New techniques for trail bounds and application to differential trails in KECCAK

Silvia Mella[1,2] Joan Daemen[1,3] Gilles Van Assche[1]

[1]STMicroelectronics [2]University of Milan [3]Radboud University

Fast Software Encryption
March 5-8, 2017

Outline

1 Introduction

2 Generating trails

3 Scanning space of trails in KECCAK-f

4 Experimental results

5 Conclusions

Outline

1 Introduction

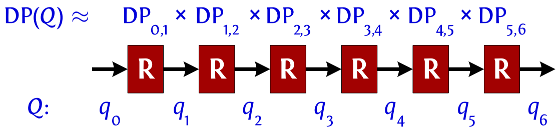
2 Generating trails

3 Scanning space of trails in KECCAK-f

4 Experimental results

5 Conclusions

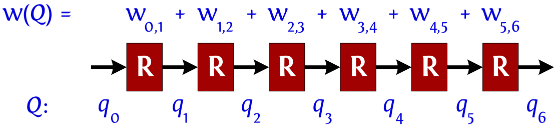
Differential trails in iterated mappings



- Trail: the sequence of differences after each round
- DP(Q): fraction of pairs that exhibit q_i differences

Differential trails and weight

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



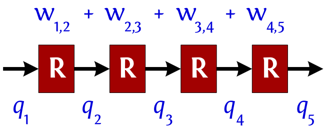
- The weight is the number of binary conditions that a pair must satisfy to exhibit q_i differences
- If *independent* conditions and $\mathrm{w}(Q) < b$: $\#\text{pairs}(Q) \approx 2^{b-\mathrm{w}(Q)}$

Trail extension

Given a trail, we can extend it

- forward: iterate over all differences R-compatible with q_5
- backward: iterate over all differences R^{-1}-compatible with q_1

Extension can be done recursively

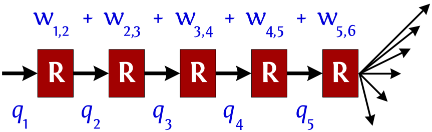


Trail extension

Given a trail, we can extend it

- forward: iterate over all differences R-compatible with q_5
- backward: iterate over all differences R^{-1}-compatible with q_1

Extension can be done recursively

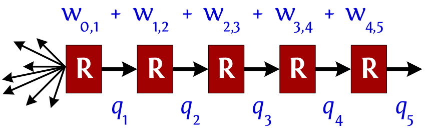


Trail extension

Given a trail, we can extend it

- forward: iterate over all differences R-compatible with q_5
- backward: iterate over all differences R^{-1}-compatible with q_1

Extension can be done recursively

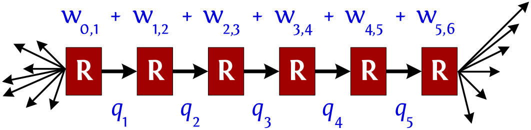


Trail extension

Given a trail, we can extend it

- forward: iterate over all differences R-compatible with q_5
- backward: iterate over all differences R^{-1}-compatible with q_1

Extension can be done recursively

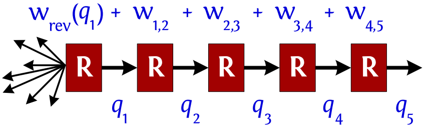


Trail cores

- Minimum reverse weight:

$$\mathrm{w}^{\mathrm{rev}}(q_1) \triangleq \min_{q_0} \mathrm{w}(q_0, q_1)$$

- Can be used to lower bound set of trails
- Trail core: set of trails with $q_1, q_2, \ldots$ in common



Goals of this work

- Present general techniques to generate trails
- Improve bounds of differential trails in Keccak-f
  - By extending the space of trails in Keccak-f that can be scanned with given computation resources

rounds	Keccak-f[200]	Keccak-f[400]	Keccak-f[800]	Keccak-f[1600]
2	8	8	8	8
3	20	this work	this work	32
4	46	this work	this work	this work
5	this work	this work	this work	this work
6	this work	this work	this work	this work

Outline

1 Introduction

2 Generating trails

3 Scanning space of trails in KECCAK-f

4 Experimental results

5 Conclusions

Generation of n-round trails of weight $\leq T$

First-order approach

Starting from 1-round differentials with weight $\leq \left\lfloor \frac{T}{n} \right\rfloor$

Second-order approach

Starting from 2-round trails with weight $\leq \left\lfloor \frac{2T}{n} \right\rfloor$

Fact

The number of 2-round trails with weight $\leq 2L$ is much smaller than the number of 1-round differentials with weight $\leq L$.

Example: AES

AES has more than 10^{11} round differentials with weight ≤ 15, but no 2-round trail with weight ≤ 30

Generating 2-round trails as tree traversal

- 2-round trails are arranged in a tree
- Children are generated by adding groups of active bits without removing bits already added
- Pruning by lower bounding the weight of a node and its children

Outline

1 Introduction

2 Generating trails

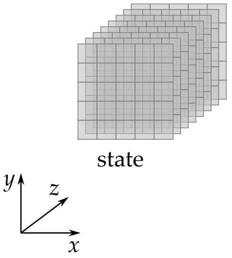
3 Scanning space of trails in KECCAK-f

4 Experimental results

5 Conclusions

KECCAK-f

Operates on 3D state:



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

Round function with 5 steps:

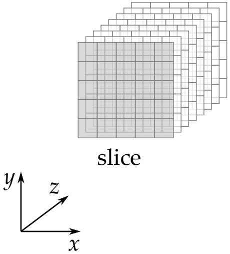
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

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

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

KECCAK-f

Operates on 3D state:



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

Round function with 5 steps:

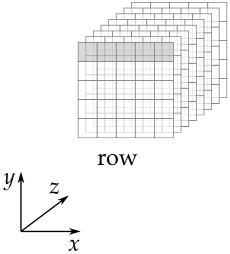
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

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

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

KECCAK-f

Operates on 3D state:



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

Round function with 5 steps:

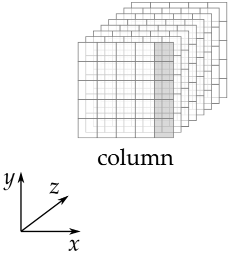
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

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

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

KECCAK-f

Operates on 3D state:



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

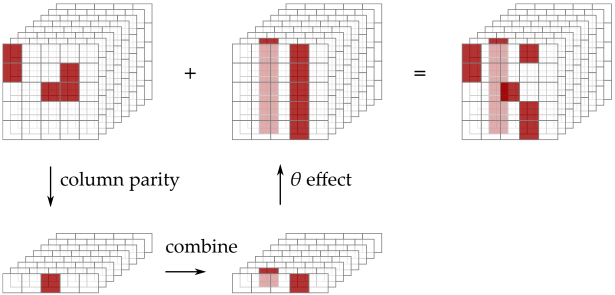
Round function with 5 steps:

- 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 $b = 2^\ell 25$

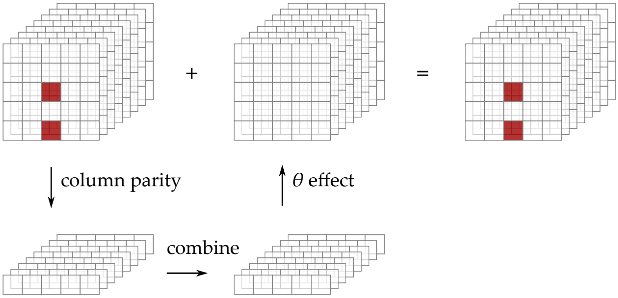
- 12 rounds in KECCAK-f[25]
- 24 rounds in KECCAK-f[1600]

Properties of θ



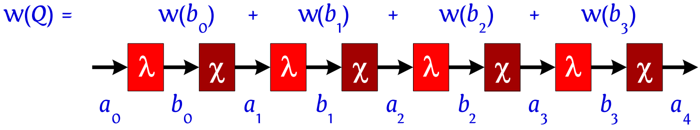
- The θ map adds a pattern, that depends on the parity, to the state.
- Affected columns are complemented
- Unaffected columns are not changed

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

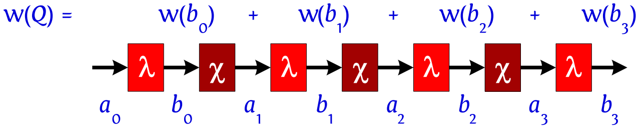


Round: linear step $\lambda = \pi \circ \rho \circ \theta$ and non-linear step χ

- 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:

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

Differential trails in Keccak-f

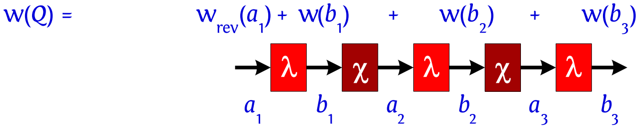


Round: linear step $\lambda = \pi \circ \rho \circ \theta$ and non-linear step χ

- 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:

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

Differential trails in KECCAK-f



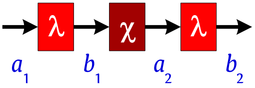
Round: linear step $\lambda = \pi \circ \rho \circ \theta$ and non-linear step χ

- 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:

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

Covering the space of 3-round trail cores

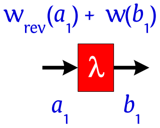
$$w(Q) = w_{rev}(a_1) + w(b_1) + w(b_2)$$



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

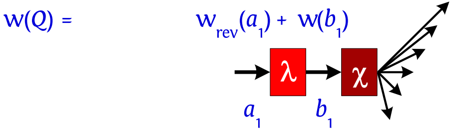
Covering the space of 3-round trail cores

w(*Q*) =



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

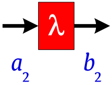
Covering the space of 3-round trail cores



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

Covering the space of 3-round trail cores

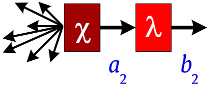
$w(Q) = \qquad w_{rev}(a_2) + w(b_2)$



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

Covering the space of 3-round trail cores

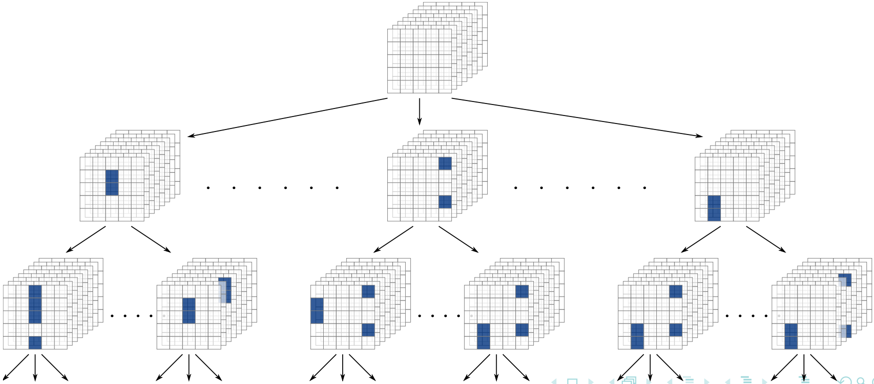
$\mathrm{w}(Q) =$ $\mathrm{w}_{\mathrm{rev}}(a_2) + \mathrm{w}(b_2)$



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

Generating trail cores in $|K|$

- To stay in $|K|$ units are *orbitals* = pairs of active bits in the same column
- A state a is a set of orbitals $a = \{u_i\}_{i=1,\ldots,n}$
- In the tree: the children of a node a are $a \cup \{u_{n+1}\}$



Order relation over units

- A total order relation over units allows avoiding duplicates
- With a total order $\prec$ over units, a state is an ordered list of units:

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

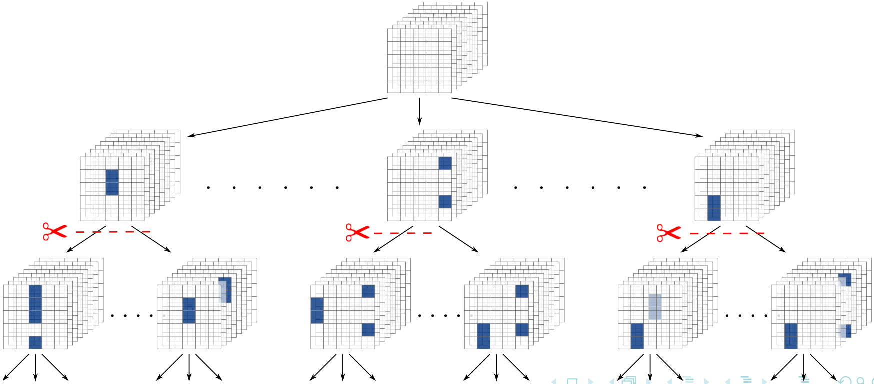
- In the tree: the children of a node a are

$$a \cup \{u_{n+1}\} \; \forall \; u_{n+1} \text{ s.t. } u_n \prec u_{n+1}$$

- For orbitals: the lexicographic order $[z, x, y_1, y_2]$

Pruning by lower bounding the weight

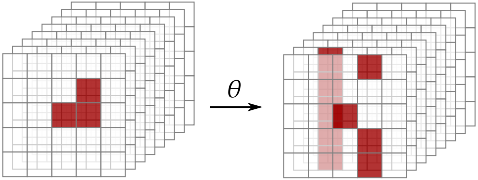
- The weight is monotonic in the addition of orbitals
- The weight of a lower bounds the weight of all descendants of a
- As soon as the search encounters a with weight above the limit, a and all its descendants can be safely pruned



Parity-bare states

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

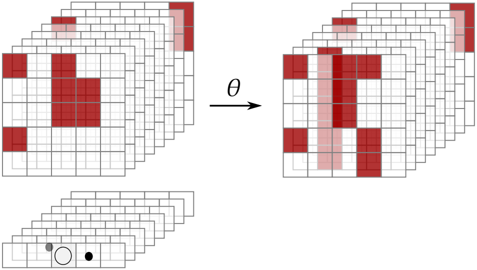
- 0 active bits in unaffected even columns
- 1 active bit in unaffected odd column
- 5 active bits in affected column either before or after θ



States in $|N|$

Lemma

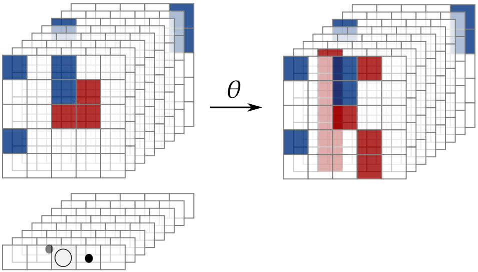
Each state can be decomposed in a unique way in a parity-bare state and a list of orbitals



States in $|N|$

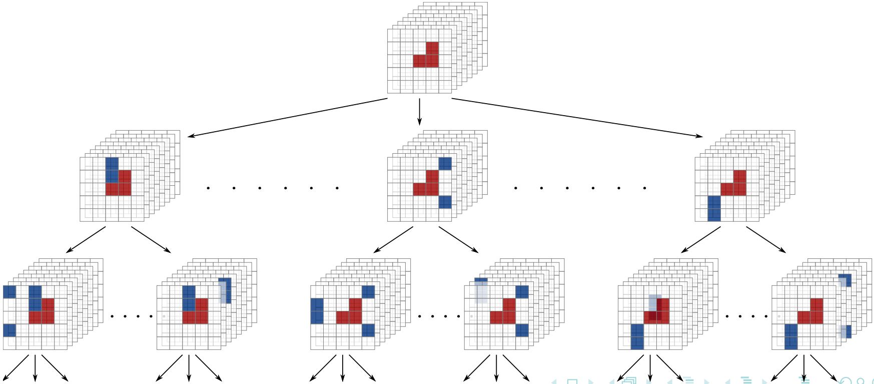
Lemma

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



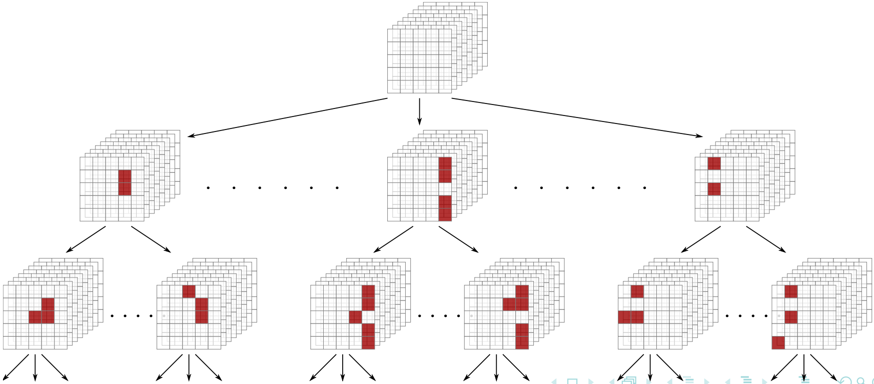
Orbital tree

- Root: a parity-bare state
- Units: orbitals in unaffected columns
- Order: the lexicographic order on $[z, x, y_1, y_2]$
- Bound: weight of the trail itself



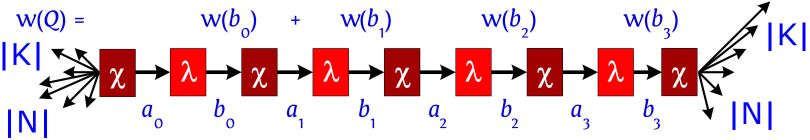
Run tree

- Root: the empty state
- Units: column assignments
- Bound: by estimating maximum weight lost due to addition of new column assignments



Trail extension

- forward: iterate a_4 over all differences χ-compatible with b_3
- backward: iterate b_{-1} over all differences χ^{-1}-compatible with a_0
- in the kernel: restrict to differences with parity zero
- outside the kernel: restrict to differences with parity non-zero



Forward extension

- Set of compatible states is an affine space $\mathcal{A}(b_r) = e + V$
- Basis transformation: $V = V_K + V_N$
- Extension in $|K|$ by scanning $e_K + V_K$
  - possible $\Leftrightarrow$ e_K exists
- Extension in $|N|$ by scanning $e + V_K + V_N$
- Scanning as a tree traversal
  - root: is the offset
  - children: by incrementally adding basis vectors
  - bound: by estimating the maximum weight lost due to addition of basis vectors not already added

Outline

1 Introduction

2 Generating trails

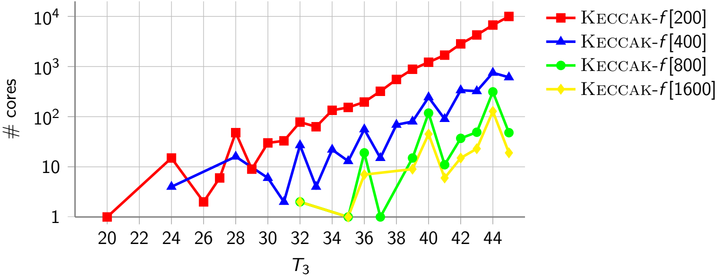
3 Scanning space of trails in KECCAK-f

4 Experimental results

5 Conclusions

Experimental results

- All 3-round trail cores with weight ≤ 45



- No 6-round trail with weight ≤ 91

Outline

1 Introduction

2 Generating trails

3 Scanning space of trails in KECCAK-f

4 Experimental results

5 Conclusions

Conclusions

- General formalism to generate differential patterns as simple and efficient tree traversal
- New bounds for KECCAK-f and new trails with the lowest known weight

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]

Table: Current bounds for the minimum weight of differential trails

Thanks for your attention