Trail Bound Techniques in Primitives with Weak Alignment

Silvia Mella[1]

based on a joint work with
Joan Daemen[2] and Gilles Van Assche[1]

[1]STMicroelectronics [2]Radboud University

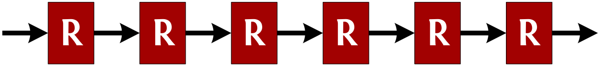
APBC 2018

Outline

Outline

Differential trails in iterated mappings

$$\mathrm{DP}(Q) \approx \mathrm{DP}_{0,1} \times \mathrm{DP}_{1,2} \times \mathrm{DP}_{2,3} \times \mathrm{DP}_{3,4} \times \mathrm{DP}_{4,5} \times \mathrm{DP}_{5,6}$$



Q: q_0 q_1 q_2 q_3 q_4 q_5 q_6

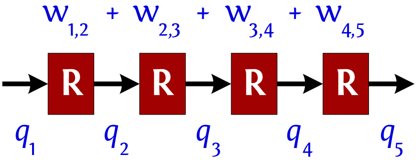
Differential trails and weight

$$\mathrm{w} = -\log_2(DP)$$

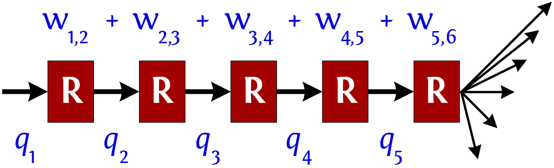
$$\mathrm{w}(Q) = \mathrm{w}_{0,1} + \mathrm{w}_{1,2} + \mathrm{w}_{2,3} + \mathrm{w}_{3,4} + \mathrm{w}_{4,5} + \mathrm{w}_{5,6}$$

$$Q:\quad q_0 \xrightarrow{R} q_1 \xrightarrow{R} q_2 \xrightarrow{R} q_3 \xrightarrow{R} q_4 \xrightarrow{R} q_5 \xrightarrow{R} q_6$$

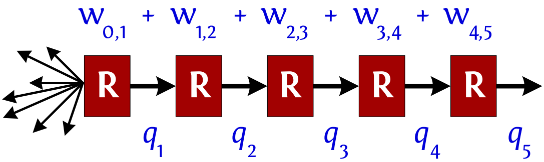
Trail extension



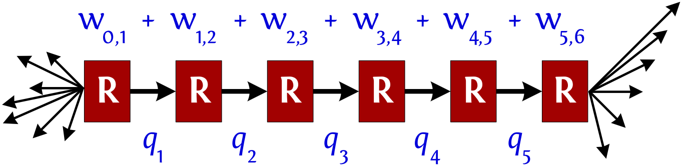
Trail extension



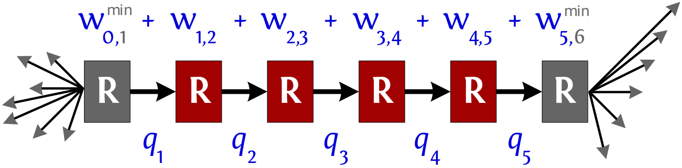
Trail extension



Trail extension

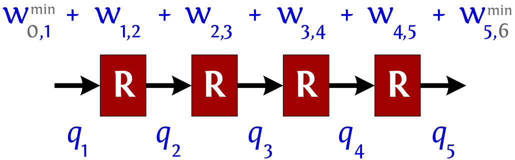


Trail cores



Bounding the weight of trails

- We restrict to trail cores...
- ...up to a given target weight T
- We start from 2-round trail cores and then extend



Outline

Definition

Set U of *units* with a total order relation $\prec$

Tree

- Node: subset of U, represented as a *unit list*

$$a = (u_i)_{i=1,\dots,n} \quad u_1 \prec u_2 \prec \cdots \prec u_n$$

- Children of a node a:

$$a \cup \{u_{n+1}\} \quad \forall\ u_{n+1} \ :\ u_n \prec u_{n+1}$$

- Root: the empty set $a = \emptyset$

Bounding the cost

Goal: tree traversal up to given cost target T

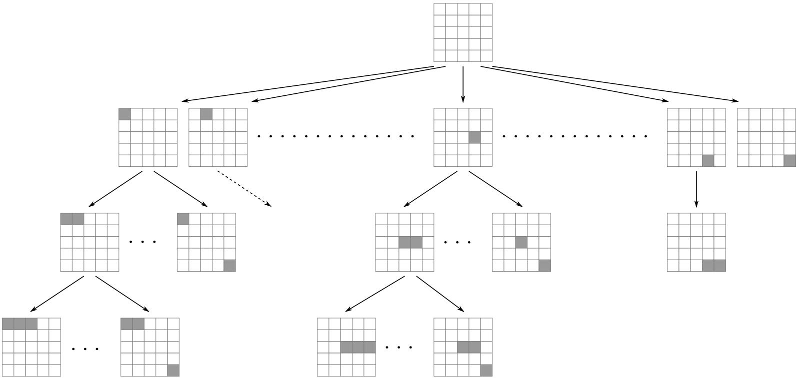
Cost-related functions

- Cost function: $\gamma(a)$ (e.g. $w^{\text{rev}}(a) + w^{\text{dir}}(a)$)
- Cost bounding function: $L(a)$ s.t.

$$\gamma(a') \geq L(a) \quad \text{for all descendants } a' \text{ of } a$$

$\Rightarrow$ Prune all the subtrees with $L(a) > T$

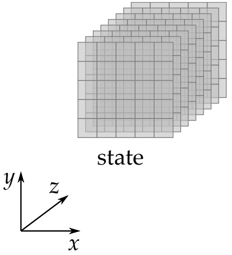
Example: active bit positions



Outline

KECCAK-f

Operates on 3D state:



- (5×5)-bit slices
- 2^ℓ-bit lanes
- parameter $0 \leq \ell < 7$

Round function with 5 steps:

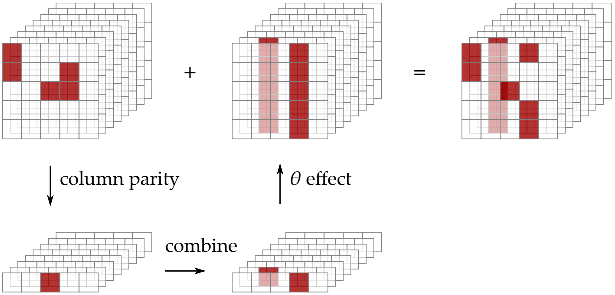
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

rounds: $12 + 2\ell$ for width $b = 2^\ell 25$

- 12 rounds in KECCAK-f[25]
- 24 rounds in KECCAK-f[1600]

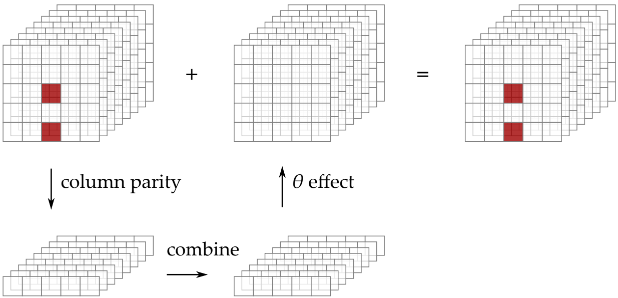
[Bertoni, Daemen, Peeters, Van Assche, 2008]

Properties of θ



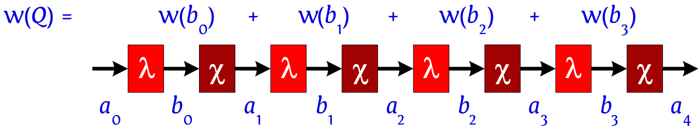
- The θ map adds a pattern, that depends on the parity, to each plane.
- Affected columns are complemented
- Unaffected columns are not changed

The parity Kernel



- θ acts as the identity if parity is zero
- A state with parity zero is in the kernel (or in $|K|$)
- A state with parity non-zero is outside the kernel (or in $|N|$)

Differential trails in KECCAK-f

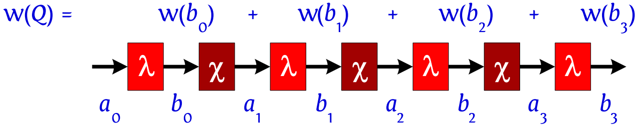


Round: linear step $\lambda = \pi \circ \rho \circ \theta$ and non-linear step χ

- a_i fully determines $b_i = \lambda(a_i)$
- χ has degree 2: $\mathrm{w}(b_{i-1})$ independent of a_i
- Minimum reverse weight:

$$\mathrm{w}_{rev}(a_1) \triangleq \min_{b_0} \mathrm{w}(b_0)$$

Differential trails in Keccak-f

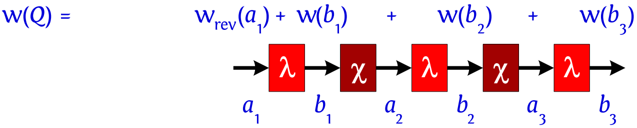


Round: linear step $\lambda = \pi \circ \rho \circ \theta$ and non-linear step χ

- a_i fully determines $b_i = \lambda(a_i)$
- χ has degree 2: $\mathrm{w}(b_{i-1})$ independent of a_i
- Minimum reverse weight:

$$\mathrm{w}_{rev}(a_1) \triangleq \min_{b_0} \mathrm{w}(b_0)$$

Differential trails in KECCAK-f



Round: linear step $\lambda = \pi \circ \rho \circ \theta$ and non-linear step χ

- a_i fully determines $b_i = \lambda(a_i)$
- χ has degree 2: $\mathrm{w}(b_{i-1})$ independent of a_i
- Minimum reverse weight:

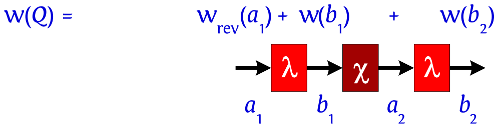
$$\mathrm{w}_{rev}(a_1) \triangleq \min_{b_0} \mathrm{w}(b_0)$$

Covering the space of 6-round trail cores

Lemma

A 6-round trail of weight W always contains a 3-round trail of weight below or equal to $\left\lfloor \frac{W}{2} \right\rfloor$

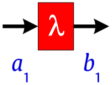
Covering the space of 3-round trail cores



- Space split based on parity of a_i
- Four classes: $|K|K|$, $|K|N|$, $|N|K|$ and $|N|N|$

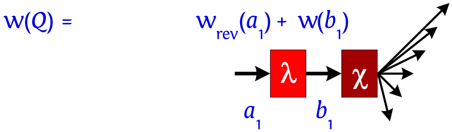
Covering the space of 3-round trail cores

$$w(Q) = w_{rev}(a_1) + w(b_1)$$



- Generating (a_1, b_1)
- Extending forward by one round

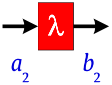
Covering the space of 3-round trail cores



- Generating (a_1, b_1)
- Extending forward by one round

Covering the space of 3-round trail cores

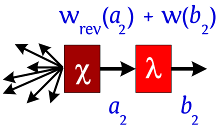
$$w(Q) = w_{rev}(a_2) + w(b_2)$$



- Generating (a_2, b_2)
- Extending backward by one round

Covering the space of 3-round trail cores

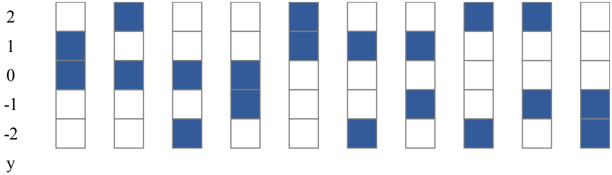
$w(Q) =$



- Generating (a_2, b_2)
- Extending backward by one round

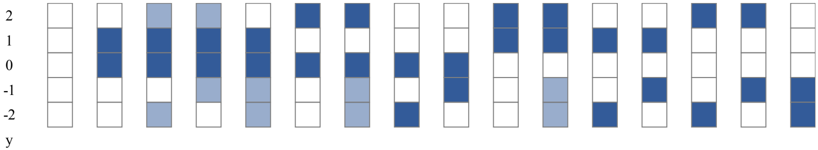
Orbitals

- $orbital = [z, x, y_1, y_2]$



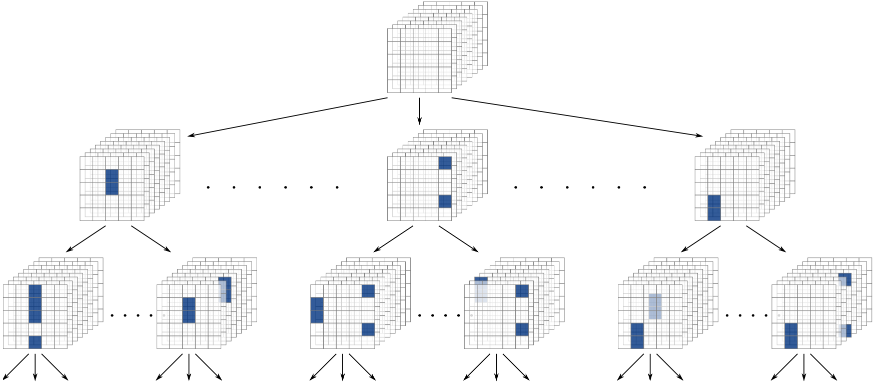
Orbitals (continued)

- $y_1' > y_2$



Generating trail cores in $|K|$

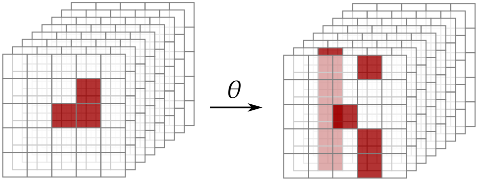
- Root: the empty state
- Units: *orbitals* $= [z, x, y_1, y_2]$
- Bound: cost of the node itself



Parity-bare states

Parity-bare state: a state with the minimum number of active bits before and after θ for a given parity

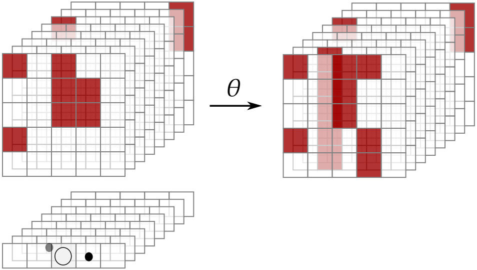
- 0 active bits in unaffected even columns
- 1 active bit in unaffected odd column
- 5 active bits in affected column either before or after θ



States in $|N|$

Lemma

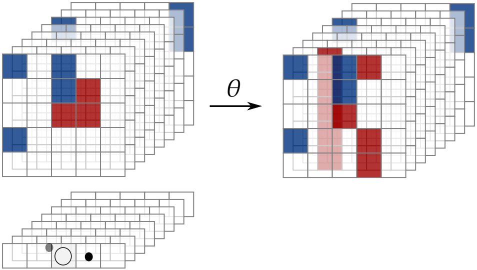
Each state can be decomposed in a unique way in a parity-bare state and a list of orbitals



States in $|N|$

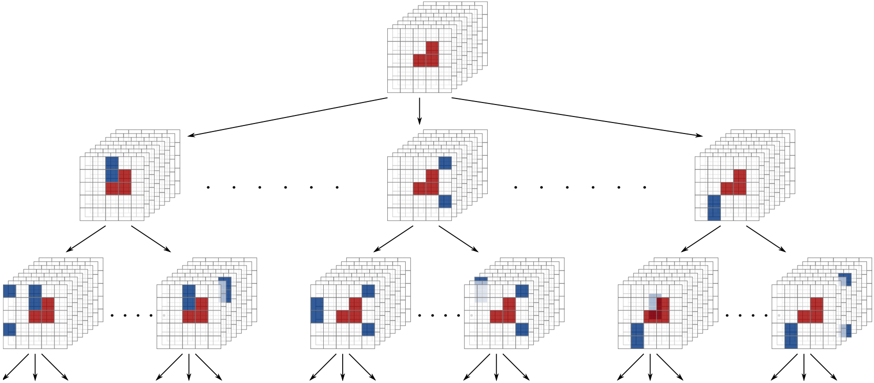
Lemma

Each state can be decomposed in a unique way in a parity-bare state and a list of orbitals



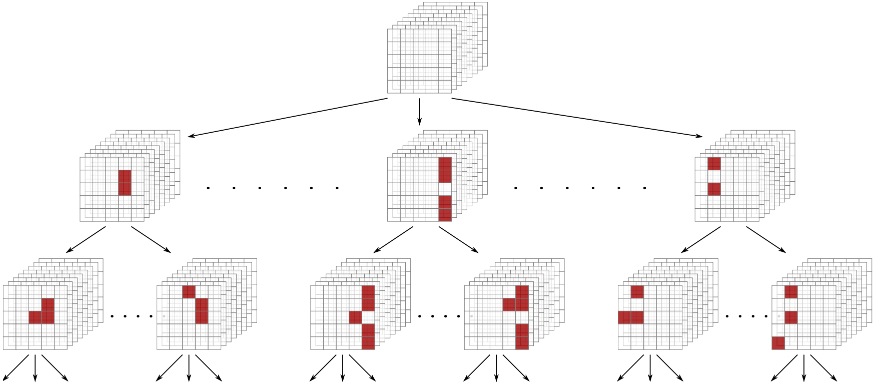
Orbital tree

- Root: a parity-bare state
- Units: orbitals in unaffected columns
- Bound: cost of the trail itself

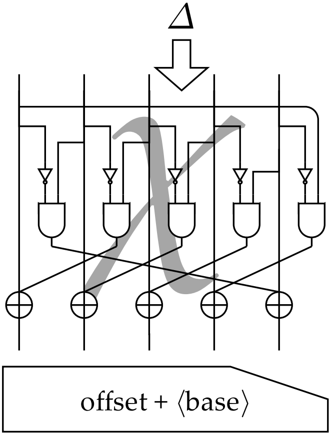


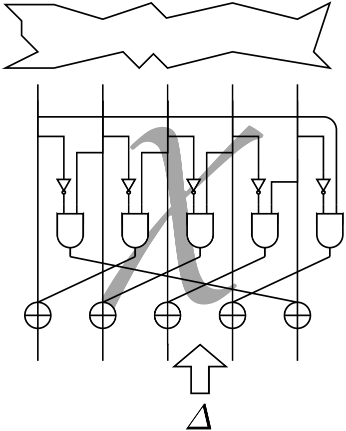
Run tree

- Root: the empty state
- Units: column assignments (x, z, odd/affected, column value)
- Bound: cost minus potential loss due to new CAs



Trail extension





Tree-search on affine space

- Affine space: $o + \langle b_1, \ldots, b_m \rangle$

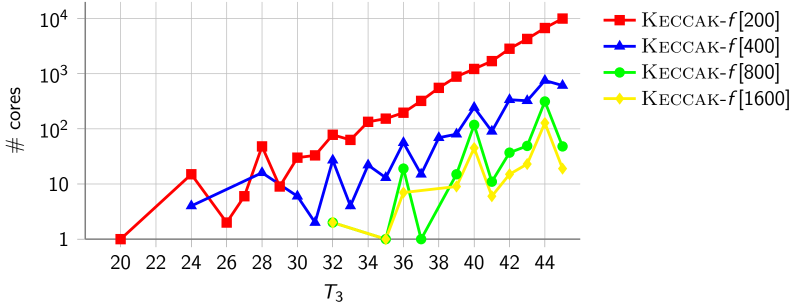
$$a = o + \sum_j \alpha_j b_j$$

- Unit set $U = \{b_1, \ldots, b_m\}$
- Root: $a = o$
- Node: $a = (b_i) \ : \ \alpha_i = 1$
- Define $L(a)$ to take advantage of stable active bits

Outline

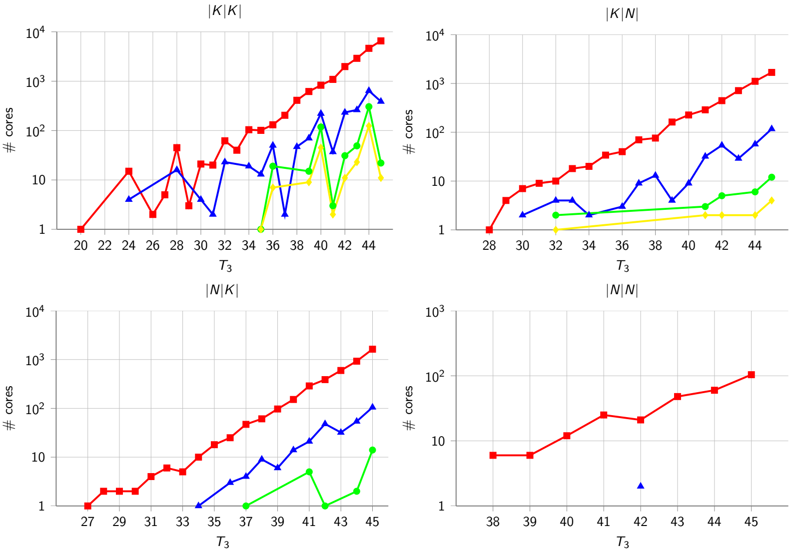
Experimental results

- All 3-round trail cores with weight ≤ 45



- No 6-round trail with weight ≤ 91

Trails for parity profile



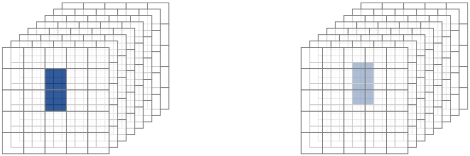
Bounds

rounds	$b = 200$	$b = 400$	$b = 800$	$b = 1600$
2	8	8	8	8
3	20	24	32	32
4	46	[48,63]	[48,104]	[48,134]
5	[50,89]	[50,147]	[50,247]	[50,372]
6	[92,142]	[92,278]	[92,556]	[92,1112]
n_r	[276,·]	[280,·]	[292,·]	[368,·]

Outline

Invariance by translation or rotation

E.g., in KECCAK-f, $w(\tau_z a) = w(a)$ for any translation τ_z along z



Canonicity

Canonical representation

- Define an order relation on states
- Define the canonical representation as the minimum one, e.g.,

$$a \text{ canonical} \;\Leftrightarrow\; a = \min_z \tau_z a$$

Tree search restricted to canonical representations

Reminder

- Set U of units with a total order relation $\prec$
- Unit list: $a = (u_i)_{i=1,\dots,n}$ with $u_1 \prec u_2 \prec \cdots \prec u_n$

Lemma

Assuming that

- $\prec_{\text{lex}}$ *is the lexicographic order on unit lists*
- *canonicity is defined w.r.t.* $\prec_{\text{lex}}$

then the parent of a canonical pattern is canonical.

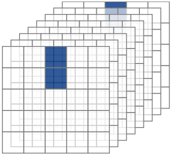
$\Rightarrow$ Complete non-canonical subtrees can be pruned

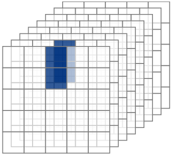
[Mella, Daemen, Van Assche, FSE 2017]

Testing for canonicity

Basic algorithm

- Input: unit list $a = (u_i)_{i=1,\dots,n}$
- For each i
  - Transform a such that $\tau(u_i)$ is $\prec$-minimum
  - Sort the resulting unit list
  - Compare it (using $\prec_{\text{lex}}$) to the currently minimum unit list
- Output: canonical representation (or just true/false)





Outline

Can the tree search be applied to your cipher?

- How to represent differences in a monotonic way?
- Can symmetry properties be exploited?
- Code available on `https://github.com/KeccakTeam/KeccakTools`

Thanks for your attention