Designing the permutation KECCAK-*f*

Our mission

To design a permutation called KECCAK-*f* that cannot be distinguished from a random permutation.

- Like a block cipher
  - sequence of identical rounds
  - round function that is nonlinear and has good diffusion
- ...but not quite
  - no need for key schedule
  - round constants instead of round keys
  - inverse permutation need not be efficient

Criteria for a strong permutation

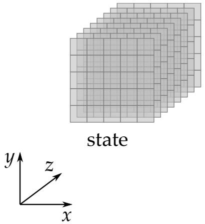
- Classical LC/DC criteria
  - Absence of large differential propagation probabilities
  - Absence of large input-output correlations
- Infeasibility of the CICO problem
  - Constrained Input Constrained Output
  - *Given partial input and partial output, find missing parts*
- Immunity to
  - Integral cryptanalysis
  - Algebraic attacks
  - Slide and symmetry-exploiting attacks
  - ...

KECCAK

- Instantiation of a *sponge function*
- the permutation KECCAK-f
  - 7 permutations: $b \in \{25, 50, 100, 200, 400, 800, 1600\}$
- Security-speed trade-offs using the same permutation, e.g.,
  - SHA-3 instance: $r = 1088$ and $c = 512$
    - permutation width: 1600
    - security strength 256: post-quantum sufficient
  - Lightweight instance: $r = 40$ and $c = 160$
    - permutation width: 200
    - security strength 80: same as SHA-1

KECCAK-f: the permutations in KECCAK

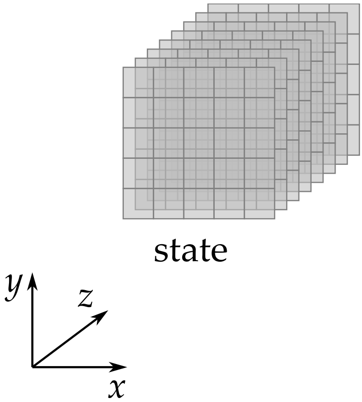
Operates on 3D state:



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

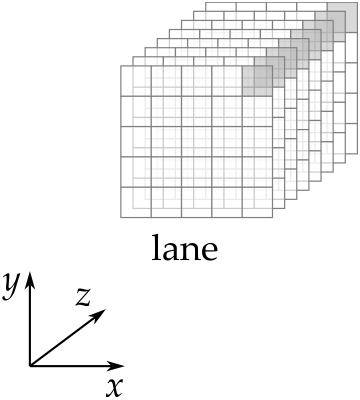
- Round function R with 5 steps:
  - θ: mixing layer
  - ρ: bit transposition
  - π: bit transposition
  - χ: non-linear layer
  - ι: round constants
- $\#$ rounds: $12 + 2\ell$ for $b = 2^\ell 25$
  - 12 rounds in KECCAK-$f[25]$
  - 24 rounds in KECCAK-$f[1600]$

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



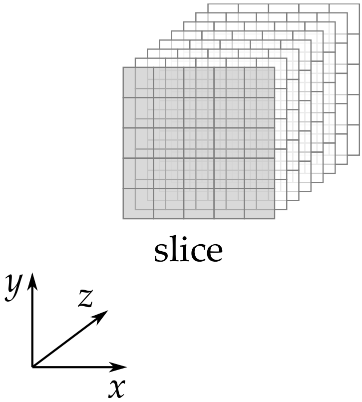
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

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



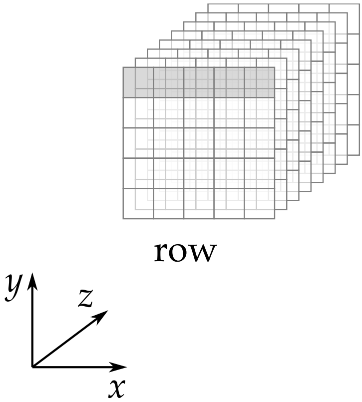
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

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



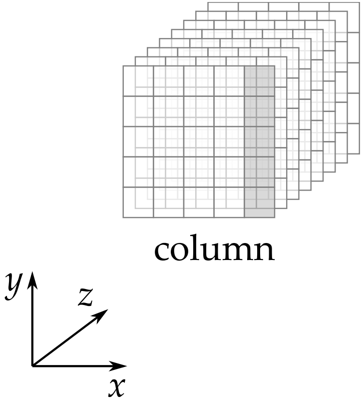
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

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



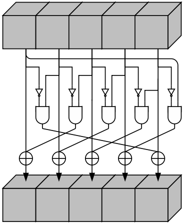
- 5×5 lanes, each containing 2^ℓ bits (1, 2, 4, 8, 16, 32 or 64)
- (5×5)-bit slices, 2^ℓ of them

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

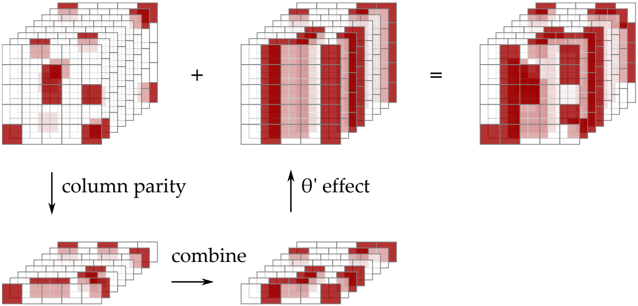


- "Flip bit if neighbors exhibit 01 pattern"
- Operates independently and in parallel on 5-bit rows
- Algebraic degree 2, inverse has degree 3
- LC/DC propagation properties easy to describe and analyze

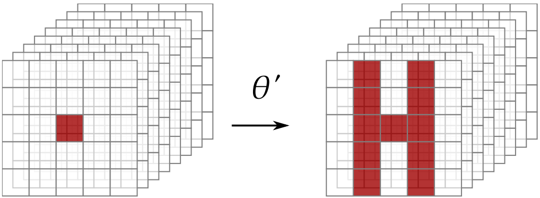
θ', a first attempt at mixing bits

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

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



Diffusion of θ'

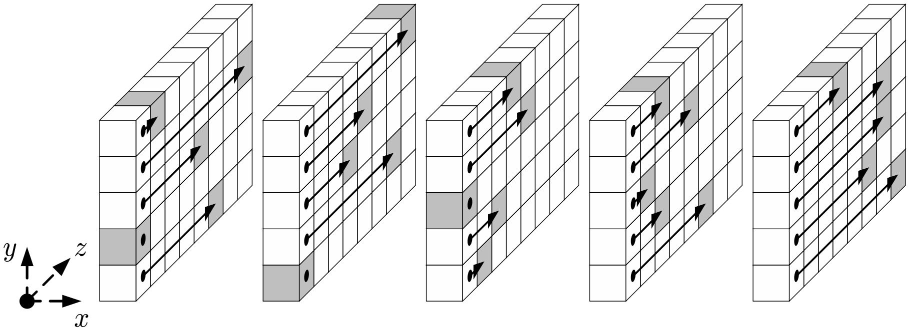


ρ for inter-slice dispersion

- We need diffusion between the slices ...
- ρ: cyclic shifts of lanes with offsets

$$i(i+1)/2 \bmod 2^{\ell}$$

- Offsets cycle through all values below 2^{ℓ}

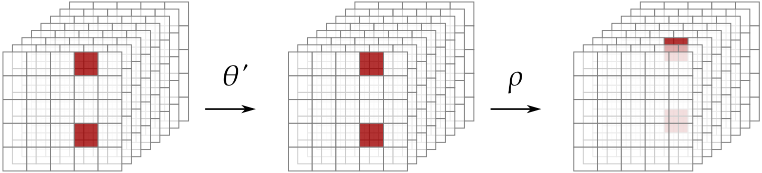


ι to break symmetry

- XOR of round-dependent constant to lane in origin
- Without ι, the round mapping would be symmetric
  - invariant to translation in the z-direction
- Without ι, all rounds would be the same
  - susceptibility to *slide* attacks
  - defective cycle structure
- Without ι, we get simple fixed points (000 and 111)

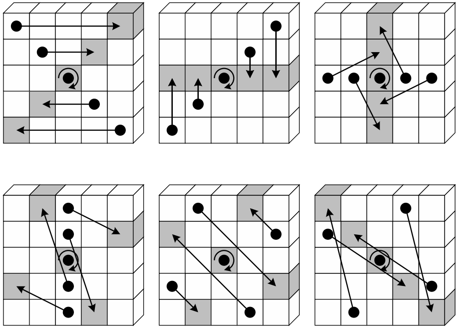
A first attempt at KECCAK-f

- Round function: $\mathrm{R} = \iota \circ \rho \circ \theta' \circ \chi$
- Problem: low-weight periodic trails by chaining:



  - χ: may propagate unchanged
  - θ': propagates unchanged, because all column parities are 0
  - ρ: in general moves active bits to different slices ...
  - ...but not always

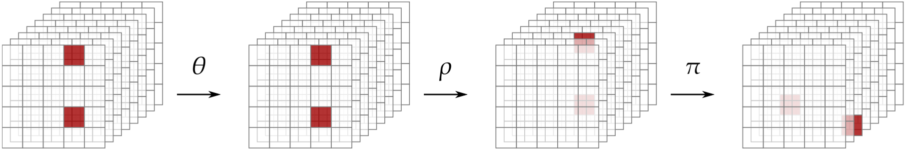
π for disturbing horizontal/vertical alignment



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

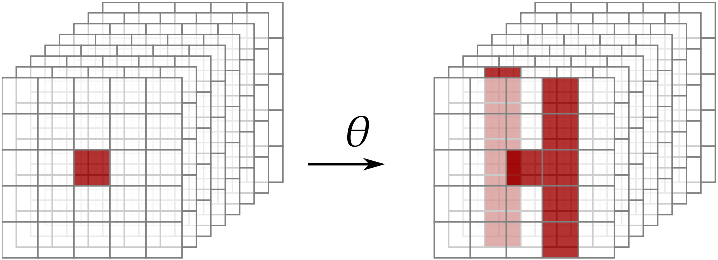
A second attempt at KECCAK-f

- Round function: $\mathrm{R} = \iota \circ \pi \circ \rho \circ \theta' \circ \chi$
- Solves problem encountered before:

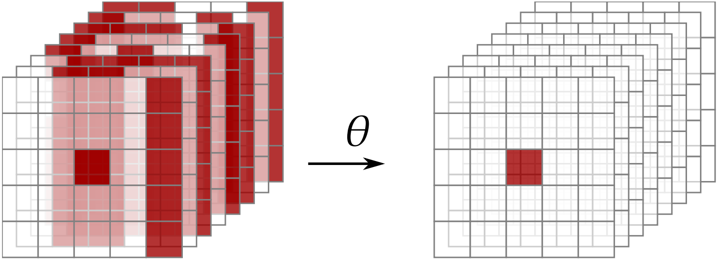


- π moves bits in same column to different columns!

Tweaking θ' to θ



Inverse of θ



- Diffusion from single-bit output to input very high
- Increases resistance against LC/DC and algebraic attacks

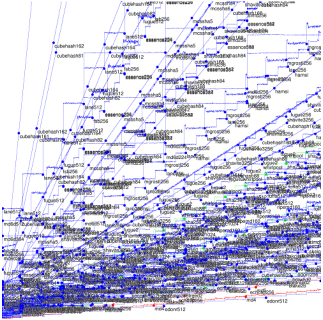
KECCAK-f summary

- Round function:

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

- Number of rounds: $12 + 2\ell$
  - KECCAK-$f[25]$ has 12 rounds
  - KECCAK-$f[1600]$ has 24 rounds
- Efficiency
  - high level of parallellism
  - flexibility: bit-interleaving
  - software: competitive on wide range of CPU
  - dedicated hardware: very competitive
  - suited for protection against side-channel attack

Performance in software



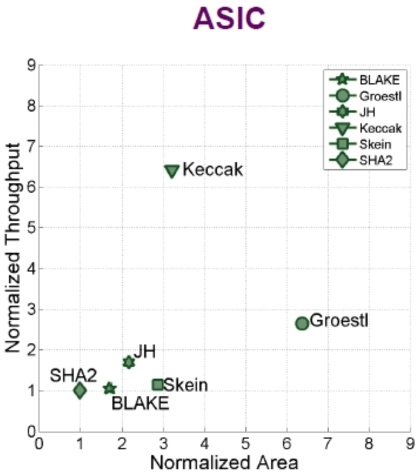
- Faster than SHA-2 on all modern PC
- KECCAKTREE faster than MD5 on some platforms

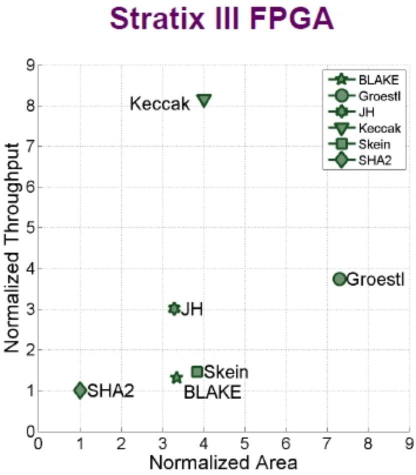
C/b	Algo	Strength
4.79	keccakc256treed2	128
4.98	md5	< 64
5.89	keccakc512treed2	256
6.09	sha1	< 80
8.25	keccakc256	128
10.02	keccakc512	256
13.73	sha512	256
21.66	sha256	128

[eBASH, hydra6, http://bench.cr.yp.to/]

Efficient and flexible in hardware

From Kris Gaj's presentation at SHA-3, Washington 2012:





Our analysis underlying the design of KECCAK-f

- Presence of large input-output correlations
- Ability to control propagation of differences
  - Differential/linear trail analysis
  - Lower bounds for trail weights
  - Alignment and trail clustering
  - This shaped θ, π and ρ
- Algebraic properties
  - Distribution of $\#$ terms of certain degrees
  - Ability of solving certain problems (CICO) algebraically
  - Zero-sum distinguishers (third party)
  - This determined the number of rounds
- Analysis of symmetry properties: this shaped ι
- See [KECCAK reference], [Ecrypt II Hash 2011], [FSE 2012]

Third-party cryptanalysis of KECCAK

Distinguishers on KECCAK-f[1600]

Rounds	Work	
3	low	CICO problem [Aumasson, Khovratovich, 2009]
4	low	cube testers [Aumasson, Khovratovich, 2009]
8	2^{491}	unaligned rebound [Duc, Guo, Peyrin, Wei, FSE 2012]
24	2^{1574}	zero-sum [Duan, Lai, ePrint 2011] [Boura, Canteaut, De Cannière, FSE 2011]

Academic-complexity attacks on KECCAK

- 6-8 rounds: second preimage [Bernstein, 2010]
  - *slightly faster* than exhaustive search, but huge memory
- attacks taking advantage of symmetry
  - 4-round pre-images [Morawiecki, Pieprzyk, Srebrny, FSE 2013]
  - 5-rounds collisions [Dinur, Dunkelman, Shamir, FSE 2013]

Third-party cryptanalysis of KECCAK

Practical-complexity attacks on KECCAK

Rounds	
2	preimages and collisions [Morawiecki, CC]
2	collisions [Duc, Guo, Peyrin, Wei, FSE 2012 and CC]
3	40-bit preimage [Morawiecki, Srebrny, 2010]
3	near collisions [Naya-Plasencia, Röck, Meier, Indocrypt 2011]
4	key recovery [Lathrop, 2009]
4	distinguishers [Naya-Plasencia, Röck, Meier, Indocrypt 2011]
4	collisions [Dinur, Dunkelman, Shamir, FSE 2012 and CC]
5	near-collisions [Dinur, Dunkelman, Shamir, FSE 2012]

CC = Crunchy Crypto Collision and Preimage Contest

Observations from third-party cryptanalysis

- Extending distinguishers of KECCAK-*f* to KECCAK is not easy
- Effect of **alignment** on differential/linear propagation
  - **Strong**: low uncertainty in prop. along block boundaries
  - Weak: high uncertainty in prop. along block boundaries
  - Weak alignment in KECCAK-*f* limits feasibility of rebound attacks
- Effect of the **inverse** of the mixing layer θ
  - θ^{-1} has very high average diffusion
  - Limits the construction of low-weight trails over more than a few rounds