Practical Complexity Cube Attacks on Round-Reduced Keccak Sponge Function

Itai Dinur[1], Paweł Morawiecki[2,3], Josef Pieprzyk[4], Marian Srebrny[2,3], and Michał Straus[3]

[1]Computer Science Department,École normale supérieure, France

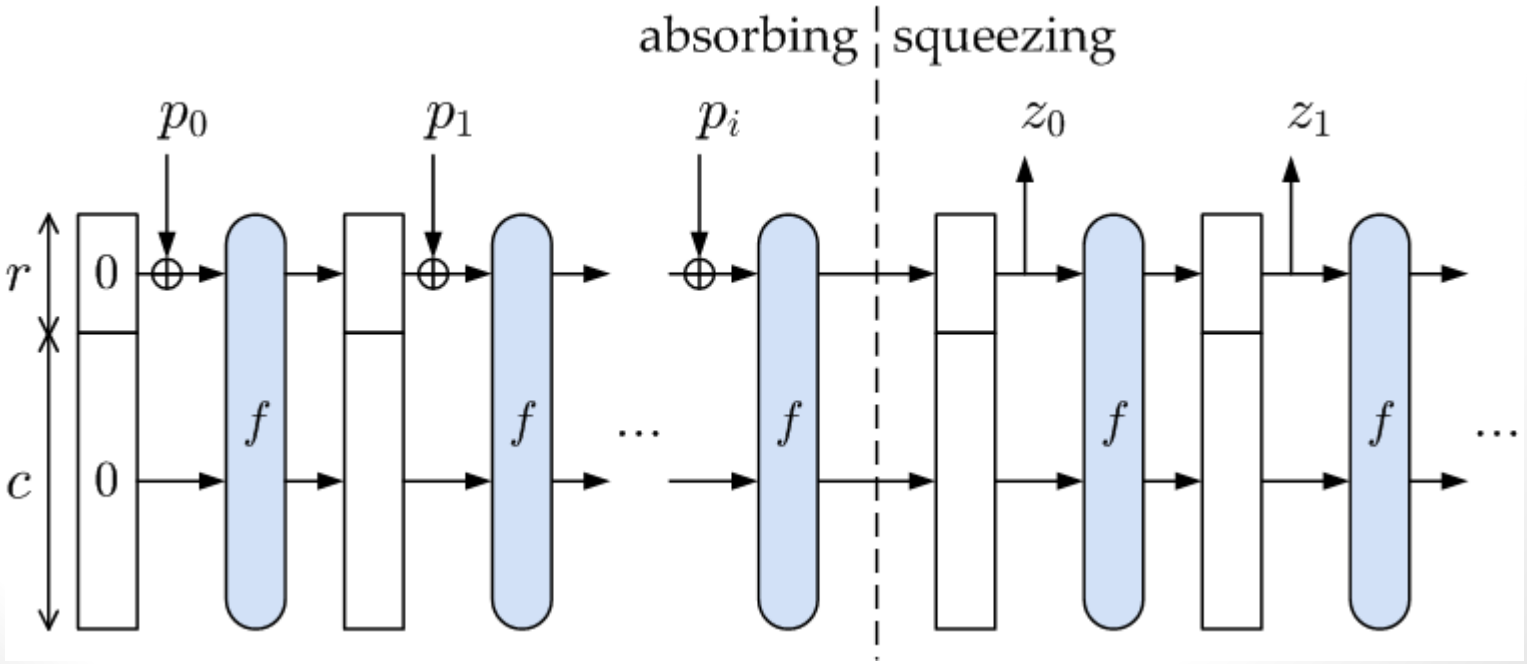
[2]Institute of Computer Science, Polish Academy of Sciences,Poland

[3]Section of Informatics, University of Commerce, Kielce, Poland

[4]Queensland University of Technology, Brisbane, Australia

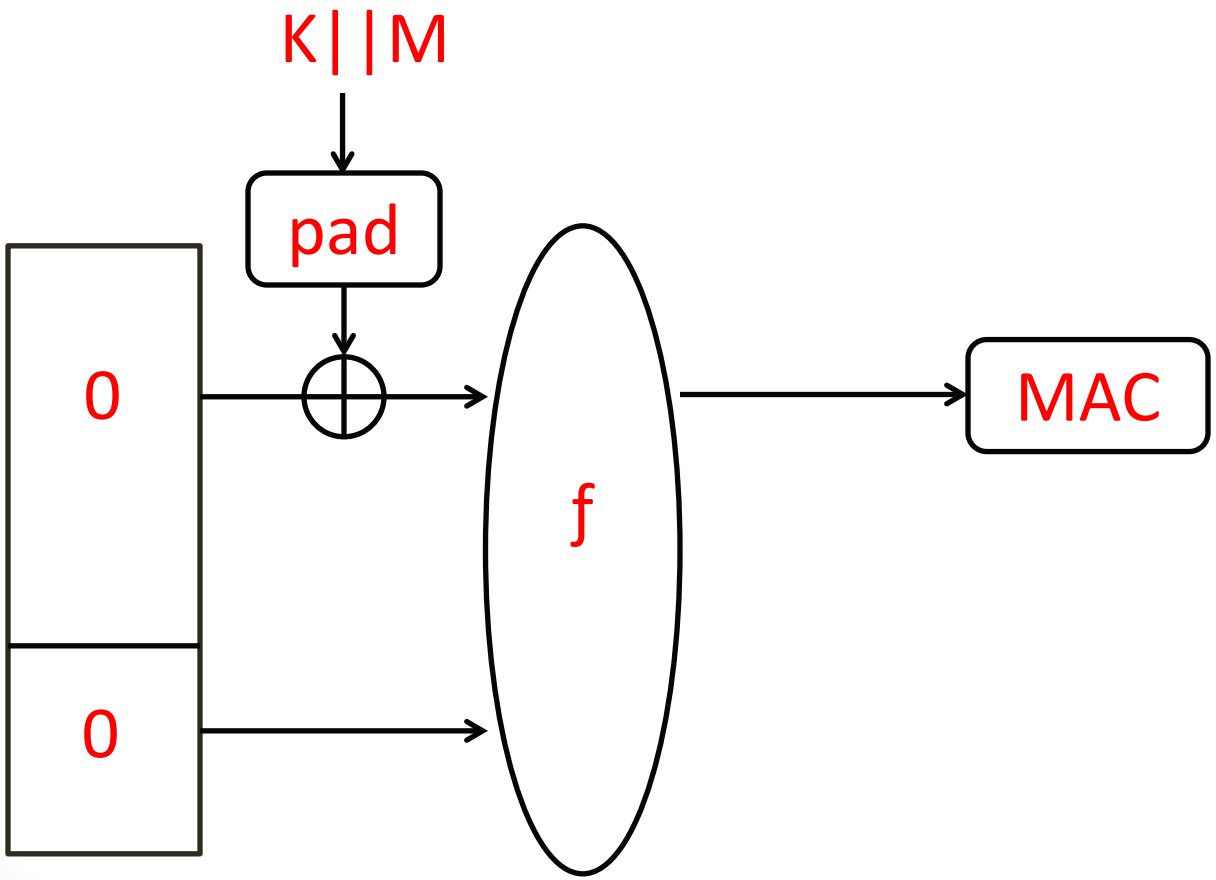
Keccak
(Bertoni, Daemen, Peeters and Van Assche)

- The new **SHA-3** standard
- Uses the **sponge construction**
- ƒ is a permutation that operates on a **1600-bit state**



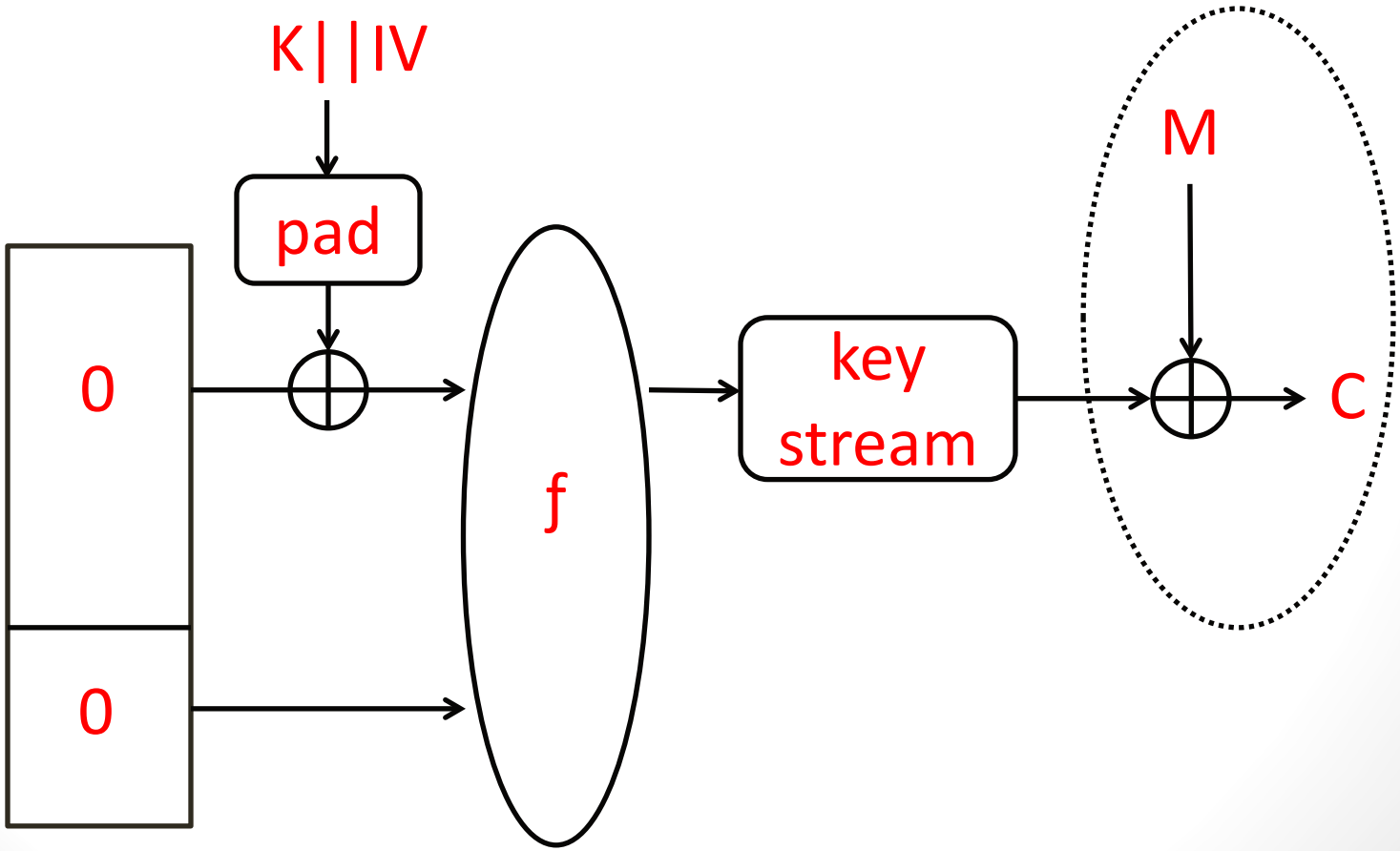
Keccak
Keyed modes

- Can be used as a **MAC**



Keccak
Keyed modes

- Can be used as a **stream cipher**



Our Results

- Analyze **keyed** modes of round-reduced Keccak
- Concentrate on **practical attacks** which can be **verified** on a standard **desktop PC**
- Mount **practical cube attacks** on round-reduced Keccak
  - The **cube attack** [DS'09] is a key recovery related to **high order differential cryptanalysis** (Lai 1994)

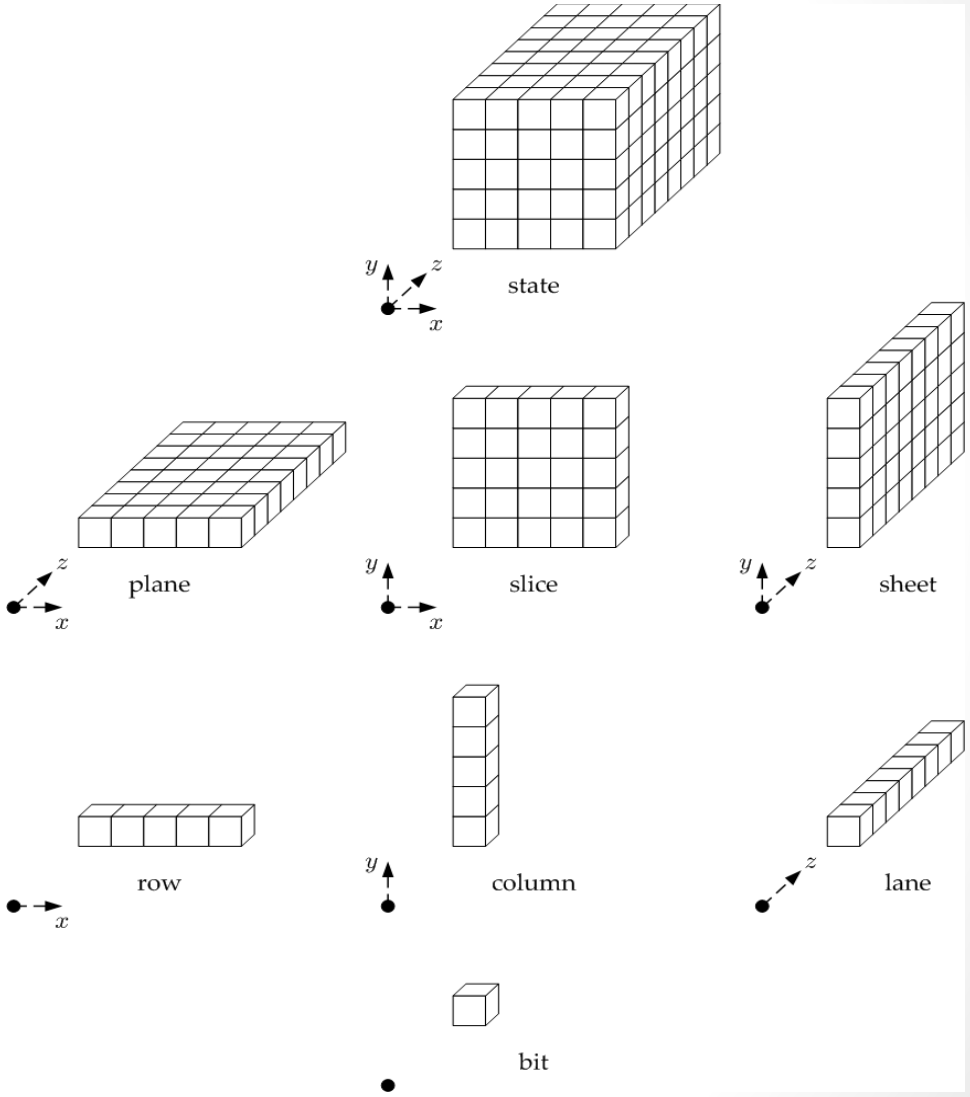
Our Results

Rounds	Mode	Attack type	Reference
2	hash function	preimage	[PRM'11]
4	hash function	collision	[DDS'12]
4	MAC	Key recovery	[J'09]
5	**MAC**	**Key recovery**	**This work**
6	**Stream cipher**	**Key recovery**	**This work**

Keccak

The Inner State

- Can be viewed as a 5x5x64-bit cube
- Or as a 5x5 matrix, where each cell is a 64-bit lane in the direction of the z axis



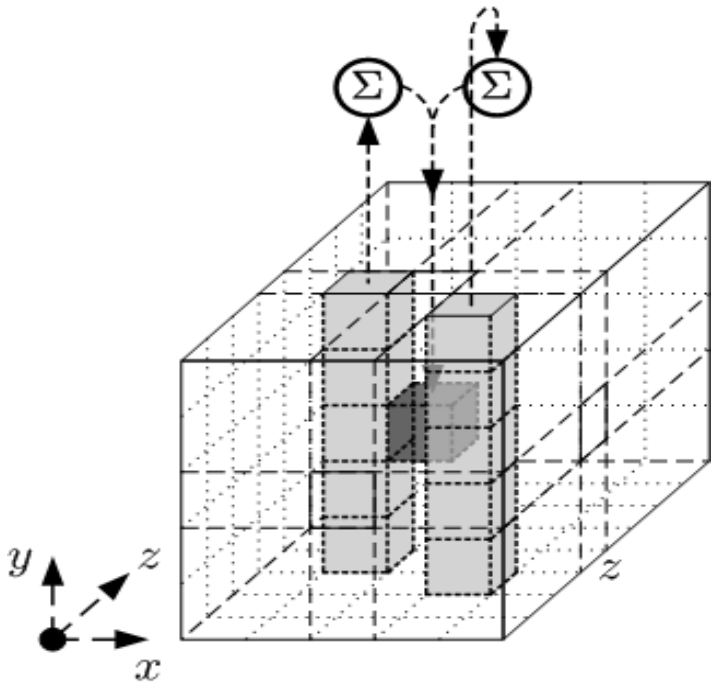
Keccak
The function f

- f is a **24-round** permutation on the 1600-bit state
- Each round consists of 5 mappings $R=\iota\circ\chi\circ\pi\circ\rho\circ\Theta$
- We refer to $\pi\circ\rho\circ\Theta$ as a "**half-round**", where $\iota\circ\chi$ make up the other half

Keccak

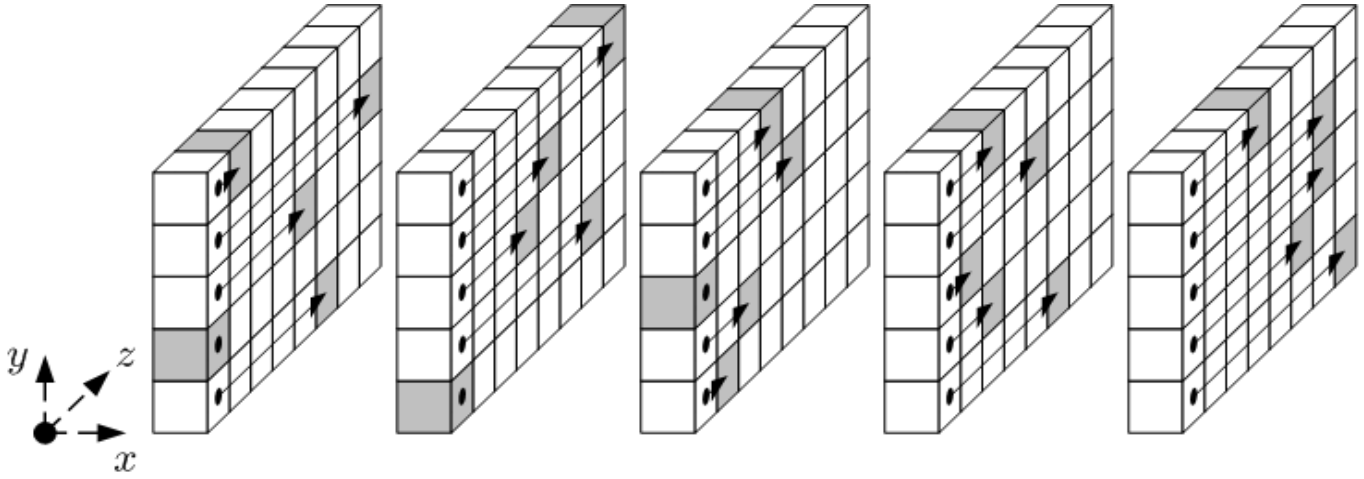
The function f

- θ is a **linear** map, which adds to each bit in a column, the parity of two other columns



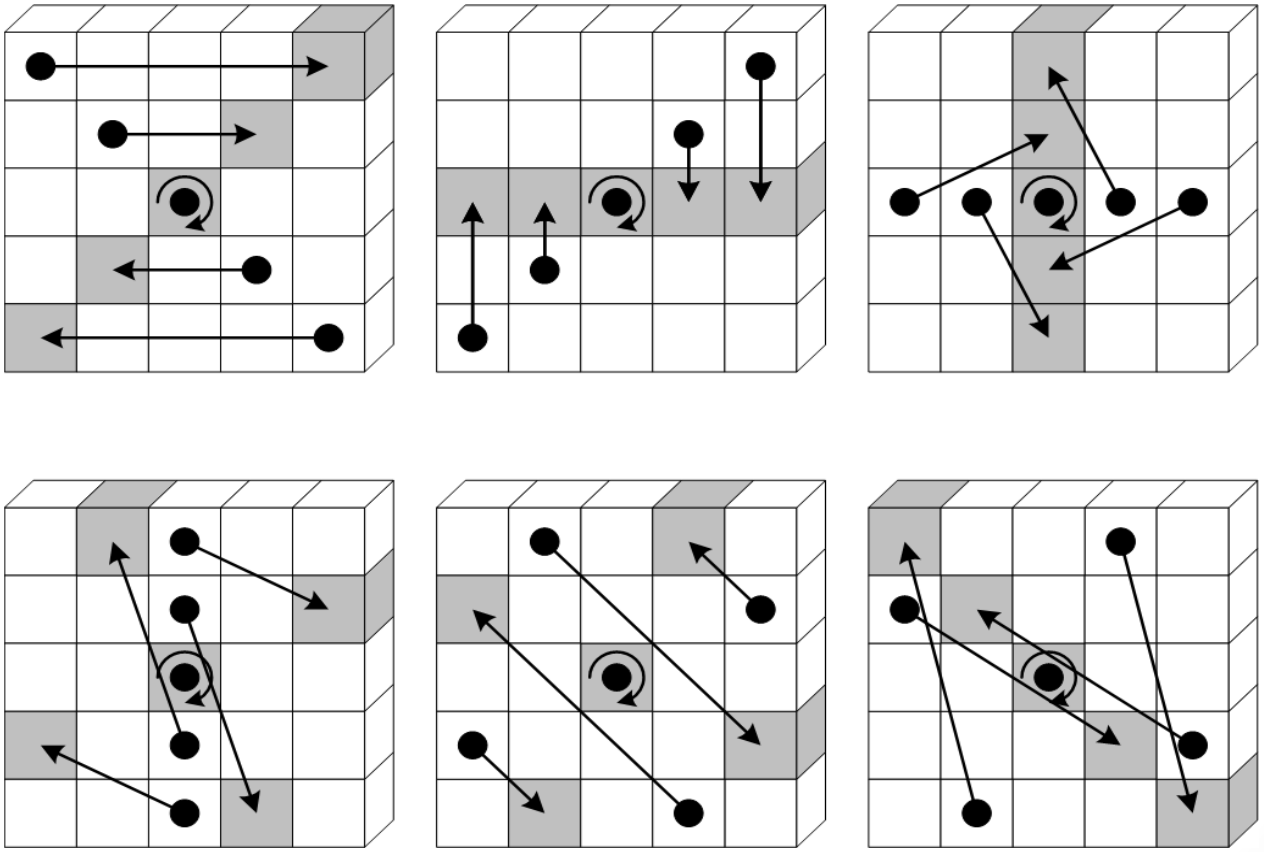
Keccak
The function f

- ρ rotates the bits within each lane by a predefined constant



Keccak
The function f

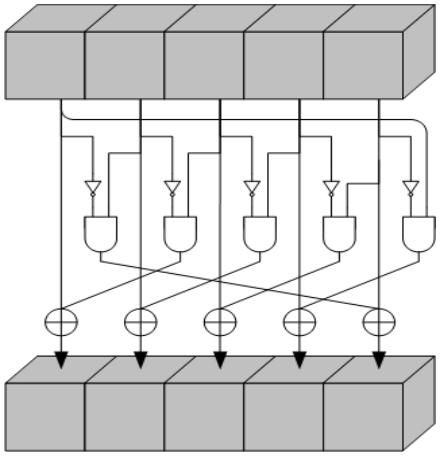
- π reorders the lanes



Keccak

The function f

- χ is the only **non-linear** mapping of Keccak
- Sbox layer applying the same **5 bits to 5 bits Sbox** to the 320 rows independently



Keccak
The function f

- ι adds a round constant to the state

- The state is initialized to **zero** before the XOR with the first message block

The Cube Attack [DS'09]

- A key recovery related to **high order differential cryptanalysis** (Lai 1994)
- Based on the **algebraic representation** of an output bit of a cryptosystem as a multivariate polynomial over GF(2): $P(v_1,\ldots,v_m,x_1,\ldots,x_n)$
  - $x_1,\ldots,x_n$ are secret variables (key bits)
  - $v_1,\ldots,v_m$ are public variables (**plaintext** bits in block ciphers and **MACs**, **IV** bits in stream ciphers)

The Cube Attack [DS'09]

- For any polynomial P and term t of variables multiplied together, we can express P as $P=tP_t+Q$ where:
  - all the variables in P_t are disjoint from the variables in t
  - each term in the multivariate polynomial Q misses at least one variable from t
- P_t is called the **superpoly** of t in P
- The **algebraic degree** of P_t is **reduced** by at least the number of variables in t

The Cube Attack [DS'09]

- Polynomial of degree 3: $P(v_1,v_2,v_3,x_1,x_2,x_3)=$

  $v_1v_2v_3+v_1v_2x_1+v_1v_3x_1+v_2v_3x_1+v_1v_2x_3+v_1v_3x_2+$
  $v_2v_3x_2+v_1v_3x_3+v_1x_1x_3+v_3x_2x_3+x_1x_2x_3+v_1v_2+$
  $v_1x_3+v_3x_1+x_1x_2+x_2x_3+x_2+v_1+v_3+1$
- $P(0,v_2,v_3,x_1,x_2,x_3) = \mathbf{v_2v_3(x_1+x_2)}+v_3x_2x_3+x_1x_2x_3+v_3x_1+$
  $x_1x_2+x_2x_3+x_2+v_3+1$
- The superpoly P_t of $t=\mathbf{v_2v_3}$ is $\mathbf{x_1+x_2}$ and its degree is (at most) 3-2=1

The Cube Attack [DS'09]

- $P(0,v_2,v_3,x_1,x_2,x_3) = \mathbf{v_2v_3(x_1+x_2)}+v_3x_2x_3+x_1x_2x_3+v_3x_1+x_1x_2+x_2x_3+x_2+v_3+1$
- We **evaluate** the **superpoly** using **cube summations** (or **differentiations**)
- An evaluation requires 2^d summations, given that t contains d variables ($2^2=4$ summations in our case)
- $P(0,0,0,x_1,x_2,x_3)+P(0,0,1,x_1,x_2,x_3)+P(0,1,0,x_1,x_2,x_3)+P(0,1,1,x_1,x_2,x_3)=\mathbf{x_1+x_2}$

The Cube Attack [DS'09]

- **Preprocessing**: Find a subset t of $\{v_1,\ldots,v_m\}$ such that P_t is **linear** in $\{x_1,\ldots,x_n\}$ and **interpolate** its linear coefficients
- Collect many linearly independent equations
- **Online**: Evaluate the linear equations (**superpolys**) in a chosen plaintext attack and recover the key $(x_1,\ldots,x_n)$

The 5-Round Cube Attack

- We attack 5-round Keccak as a **MAC** with $|K|=|M|=128$
- The algebraic **degree** of Keccak after 5 rounds is (at most) $2^5=32$
- **Preprocessing**: We **randomly** selected cubes of 31 variables from the message
  - The **superpoly** is guaranteed to have degree of **at most** 1

The 5-Round Cube Attack

- We found 117 linearly independent **superpolys** is a few days using **only** 19 cubes
- **Online**: complexity about $19 \cdot 2^{31} \approx 2^{35}$

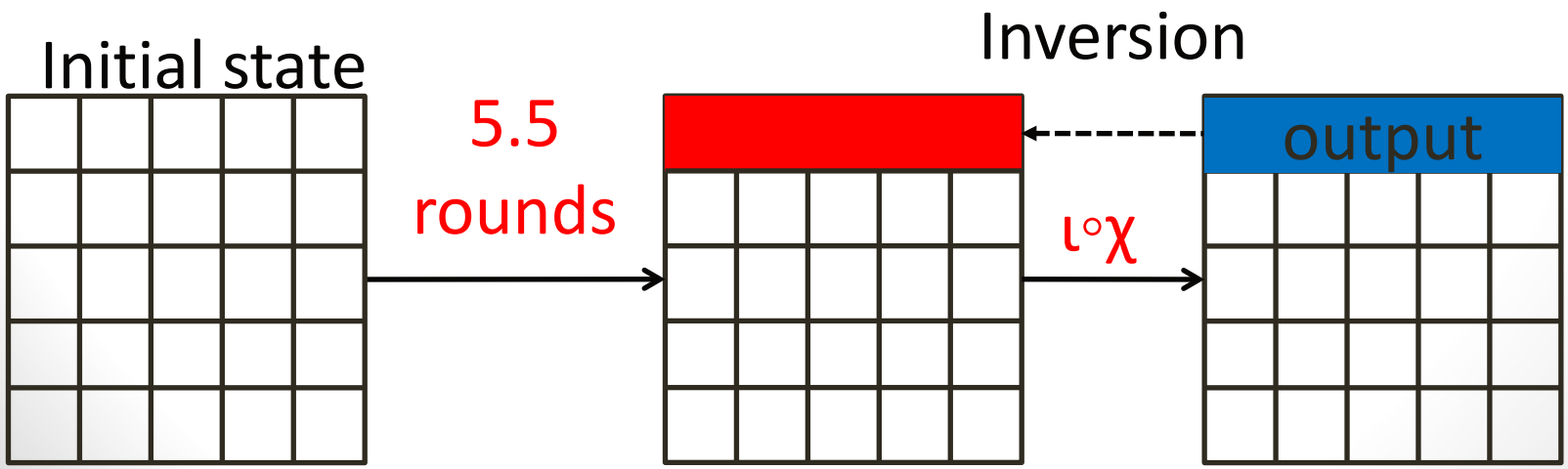
cube: 128,130,131,139,145,146,147,148,151,155,158,160,161,163,164,165,185,186,189,190,193,196,205,212,220,225,229,238,242,245,249			
superpoly	output bit	superpoly	output bit
x_{77}	7	$1 + x_{110}$	13
$1 + x_{113}$	15	x_{25}	31
$1 + x_{103}$	42	$1 + x_{105}$	69
x_{44}	84	x_{123}	87
$1 + x_{100}$	96	$1 + x_{104}$	100
x_{17}	112	$x_{38} + x_{51}$	71
$1 + x_7 + x_{19}$	91	$1 + x_{80} + x_{122}$	113
$x_{17} + x_{68} + x_{116}$	114		

The 6-Round Cube Attack

- In **stream cipher** mode, the number of output bits is typically large
- We assume that the attacker obtains (at least) 320 key stream bits
- We attack 6-round Keccak as a **stream cipher** with $|K|=128$ and $|IV|=128$
- The algebraic **degree** after 6 rounds is about $2^6=64$ which seems **too high** for practical attacks

Partial Inversion

- Given 320 output (key stream) we can **invert** χ and ι on these bits
- We compute 320 state bits after 5.5 rounds
- The degree of each such state bit in the initial state is **only** $2^5=32$
- We can **easily apply** the cube attack to this variant

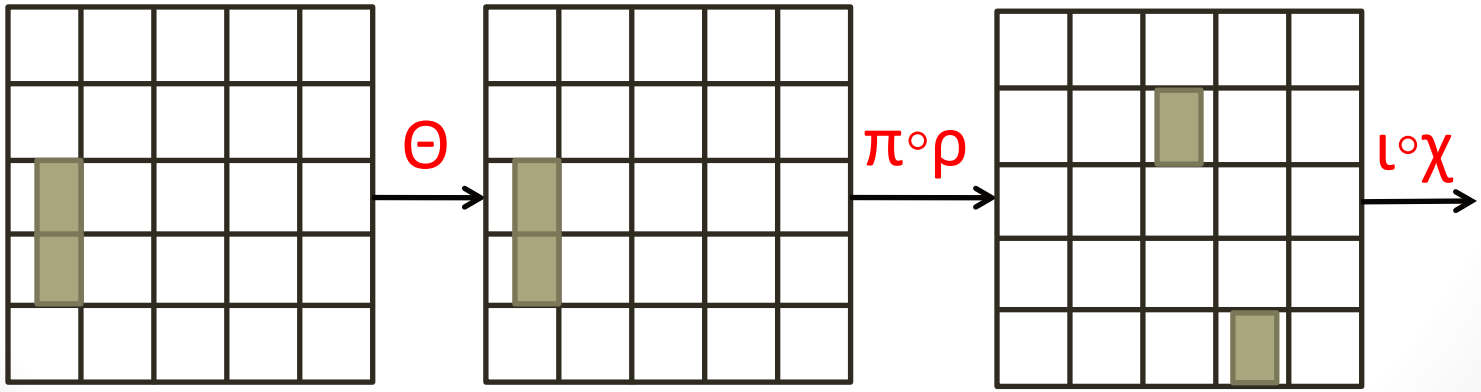


6-Round Attack on Keccak as a MAC

- **MACs** are typically at most 256-bits long
- The previous key recovery attack cannot be applied
- We can still mount a **distinguishing attack** given that we can **control sufficiently many bits** of the initial state with a chosen message attack

6-Round Attack on Keccak as a MAC

- We select 33 public variables that are **not multiplied together** in the first round
- The degree after 6 rounds is only $2^5=32$
- The cube sum is **zero**



Conclusions

- We mounted **practical cube attacks** on round-reduced keyed modes of Keccak
- We increased from 4 to 6 the number of Keccak rounds which can be attacked in **practical** times

Work in Progress

- Our attacks can be applied to **more rounds** with impractical complexity, but **much faster** than exhaustive search

Rounds	Mode	Attack type
7	**MAC**	**Key recovery**
9	**Stream cipher**	**Key stream predication**

Thank you for your attention!