac{\binom{2^{n-1}}{2^{n-2+z}}}{\binom{2^n}{2^{n-1}}}.$$

- Always even, signed.
- Typically between -40 and 40.
- Lower absolute value is better.

## Looking Only at the Maximum

| $\delta$ | $\log_2 (\Pr [\max(\text{DDT}) \leq \delta])$ |
|----------|---|
| 14       | -0.006  |
| 12       | -0.094  |
| 10       | -1.329  |
| 8        | -16.148                                       |
| 6        | -164.466                                      |
| 4        | -1359.530                                     |

**DDT**

| $\ell$ | $\log_2 (\Pr [\max(\text{LAT}) \leq \ell])$ |
|--------|---|
| 38     | -0.084                                      |
| 36     | -0.302                                      |
| 34     | -1.008                                      |
| 32     | -3.160                                      |
| 30     | -9.288                                      |
| 28     | -25.623                                     |
| 26     | -66.415                                     |
| 24     | -161.900                                    |
| 22     | -371.609                                    |

**LAT**

Probability that the maximum coefficient in the DDT/LAT of an 8-bit permutation is at most equal to a certain threshold.

## Looking Only at the Maximum

| $\delta$ | $\log_2 (\Pr [\max(\text{DDT}) \leq \delta])$ |
|----------|---|
| 14       | -0.006  |
| 12       | -0.094  |
| 10       | -1.329  |
| 8        | -16.148                                       |
| 6        | -164.466                                      |
| 4        | -1359.530                                     |

**DDT**

| $\ell$ | $\log_2 (\Pr [\max(\text{LAT}) \leq \ell])$ |
|--------|---|
| 38     | -0.084                                      |
| 36     | -0.302                                      |
| 34     | -1.008                                      |
| 32     | -3.160                                      |
| 30     | -9.288                                      |
| 28     | -25.623                                     |
| 26     | -66.415                                     |
| 24     | -161.900                                    |
| 22     | -371.609                                    |

**LAT**

Probability that the maximum coefficient in the DDT/LAT of an 8-bit permutation is at most equal to a certain threshold.

## What is Skipjack? (1/2)

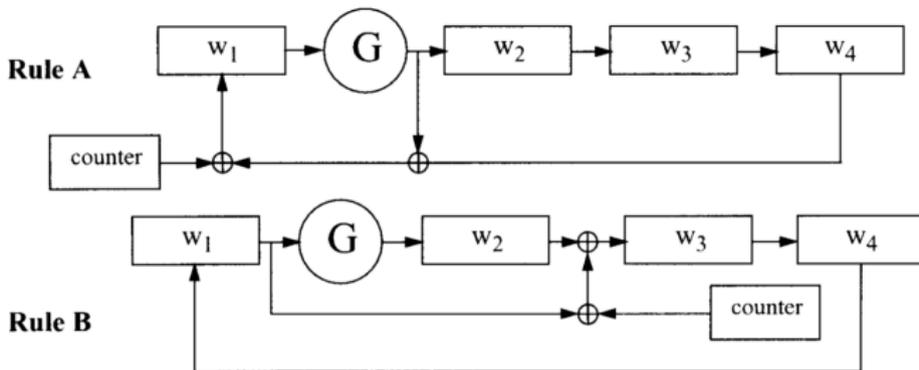
Type Block cipher

Bloc 64 bits

Key 80 bits

Authors NSA

Publication 1998



## What is Skipjack? (2/2)

- Skipjack was supposed to be secret...
- ... but eventually published in 1998.

## What is Skipjack? (2/2)

- Skipjack was supposed to be secret...
- ... but eventually published in 1998.
- Skipjack was to be used by the *Clipper Chip*,

## What is Skipjack? (2/2)

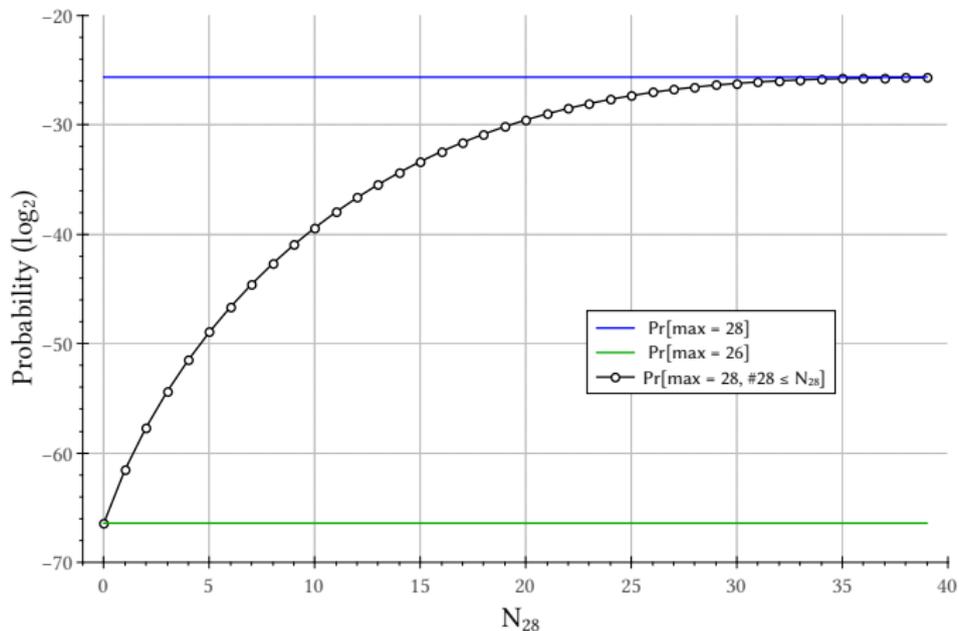
- Skipjack was supposed to be secret...
- ... but eventually published in 1998.
- Skipjack was to be used by the *Clipper Chip*,
- It uses an  $8 \times 8$  S-Box ( $F$ ) specified only by its LUT.

## Reverse-Engineering $F$

For Skipjack's  $F$ ,  $\max(\text{LAT}) = 28$  and  $\#28 = 3$ .

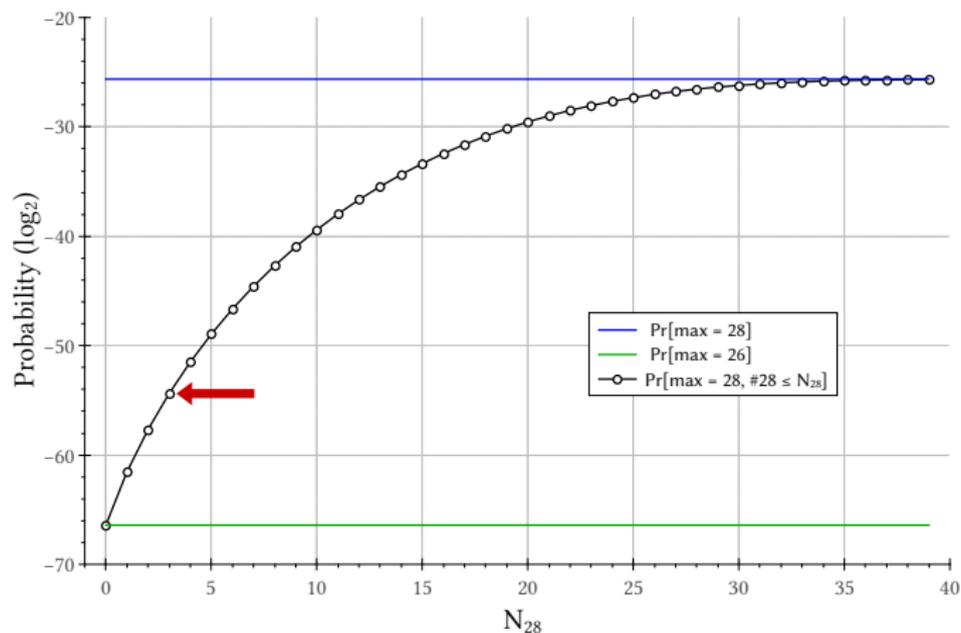
## Reverse-Engineering F

For Skipjack's  $F$ ,  $\max(\text{LAT}) = 28$  and  $\#28 = 3$ .



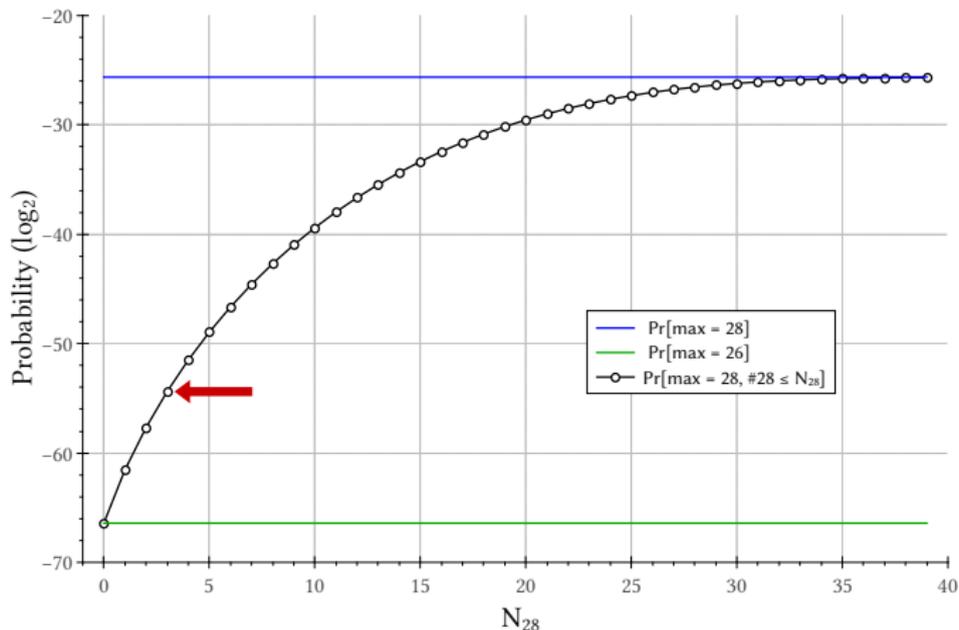
## Reverse-Engineering F

For Skipjack's  $F$ ,  $\max(\text{LAT}) = 28$  and  $\#28 = 3$ .



## Reverse-Engineering F

For Skipjack's  $F$ ,  $\max(\text{LAT}) = 28$  and  $\#28 = 3$ .



$$\text{Pr}[\max(\text{LAT}) = 28 \text{ and } \#28 \leq 3] \approx 2^{-55}$$

## What Can We Deduce?

- $F$  has not been picked uniformly at random.
- $F$  has not been picked among a feasibly large set of random S-Boxes.
- Its linear properties were optimized (though poorly).

## What Can We Deduce?

- $F$  has not been picked uniformly at random.
- $F$  has not been picked among a feasibly large set of random S-Boxes.
- Its linear properties were optimized (though poorly).

**The S-Box of Skipjack was built  
using a dedicated algorithm.**

## Timeline

**Jun 98** Declassification of Skipjack

## Timeline

**1987** Initial design of Skipjack

**Jul 93** “interim report” on Skipjack published by external cryptographers

**Jun 98** Declassification of Skipjack

## Timeline

**1987** Initial design of Skipjack

- Jul 93** “interim report” on Skipjack published by external cryptographers
- Aug 95** Alleged “Skipjack” (actually not) is leaked to usenet
- Sep 95** Schneier published his thoughts on “alleged Skipjack”, including the result of a FOIA request
- Jun 98** Declassification of Skipjack

## Timeline

**1987** Initial design of Skipjack

**Aug 92** The S-Box (“F-table”) of Skipjack is changed

**Jul 93** “interim report” on Skipjack published by external cryptographers

**Aug 95** Alleged “Skipjack” (actually not) is leaked to usenet

**Sep 95** Schneier published his thoughts on “alleged Skipjack”, including the result of a FOIA request

**Jun 98** Declassification of Skipjack

## Timeline

- 1987** Initial design of Skipjack
- Aug 90** (CRYPTO) Gilbert et al. use linear relations for key recovery (FEAL)
- Aug 91** (CRYPTO) Attack against FEAL using linear relations between key, plaintext and ciphertext
- May 92** (EUROCRYPT) Other attack against FEAL using linear relations between key, plaintext and ciphertext
- Aug 92** The S-Box ("F-table") of Skipjack is changed
- Jul 93** "interim report" on Skipjack published by external cryptographers
- Aug 95** Alleged "Skipjack" (actually not) is leaked to usenet
- Sep 95** Schneier published his thoughts on "alleged Skipjack", including the result of a FOIA request
- Jun 98** Declassification of Skipjack

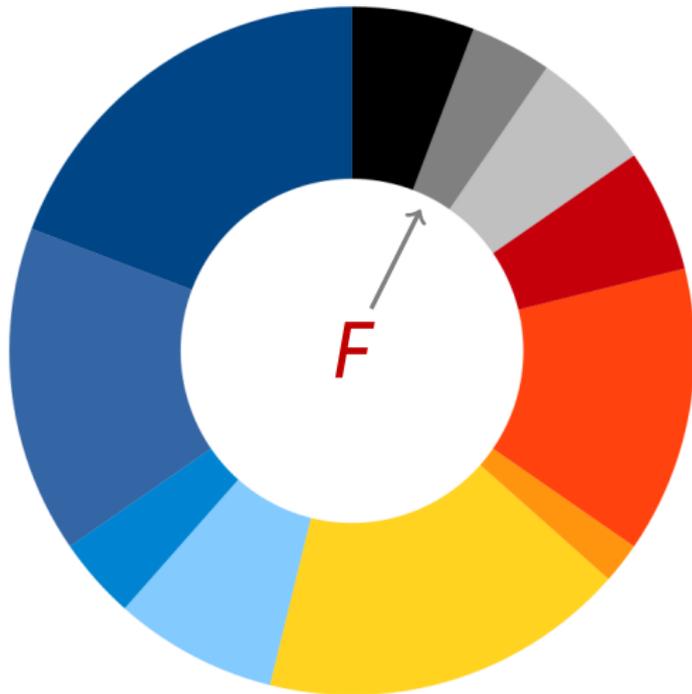
## Conclusion on Skipjack

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



## Conclusion on Skipjack

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



# Outline

- 1 Building Blocks for Symmetric Cryptography
- 2 Statistics and Skipjack
- 3 TU-Decomposition and Kuznyechik**
- 4 The Butterfly Permutations and Functions
- 5 Conclusion

## Summary



We can recover an **actual decomposition** using patterns in the LAT.

- 1 Our target, the S-Box of Kuznyechik and Streebog
- 2 TU-decomposition: what is it and how to apply it to Kuznyechik

## Kuznyechik/Stribog

### Stribog

Type Hash function

Publication 2012

### Kuznyechik

Type Block cipher

Publication 2015



## Kuznyechik/Stribog

### Stribog

Type Hash function

Publication 2012

### Kuznyechik

Type Block cipher

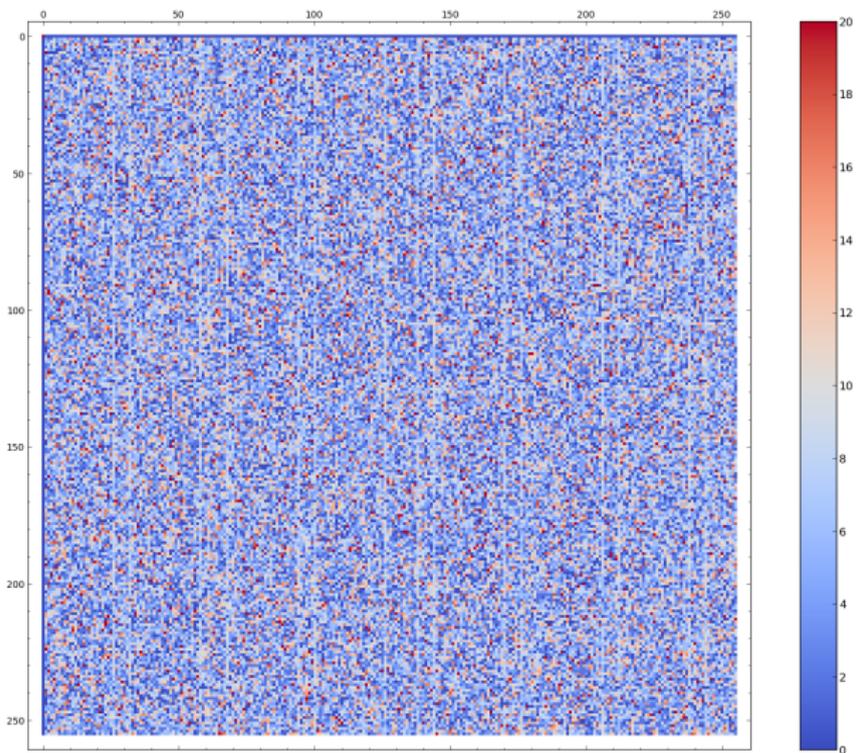
Publication 2015



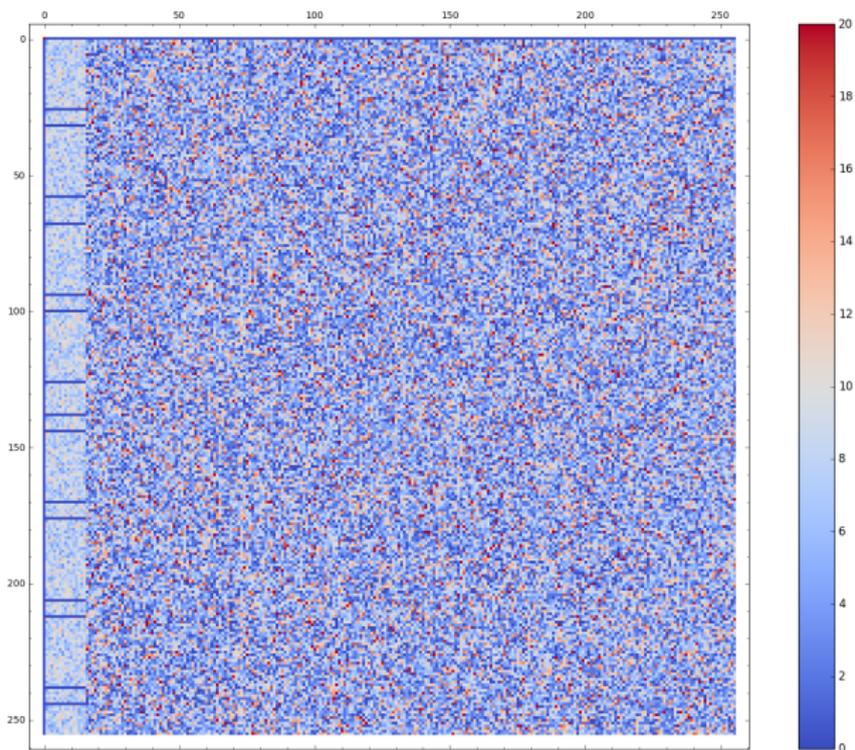
### Common ground

- Both are standard symmetric primitives in Russia.
- Both were designed by the FSB (TC26).
- Both use the same  $8 \times 8$  S-Box,  $\pi$ .

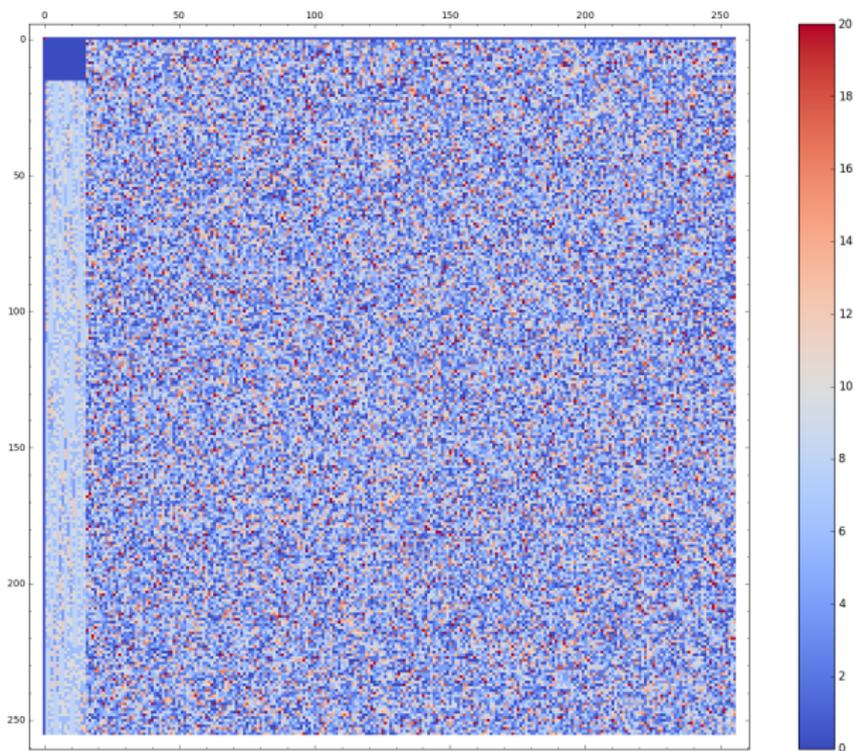
## The LAT of $\pi$



## The LAT of $\eta$ (reordered columns)



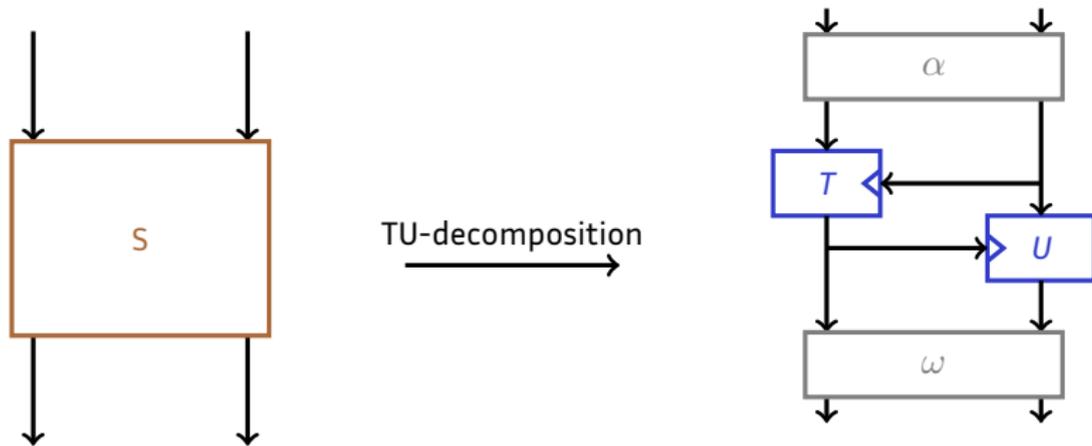
## The LAT of $\eta \circ \pi \circ \mu$



## The TU-Decomposition

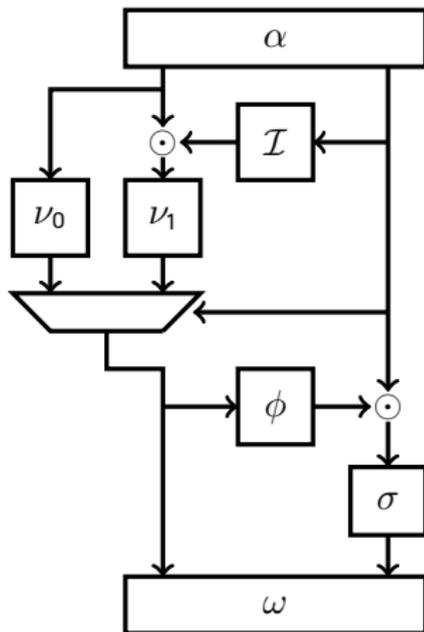
### Definition

The **TU-decomposition** is a decomposition algorithm working against S-Boxes with vector spaces of zeroes in their LAT.



$T$  and  $U$  are mini-block ciphers;  $\mu$  and  $\eta$  are linear permutations.

## Final Decomposition Number 1



$\odot$  Multiplication in  $\mathbb{F}_{2^4}$

$\alpha$  Linear permutation

$\mathcal{I}$  Inversion in  $\mathbb{F}_{2^4}$

$\nu_0, \nu_1, \sigma$   $4 \times 4$  permutations

$\phi$   $4 \times 4$  function

$\omega$  Linear permutation

## Hardware Performance

| Structure                       | Area ( $\mu m^2$ ) | Delay (ns) |
|---------------------------------|--------------------|------------|
| Naive implementation            | 3889.6             | 362.52     |
| Feistel-like                    | 1534.7             | 61.53      |
| Multiplications-first           | 1530.3             | 54.01      |
| Feistel-like (with tweaked MUX) | 1530.1             | 46.11      |

## Conclusion for Kuznyechik/Stribog?

**The Russian S-Box was built like a  
strange Feistel...**

## Conclusion for Kuznyechik/Stribog?

**The Russian S-Box was built like a  
strange Feistel...**

**... or was it?**

## Conclusion for Kuznyechik/Streebog?

**The Russian S-Box was built like a  
strange Feistel...**

**... or was it?**

### Belarussian inspiration

- The last standard of Belarus (BelT) uses an 8-bit S-box,
- somewhat similar to  $\pi$ ...

## Conclusion for Kuznyechik/Streebog?

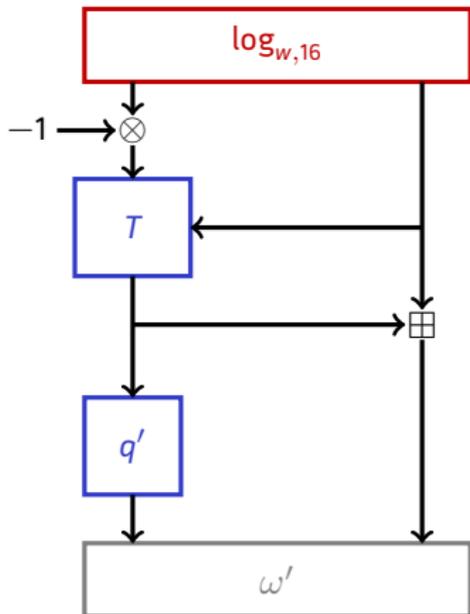
The Russian S-Box was built like a  
strange Feistel...

... or was it?

### Belarussian inspiration

- The last standard of Belarus (BelT) uses an 8-bit S-box,
- somewhat similar to  $\pi$ ...
- ... based on a **finite field exponential!**

## Final Decomposition Number 2 (!)



|       | 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 | f | 6 | 7 | 8 | 9 | a | b | c | d | e |   |
| $T_b$ | 0 | 1 | 2 | 3 | f | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e |   |
| $T_c$ | 0 | 1 | 2 | f | 4 | 5 | 6 | 7 | 8 | 9 | a | b | c | d | e |   |
| $T_d$ | 0 | 1 | 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 |

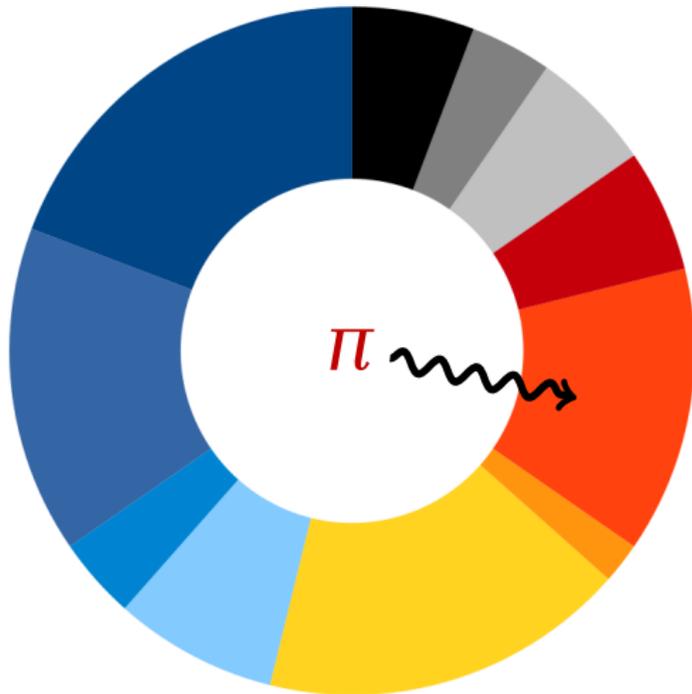
## Conclusion on Kuznyechik/Streebog

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



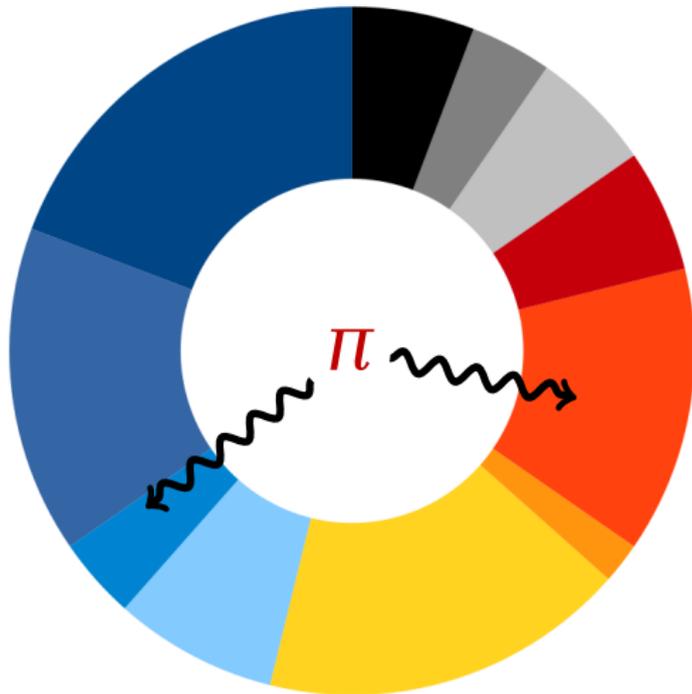
## Conclusion on Kuznyechik/Streebog

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



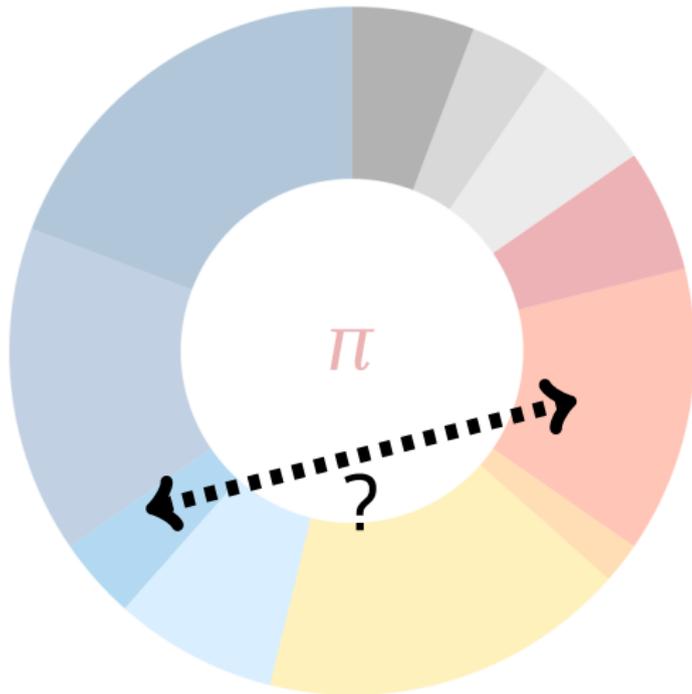
## Conclusion on Kuznyechik/Streebog

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



## Conclusion on Kuznyechik/Streebog

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



# Outline

- 1 Building Blocks for Symmetric Cryptography
- 2 Statistics and Skipjack
- 3 TU-Decomposition and Kuznyechik
- 4 The Butterfly Permutations and Functions**
- 5 Conclusion

## Summary



We can obtain new mathematical results using reverse-engineering techniques.

- 1 The big APN problem and its only known solution
- 2 Decomposing and generalizing this solution as butterflies

## NSUCRYPTO (Olympiad in Cryptography)

Siberian Student's Olympiad in Cryptography with International participation — 2014

Second round

NSUCRYPTO

November 17-24



Task 2. «An APN Permutation»

*“Try to find an APN permutation on 8 variables or prove that it doesn't exist.”*

<https://nsucrypto.nsu.ru/>

# The Big APN Problem

## Definition (APN function)

A function  $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  is **Almost Perfect Non-linear (APN)** if

$$S(x \oplus a) \oplus S(x) = b$$

has 0 or 2 solutions for all  $a \neq 0$  and for all  $b$ .

# The Big APN Problem

## Definition (APN function)

A function  $S : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$  is **Almost Perfect Non-linear (APN)** if

$$S(x \oplus a) \oplus S(x) = b$$

has 0 or 2 solutions for all  $a \neq 0$  and for all  $b$ .

## Big APN Problem

Are there APN permutations operating on  $\mathbb{F}_2^n$  where  $n$  is even?

## Dillon et al.'s Permutation

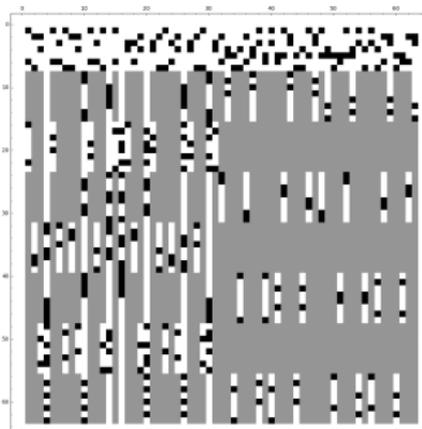
### Only One Known Solution!

For  $n = 6$ , Dillon et al. found an APN permutation.

## Dillon et al.'s Permutation

### Only One Known Solution!

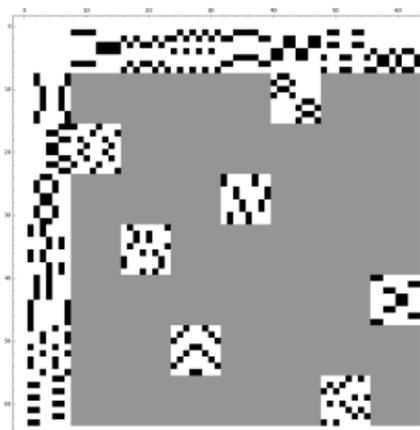
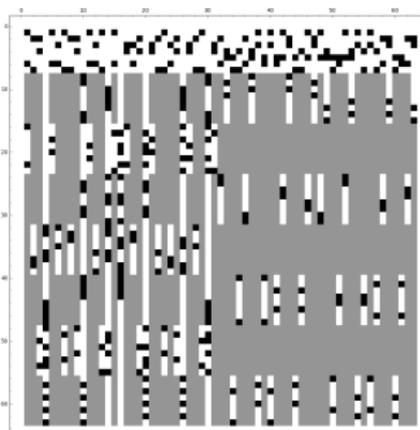
For  $n = 6$ , Dillon et al. found an APN permutation.



## Dillon et al.'s Permutation

### Only One Known Solution!

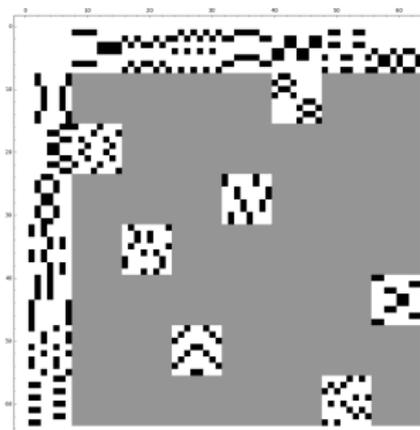
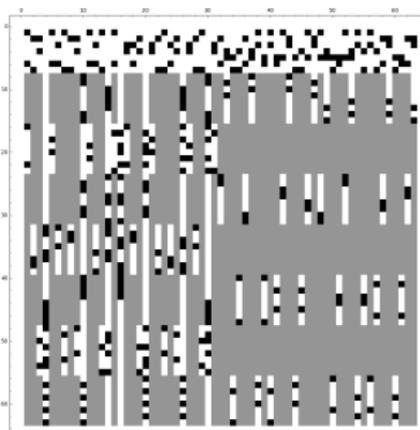
For  $n = 6$ , Dillon et al. found an APN permutation.



## Dillon et al.'s Permutation

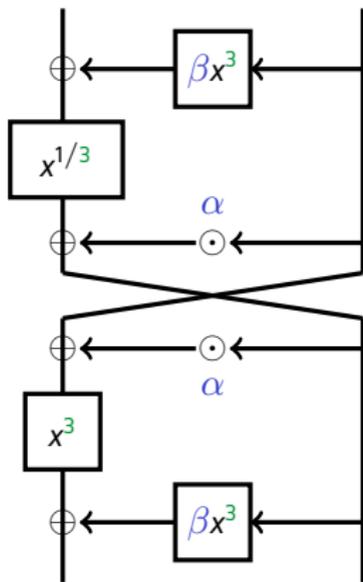
### Only One Known Solution!

For  $n = 6$ , Dillon et al. found an APN permutation.



It is possible to make a TU-decomposition!

## On the Butterfly Structure

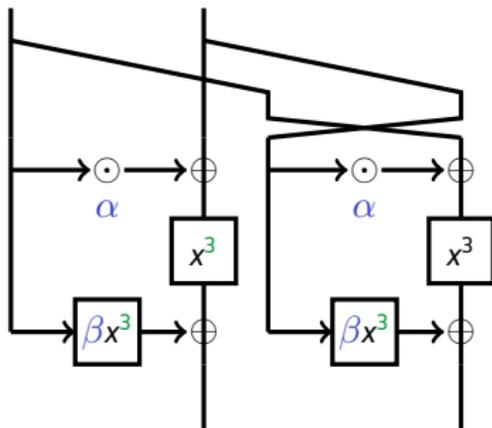


Definition (Open Butterfly  $H_{\alpha,\beta}^3$ )

This permutation is an **open butterfly**.



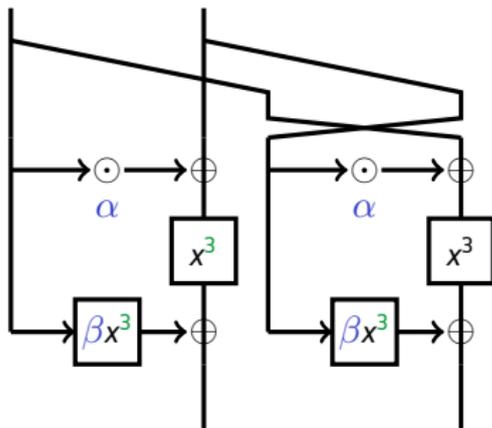
## Closed Butterflies



Definition (Closed butterfly  $V_{\alpha, \beta}^3$ )

This quadratic function is a **closed butterfly**.

## Closed Butterflies



**Definition (Closed butterfly  $V_{\alpha, \beta}^3$ )**

This quadratic function is a **closed butterfly**.

**Lemma (Equivalence)**

*Open and closed butterflies with the same parameters are CCZ-equivalent.*

## Some Properties of Butterflies

### Theorem (Properties of butterflies)

Let  $V_{\alpha,\beta}^3$  and  $H_{\alpha,\beta}^3$  be butterflies operating on  $2n$  bits,  $n$  odd. Then:

- $\deg(V_{\alpha,\beta}^3) = 2$ ,
- if  $n = 3$ ,  $\text{Tr}(\alpha) = 0$  and  $\beta + \alpha^3 \in \{\alpha, 1/\alpha\}$ , then
 
$$\max(\text{DDT}) = 2, \max(\mathcal{W}) = 2^{n+1} \text{ and } \deg(H_{\alpha,\beta}^3) = n + 1,$$
- if  $\beta = (1 + \alpha)^3$ , then
 
$$\max(\text{DDT}) = 2^{n+1}, \max(\mathcal{W}) = 2^{(3n+1)/2} \text{ and } \deg(H_{\alpha,\beta}^3) = n,$$
- otherwise,
 
$$\max(\text{DDT}) = 4, \max(\mathcal{W}) = 2^{n+1} \text{ and } \deg(H_{\alpha,\beta}^3) \in \{n, n + 1\}$$
 and  $\deg(H_{\alpha,\beta}^3) = n$  if and only if
 
$$1 + \alpha\beta + \alpha^4 = (\beta + \alpha + \alpha^3)^2.$$

# Outline

- 1 Building Blocks for Symmetric Cryptography
- 2 Statistics and Skipjack
- 3 TU-Decomposition and Kuznyechik
- 4 The Butterfly Permutations and Functions
- 5 Conclusion**

## Open Problem

### Cellular Message Encryption Algorithm

From Wikipedia, the free encyclopedia

In [cryptography](#), the **Cellular Message Encryption Algorithm** (**CMEA**) is a [block cipher](#) which was used for securing [mobile phones](#) in the [United States](#). CMEA is one of four cryptographic primitives specified in a [Telecommunications Industry Association](#) (TIA) standard, and is designed to [encrypt](#) the control channel, rather than the voice data. In 1997, a group of cryptographers published attacks on the [cipher](#) showing it had several weaknesses which give it a trivial effective strength of a 24-bit to 32-bit cipher.<sup>[1]</sup>

#### CMEA

##### General

**Designers** [James A. Reeds III](#)

**First published** 1991

##### Cipher detail

**Key sizes** 64 bits

**Block sizes** 16-64 bits

**Rounds** 3

## Open Problem

### Cellular Message Encryption Algorithm

From Wikipedia, the free encyclopedia

In [cryptography](#), the **Cellular Message Encryption Algorithm** (**CMEA**) is a [block cipher](#) which was used for securing [mobile phones](#) in the [United States](#). CMEA is one of four cryptographic primitives specified in a [Telecommunications Industry Association](#) (TIA) standard, and is designed to [encrypt](#) the control channel, rather than the voice data. In 1997, a group of cryptographers published attacks on the [cipher](#) showing it had several weaknesses which give it a trivial effective strength of a 24-bit to 32-bit cipher.<sup>[1]</sup>

| CMEA                   |                                    |
|------------------------|------------------------------------|
| General                |                                    |
| <b>Designers</b>       | <a href="#">James A. Reeds III</a> |
| <b>First published</b> | 1991                               |
| Cipher detail          |                                    |
| <b>Key sizes</b>       | 64 bits                            |
| <b>Block sizes</b>     | 16-64 bits                         |
| <b>Rounds</b>          | 3                                  |

### A hidden structure!

CMEA uses an 8-bit (non-bijective) S-Box... With a TU-decomposition!

**What is its actual structure?**

## Conclusion

- 1 Cryptographers use mathematics but mathematicians could also use crypto!

## Conclusion

- 1 Cryptographers use mathematics but mathematicians could also use crypto!
- 2 If you **design** a cipher, **justify** every step of your design.

## Conclusion

- 1 Cryptographers use mathematics but mathematicians could also use crypto!
- 2 If you **design** a cipher, **justify** every step of your design.
- 3 If you **choose** a cipher, **demand** a full design explanation.

## The Last S-Box

|    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |    |
|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 14 | 11 | 60 | 6d | e9 | 10 | e3 | 2  | b  | 90 | d  | 17 | c5 | b0 | 9f | c5 |
| d8 | da | be | 22 | 8  | f3 | 4  | a9 | fe | f3 | f5 | fc | bc | 30 | be | 26 |
| bb | 88 | 85 | 46 | f4 | 2e | e  | fd | 76 | fe | b0 | 11 | 4e | de | 35 | bb |
| 30 | 4b | 30 | d6 | dd | df | df | d4 | 90 | 7a | d8 | 8c | 6a | 89 | 30 | 39 |
| e9 | 1  | da | d2 | 85 | 87 | d3 | d4 | ba | 2b | d4 | 9f | 9c | 38 | 8c | 55 |
| d3 | 86 | bb | db | ec | e0 | 46 | 48 | bf | 46 | 1b | 1c | d7 | d9 | 1b | e0 |
| 23 | d4 | d7 | 7f | 16 | 3f | 3  | 3  | 44 | c3 | 59 | 10 | 2a | da | ed | e9 |
| 8e | d8 | d1 | db | cb | cb | c3 | c7 | 38 | 22 | 34 | 3d | db | 85 | 23 | 7c |
| 24 | d1 | d8 | 2e | fc | 44 | 8  | 38 | c8 | c7 | 39 | 4c | 5f | 56 | 2a | cf |
| d0 | e9 | d2 | 68 | e4 | e3 | e9 | 13 | e2 | c  | 97 | e4 | 60 | 29 | d7 | 9b |
| d9 | 16 | 24 | 94 | b3 | e3 | 4c | 4c | 4f | 39 | e0 | 4b | bc | 2c | d3 | 94 |
| 81 | 96 | 93 | 84 | 91 | d0 | 2e | d6 | d2 | 2b | 78 | ef | d6 | 9e | 7b | 72 |
| ad | c4 | 68 | 92 | 7a | d2 | 5  | 2b | 1e | d0 | dc | b1 | 22 | 3f | c3 | c3 |
| 88 | b1 | 8d | b5 | e3 | 4e | d7 | 81 | 3  | 15 | 17 | 25 | 4e | 65 | 88 | 4e |
| e4 | 3b | 81 | 81 | fa | 1  | 1d | 4  | 22 | 0  | 6  | 1  | 27 | 68 | 27 | 2e |
| 3b | 83 | c7 | cc | 25 | 9b | d8 | d5 | 1c | 1f | e5 | 59 | 7f | 3f | 3f | ef |

