Alignment in crypto primitives

Joan Daemen[1]

Joint work with
Guido Bertoni[1], Michaël Peeters[2] and Gilles Van Assche[1]

[1]STMicroelectronics [2]NXP Semiconductors

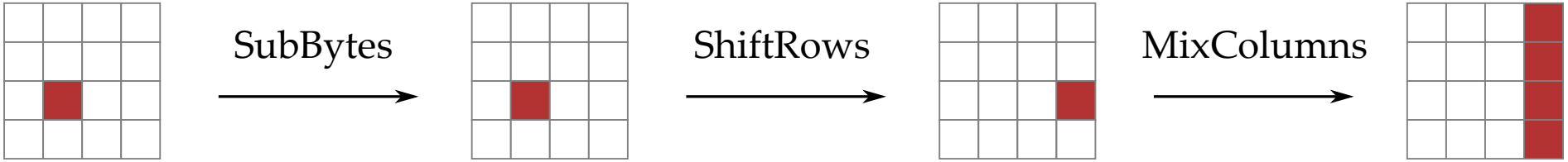
Crypto summer school 2014
Šibenik, Croatia, June 1-6, 2014

Outline

Outline

Difference propagation in RIJNDAEL: strong alignment

- Propagation of differences:
  - MixColumns, ShiftRows and AddRoundKey: 1-to-1
  - SubBytes: 1-to-N
    - state with x active bytes at input: $N = 126^x \approx 2^{7x}$
- Propagation of truncated differences (active/passive bytes)
  - SubBytes, ShiftRows and AddRoundKey: 1-to-1
  - MixColumns: 1-to-N
    - column with 1 active bytes at input: $N = 1$
    - column with 2 active bytes in input: $N = 5$
    - column with 3 active bytes in input: $N = 11$
    - column with 4 active bytes in input: $N = 15$

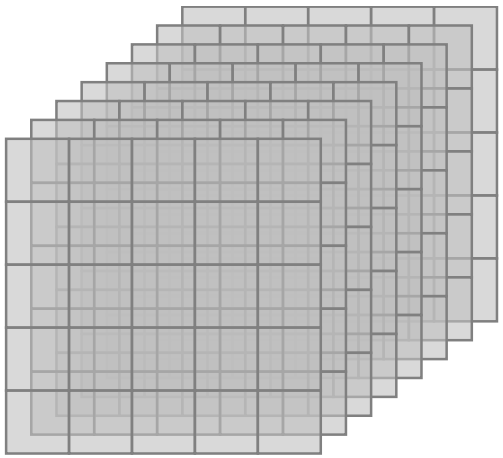


Alignment

- Property of round function
  - relative to partition of state in blocks
- **Strong alignment**
  - low uncertainty in propagation along block boundaries
  - e.g., Rijndael strongly aligned on byte boundaries
- Weak alignment
  - high uncertainty in propagation along block boundaries
  - e.g., Keccak weakly aligned on row boundaries…

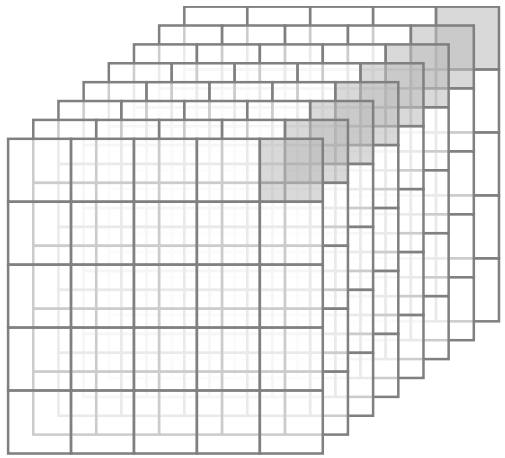
Outline

The state: an array of $5 \times 5 \times 2^\ell$ bits



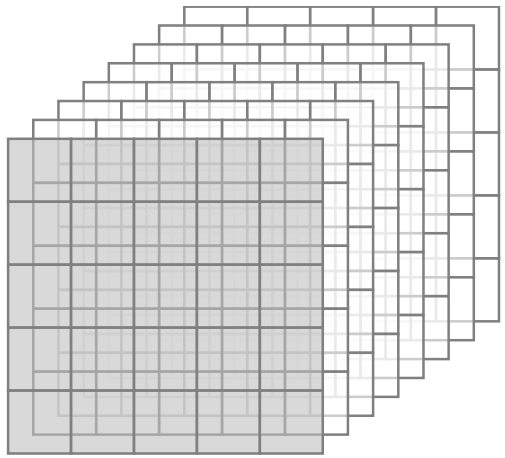
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

The state: an array of $5 \times 5 \times 2^\ell$ bits



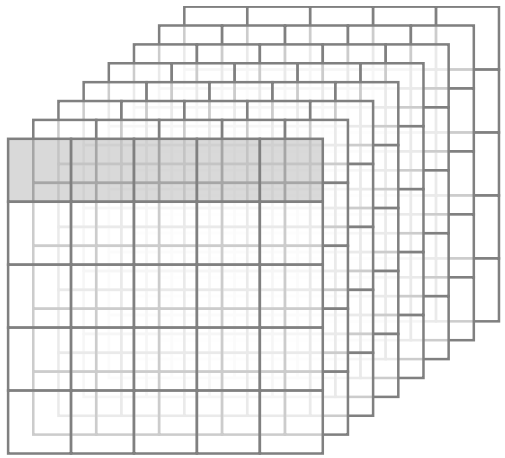
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

The state: an array of $5 \times 5 \times 2^\ell$ bits



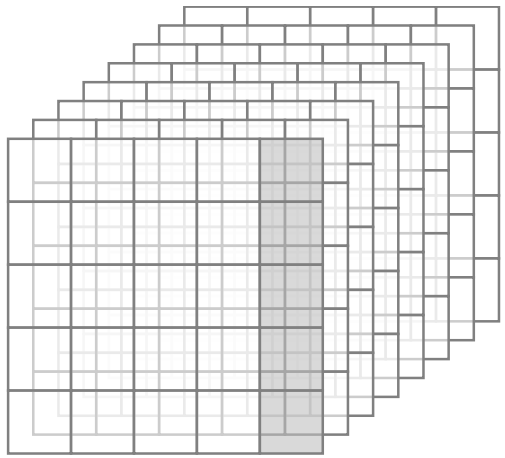
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

The state: an array of $5 \times 5 \times 2^\ell$ bits



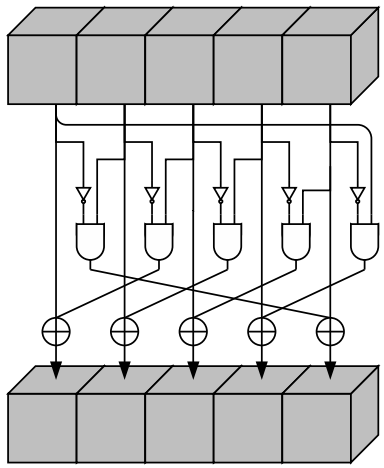
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

The state: an array of $5 \times 5 \times 2^\ell$ bits



- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

χ, the nonlinear mapping in Keccak-f

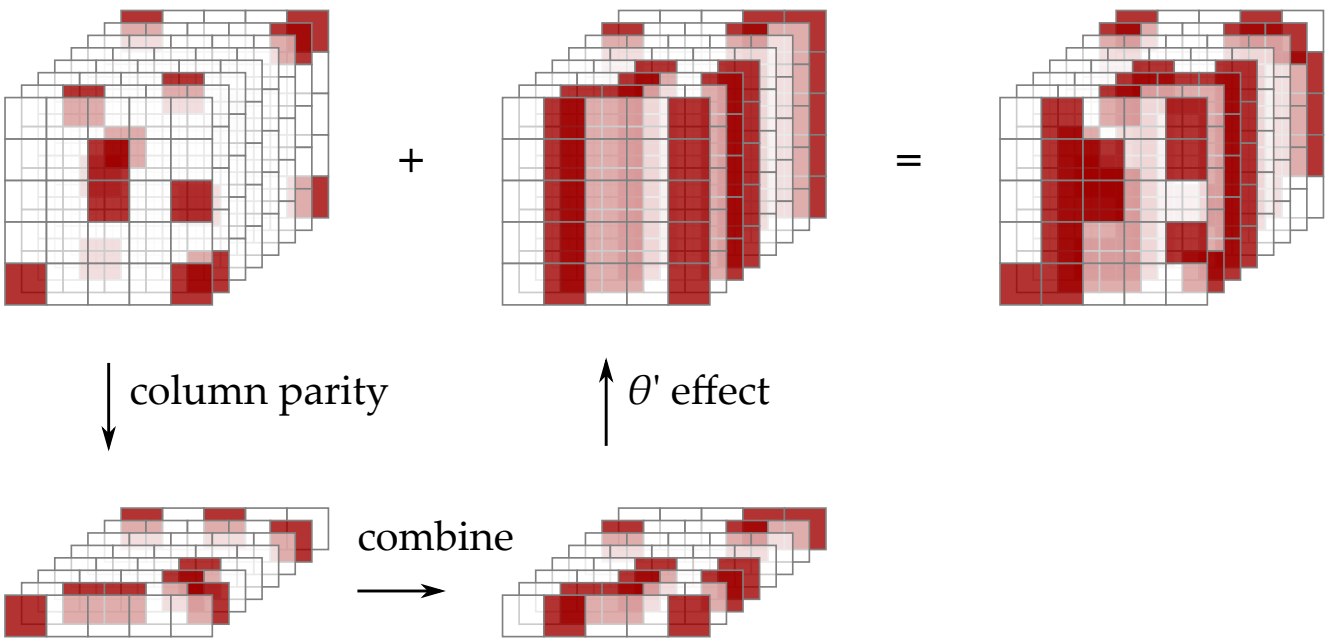


- "Flip bit if neighbors exhibit 01 pattern"
- Operates independently and in parallel on 5-bit rows
- Algebraic degree 2, inverse has degree 3

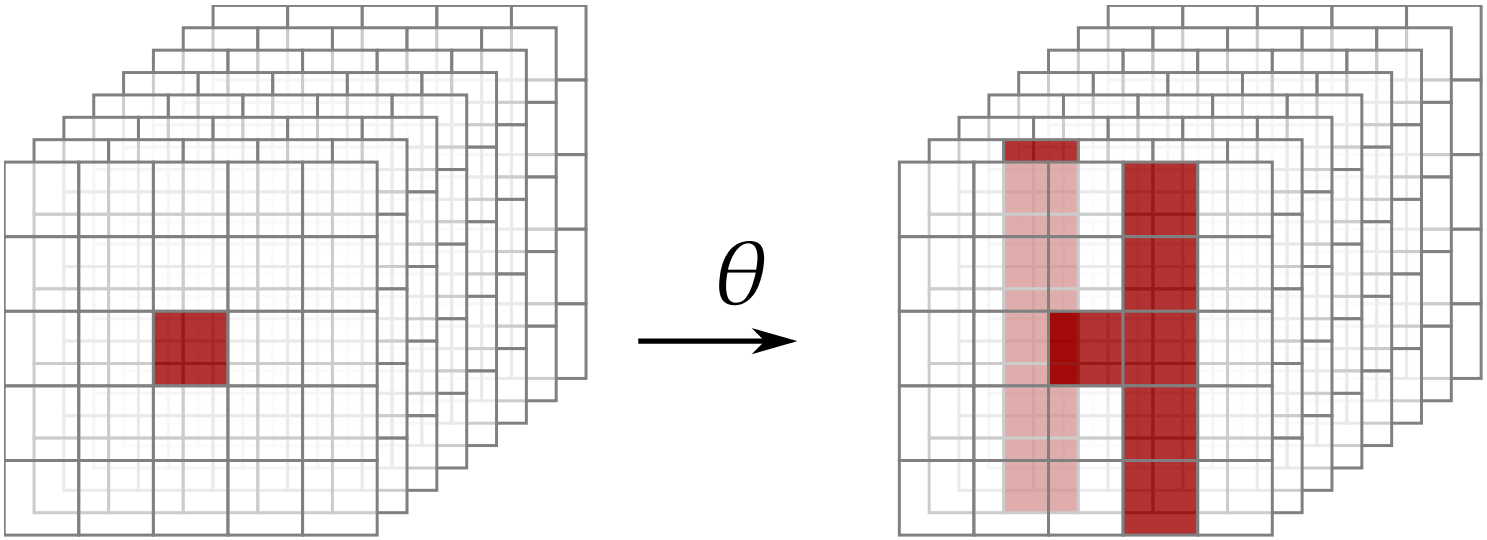
The mixing layer θ

- Compute parity $c_{x,z}$ of each column
- Add to each cell parity of neighboring columns:

$$b_{x,y,z} = a_{x,y,z} \oplus c_{x-1,z} \oplus c_{x+1,z-1}$$

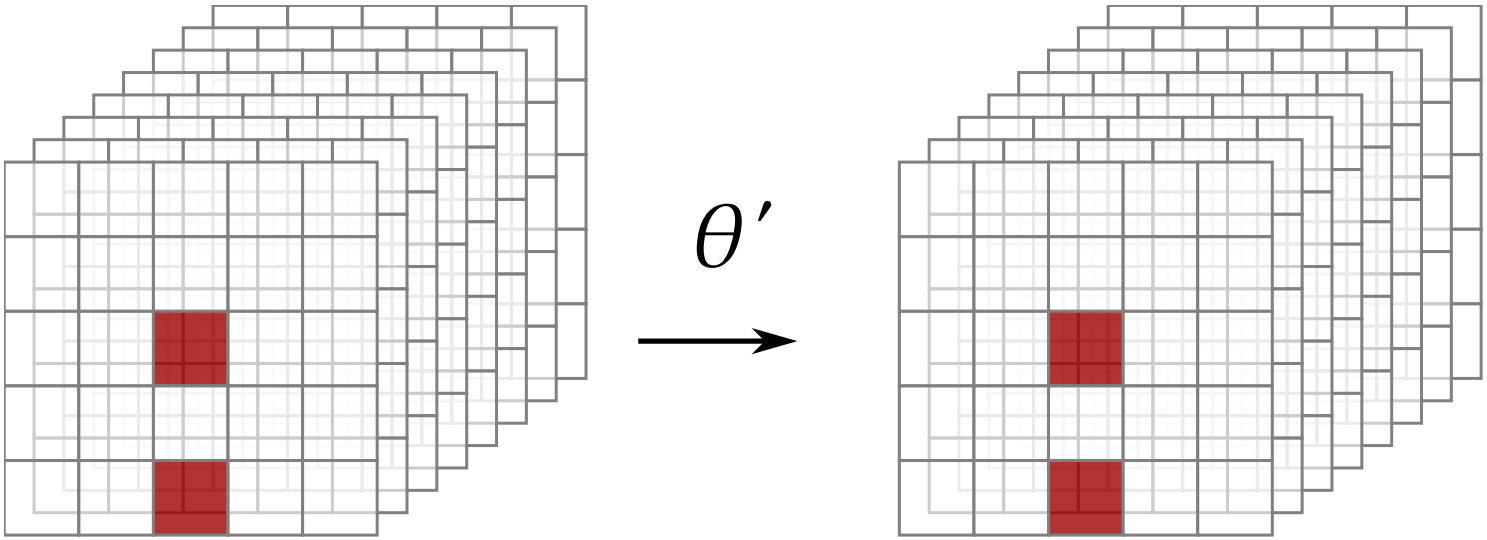


Difference propagation due to θ



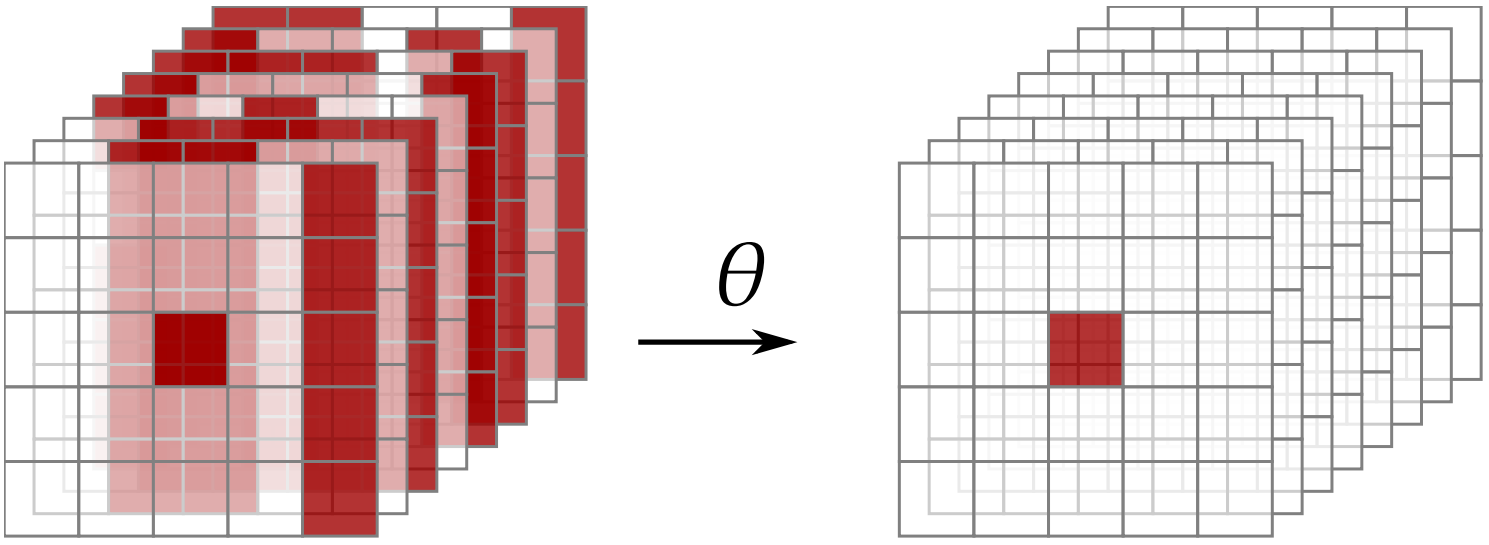
$$1 + \left(1 + y + y^2 + y^3 + y^4\right)\left(x + x^4 z\right) \left(\mathrm{mod}\ \left\langle 1 + x^5, 1 + y^5, 1 + z^w \right\rangle\right)$$

Difference propagation due to θ (kernel)



$$1 + \left(1 + y + y^2 + y^3 + y^4\right)\left(x + x^4 z\right) \left(\mathrm{mod}\ \left\langle 1 + x^5, 1 + y^5, 1 + z^w \right\rangle\right)$$

Inverse of θ is dense

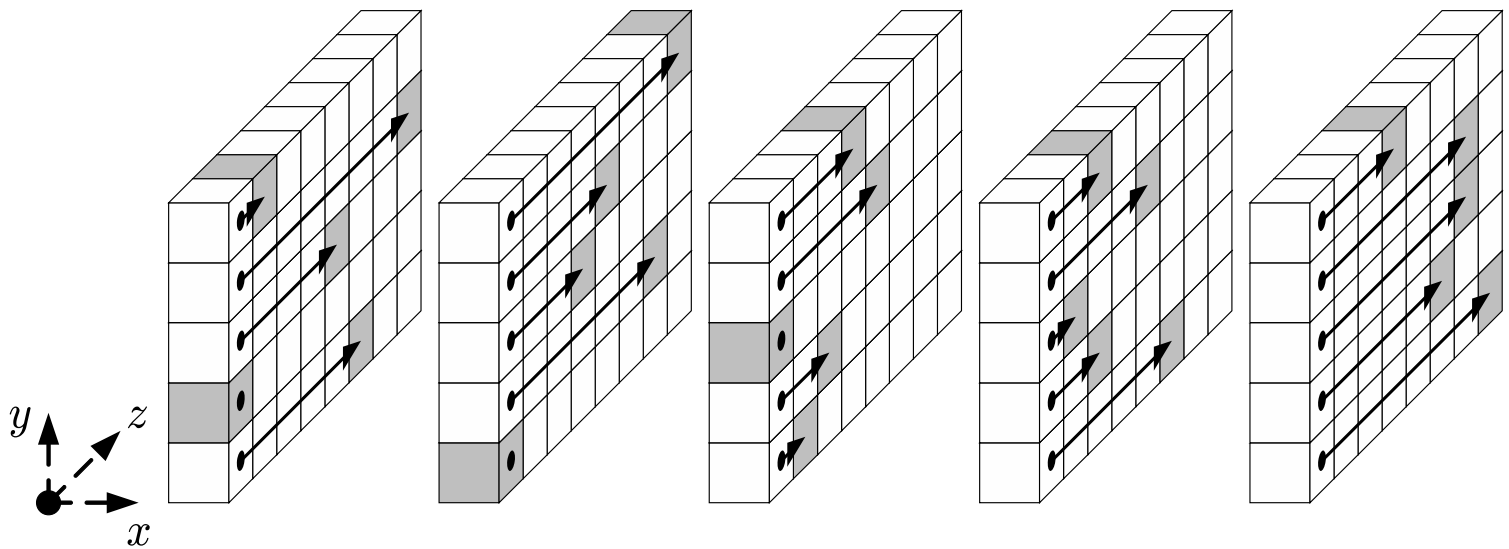


$$1 + \left(1 + y + y^2 + y^3 + y^4\right) \mathbf{Q},$$

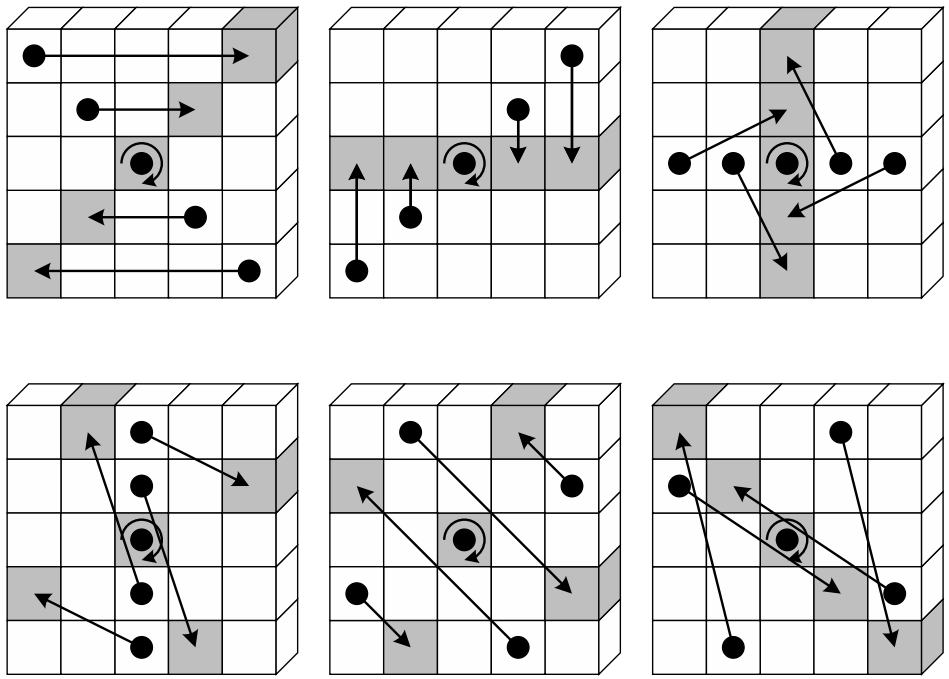
$$\text{with } \mathbf{Q} = 1 + \left(1 + x + x^4 z\right)^{-1} \bmod \left\langle 1 + x^5, 1 + z^w \right\rangle$$

ρ for inter-slice dispersion

- We need diffusion between the slices …
- ρ: cyclic shifts of lanes
- Offsets cycle through all values below 2^ℓ



π for disturbing horizontal/vertical alignment



$$a_{x,y} \leftarrow a_{x',y'} \text{ with } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} x' \\ y' \end{pmatrix}$$

Keccak-f summary

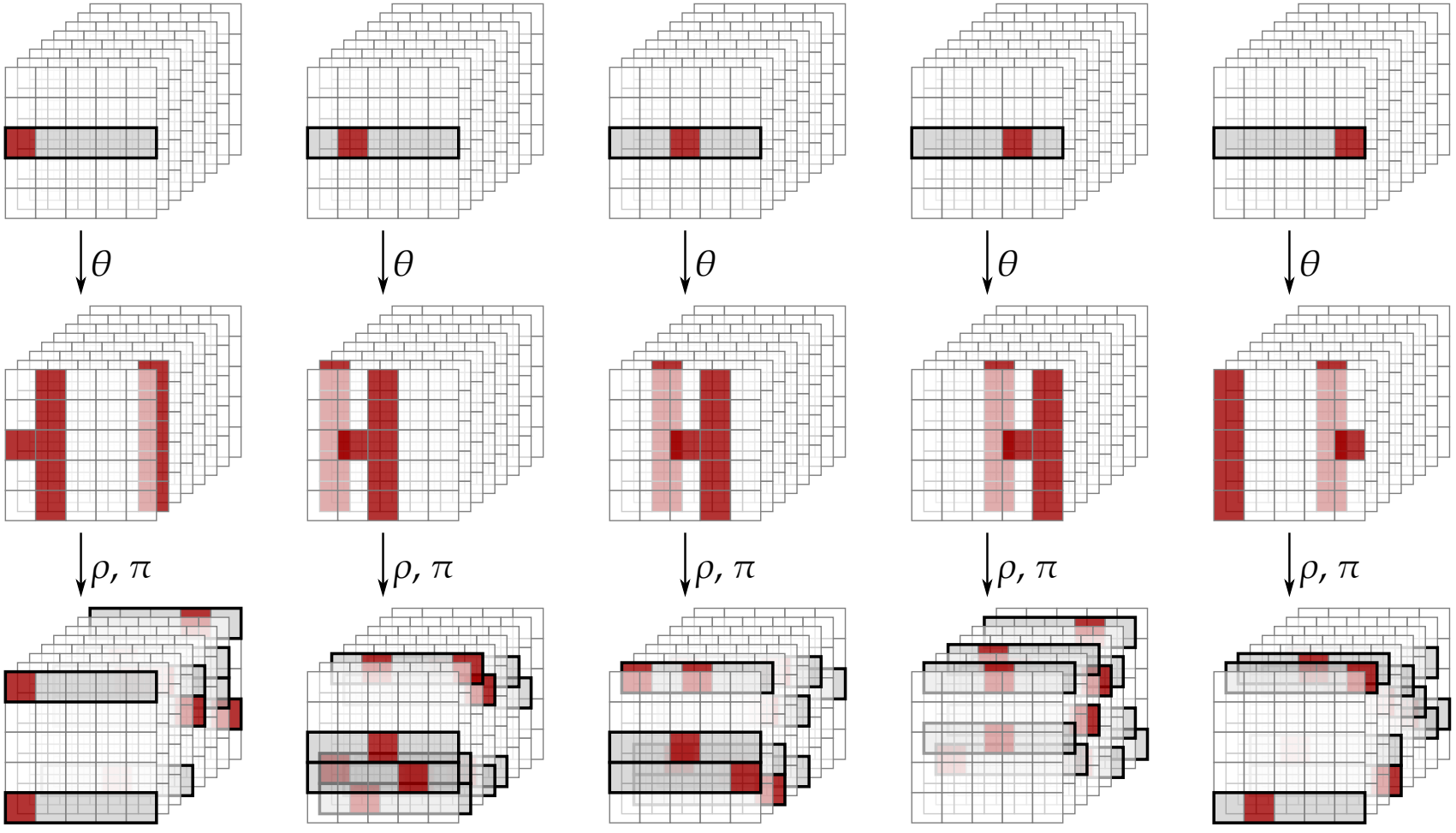
- Round function:
  - θ for diffusion
  - ρ for inter-slice dispersion
  - π for disturbing horizontal/vertical alignment
  - χ for non-linearity
  - ι to break symmetry

$$\mathsf{R} = \iota \circ \chi \circ \pi \circ \rho \circ \theta$$

- Number of rounds: $12 + 2\ell$
  - Keccak-$f[25]$ has 12 rounds
  - Keccak-$f[1600]$ has 24 rounds

Outline

Differential patterns



Attempt at quantifying alignment

For a given input activity pattern (specified in blocks)

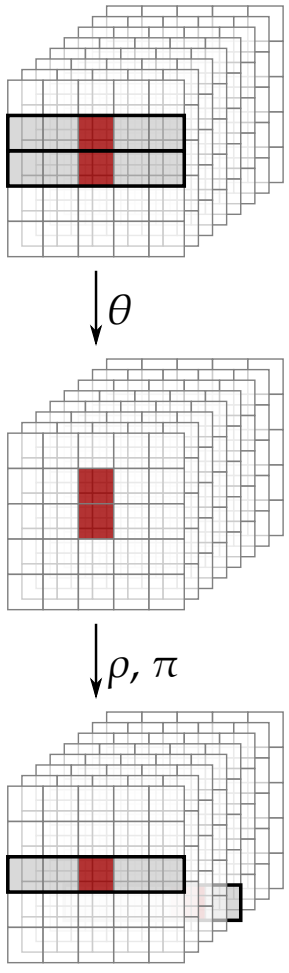
- N: number of possible different output activity patterns
  - e.g., MixColumns 1 active byte: $N = 1$ (4 active bytes)
  - e.g., MixColumns 4 active bytes: $N = 15$ (1-4 active bytes)
- $h = -\sum_z \Pr(z|A) \log_2 \Pr(z|A)$: "entropy"
  - e.g., MixColumns 4 active bytes: $h \approx 0$ (most often 4)
- $\overline{w}$: average number of active blocks
  - e.g., MixColumns 4 active bytes: $\overline{w} \approx 4$ (most often 4)

Row activity: typical results

Output row-activity for single-row differences in row $y = 0$ at round input:

2^ℓ	N	h	$\overline{w}$
1	1	0.00	5.00
2	11	1.97	9.35
4	26	4.60	15.54
8	31	4.95	19.22
16	31	4.95	23.09
32	31	4.95	25.29
64	31	4.95	25.54

Differential patterns (kernel)

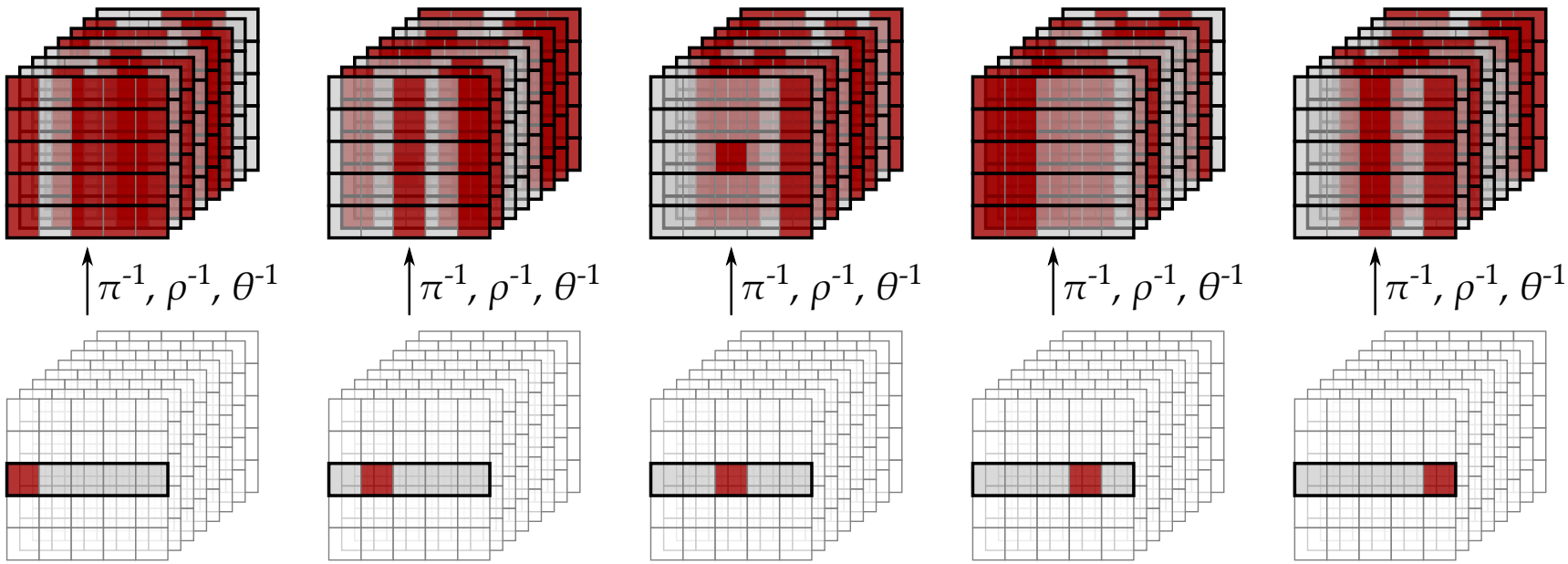


Slice activity: the results

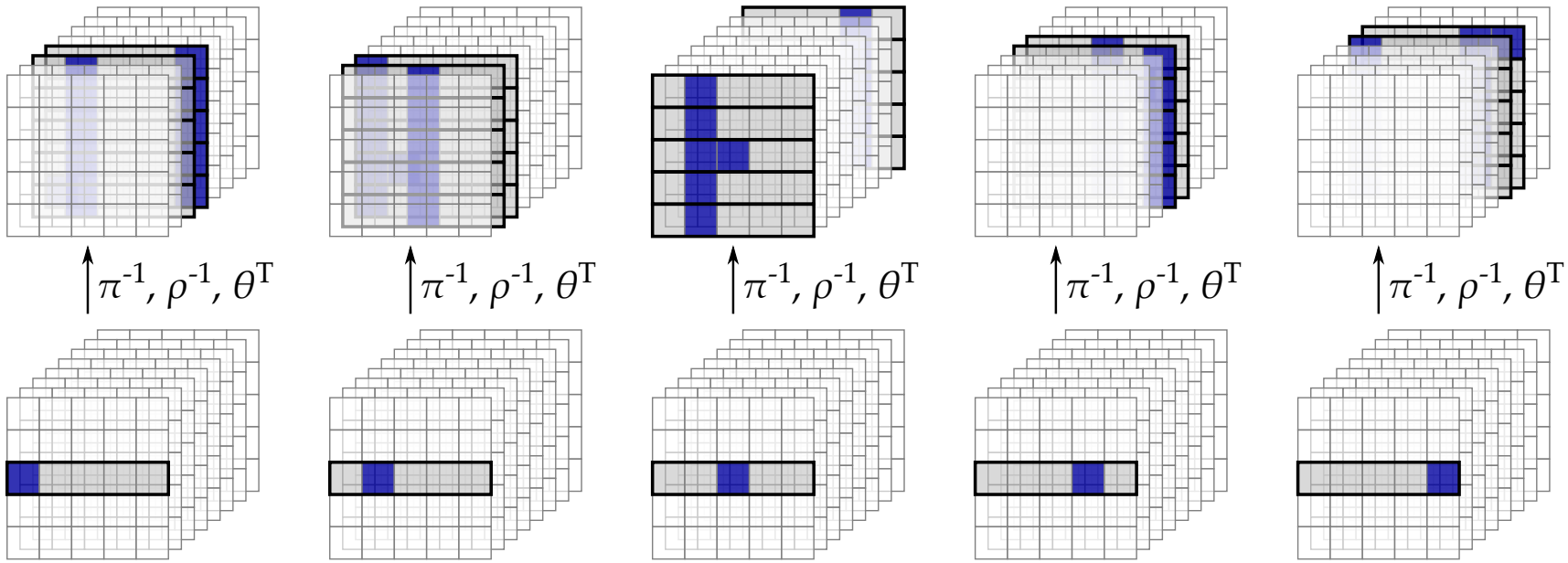
Output slice-activity for single-slice differences at round input:

2^ℓ	full single-slice set			in-kernel subset		
	N	h	$\overline{w}$	N	h	$\overline{w}$
1	1	0.00	1.00	1	0.00	1.00
2	3	0.0002	1.99	3	0.005	1.99
4	15	0.04	3.99	15	0.41	3.94
8	247	0.98	7.85	247	4.14	7.06
16	50622	7.86	13.93	49999	14.18	10.25
32	5611775	19.66	20.25	1048575	20.00	12.50
64	12599295	22.87	22.50	1048575	20.00	12.50

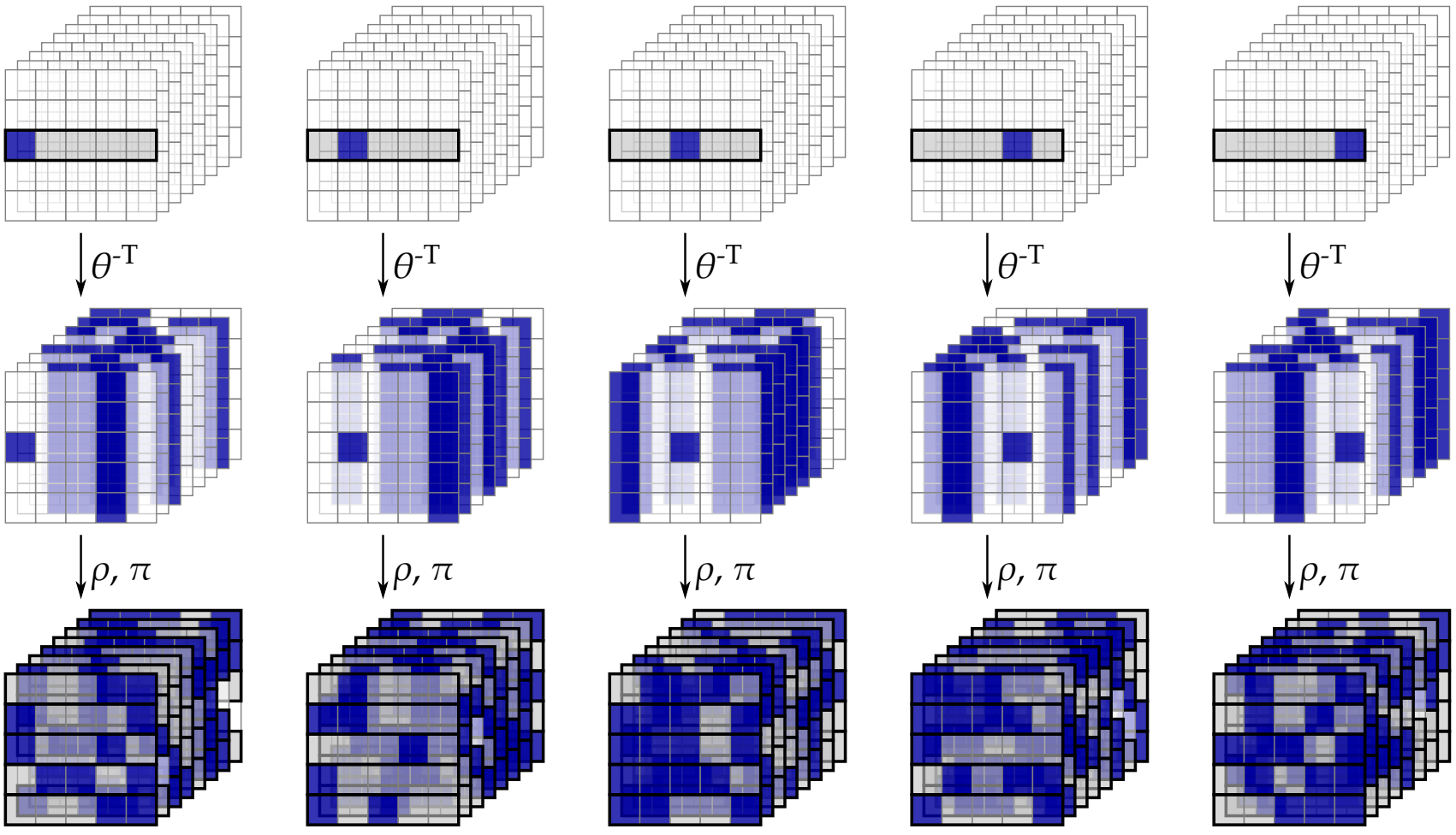
Differential patterns (backwards)



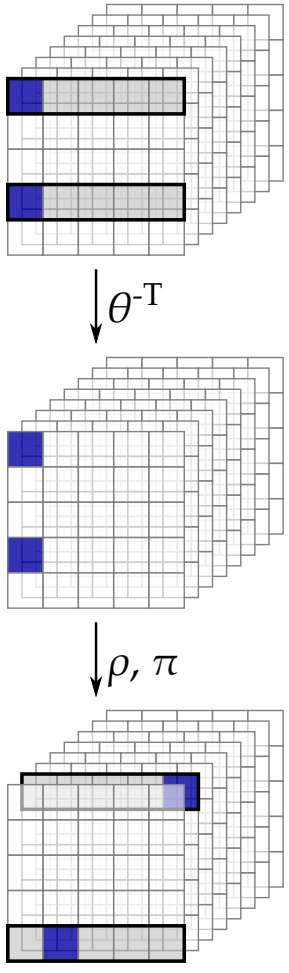
Linear patterns



Linear patterns (backwards)



Linear patterns (backwards, kernel)

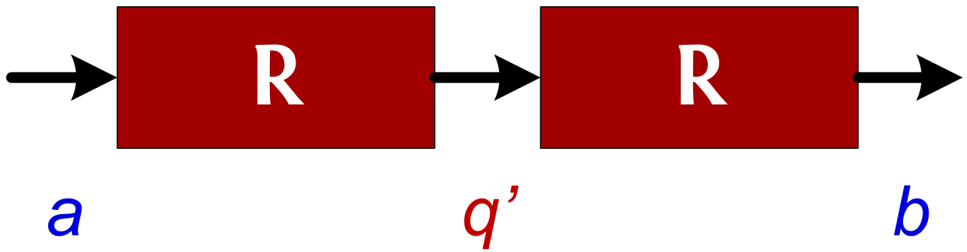


Outline

Strong versus weak alignment

- Benefits of strong alignment
  - propagation analysis easy to describe and understand
  - strong trail bounds with simple proofs, e.g. 4R AES: 25 S-boxes
  - allows efficient table-lookup implementations
- Benefits of weak alignment
  - low clustering of trails
  - hard to build truncated differential trails
  - rebound attacks become very expensive
- impacts how attacks work: integral, impossible, zero-correlation, ...

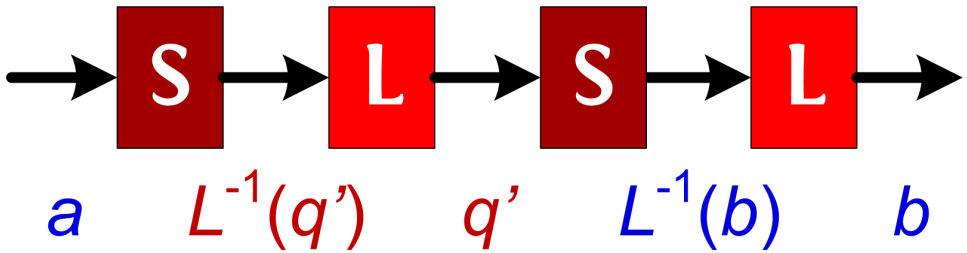
Clustering of differential trails



$$\mathrm{DP}_{2\mathrm{R}}(a,b) = \sum_{Q \in (a,b)} DP(Q) \approx \sum_{q'} \mathrm{DP}_{\mathrm{R}}(a,q')\mathrm{DP}_{\mathrm{R}}(q',b)$$

- Necessary conditions for a trail Q to contribute to (a,b):
  - a and q have same S-box activity pattern
  - b' and $L(q)$ have same S-box activity pattern
- Relevance of alignment of L along S-box boundaries:
  - strong alignment: $L(q)$ has low variety in activity pattern
  - weak alignment: $L(q)$ has wide variety in activity pattern
- Similar arguments apply for correlations and linear trails

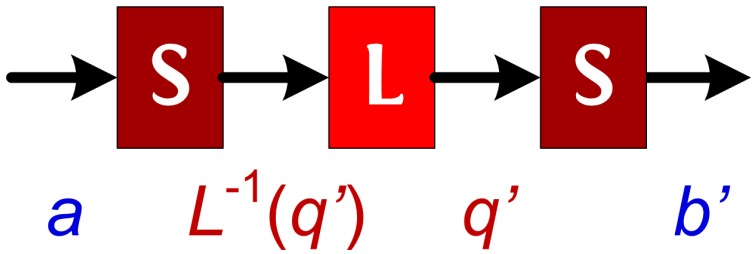
Clustering of differential trails



$$\mathrm{DP}_{2\mathrm{R}}(a,b) = \sum_{Q \in (a,b)} DP(Q) \approx \sum_{q'} \mathrm{DP}_{\mathrm{R}}(a,q')\mathrm{DP}_{\mathrm{R}}(q',b)$$

- Necessary conditions for a trail Q to contribute to (a, b):
  - a and q have same S-box activity pattern
  - b' and $L(q)$ have same S-box activity pattern
- Relevance of alignment of L along S-box boundaries:
  - strong alignment: $L(q)$ has low variety in activity pattern
  - weak alignment: $L(q)$ has wide variety in activity pattern
- Similar arguments apply for correlations and linear trails

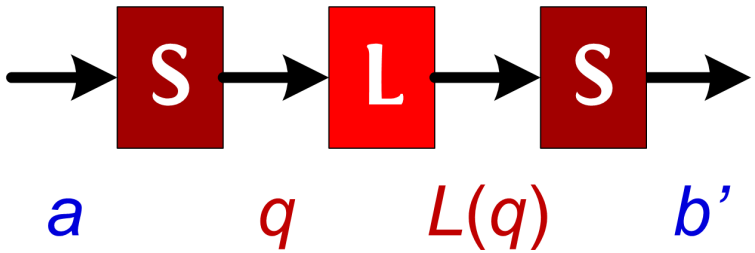
Clustering of differential trails



$$\mathrm{DP}_{2\mathrm{R}}(a,b) = \sum_{Q \in (a,b)} DP(Q) \approx \sum_{q'} \mathrm{DP}_{\mathrm{R}}(a,q')\mathrm{DP}_{\mathrm{R}}(q',b)$$

- Necessary conditions for a trail Q to contribute to (a,b):
  - a and q have same S-box activity pattern
  - b' and $L(q)$ have same S-box activity pattern
- Relevance of alignment of L along S-box boundaries:
  - strong alignment: $L(q)$ has low variety in activity pattern
  - weak alignment: $L(q)$ has wide variety in activity pattern
- Similar arguments apply for correlations and linear trails

Clustering of differential trails



$$\mathrm{DP}_{2R}(a,b) = \sum_{Q \in (a,b)} DP(Q) \approx \sum_{q} \mathrm{DP}_S(a,q)\,\mathrm{DP}_S(L(q),b')$$

- Necessary conditions for a trail Q to contribute to (a, b):
  - a and q have same S-box activity pattern
  - b' and $L(q)$ have same S-box activity pattern
- Relevance of alignment of L along S-box boundaries:
  - strong alignment: $L(q)$ has low variety in activity pattern
  - weak alignment: $L(q)$ has wide variety in activity pattern
- Similar arguments apply for correlations and linear trails

Truncated differentials and rebound attacks

- Weak alignment means trails tend to diverge
  - low clustering of differential trails
  - hard to construct a truncated differential trail
- Open question for Keccak
  - generalize truncation other than on block boundaries?
- Rebound attack typically requires truncated trails
  - it can also be done exploiting saturation
    [Duc et al., Unaligned Rebound Attack: Appl. to Keccak, FSE 2012]
  - still rather expensive

Outline

Conclusions

- Alignment is a relevant aspect in design and cryptanalysis
- Rijndael has strong byte-alignment
- Keccak-*f* has weak row-alignment, modulo saturation
- Alignment of other designs, e.g. ARX?
- Interested? Start with:
  - [Keccak team, On alignment in Keccak]
  - [Daemen and Rijmen, Understanding two-round AES differentials]

Thanks for your attention!