Differential analysis of the ternary hash function Troika

Christina Boura   Margot Funk   Yann Rotella

Paris-Saclay University - Versailles University

Permutation-Based Crypto workshop
April 23 2023

Context

Troika: a ternary cryptographic hash function

- Kölbl, Tischhauser, Derbez and Bogdanov [DCC 2019]
- Designed for IOTA's distributed ledger
- Follows the KECCAK philosophy

Computer-assisted proofs for differential analysis over $\mathbb{F}_2$

- Tool assisted approach (MILP, SAT solvers...)
- Dedicated programs based on a tree traversal [Mella, Daemen, Van Assche, ToSC 2017]

PART 1:

Basics of differential analysis

Differential cryptanalysis

A **differential** $(\Delta_{\text{in}}, \Delta_{\text{out}})$ is a couple of differences.

$$x \longrightarrow \boxed{f} \longrightarrow f(x)$$

$$x' \longrightarrow \boxed{f} \longrightarrow f(x')$$

$$\underbrace{x - x'}_{\Delta_{\text{in}}} \qquad\qquad \underbrace{f(x) - f(x')}_{\Delta_{\text{out}}}$$

A **differential trail** Q is a tuple of intermediate differences.

$$q_0 \xrightarrow{\mathrm{R}_0} q_1 \xrightarrow{\mathrm{R}_1} \cdots\ q_{k-1} \xrightarrow{\mathrm{R}_{k-1}} q_k$$

Differential cryptanalysis

- $\mathrm{DP}_f(q_0, q_k) \approx \mathrm{DP}_{\mathrm{R}_0}(q_0, q_1) \times \mathrm{DP}_{\mathrm{R}_1}(q_1, q_2) \times \ldots \times \mathrm{DP}_{\mathrm{R}_{k-1}}(q_{k-1}, q_k)$
- Existence of a trail of **high probability**?
- Convenient to work with the **weight**:

$$\mathrm{w}_f(\Delta_{\mathrm{in}}, \Delta_{\mathrm{out}}) := -\log\left(\mathrm{DP}_f\left(\Delta_{\mathrm{in}}, \Delta_{\mathrm{out}}\right)\right)$$

Differential trails and trail cores

A 3-round trail $b_0 \xrightarrow{\text{S}} a_1 \xrightarrow{\text{L}} b_1 \xrightarrow{\text{S}} a_2 \xrightarrow{\text{L}} b_2 \xrightarrow{\text{S}} a_3 \xrightarrow{\text{L}} b_3$

Weight $\mathrm{w}_{\text{S}}(b_0, a_1) \quad + \quad \mathrm{w}_{\text{S}}(b_1, a_2) \quad + \quad \mathrm{w}_{\text{S}}(b_2, a_3)$

Differential trails and trail cores

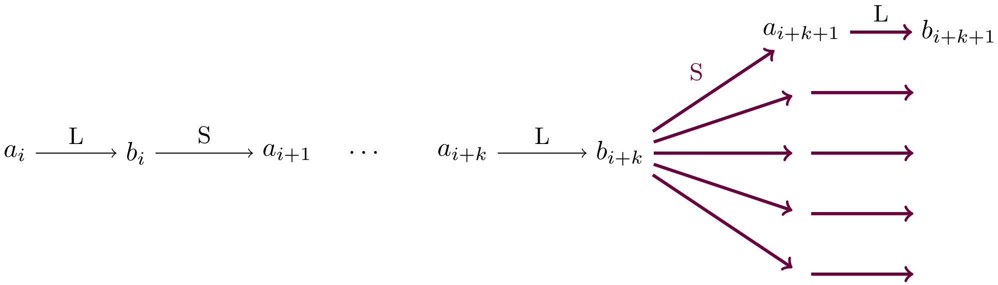
A 3-round trail core

$$a_1 \xrightarrow{\mathrm{L}} b_1 \xrightarrow{\mathrm{S}} a_2 \xrightarrow{\mathrm{L}} b_2$$

Weight

$$\min_{b_0} \mathrm{w}_{\mathrm{S}}(b_0, a_1) \quad + \quad \mathrm{w}_{\mathrm{S}}(b_1, a_2) \quad + \quad \min_{a_3} \mathrm{w}_{\mathrm{S}}(b_2, a_3)$$

Trail core extension



Forward extension

Lower bounding the weight of trails [MDV17]

Framework:

1. Collect **all 2-round trail cores** up to a “weight target” with a **tree traversal**.
2. Try (and fail) to **extend** these trail cores into trail cores of small weight.

Related work:

- Analysis of XOODOO [DHVV18b, DMA22], ASCON [EMMD22], SUBTERRANEAN [MMGD22]

Our work:

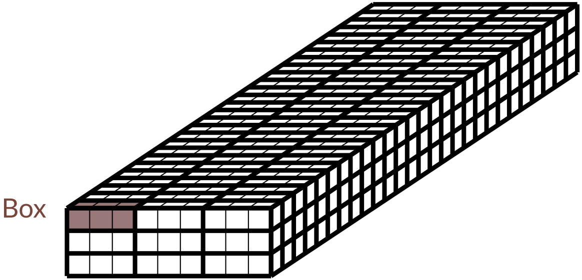
- Define the tree and the extension algorithms for Troika.

PART 2:

Troika round function

The Troika round function $\mathrm{R}_i : \mathbb{F}_3^{729} \to \mathbb{F}_3^{729}$

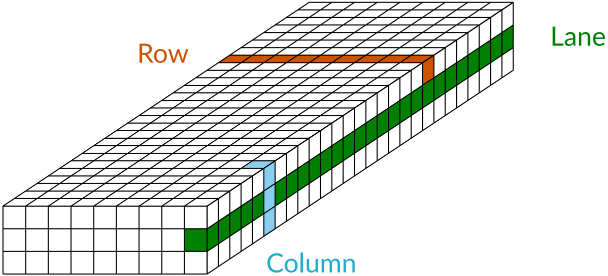
$\mathrm{R}_i = \iota_i \circ \mathrm{L} \circ \mathrm{S}$
$\mathrm{L} =$ AddColumnParity $\circ$ ShiftLanes $\circ$ ShiftRows



Troika state of $9 \times 3 \times 27$ trits

The Troika round function $\mathrm{R}_i : \mathbb{F}_3^{729} \to \mathbb{F}_3^{729}$

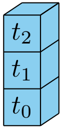
$\mathrm{R}_i = \iota_i \circ \mathrm{L} \circ \mathrm{S}$
$\mathrm{L} = \text{AddColumnParity} \circ \text{ShiftLanes} \circ \text{ShiftRows}$



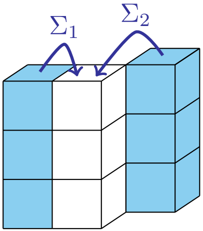
Troika state of $9 \times 3 \times 27$ trits

AddColumnParity

It **adds** to each trit of a column the **parity of two other columns**.



Column of parity
$t_0 + t_1 + t_2 \in \mathbb{F}_3$



Kernel of AddColumnParity : $b \in K \iff \text{AddColumnParity}(b) = b$

Question for the 2-round trail cores generation

$$\xleftarrow{\mathrm{S}} a \xrightarrow{\text{ShiftRows}} \xrightarrow{\text{ShiftLanes}} \xrightarrow{\text{AddColumnParity}} b \xrightarrow{\mathrm{S}}$$

A 2-round trail core

Can we only specify the positions of the active trits (1, 2)?

- ✓ for ShiftRows and ShiftLanes
- ✗ for AddColumnParity

$\rightarrow$ Yes, when $b \in K$.

PART 3:

The space of 3-round trail cores

Split the 3-round trail cores as in [MDV17]

$$\overset{S}{\dashleftarrow} \; a_1 \xrightarrow{L} b_1 \xrightarrow{S} a_2 \xrightarrow{L} b_2 \; \overset{S}{\dashrightarrow}$$

A 3-round trail core

For 3-round trail cores with b_1 and b_2 in the Kernel

- ▷ **specific algorithm**

For 3-round trail cores with b_1 or b_2 outside the Kernel

1. **Collect 2-round trail cores** (distinguish between trail cores **inside** / **outside the Kernel**)
2. **Extend** the 2-round trail cores **into 3-round trail cores**

3-round trail cores with b_1 and b_2 in the Kernel

We were able to scan all the trail cores of weight ≤ 65 (versus 41 for the other cases).

$$b_1 \xrightarrow{S\text{-boxes}} a_2 \xrightarrow{\text{shuffling layer}} b_2$$

$z = 1$

0	0	0	0	**1**	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	**2**	0	0	0	0

$z = 6$

0	**1**	0	0	0	0	0	0	0
0	**2**	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

$z = 1$

0	0	0	**1**	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	0	0	0	**2**	0	0	0

$z = 6$

0	0	**1**	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0

Active boxes alignment

$z = 0$

0	0	**1**	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0
0	0	**2**	0	0	0	0	0	0

$z = 11$

0	0	0	**1**	0	0	0	0	0
0	0	0	**2**	0	0	0	0	0
0	0	0	0	0	0	0	0	0

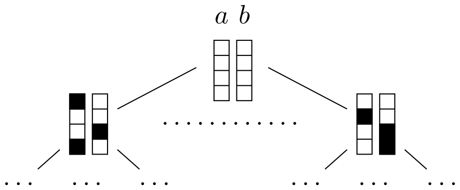
Active trits alignment

PART 4:
The tree to scan the 2-round trail cores

Generate 2-round trail cores $a \xrightarrow{\mathbf{L}} b$ with a tree [MDV17]

Goal: collect all the 2-round trail cores (a, b) with “few active boxes”

Root of the tree: the 2-round trail core $(a, b) = (0, 0) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$
Child of a node: is generated by adding some vector $(u_i, v_i) \in \mathbb{F}_2^n \times \mathbb{F}_2^n$, called **unit**

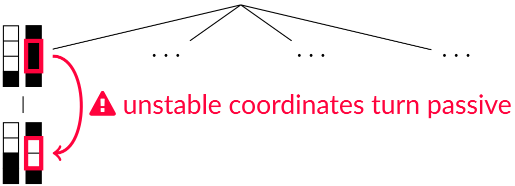


Generate 2-round trail cores $a \xrightarrow{\mathrm{L}} b$ with a tree [MDV17]

Tree pruning:

- by lower bounding the number of active boxes of a node and its descendants
- + criteria to take into account symmetry properties (e.g. z-invariance)

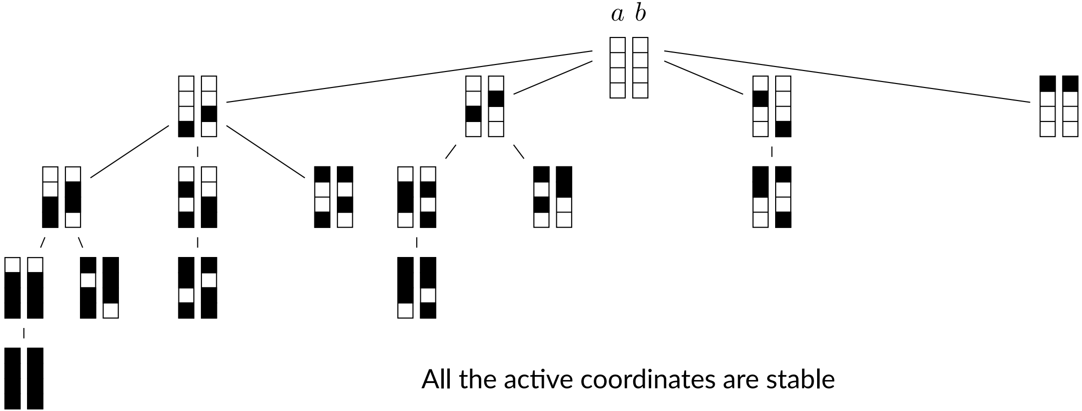
Unstable active coordinates: can be removed by adding a new unit (u_i, v_i).



Question: How can we define a tree with few unstable coordinates?

Generate 2-round trail cores $a \xrightarrow{\mathrm{L}} b$ with a tree [MDV17]

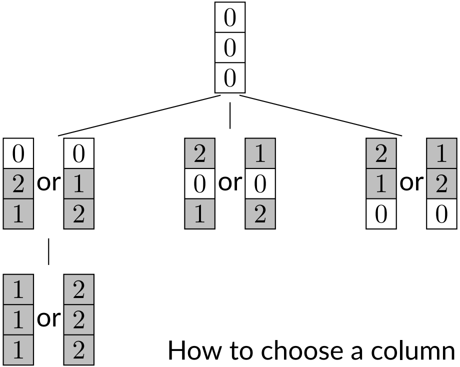
Toy example with a shuffling layer $\mathrm{L} : \mathbb{F}_2^4 \mapsto \mathbb{F}_2^4$ and $(u_i, v_i) = (e_i, \mathrm{L}(e_i))$



All the active coordinates are stable

The tree to collect 2-round trail cores with $b \in K$

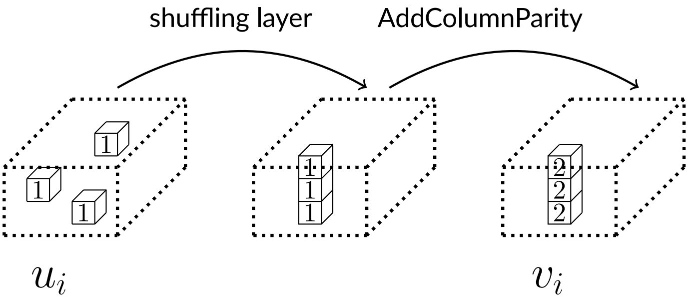
✓ Nodes with only stable coordinates



How to choose a column of b

The tree to collect 2-round trail cores with $b \notin K$

Choose the **columns**' values on **either side of AddColumnParity** in an appropriate order.



The tree to collect 2-round trail cores with $b \notin K$

Choose the **columns**' values on **either side of AddColumnParity** in an appropriate order.

$$\begin{array}{|c|}\hline 0\\\hline 1\\\hline 2\\\hline\end{array} \xrightarrow{\text{AddColumnParity}} \begin{array}{|c|}\hline 1\\\hline 2\\\hline 0\\\hline\end{array}$$

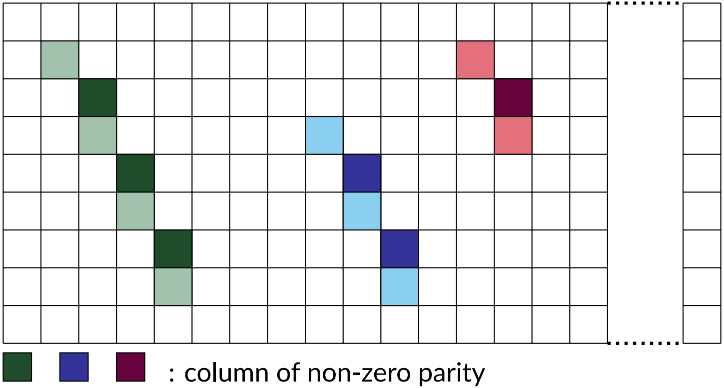
Affected

$$\begin{array}{|c|}\hline 0\\\hline 2\\\hline 0\\\hline\end{array} \xrightarrow{\text{AddColumnParity}} \begin{array}{|c|}\hline 0\\\hline 2\\\hline 0\\\hline\end{array}$$

Non-affected

The tree to collect 2-round trail cores with $b \notin K$

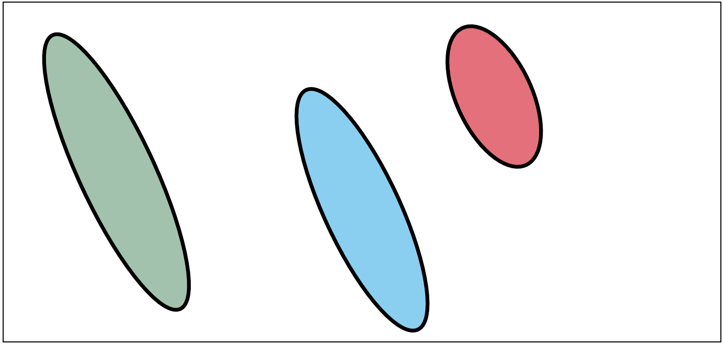
top view of the state



: column of non-zero parity

The tree to collect 2-round trail cores with $b \notin K$

diagram of a state with 3 supra-units (runs)



The tree to collect 2-round trail cores with $b \notin K$

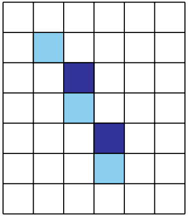
Reduce the number of unstable coordinates

Motivation:

- the tree pruning is more efficient when there are few unstable coordinates

Where do unstable coordinates come from?

- from supra-units overlappings (can change the value of a column already active)



The tree to collect 2-round trail cores with $b \notin K$

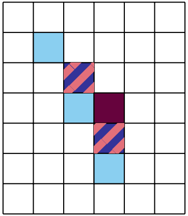
Reduce the number of unstable coordinates

Motivation:

- the tree pruning is more efficient when there are few unstable coordinates

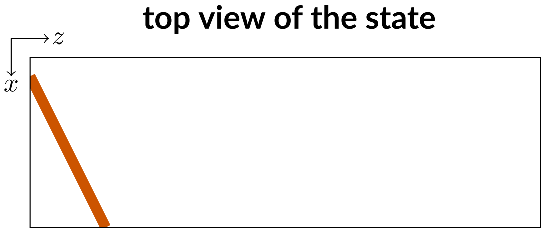
Where do unstable coordinates come from?

- from supra-units overlappings (can change the value of a column already active)



The tree to collect 2-round trail cores with $b \notin K$

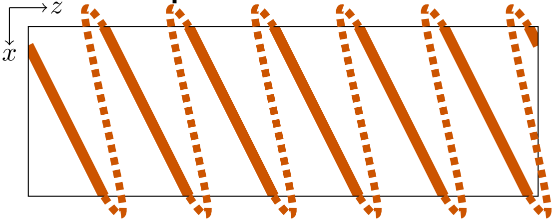
Reduce the number of unstable coordinates



The tree to collect 2-round trail cores with $b \notin K$

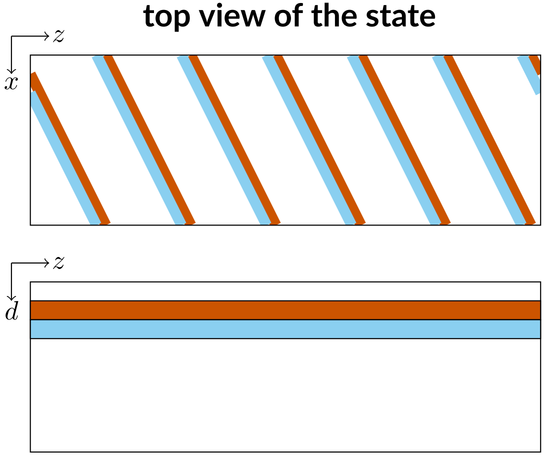
Reduce the number of unstable coordinates

top view of the state



The tree to collect 2-round trail cores with $b \notin K$

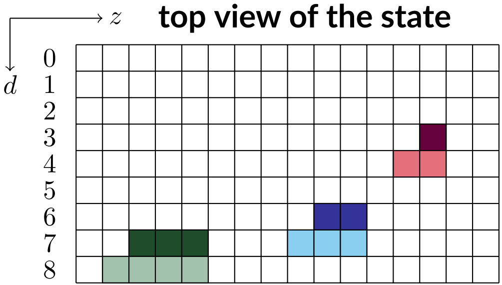
Reduce the number of unstable coordinates



The tree to collect 2-round trail cores with $b \notin K$

Reduce the number of unstable coordinates

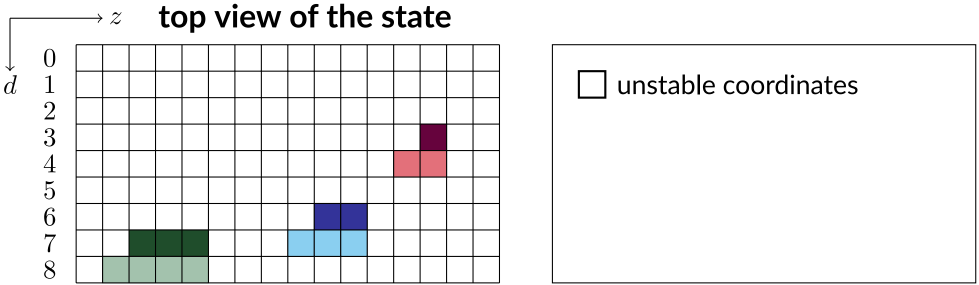
Ordering of supra-units: from diagonal 0 to diagonal 8.



The tree to collect 2-round trail cores with $b \notin K$

Reduce the number of unstable coordinates

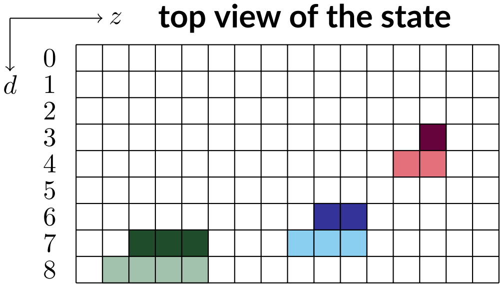
Ordering of supra-units: from diagonal 0 to diagonal 8.

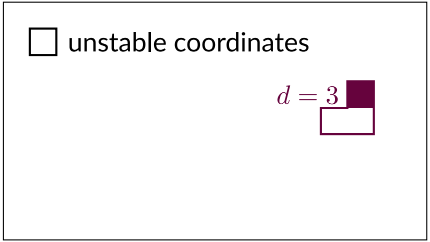


The tree to collect 2-round trail cores with $b \notin K$

Reduce the number of unstable coordinates

Ordering of supra-units: from diagonal 0 to diagonal 8.



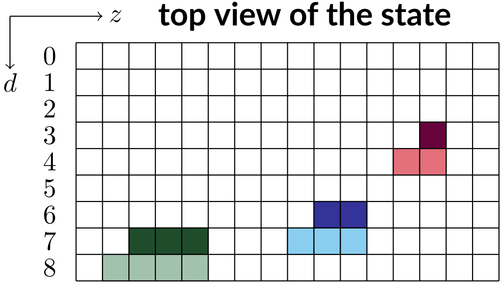


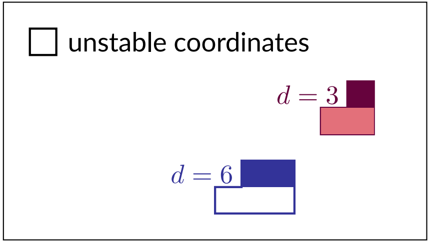
The tree to collect 2-round trail cores with $b \notin K$

Reduce the number of unstable coordinates

Ordering of supra-units: from diagonal 0 to diagonal 8.

top view of the state

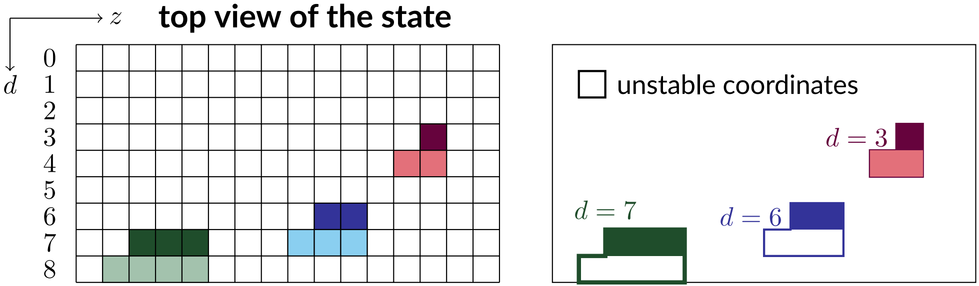




The tree to collect 2-round trail cores with $b \notin K$

Reduce the number of unstable coordinates

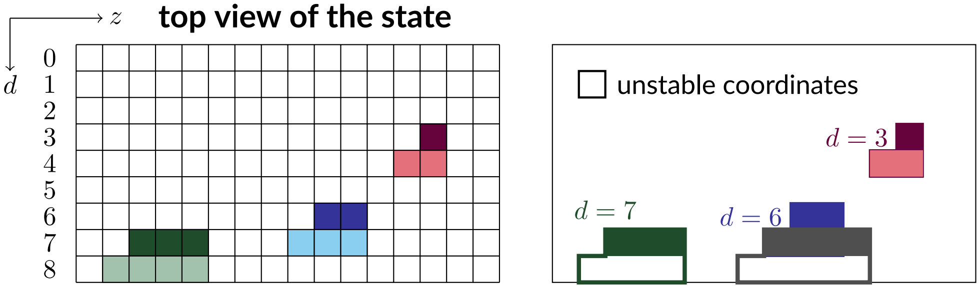
Ordering of supra-units: from diagonal 0 to diagonal 8.



The tree to collect 2-round trail cores with $b \notin K$

Reduce the number of unstable coordinates

Ordering of supra-units: from diagonal 0 to diagonal 8.



The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

Types of columns:

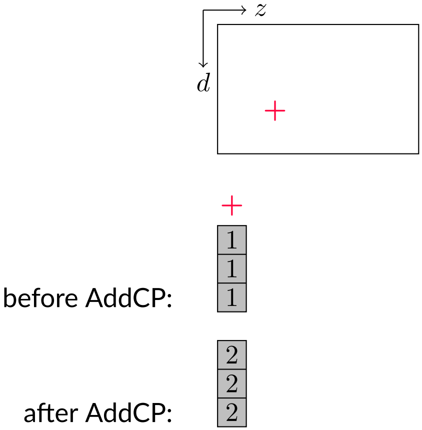
- $+$: affected by $+1$
- $-$: affected by -1
- $\bigcirc$: parity 1
- $\diamond$: parity 2

The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

Types of columns:

- $+$: affected by $+1$
- $-$: affected by -1
- ◯ : parity 1
- ◇ : parity 2



The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

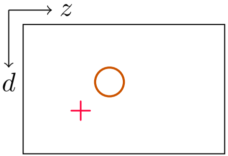
Types of columns:

$+$: affected by $+1$

$-$: affected by -1

○ : parity 1

◇ : parity 2



before AddCP:

$+$	○
1	0
1	0
1	1

after AddCP:

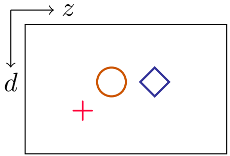
2	0
2	0
2	1

The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

Types of columns:

- $+$: affected by $+1$
- $-$: affected by -1
- $\bigcirc$: parity 1
- $\diamond$: parity 2



$$\begin{array}{ccc} + & \bigcirc & \diamond \end{array}$$

before AddCP: $\begin{array}{|c|c|c|} 1 & 0 & 2 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{array}$

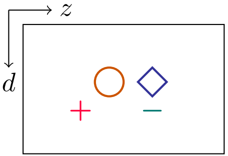
after AddCP: $\begin{array}{|c|c|c|} 2 & 0 & 2 \\ 2 & 0 & 0 \\ 2 & 1 & 0 \end{array}$

The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

Types of columns:

- $+$: affected by $+1$
- $-$: affected by -1
- $\bigcirc$: parity 1
- $\Diamond$: parity 2



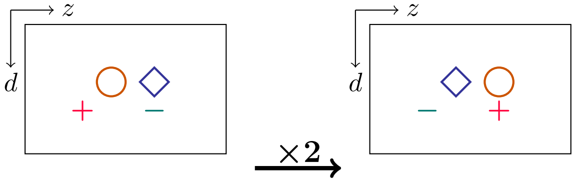
	$+$	$\bigcirc$	$\Diamond$	$-$
	1	0	2	1
	1	0	0	2
before AddCP:	1	1	0	0
	2	0	2	0
	2	0	0	1
after AddCP:	2	1	0	2

The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

Types of columns:

- $+$: affected by $+1$
- $-$: affected by -1
- ○ : parity 1
- ◇ : parity 2



before AddCP:

$+$	○	◇	$-$		$-$	◇	○	$+$
1	0	2	1		2	0	1	2
1	0	0	2		2	0	0	1
1	1	0	0		2	2	0	0

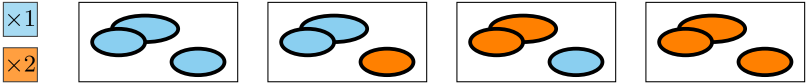
after AddCP:

2	0	2	0		1	0	1	0
2	0	0	1		1	0	0	2
2	1	0	2		1	2	0	1

The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation

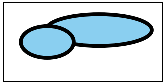
Diagrams of states in the same equivalence class



Handle the overlappings

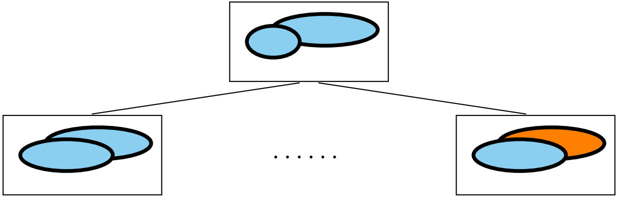
The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation



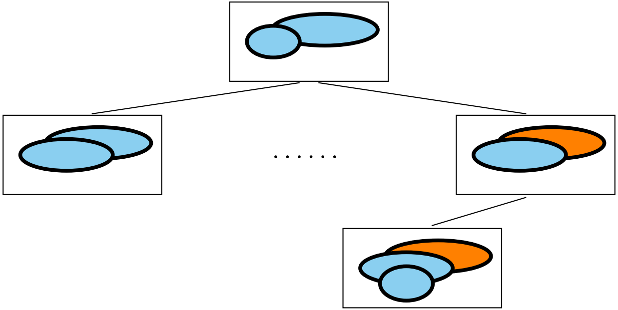
The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation



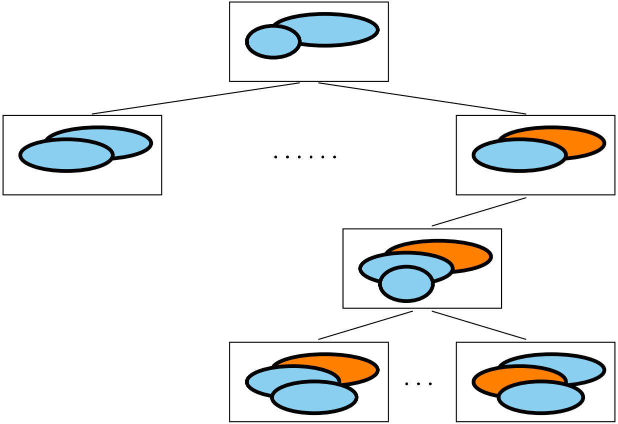
The tree to collect 2-round trail cores with $b \notin K$

Equivalence relation



The tree to collect 2-round trail cores with $b \notin K$

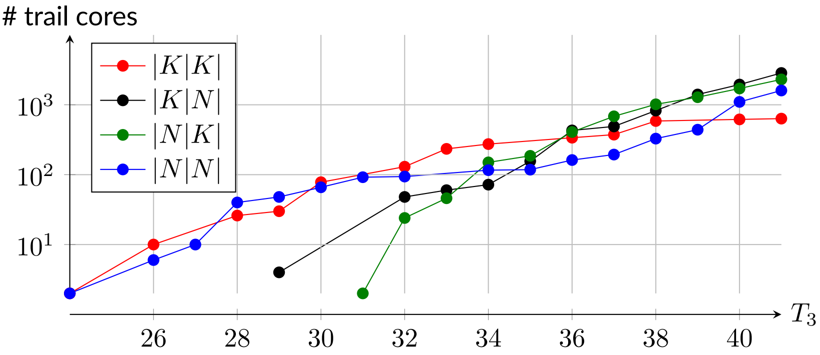
Equivalence relation



PART 5:

Results

All 3-round trail cores with weight ≤ 41



Number of 3-round trail cores of weight W such that $\lceil W \rceil \leq T_3$ for different parity profiles

Result

No 6-round trail cores of weight $\leq$ 82.

Differential probability of a 24-round differential trail $< 3^{-328}$.

Previous bound: 3^{-300} (on a scaled-down version of Troika with 9 slices).

Execution time

Parity profile	Direction	Time	Parity profile	Direction	Time
$\|K\|K\|$	backward	22m40s	$\|K\|N\|$	forward backward	5m7s 5h19m
$\|N\|N\|$	forward backward	9h16m 17h7m	$\|N\|K\|$	forward backward	6h32m 26m10s