Differential propagation analysis of KECCAK

Joan DAEMEN and Gilles VAN ASSCHE

STMicroelectronics

Fast Software Encryption,
March 19-21, 2012

Outline

Outline

Differential trails in iterated mappings

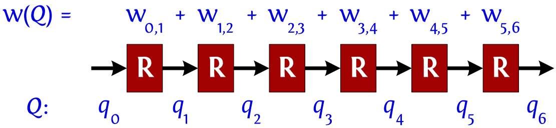
$$\mathrm{DP}(Q) \approx \mathrm{DP}_{0,1} \times \mathrm{DP}_{1,2} \times \mathrm{DP}_{2,3} \times \mathrm{DP}_{3,4} \times \mathrm{DP}_{4,5} \times \mathrm{DP}_{5,6}$$

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

- Trail: sequence of differences
- $\mathrm{DP}(Q)$: fraction of pairs that exhibit q_i differences

Differential trails and weight

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



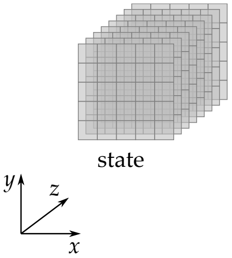
If *independent* rounds and $\mathrm{w}(Q) < b$: $\#\mathrm{pairs}(Q) \approx 2^{b-\mathrm{w}(Q)}$

Different design approaches

- Rijndael-inspired: strong alignment
  - estimating $\#\text{pairs}(Q)$ from Q: easy
  - easy demonstration of strong trail weight bounds
  - still, truncated trails, rebound attack, ...
- ARX
  - estimating $\#\text{pairs}(Q)$ from Q: hard
  - no strong trail weight bounds
  - revert to pre-DC/LC folklore such as *avalanche effect*
- KECCAK: weak alignment
  - $\#\text{pairs}(Q)$ from Q: easy
  - cryptanalysis seems hard
  - ...but proving strong lower bounds also

KECCAK-f: an iterative permutation

Operates on 3D state:



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

Round function with 5 steps:

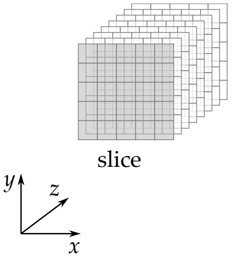
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

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

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

KECCAK-f: an iterative permutation

Operates on 3D state:



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

Round function with 5 steps:

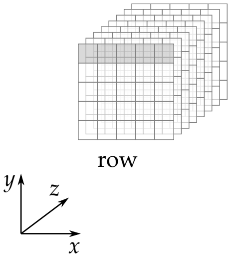
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

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

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

KECCAK-f: an iterative permutation

Operates on 3D state:



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

Round function with 5 steps:

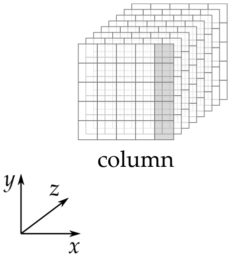
- θ: mixing layer
- ρ: inter-slice bit transposition
- π: intra-slice bit transposition
- χ: non-linear layer
- ι: round constants

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

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

KECCAK-f: an iterative permutation

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-$f[1600]$

This work

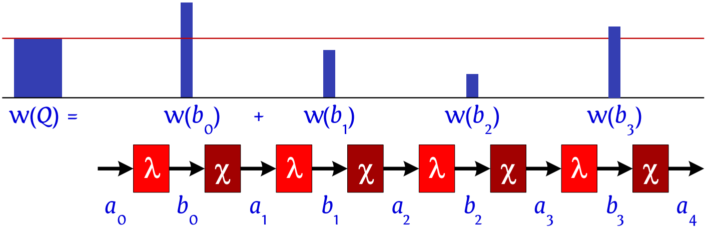
- Security of KECCAK relies on **absence** of exploitable trails
  ...and not on presumed hardness of finding them
- Bounds for small versions of KECCAK-f

b	bound	
25	30 per 5 rounds	tight
50	54 per 6 rounds	tight
100	146 per 16 rounds	non-tight
200	206 per 18 rounds	non-tight
1600	this work	

- Inspired by similar efforts for
  - Noekeon [Nessie, 2000]
  - MD6 [Rivest et al., SHA-3 2008][Heilman, Ecrypt Hash 2011]

Outline

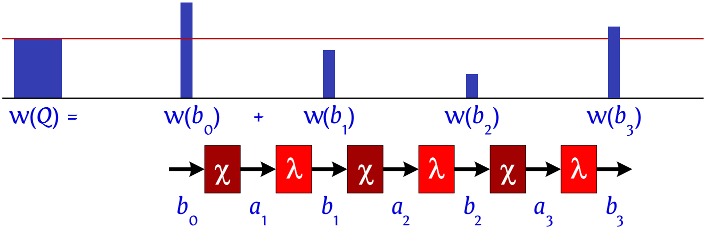
Trails in Keccak-f



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

Trails in KECCAK-f



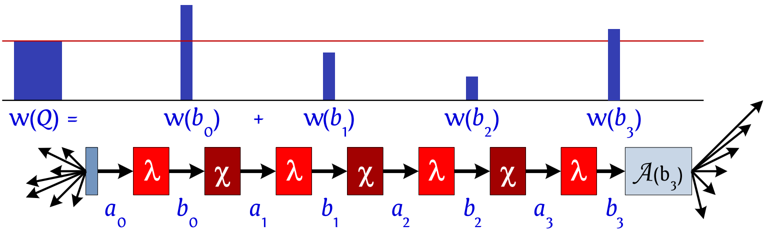
For KECCAK-f:

$\mathrm{w}(Q)$: # conditions on intermediate state bits

b: # degree of freedom

Trail generation techniques

- Given a trail, we can extend it:
  - forward: iterate a_{r+1} over $\mathcal{A}(b_r)$
  - backward: iterate b_{-1} over all differences χ^{-1}-compatible with $a_0 = \lambda^{-1}(b_0)$
- Tree search:
  - extension can be done recursively
  - pruning as soon as weight exceeds some limit

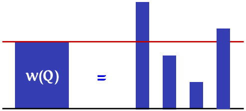


Outline

First-order approach

Fact

An r-round trail Q with $\mathrm{w}(Q) \leq T$ has at least one b_i with weight $\leq T/r$

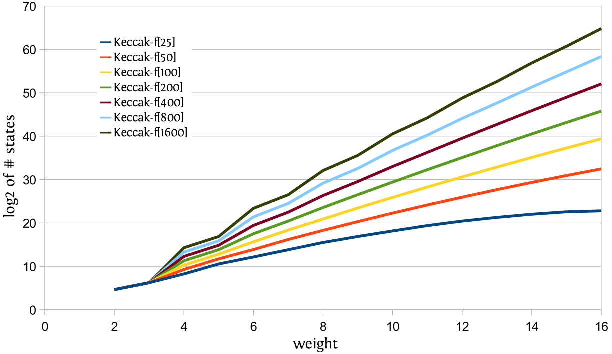


Generating trails up to weight T, first order approach

- Generate $\mathcal{V}_1 = \{b | \mathrm{w}(b) \leq t_{\text{avg}}\}$ with $t_{\text{avg}} = T/r$
- $\forall 0 \leq i < r$, iterate b_i over $\mathcal{V}_1$
  - extend forward up to b_{r-1}
  - extend backward down to b_0
  - prune as soon as weight exceeds T

Limits of first-order approach

$\mathcal{V}_1$ grows quickly with t_{avg} and KECCAK-f width:

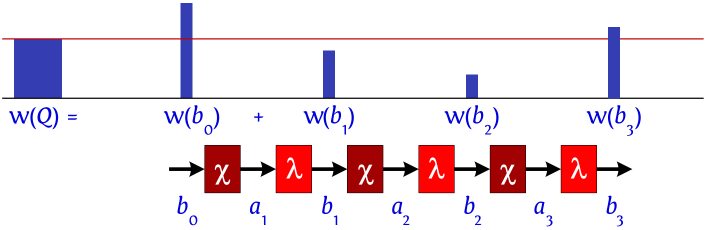


Definitions: minimum reverse weight and trail cores

- **Minimum reverse weight:**

$$\mathrm{w}^{\mathrm{rev}}(a) \triangleq \min_{b\,:\,a \in \mathcal{A}(b)} \mathrm{w}(b)$$

- Can be used to lower bound of set of trails
- Trail **core:** set of trails with $b_1, b_2, \ldots$ in common

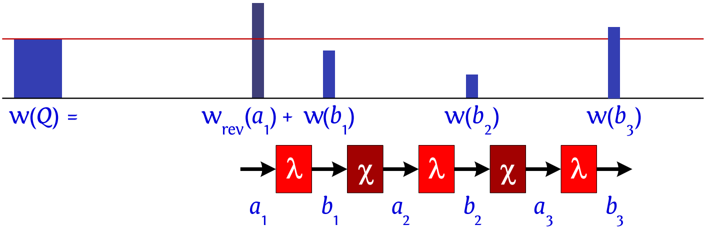


Definitions: minimum reverse weight and trail cores

- **Minimum reverse weight**:

$$\mathrm{w}^{\mathrm{rev}}(a) \triangleq \min_{b\,:\,a \in \mathcal{A}(b)} \mathrm{w}(b)$$

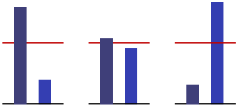
- Can be used to lower bound of set of trails
- Trail **core**: set of trails with $b_1, b_2, \ldots$ in common



Second-order approach

Observation

For most low-weight a, $b = \lambda(a)$ has high weight and vice versa

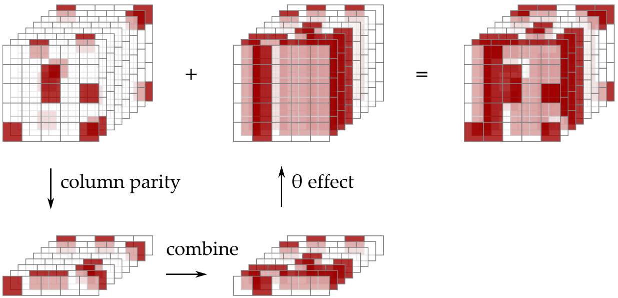


Generating trails up to weight T, second order approach

- Generate $\mathcal{V}_2 = \{b | b = \lambda(a) \text{ and } \mathrm{w}^{\mathrm{rev}}(a) + \mathrm{w}(b) \leq 2t_{\mathrm{avg}}\}$
- $\forall 0 \leq i < r$, iterate b_i over $\mathcal{V}_2$
  - extend forward up to b_{r-1}
  - extend backward down to b_0
  - prune as soon as weight exceeds T

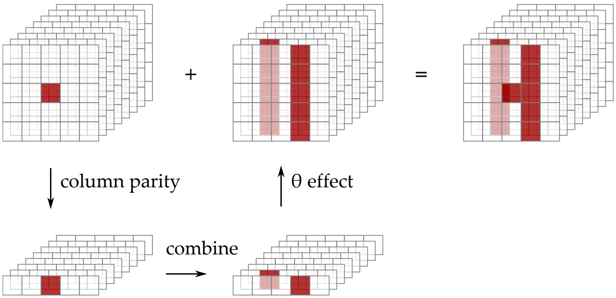
But how does the size of $\mathcal{V}_2$ behave with t_{avg}?

θ, the mixing layer



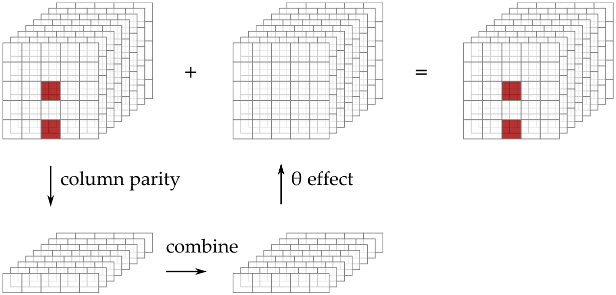
- Compute parity $c_{x,z}$ of each column
- Add to each cell the parities of two nearby columns

θ, the mixing layer



- Single-bit parity flips already 10 bits
- Other linear mapping ρ and π just move bits around

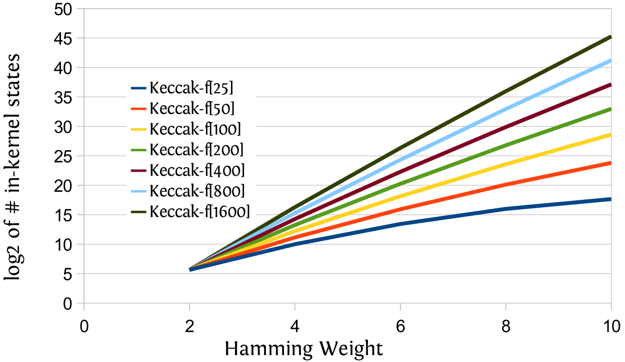
θ, the mixing layer



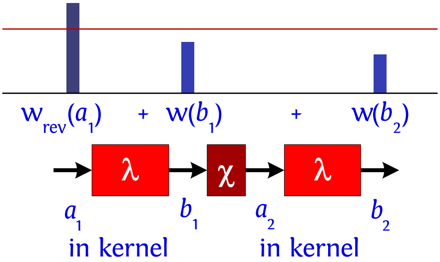
- Effect collapses if parity is zero
- The kernel

Limits of second-order approach

- $\mathcal{V}_2$ still grows quickly with t_{avg} and Keccak-f width
- Reason: $\mathcal{V}_2$ contains states in kernel

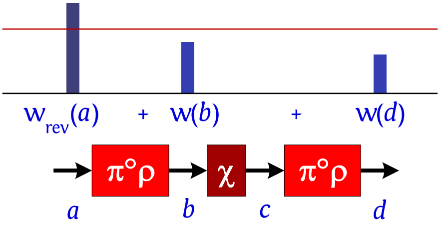


Third-order approach: dealing with the kernel



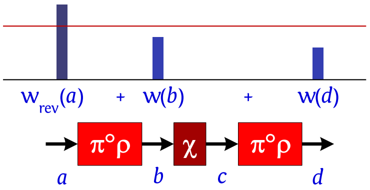
- $\mathcal{V}_3$: trail cores (b, d) with $\mathrm{w}^{\mathrm{rev}}(a) + \mathrm{w}(b) + \mathrm{w}(d) \leq 3t_{\mathrm{avg}}$
  - $a = \lambda^{-1}(b)$ is in the kernel
  - $c = \lambda^{-1}(d)$ is in the kernel
- Elements of $\mathcal{V}_3$ can then be extended as usual

Third-order approach: dealing with the kernel



- $\mathcal{V}_3$: trail cores (b, d) with $w^{rev}(a) + w(b) + w(d) \leq 3t_{avg}$
  - $a = \lambda^{-1}(b)$ is in the kernel
  - $c = \lambda^{-1}(d)$ is in the kernel
- Elements of $\mathcal{V}_3$ can then be extended as usual

Tame states

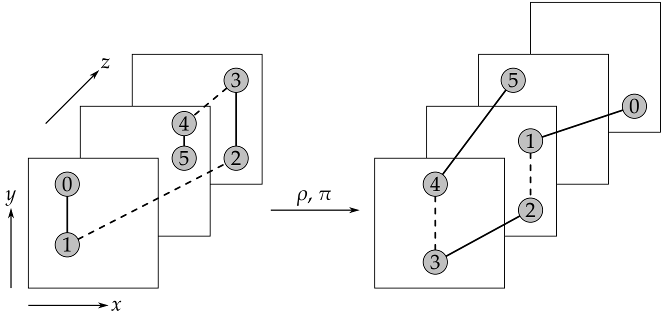


- **Tame state**: value of b that satisfies two conditions
  1. $a = \lambda^{-1}(b)$ is in the kernel
  2. Intersection of $\mathcal{A}(b)$ and kernel is not empty
- Second condition can be handled slice-by-slice:
  - orbital: two bits in the same column
  - knot: at least 3 active bits
- First condition: bits occur in pairs per column in a
  - Combined with orbitals these form chains between knots

Chains

Sequence of active bits p_i with:

- p_{2i} and p_{2i+1} are in same column in a
- p_{2i+1} and p_{2i} are in same column in b

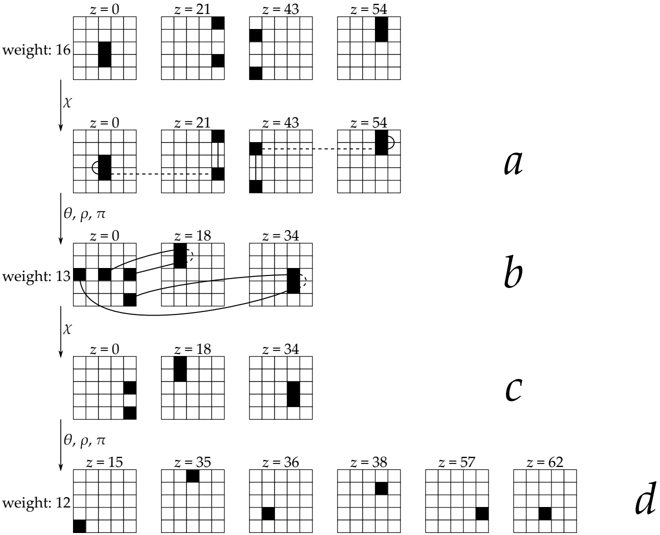


Third-order approach

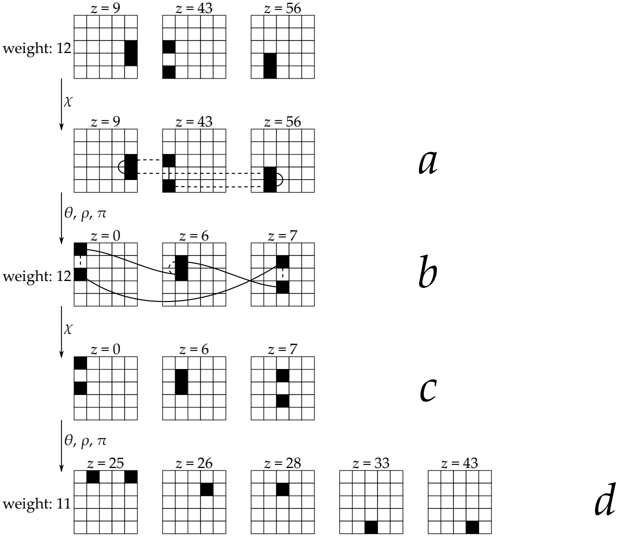
- We efficiently generate $\mathcal{V}_3$ using this representation
  - set of chains between knots
  - plus some circular chains: **vortices**
- Full coverage guaranteed by
  - monotonous weight prediction function
  - well-defined order of chains

Outline

An in-kernel 3-round trail with a single knot



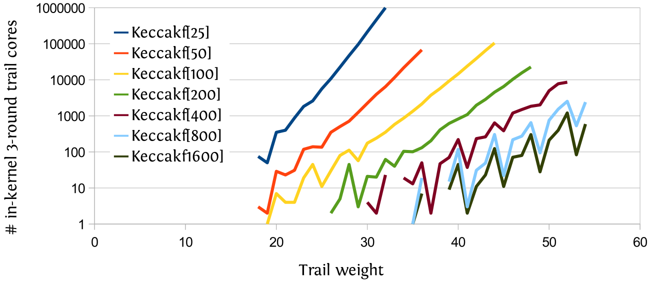
An in-kernel 3-round trail with a vortex



Outline

Conclusions

- Current bound for KECCAK-f[1600]:
  - scanned all 3-round trails up to weight 36
  - after extension: minimum weight 74 for 6-round trails
- Work in progress:
  - improving bounds by increasing t_{avg}
  - probabilistic evidence for absence of low-weight trails



Questions?

Thanks for your attention!

Q?

http://keccak.noekeon.org/