

Practical Collisions in Round-Reduced Keccak

[Itai Dinur](#)¹, Orr Dunkelman^{1,2} and Adi Shamir¹

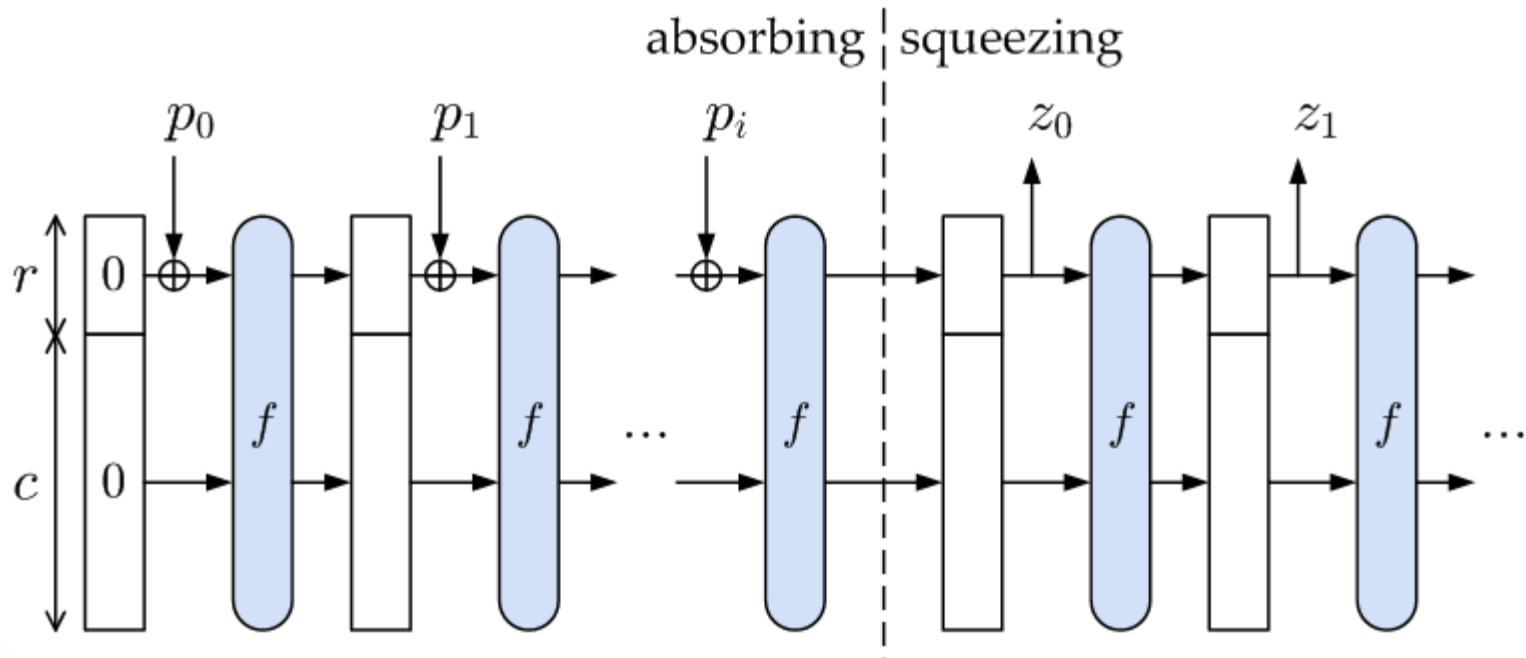
¹The Weizmann Institute, Israel

²University of Haifa, Israel

Keccak

(Bertoni, Daemen, Peeters and Van Assche)

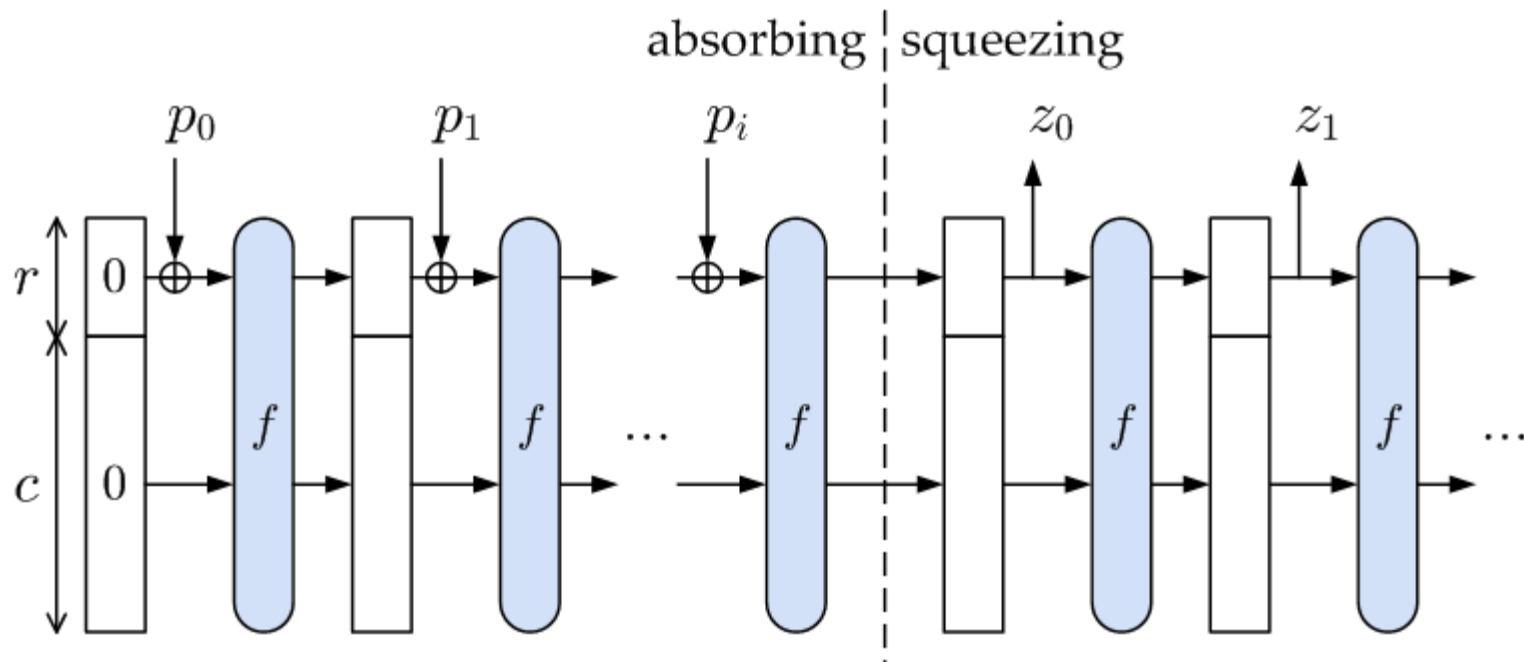
- One of the 5 **finalists** of the SHA-3 competition
 - Version submitted to support hash sizes n of **224, 256, 384** and **512** bits
- Uses the **sponge construction**



Keccak

(Bertoni, Daemen, Peeters and Van Assche)

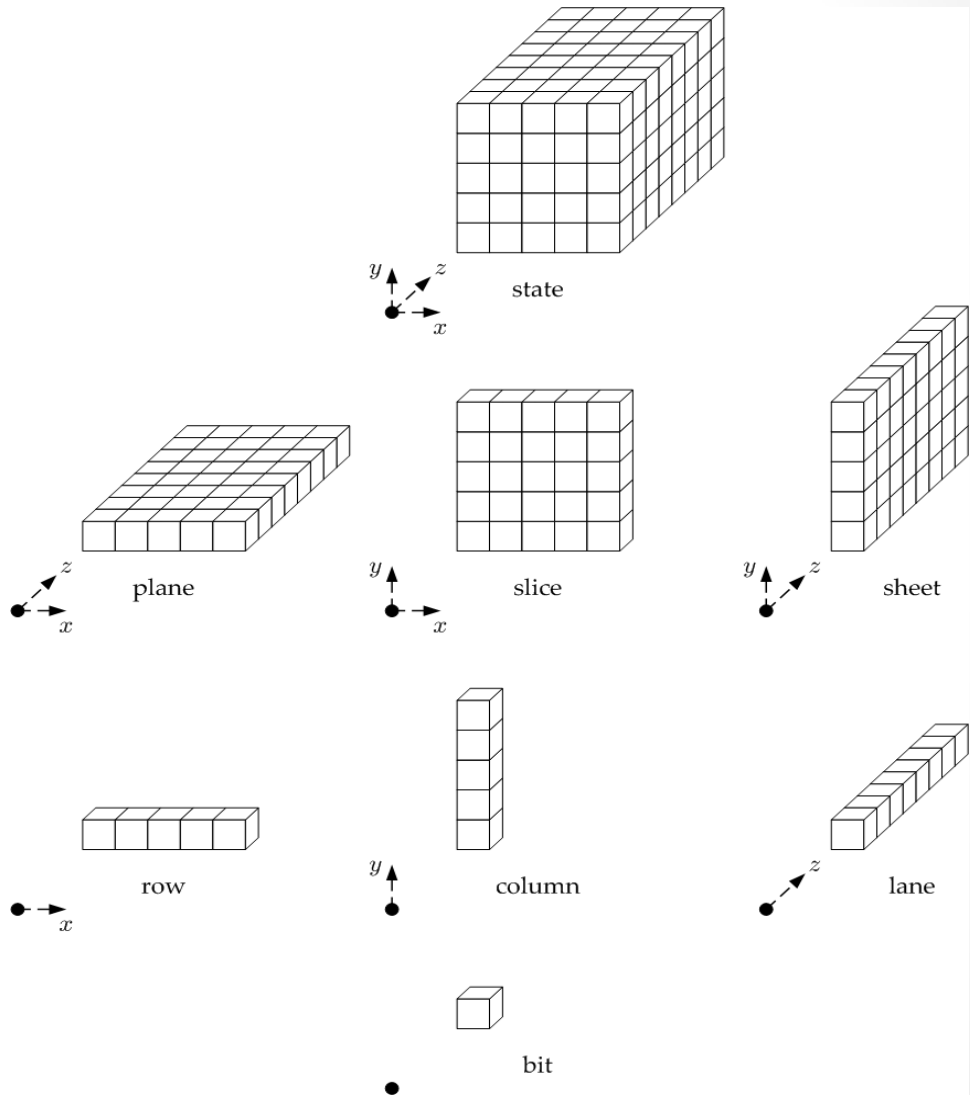
- f is a permutation that operates on a **1600-bit state**
- $c=2n$ and $r=1600-2n$



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



Keccak

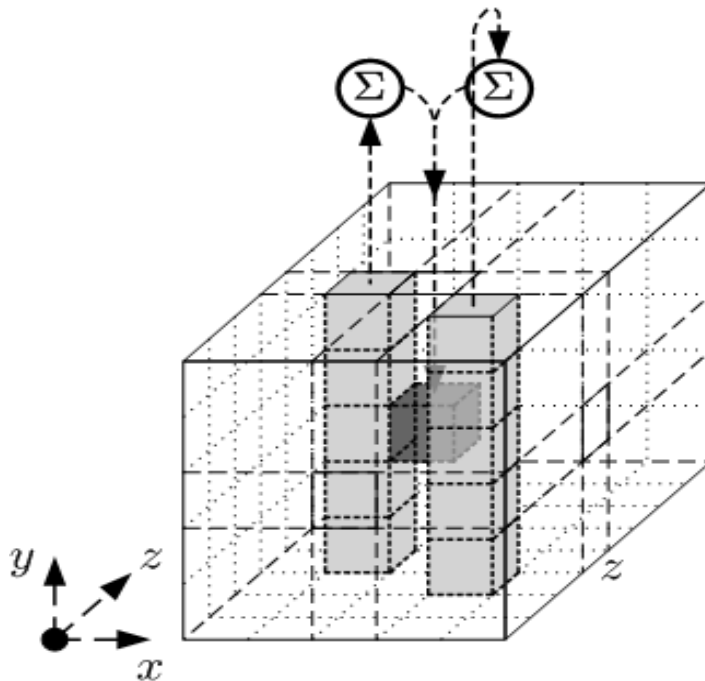
The function f

- f is a **24-round** permutation on the 1600-bit state
- Each round consists of 5 mappings $R = \iota \circ \chi \circ \pi \circ \rho \circ \Theta$

Keccak

The function f

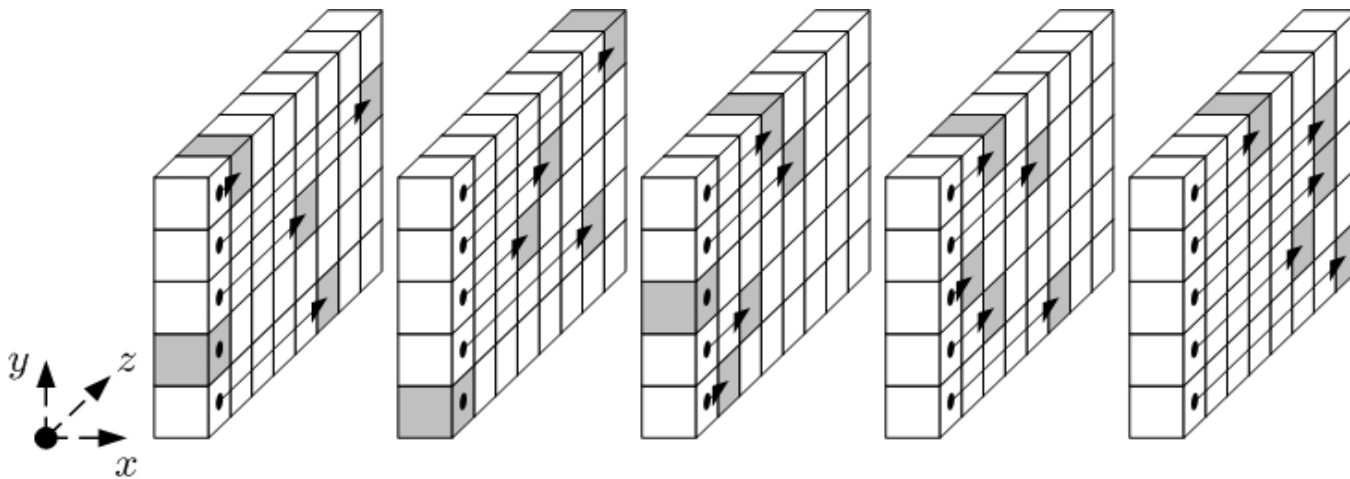
- Θ is a **linear** map, which adds to each bit in a column, the parity of two other columns
- For Θ^{-1} , flipping the value of any input bit, flips the value of **more than half** of the output bits



Keccak

The function f

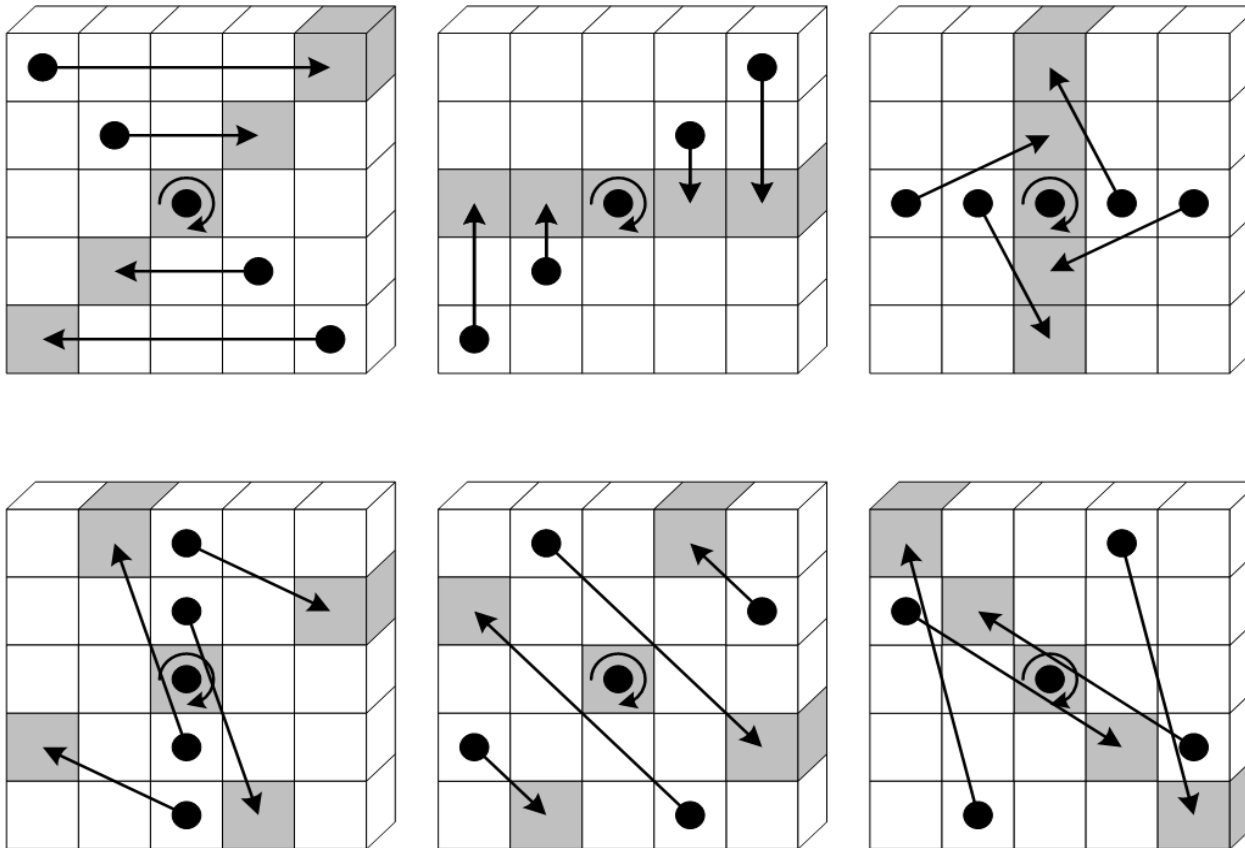
- ρ rotates the bits within each lane by a predefined constant



Keccak

The function f

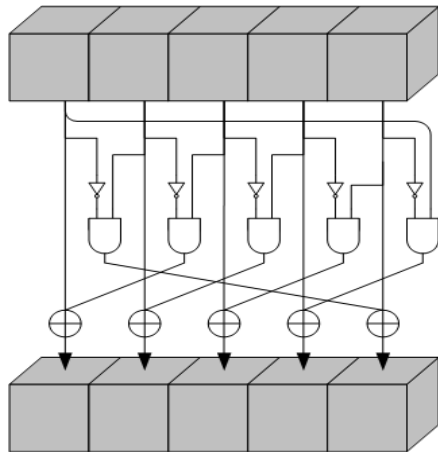
- π reorders the lanes



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
- **Algebraic degree of 2**



Keccak

The function f

- ι adds a round constant to the state
- We denote $L = \pi \circ \rho \circ \Theta$

Keccak

Previous Attacks

- Several results on Keccak's **building blocks**
- Most notably **Zero-sums** due to Aumasson and Meier (and extended in several papers)
- Results on versions that were not submitted to the SHA-3 contest

Keccak

Previous Attacks

- We concentrate on the **versions submitted** to the SHA-3 contest
 - **Only** changed by reducing the number of rounds
- A pre-image attack by Bernstein
 - extends up to 8 rounds of Keccak
 - marginally faster than exhaustive search
 - uses a huge amount of memory

Keccak

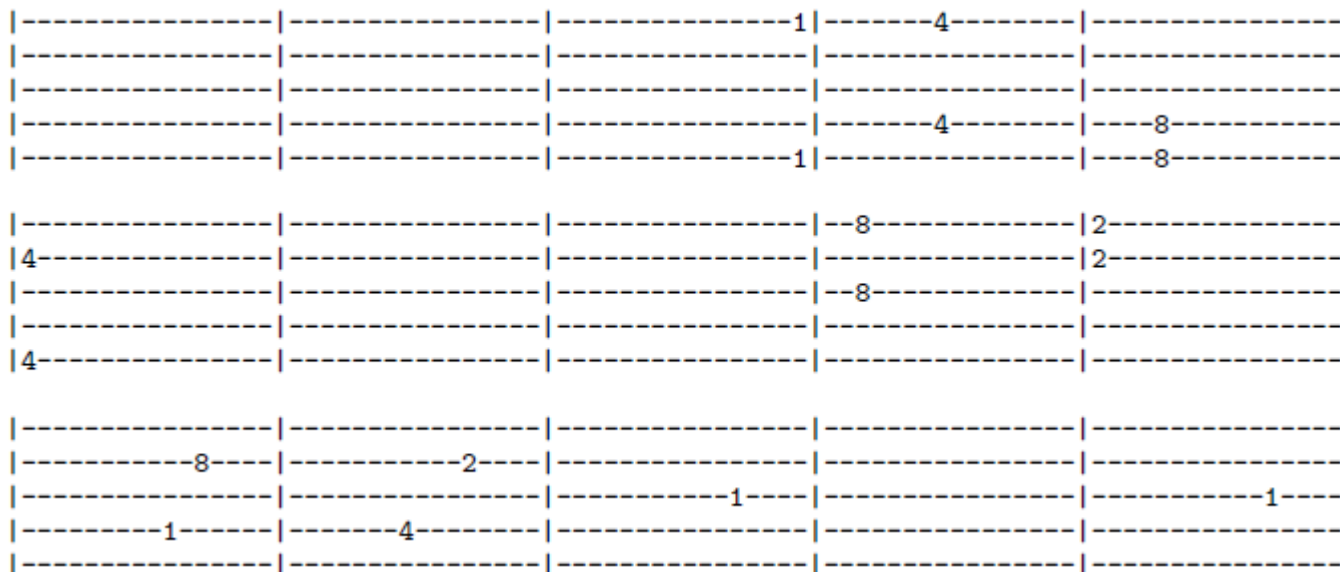
Differential Characteristics

- Analyzed in the submission document and in several separate papers:
 - “Practical analysis of reduced-round Keccak” by Naya-Plasencia, Röck and Meier (Indocrypt 2011)
 - “Unaligned Rebound Attack - Application to Keccak” by Duc, Guo, Peyrin, and Wei (FSE 2012)
- Find **low Hamming weight differential characteristics** for **2** rounds
- Can be extended by an **additional round** forwards with a **moderate** increase in HW

Keccak

Differential Characteristics

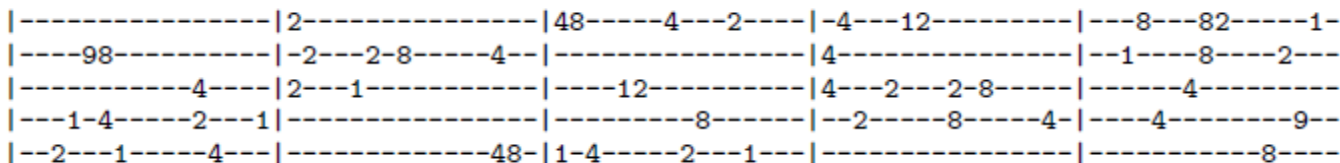
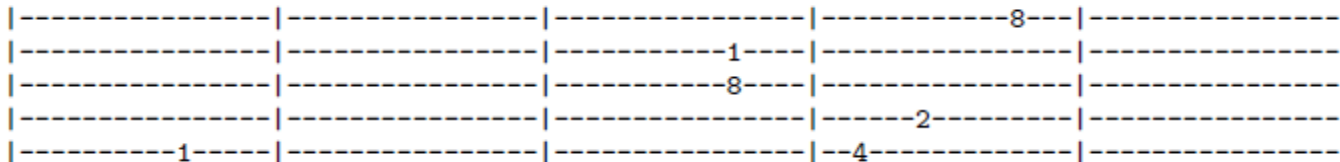
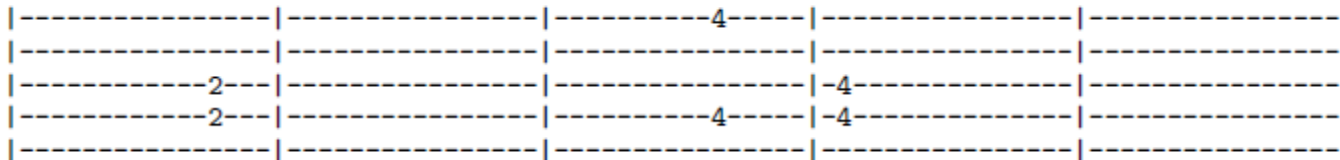
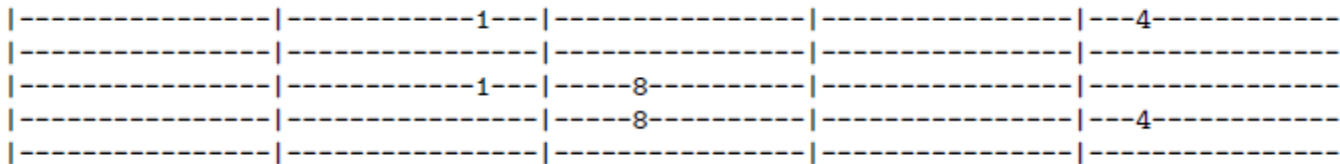
- 2-round differential characteristic
 - Leads to a collision



Keccak

Differential Characteristics

- 3-round differential characteristic
 - Leads to a near-collision



Keccak

Collision Attacks

- The **HW** of the starting state difference of these characteristics is **very low**
- Some can be used as an **initial state** of Keccak

Keccak

Collision Attacks

- Naya-Plasencia, Röck and Meier found:
 - Actual **collisions** in **2-round** Keccak-224 and Keccak 256
 - Actual **near-collisions** in **3-round** Keccak-224 and Keccak-256
- We extend these results by **2 more rounds**
 - **Double** the number of rounds for practical collisions

Our Results

- **Collisions in 4-round Keccak-224 and Keccak-256 within a few minutes**

M1=

4C4F31C32 4C59AE6D 5D19F0F4 25C4E44B D8853032 8D5E12F2 BB6E6EE2 27C33B1E 6C091058 EB9002D5
3BA4A06F 4A0CC7F1 CCB55E51 8D0DD983 2B0A0843 9B21D3B0 53679075 526DDED2 48294844 6FF4ED2C
1ACE2C15 471C1DC7 D4098568 F1EBF639 EAF7B257 09FDAE87 688878E6 4875EB30 C9C32D80 3C9E6FCB
3C2ABCFA E6A4807B 2AB281B8 812332B3

M2=

A4D30EF7 80BB8F69 90C048DF EB7213B9 A6650424 3A65F63E 8C268881 B651B81F AADAF3C EE2CA5C3
DB78EAC2 C8EAE779 442F9C35 3221E287 B3017A5A 90790712 1B1C8BDC E08B10A8 9A9D25CA 1BE7AAAC
4E2F3E9C 73717DAD 5566015A A198CFB9 5A1CA8C2 A0E3348A AE6C0BB1 3980F9E4 A4FA8B91 6E81A989
89A9BCAA E12BF1F1 30EF9595 812E8B45

Output=

61FB1891 F326B6D5 24DD94DF 73274984 05DA9A1D 3FD359B9 78B8393B F2E7990B

Our Results

- **Near-collisions in 5-round Keccak-224 and Keccak-256 within a few hours**

M1=

23296F07 44536A2B 16E1E363 09B509F9 639CA324 2B834133 61457E6D 9CF07597 6797B3D4 D1715ABA
6D8F4F9F 70D12920 E014BB37 54C32ADE 6117B3FB 30114566 4BA7D70A 00F055F0 71CFFDD4 B53F2563
E223A16D CC8DDAC4 7A59836B A53FBDDE 9FFEC45F 6A3476DC 7349BB92 56AF6E92 83866932 56624032
A936E410 60AC00FA 7E7C61F9 81583CAC

M2=

49D48DE2 9FA843CA 747C88E0 55425134 098CA5B3 C97DC68A B82BC6FD 0F864996 26B13425 D9F73B75
932CD02F FB12E036 47706100 9DEFFFE4 79435F9C DA727EF0 D9CA67C6 520BE2D1 19CF3933 3136D1A9
EEBEA9DD 150CA247 D494BF4A 492EFB26 11CB4C8D F5A10A05 69128FF4 B142742F CA59FE32 4FE68436
068F76AB 041A673E 461575B5 81AA2A54

Output1=

407D4466 FEA8B231 EC968181 DF902165 23C219FF 54571D70 2800F506 E818644B

Output2=

407D4466 FEA8B231 EC928181 FF902165 23C019FF 1C571D74 2800F516 E810656B

Our Techniques

- Combine **algebraic** techniques with **differential** cryptanalysis
- Use novel **linearization** techniques to efficiently exploit the available degree of freedom

Our Attack

Extending Characteristics

- We first **extend** a given characteristic **backwards** by one round
- The **HW** of its starting state difference is **low**
 - Passes χ with (relatively) high probability

Our Attack

Extending Characteristics

- Used by Duc, Guo, Peyrin, and Wei to construct characteristics on the permutation
- However, Θ **diffuses** backwards **very fast**
- The **HW** of the new starting state difference is **very high**
- Cannot be used as an initial state of Keccak

Our Attack

Extending Characteristics

- A 2-round differential characteristic extended backwards by an additional round

```
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E2656F26B | 357C4789AF3-6AF1 | 78D3526BC6A74C4D |
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E2656F26B | 357C4789AF3-6AF1 | 78D3526BC6A74C4D |
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E2676F26B | 357C4789AF3-6AF1 | 78D3526BC4A74C4D |
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E265EF26B | 357C4789AF3-4AF1 | 78D3526BC6A74C4D |
| 26978AF134CB835E | AF226C4D78366789 | C4DAE35E2656F26B | 35FC4789AF3-6AF1 | 78D3526BC6A74C4D |
```

```
|-----|-----|-----1|-----4-----|-----|
|-----|-----|-----|-----|-----|
|-----|-----|-----|-----|-----|
|-----|-----|-----|-----4-----|-----8-----|
|-----|-----|-----1|-----|-----8-----|
```

```
|-----|-----|-----|-----8-----|2-----|
|4-----|-----|-----|-----8-----|2-----|
|-----|-----|-----|-----|-----|
|-----|-----|-----|-----|-----|
|4-----|-----|-----|-----|-----|
```

```
|-----|-----|-----|-----|-----|
|-----8-----|-----2-----|-----|-----|-----|
|-----|-----|-----1-----|-----|-----1-----|
|-----1-----|-----4-----|-----|-----|-----|
|-----|-----|-----|-----|-----|
```

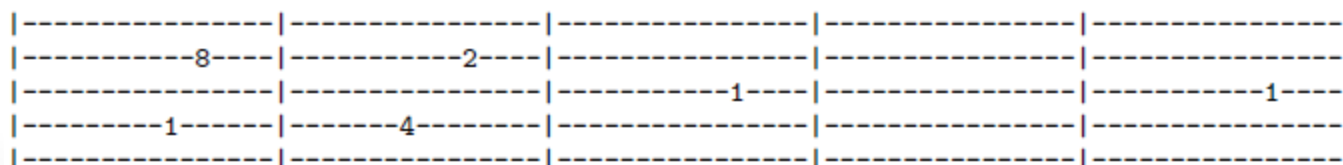
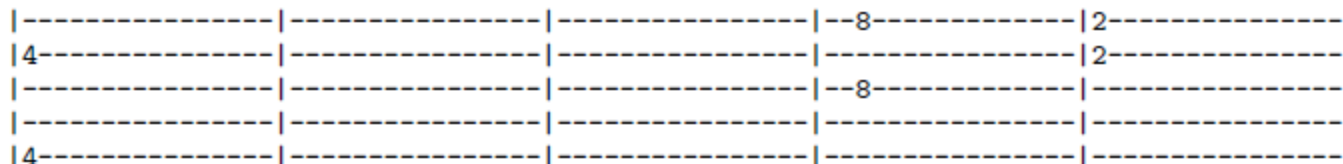
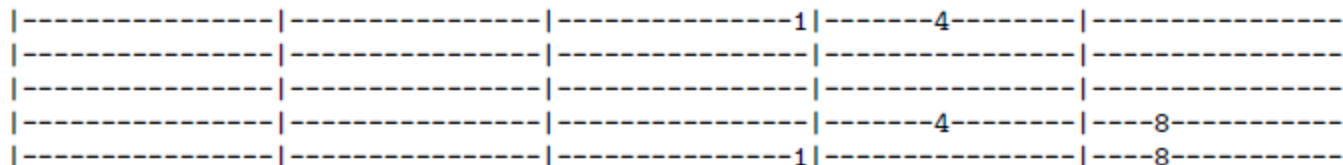
Our Attack

Linking a Characteristic Form an Initial State



1 Round \updownarrow

```
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E2656F26B | 357C4789AF3-6AF1 | 78D3526BC6A74C4D |
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E2656F26B | 357C4789AF3-6AF1 | 78D3526BC6A74C4D |
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E2676F26B | 357C4789AF3-6AF1 | 78D3526BC4A74C4D |
| 26978AF134CB835E | AF224C4D78366789 | C4DAE35E265EF26B | 357C4789AF3-4AF1 | 78D3526BC6A74C4D |
| 26978AF134CB835E | AF226C4D78366789 | C4DAE35E2656F26B | 35FC4789AF3-6AF1 | 78D3526BC6A74C4D |
```



Our Attack

Linking a Characteristic Form an Initial State

- The initial state difference of the characteristic is called the **target difference**

Controllable Part

0

1 Round


26978AF134CB835E	AF224C4D78366789	C4DAE35E2656F26B	357C4789AF3-6AF1	78D3526BC6A74C4D
26978AF134CB835E	AF224C4D78366789	C4DAE35E2656F26B	357C4789AF3-6AF1	78D3526BC6A74C4D
26978AF134CB835E	AF224C4D78366789	C4DAE35E2676F26B	357C4789AF3-6AF1	78D3526BC4A74C4D
26978AF134CB835E	AF224C4D78366789	C4DAE35E265EF26B	357C4789AF3-4AF1	78D3526BC6A74C4D
26978AF134CB835E	AF226C4D78366789	C4DAE35E2656F26B	35FC4789AF3-6AF1	78D3526BC6A74C4D

Our Attack

Linking a Characteristic Form an Initial State

- The main tool we develop is the **target difference algorithm**
- Finds many initial message pairs that **satisfy** the **target difference after one round**



1 Round 

```
|26978AF134CB835E|AF224C4D78366789|C4DAE35E2656F26B|357C4789AF3-6AF1|78D3526BC6A74C4D|
|26978AF134CB835E|AF224C4D78366789|C4DAE35E2656F26B|357C4789AF3-6AF1|78D3526BC6A74C4D|
|26978AF134CB835E|AF224C4D78366789|C4DAE35E2676F26B|357C4789AF3-6AF1|78D3526BC4A74C4D|
|26978AF134CB835E|AF224C4D78366789|C4DAE35E265EF26B|357C4789AF3-4AF1|78D3526BC6A74C4D|
|26978AF134CB835E|AF226C4D78366789|C4DAE35E2656F26B|35FC4789AF3-6AF1|78D3526BC6A74C4D|
```

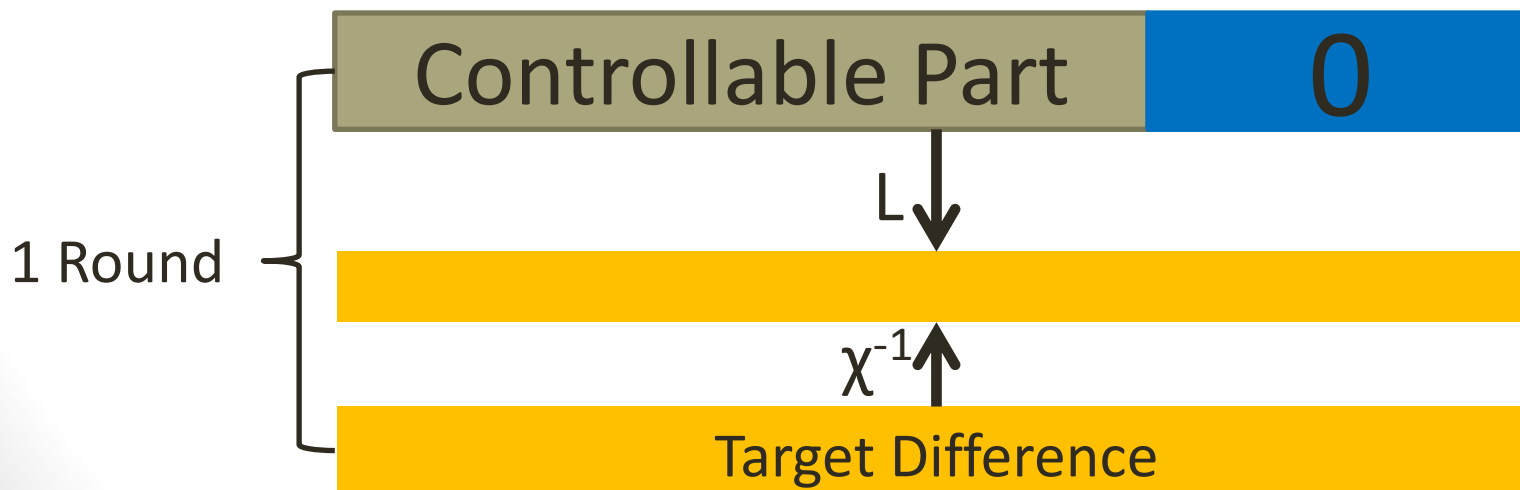
Our Attack

- 1) Obtain a **large set** of message pairs that **satisfy the target difference**
- 2) Execute a **differential attack** to search for collisions (or near-collisions) within the **specific set**
 - Exploiting the high probability differential characteristic beyond the first round

The Target Difference Algorithm

Problems

- 1) The target difference extends backwards, beyond the first Keccak Sbox layer, with **very low probability**
- 2) The initial state **fixes** many of the state bits to **predefined** values



The Target Difference Algorithm

Degrees of Freedom

- **704** and **576 degrees of freedom** for Keccak-224 and Keccak-256, respectively
- We expect **many solutions** for an **arbitrary** target difference
- However, their density is **very small**

The Target Difference Algorithm

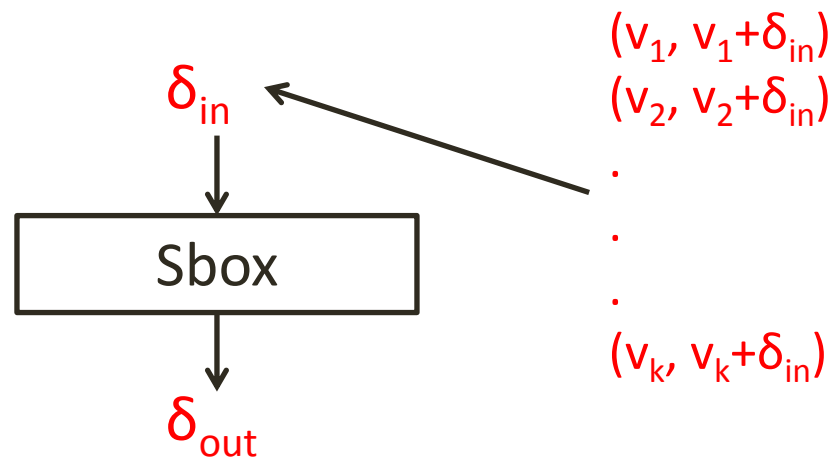
Formulating the Constraints

- **R** has algebraic degree of **2**
- The problem can be formulated using **quadratic equations**
- Standard linearization uses **too many** degrees of freedom

Solving the Constraints

Using differences

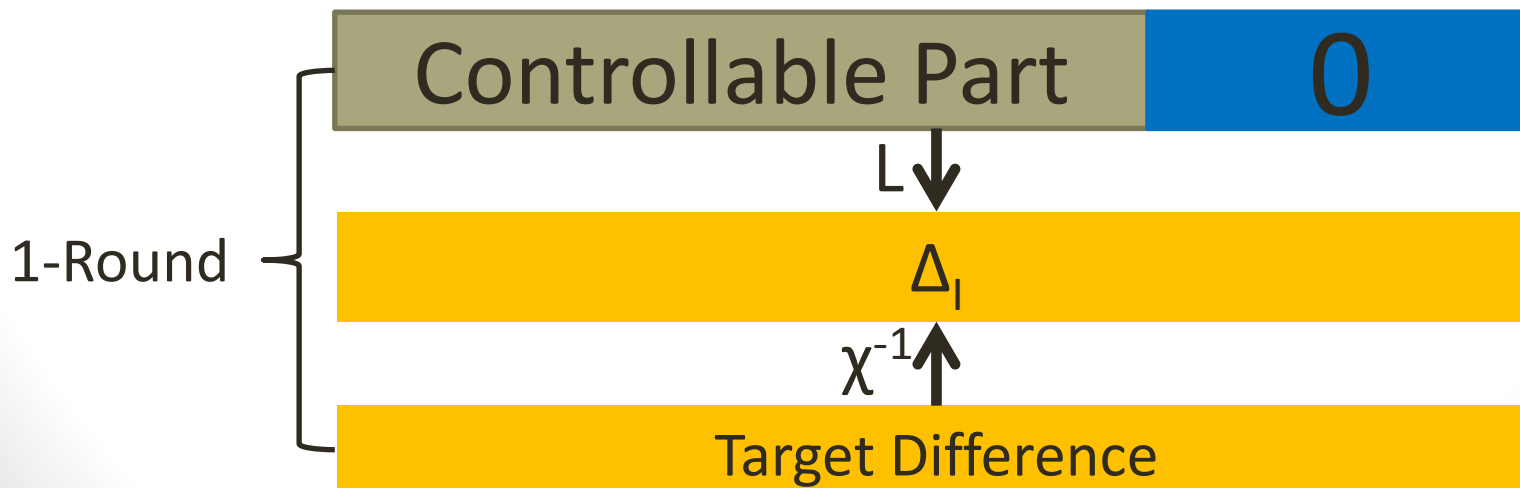
- The algebraic degree of the Keccak Sbox is only **2**
- **Differentiating** polynomials of degree **2** reduces their degree to **1**
- Fix an input **input-output difference** to an Sbox $(\delta_{in}, \delta_{out})$
- All the pairs of input **values** that satisfy $(\delta_{in}, \delta_{out})$ form an **affine subspace**



Solving the Constraints

Two-Phase Approach

- We have two phases:
- 1) **Difference phase**: find a 1600-bit **input difference** Δ_I to the Sbox layer
- 2) **Value phase**: obtain the **actual message pairs** that lead to the target difference



Solving the Constraints

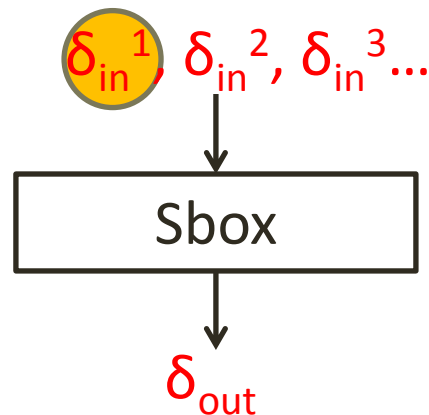
Solving the Value Constraints

- Given Δ_1 , the value phase reduces to solving **linear equations**
 - However the equations may be inconsistent
- The output is an **affine subspace** of message pairs

The Difference Phase

Solving the Difference Constraints

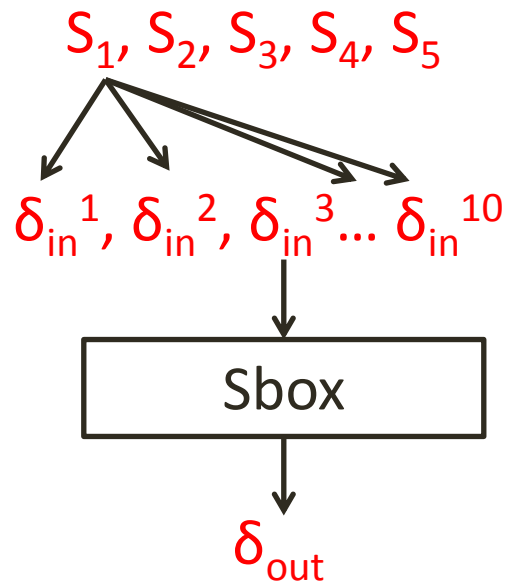
- Given an **output difference** to an Sbox δ_{out}
- The **possible input differences** are **not related** by simple affine relations
- Standard “Guess and Determine” techniques **commit to many values** in advance
 - Restrict the solution space
 - very inefficient



The Difference Phase

Solving the Difference Constraints

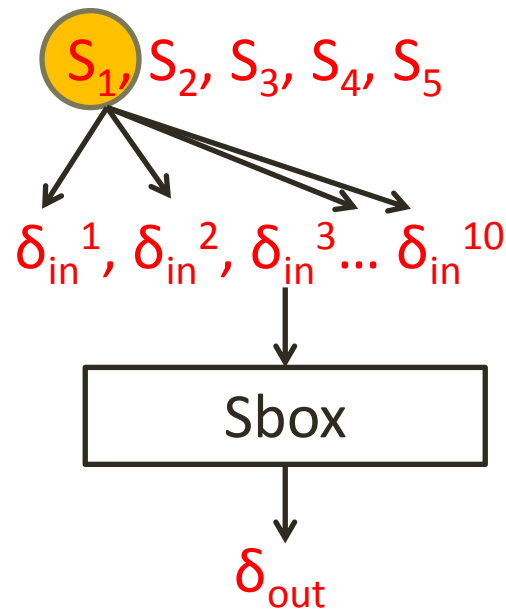
- Another property of Keccak Sbox:
- Given any non-zero **output difference** to an Sbox δ_{out}
- The **set of possible input differences** contains at least five **2-dimensional affine subspaces**



The Difference Phase

Solving the Difference Constraints

- For each active Sbox, choose an affine subspace with **4 potential input differences**
- A more flexible approach



Results

- We performed simulations on **dozens of target differences**
- For each one we were able to find a **large subspace** of message pairs that satisfy it

Conclusions and Future Work

- We **extended** previous collision attacks on Keccak-224 and Keccak-256 by **two rounds**:
 - **Collisions** in **4-round** Keccak-224 and Keccak-256 within a **few minutes**
 - **Near-collisions** in **5-round** Keccak-224 and Keccak-256 within a **few hours**
 - Keccak has **24** rounds...
- Find **longer** high probability differential characteristics for the Keccak permutation

Thank you for your attention!