CONFERENCE PRESENTATION • CRYPTANALYSIS

Kuznyechik’s Differential and Linear Cryptanalysis

Three-round characteristic search with 18 active S-boxes

Evgeniya Ishchukova

Southern Federal University
Taganrog, Russia

Research problem and motivation

How strong are the initial rounds of the Kuznyechik cipher against classical statistical cryptanalysis?

THE CIPHER

A Russian block-cipher standard adopted in 2015 (GOST R 34.12–2015).

THE GAP

Earlier work established strong two-round characteristics, but extending them to three rounds sharply increases active S-boxes.

THE GOAL

Find stronger three-round differential and linear characteristics while limiting the total to 18 active S-boxes.

Focus: structural evaluation of reduced-round behavior — not an attack on the full cipher.

Kuznyechik: the structure relevant to this study

128-bit data block | 9 encryption rounds | 10 round subkeys



S transformation
16 parallel 8-bit bijective S-boxes

L transformation
16 successive R steps mix all 16 state bytes

The L layer drives diffusion: a single active byte can spread across the full state.

What propagates through the cipher?

DIFFERENTIAL ANALYSIS

Tracks input/output differences:

$\Delta X = X \oplus X'$

- XOR with a round key preserves the difference.
- L transforms differences deterministically.
- The S-box transition probabilities are taken from the 256 × 256 DDT.

LINEAR ANALYSIS

Tracks correlations between input and output masks:

$\alpha \cdot X \approx \beta \cdot S(X)$

- XOR with a round key changes the phase, not the mask propagation.
- L propagates masks through the transposed linear map.
- The S-box correlations are evaluated using a 256 × 256 LAT.

The key search problem is to connect high-probability / high-bias S-box transitions across rounds.

Why the best two-round trails do not extend directly

Previously reported two-round results [12]

17 active S-boxes

Differential: $2^{-86.66}$ | Linear: $2^{-76.39}$

—

Naive extension to a third round

All 16 S-boxes become active

A sharp drop in characteristic probability

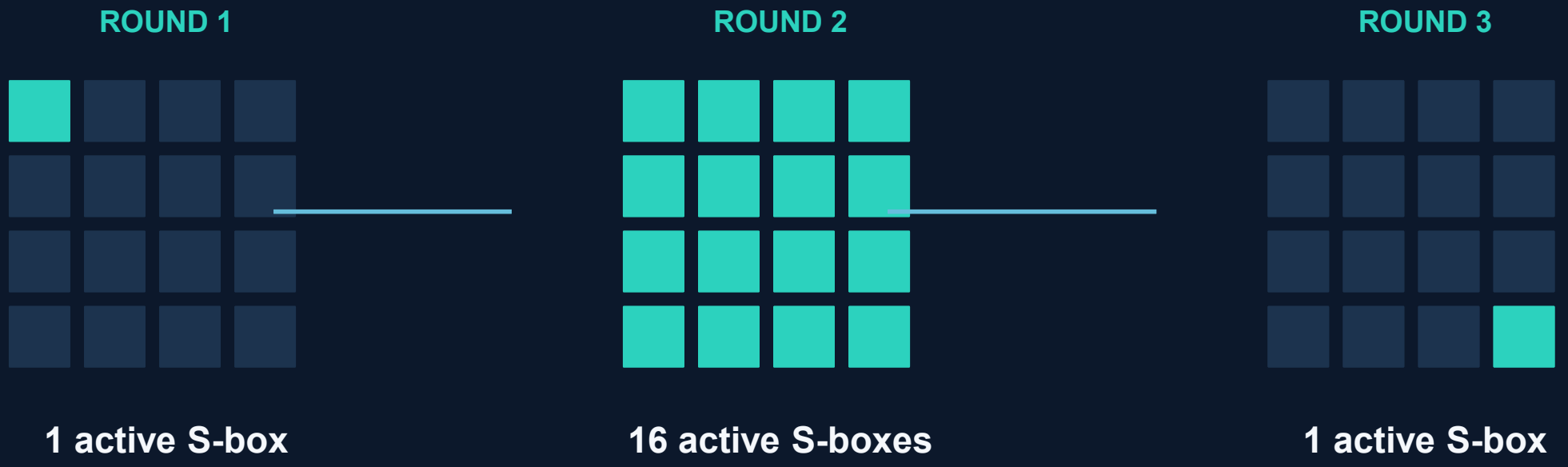
Key observation

A good two-round characteristic is not necessarily a good three-round characteristic. The search must optimize the complete three-round trail.

This motivates a constrained search for a 1 → 16 → 1 active-S-box pattern.

Core idea: constrain the trail to 18 active S-boxes

A three-round pattern: one active byte → full diffusion → one active byte



Total: 1 + 16 + 1 = 18 active S-boxes

Meet-in-the-Middle search strategy

Enumerate all possible non-zero byte values at each end of the diffusion layer

Forward set

16 positions × 255 values
= 4,080 candidates

MATCHING STAGE

Apply L / L^{-1}
and test S-box transitions
using DDT or LAT

Backward set

16 positions × 255 values
= 4,080 candidates

Differential search: 13 matching transformations were found.

Linear search: 18 combinations remained after applying the stated bias threshold.

Differential cryptanalysis: best three-round result

BEST CHARACTERISTIC

$$2^{-115.2}$$

18 active S-boxes
across 3 rounds

Search outcome

- Only 13 candidate transformations matched the constrained pattern.
- The two best candidates were evaluated; the strongest gives probability $2^{-115.2}$.
- The earlier two-round optimum does not remain optimal when extended.

Interpretation: a substantially more structured three-round trail is found by optimizing the full path.

Linear cryptanalysis: best three-round result

BEST CHARACTERISTIC

$$2^{-118.8}$$

18 active S-boxes
across 3 rounds

Search outcome

- Mask propagation must account for the transpose of the L transformation.
- The LAT is used to evaluate byte-wise correlations.
- 18 candidate combinations passed the selected aggregate-bias threshold; the best reported characteristic has probability $2^{-118.8}$.

The transposed diffusion map is essential to the linear search.

Results and scope: what do these numbers mean?

Measure	Differential	Linear
Best 3-round probability	$2^{-115.2}$	$2^{-118.8}$
Active S-boxes	18	18

WHAT IS ESTABLISHED

Optimal / best-found three-round characteristics under the paper's 18-active-S-box constraint.

WHAT IS NOT CLAIMED

No practical distinguishing attack on the full 9-round Kuznyechik cipher is demonstrated.

The paper's scope is theoretical evaluation of the initial rounds and their security margin.

Conclusions

The study extends the analysis from two rounds to three rounds.

01 STRUCTURE

A constrained 1–16–1 activity pattern limits the trail to 18 active S-boxes.

02 SEARCH

A Meet-in-the-Middle framework links candidate states through L / L^{-1} and S-box tables.

03 RESULTS

Best reported probabilities: $2^{-115.2}$ (differential) and $2^{-118.8}$ (linear).

These results refine the theoretical picture of reduced-round Kuznyechik; they do not break the full cipher.

Thank you for your attention

Selected references

[12] V. Kiryukhin, “Exact maximum expected differential and linear probability for 2-round Kuznyechik,” IACR ePrint 2018/1085, 2018.

[13] E. Ishchukova, E. Tolomanenko, L. Babenko, “Differential analysis of 3-round Kuznyechik,” 2020, pp. 29–36. DOI: 10.1145/3136825.3136880.

[14] T. Ashur and E. Takke, “A New Linear Distinguisher for Four-Round AES,” IACR ePrint 2023/398, 2023.

Cipher standard: GOST R 34.12–2015.

The presentation is based on the submitted article by Evgeniya Ishchukova.