Differential Cryptanalysis of Keccak Variants

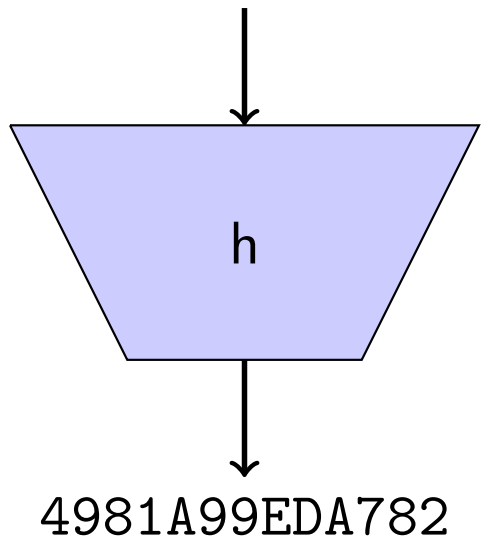
Stefan Kölbl [1], Florian Mendel [2],
Tomislav Nad and Martin Schläffer [2]

[1]DTU - Technical University of Denmark
[2]IAIK - Graz University of Technology

December 18, 2013

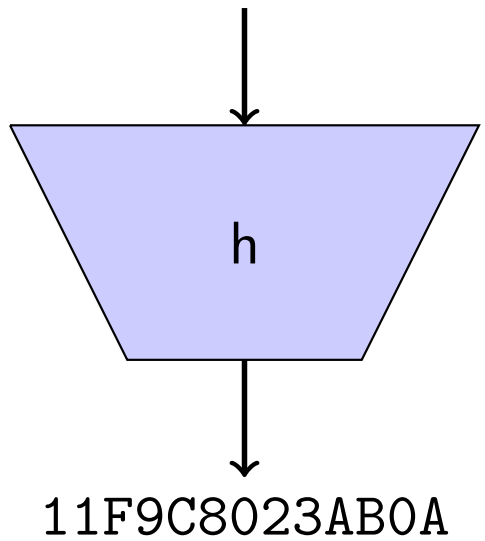
Cryptographic Hash Functions

"Today is the 18th of December..."



Cryptographic Hash Functions

"Today is the 19th of December..."



Cryptographic Hash Functions

Applications:

- Message Integrity
- Digital Signature Schemes
- Password Protection
- Key Derivation
- Payment Schemes (Bitcoin)
- ...

Requirements:

- no secret parameter
- fast to compute
- secure

Cryptographic Hash Functions

Security Requirements

- Preimage Resistance:
  Given $h(x)$ find x
- Second-Preimage Resistance:
  Given $x, h(x)$ find $y \neq x$ s.t. $h(x) = h(y)$
- Collision Resistance:
  Find x, y with $x \neq y$ s.t. $h(x) = h(y)$

Generic Attack

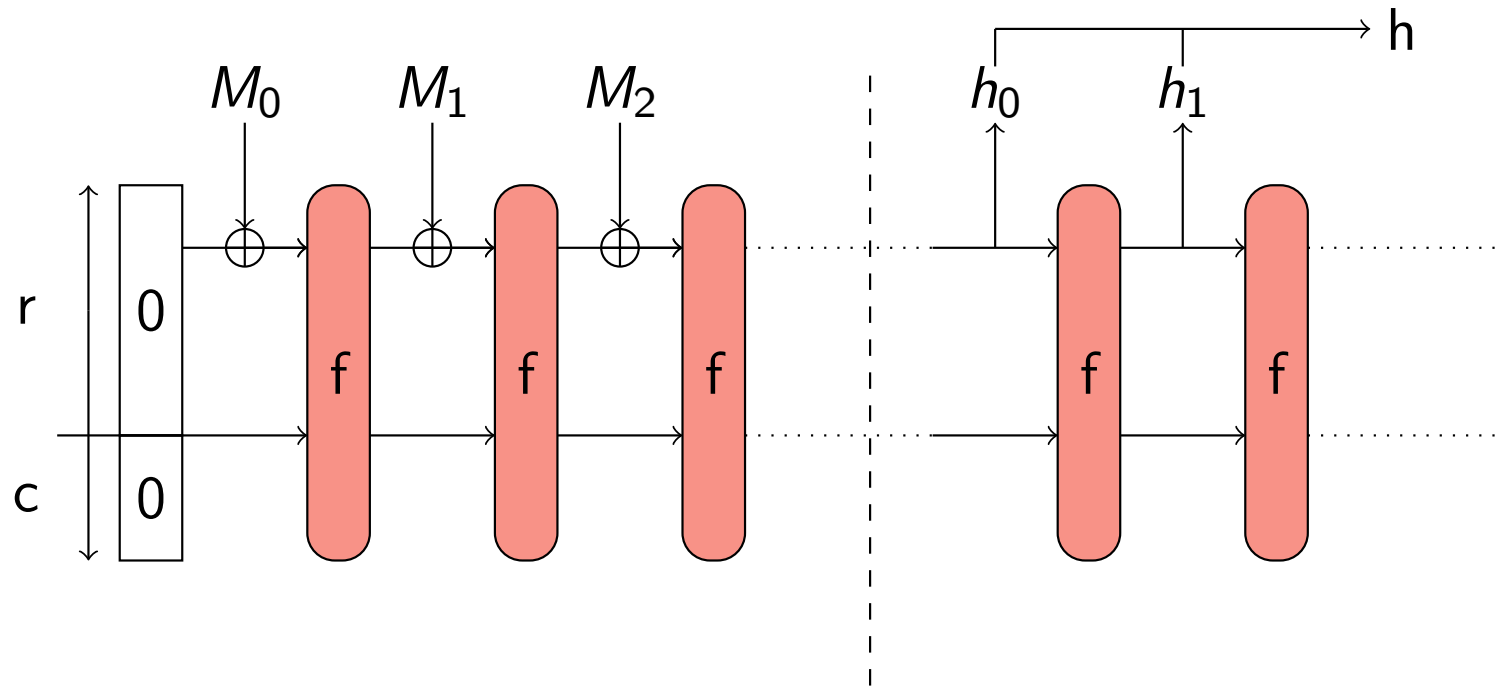
Complexity 2^n for (second) preimage and $2^{n/2}$ for collisions.

Keccak

- Designed by Bertoni, Daemen, Peeter and Van Assche
- Selected by NIST in October 2012 to become the new SHA-3 standard.
- Based on the sponge construction.
- Uses fixed size permutation Keccak-f.
- Uses 1600-bit permutation for SHA-3.
- Supports output sizes of $\{224, 256, 384, 512\}$-bit.

Sponge Construction

Takes arbitrary sized input and produces arbitrary sized output.



- The permutation is of size $b = r + c$.
- Security claim of $2^{c/2}$

Sponge Construction

Comparison of Keccak with $c = 2n$ and $c = n$.

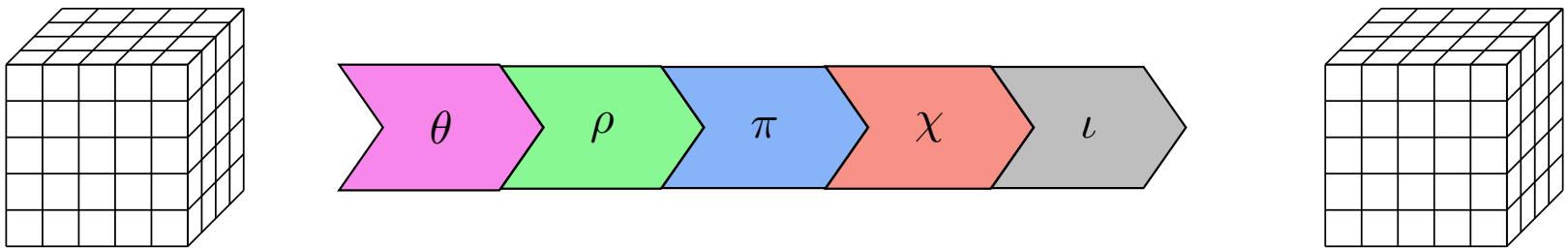
	Keccak-256		Keccak-512	
Capacity	512	256	1024	512
Rate	1088	1344	576	1088
Coll. Res.	2^{128}	2^{128}	2^{256}	2^{256}
Preimg Res.	2^{256}	2^{128}	2^{512}	2^{256}
Performance		+23.5%		+88.9%

Keccak

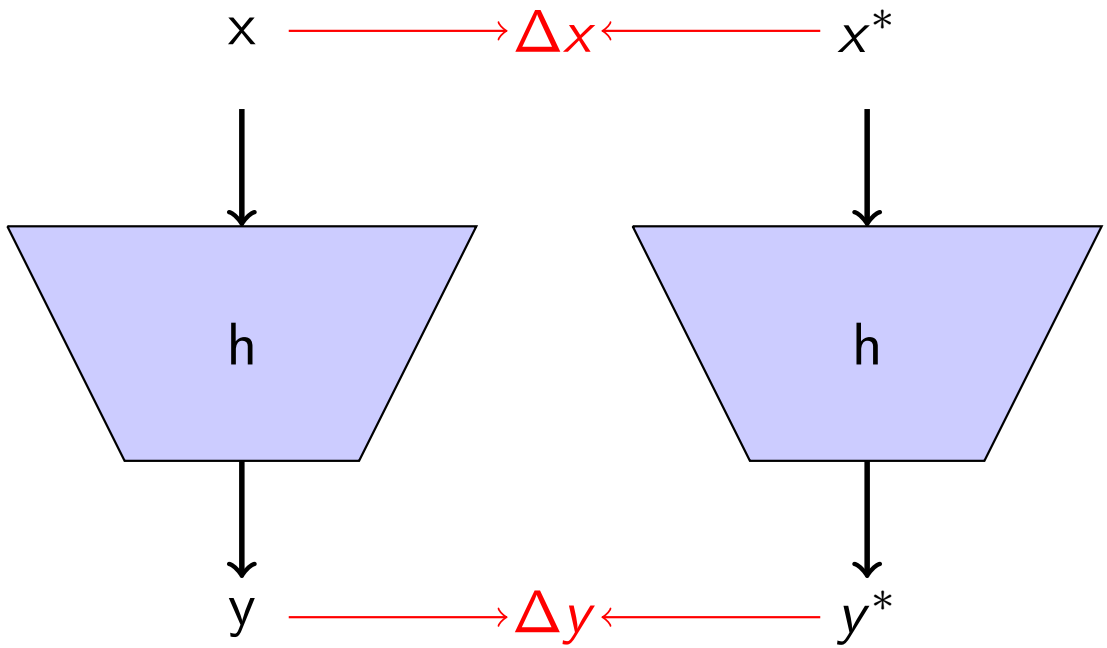
The Keccak-f function

- 24 rounds
- Each round is composed of five steps $\theta, \rho, \pi, \chi, \iota$.
- Only XOR, AND, NOT and data-independent rotations are used.

One round of Keccak-f:



Differential Cryptanalysis



- $\Delta x \neq 0$ and $\Delta y = 0$ gives a collision.
- Find a differential characteristic leading to zero output difference.
- Find a confirming message pair.

Related Work

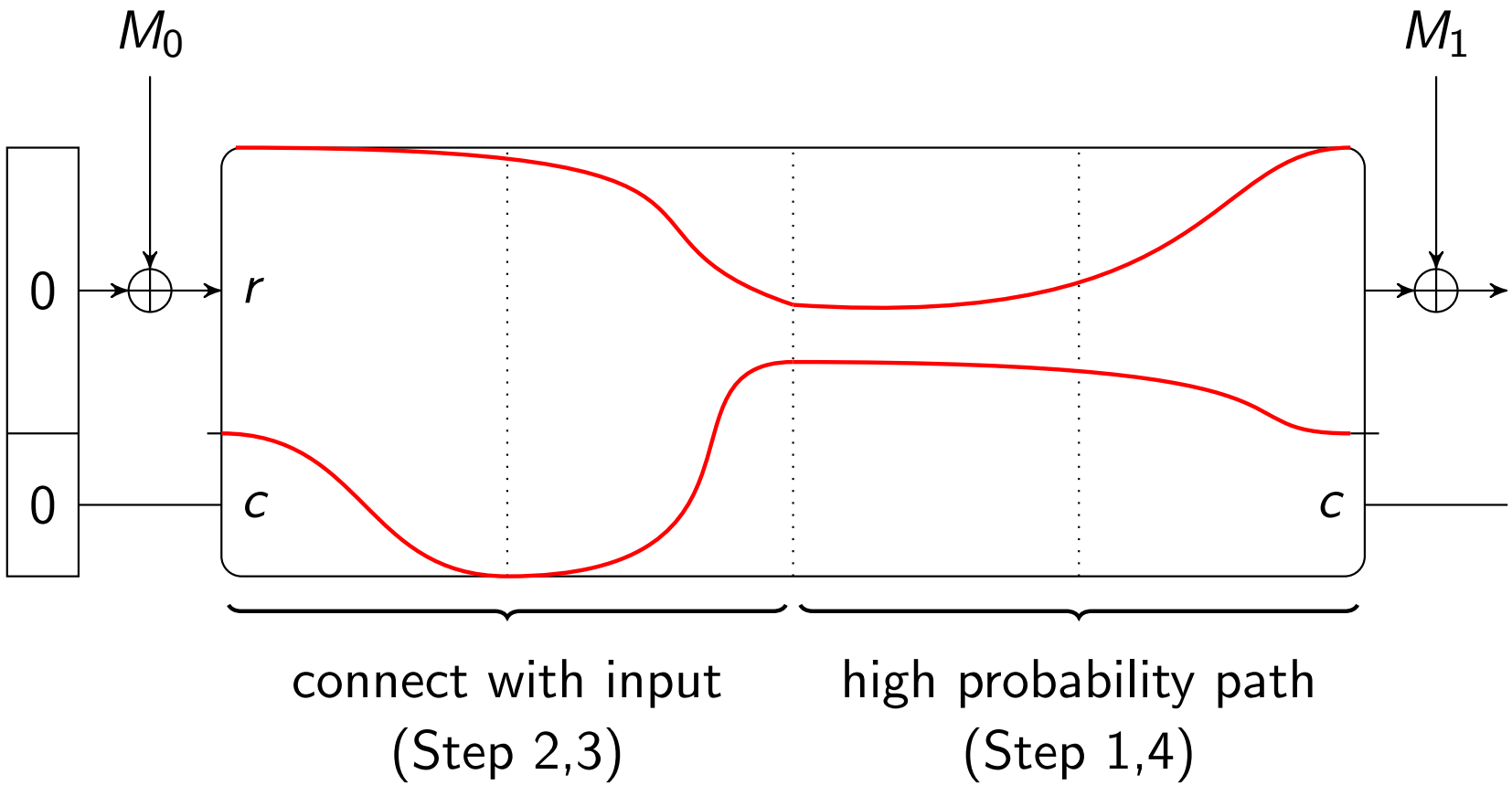
Attack by Naya-Plasencia et al.

- A 2-round practical attack using high probability paths [NPRM11].

Attack by Dinur et al.

- A 4-round practical attack on Keccak-224/256 by using the same high probability path [DDS12].
- Theoretical attacks on 5-round Keccak-256, 4-round Keccak-384 and 3-round Keccak-512 [DDS13].
- Connect to the starting point using an algebraic method.

Attack Strategy



Attack Strategy

Finding the high probability paths

- Using linearized model of Keccak
- Gives a linear code over $\mathbb{F}_2$
- Probability that characteristic holds related to the Hamming weight
- Find codewords with low Hamming weight[1]

Gives us high probability paths leading to (internal) collisions for different Keccak variants.

[1] `http://www.iaik.tugraz.at/content/research/krypto/codingtool/`

Connecting the paths

Using an automatic search tool to connect the path to the start.

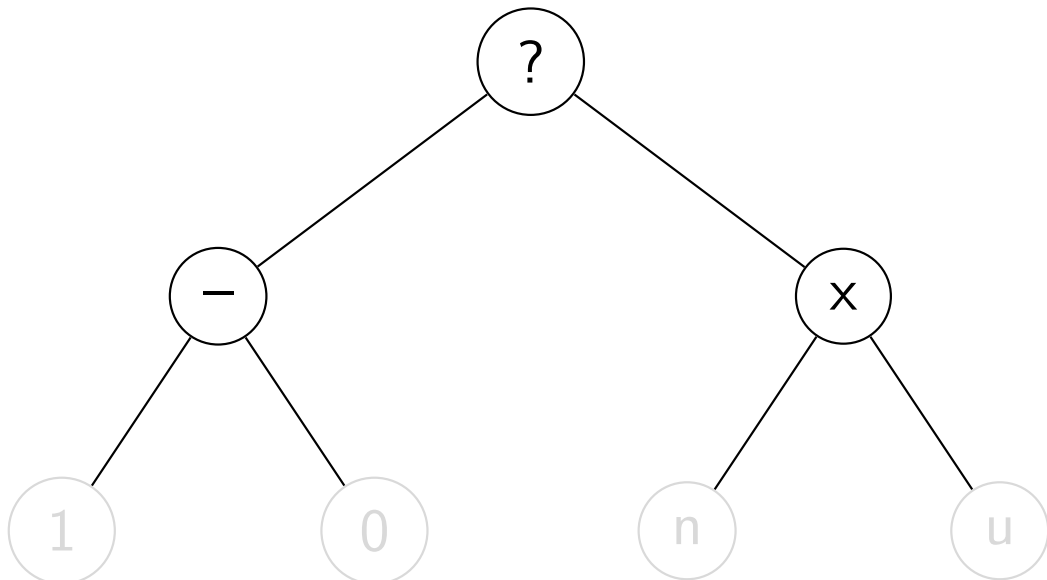
- Used for instance on SHA-2 [MNS11][MNS13].
- Guess and determine strategy.

(X_i, X_i')	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓			✓
x		✓	✓	
0	✓			
u		✓		
n			✓	
1				✓
⋮				

Connecting the paths

Search Algorithm [DR06][MNS11]

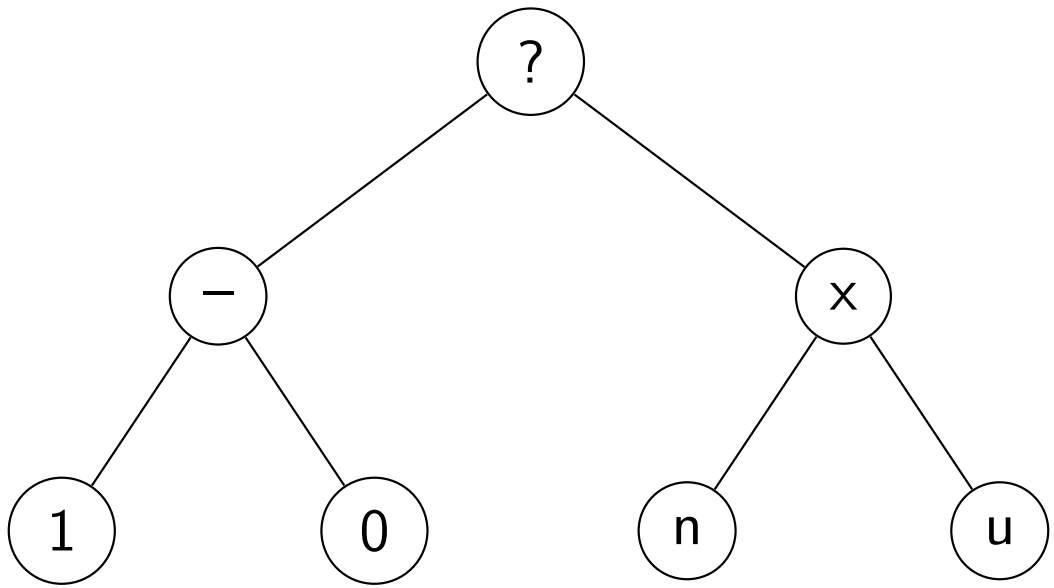
1. **Decision:** Select bit to guess.
2. **Deduction:** Propagate conditions [EMN+13].
3. **Backtracking:** Resolve contradictions.



Connecting the paths

Search Algorithm [DR06][MNS11]

1. **Decision:** Select bit to guess.
2. **Deduction:** Propagate conditions [EMN$^+$13].
3. **Backtracking:** Resolve contradictions.



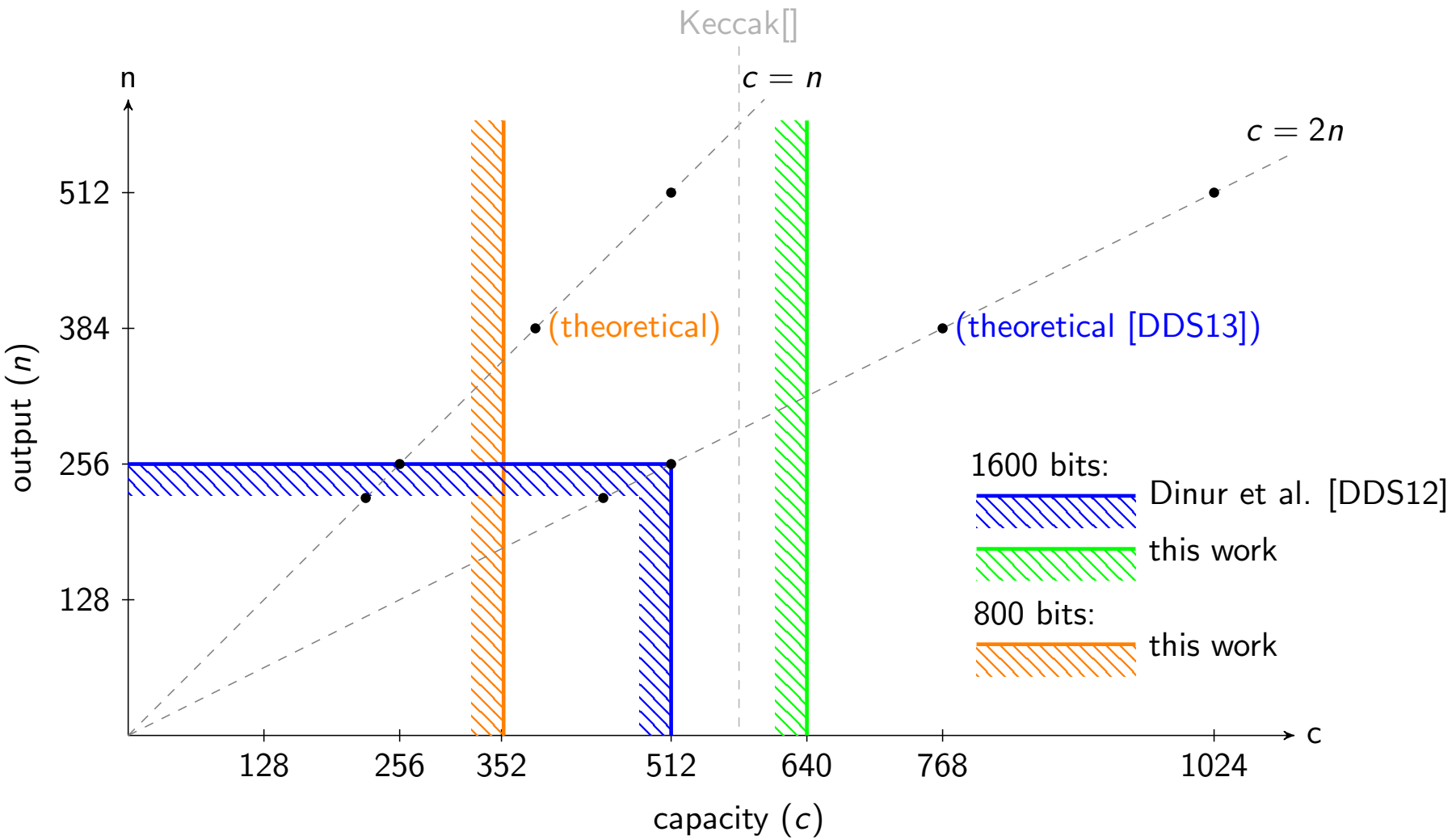
Example

State

737bc39f15b62ce3	4-ae-67d9-f67961	72c17e19ecf12b7b	2ba7b749c7949634	fc-cfc935859fb2e
3d196398efcd8-85	fce83de1dec57822	585c3e88-e91a216	7abfed54f57e1dd9	d9a96ed7944d8ede
147b6be6e6-24fdb	--4a7743-1159181	-1df19ab97369543	77a1e8bca7-c--6f	-5e697e1852d7fd5
1a9b2c7d9b5a9abf	2913f4ef6ca6b829	4--b84511febc4ff	236c8edaa59db4a3	fa16a175b84e4326
6c34feb1242754fb	cb2ea33a4c-db176	b2c5aa5a8-df6238	7bafafd7ee121941	8b4cf1f55781e-9f
96--3182f1fad467	22--9-644fa7e-f-	de--54fb5f2e9a6b	7e--726f824-bd4c	d2--114a6bb11583
96-171-2f1fad467	26--9-644fa7e-f-	de--54fb5f2e9a6b	7e--726f8244b14c	d2--114a6fb51583
96-17112f1fad467	22--b-244fa7e-f-	de--54fb5f2e9a4b	7e--726f8244b14c	d2--114a6bb11583
96-171-2f1fad467	26--9-644fa7e-f2	de--54fb5f2e9a6b	7e--726f884-b14c	d2--114a6bb11583
96-171-2f1fad467	22--9-644fa7e-f-	da--5-fb5f2e9a6b	fe--726f8244b14c	d2--114a6ab11583
----4-8---------	------4---------	---1------------	----------------	----------------
----4-8---------	------4---------	----------------	----------------	--8-------------
----------------	----------------	----------------	----------------	----------------
----------------	----------------	---1------------	----------------	--8-------------
----------------	----------------	----------------	----------------	----------------
----4-8---------	----------4-----	----------------	----------------	----------------
----------------	------------8---	----------------	----------------	----------------
------8---------	----------------	----------------	8---------------	----------------
----------------	----------4-8---	----------------	8---------------	----------------
----4-----------	----------------	----------------	----------------	----------------
----4-8---------	--8-------------	----------1-----	------8---1-----	--8-4-----------
----------------	-1---4----------	-----4----------	81--------------	----------------
---------1-8----	----------------	---------1-----1	---------------1	---------------1
----------------	----------------	----------------	----------------	----------------
----------------	----------------	----------------	----------------	----------------

Overview

4-round attacks on Keccak



Conclusion

Results:

- 4-round practical attack on different Keccak variants.
- New method to connect paths to the starting point.
- High probability paths for new variants of Keccak
- Internal collisions for these variants

Thank you for your attention!

References I


Itai Dinur, Orr Dunkelman, and Adi Shamir, *New Attacks on Keccak-224 and Keccak-256*, FSE (Anne Canteaut, ed.), LNCS, vol. 7549, Springer, 2012, pp. 442–461.


_____, *Collision Attacks on Up to 5 Rounds of SHA-3 Using Generalized Internal Differentials*, FSE (Shiho Moriai, ed.), LNCS, Springer, 2013, to appear.


Christophe De Cannière and Christian Rechberger, *Finding SHA-1 Characteristics: General Results and Applications*, ASIACRYPT (Xuejia Lai and Kefei Chen, eds.), LNCS, vol. 4284, Springer, 2006, pp. 1–20.


Maria Eichlseder, Florian Mendel, Tomislav Nad, Vincent Rijmen, and Martin Schläffer, *Linear Propagation in Efficient Guess-and-Determine Attacks*, WCC (Lilya Budaghyan, Tor Helleseth, and Matthew G. Parker, eds.), 2013, `http://www.selmer.uib.no/WCC2013/`.

References II


Florian Mendel, Tomislav Nad, and Martin Schläffer, *Finding SHA-2 Characteristics: Searching through a Minefield of Contradictions*, ASIACRYPT (Dong Hoon Lee and Xiaoyun Wang, eds.), LNCS, vol. 7073, Springer, 2011, pp. 288–307.


_____, *Improving Local Collisions: New Attacks on Reduced SHA-256*, EUROCRYPT (Thomas Johansson and Phong Q. Nguyen, eds.), LNCS, vol. 7881, Springer, 2013, pp. 262–278.


María Naya-Plasencia, Andrea Röck, and Willi Meier, *Practical Analysis of Reduced-Round Keccak*, INDOCRYPT (Daniel J. Bernstein and Sanjit Chatterjee, eds.), LNCS, vol. 7107, Springer, 2011, pp. 236–254.