New Results on the SymSum Distinguisher on Round-Reduced SHA3.

Sahiba Suryawanshi, Dhiman Saha, Satyam Sachan

de.ci.phe.red LAB
Indian Institute of Technology Bhilai

AFRICACRYPT 2020

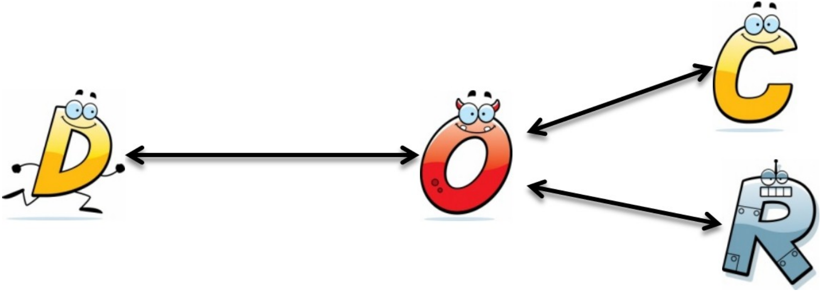
The Problem

To distinguish

What and Why?

Distinguishers exhibit non-random behaviour

1. "D" tries to distinguish between C and R
2. Can make queries to O
3. O behaves as either C or R
4. At the end "D" has to guess who is O impersonating
5. "D" wins if its guess is right



The Target

Which crypto primitive are we looking at?

Cryptographic Hash Functions

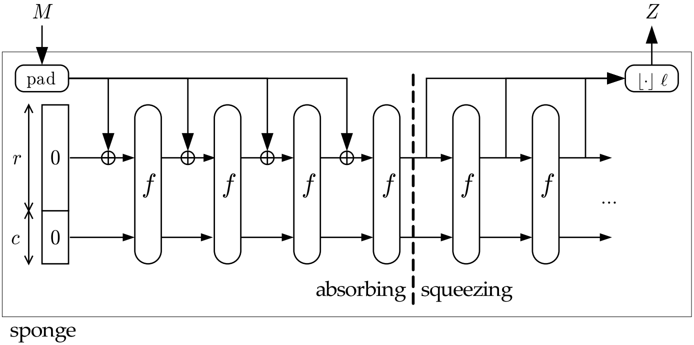
SHA-3

Basics

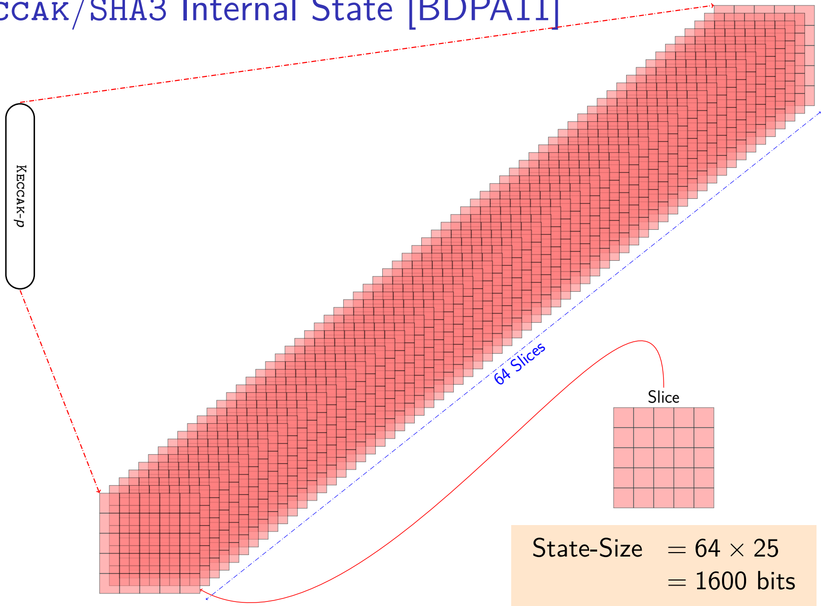
- Follows SPONGE construction [BDPA]
- Internal permutation called KECCAK-f/KECCAK-p
- SHA3 Family

Fixed-Length $\rightarrow$ SHA3-224/256/384/512

XOF $\rightarrow$ SHAKE128/256

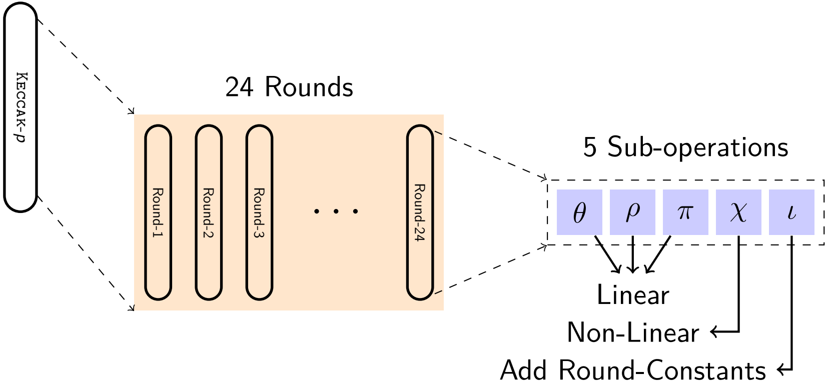


Keccak/SHA3 Internal State [BDPA11]



State-Size $= 64 \times 25$
$= 1600$ bits

Inside KECCAK-p Permutation



Round Constants added to destroy symmetry

Distinguishers Based on Higher Order Boolean Derivatives

The Strategy

What is a Boolean Derivative? [PS04]

- Boolean function of n variables:

$$f(\mathbf{x}) = f(x_1, x_2, \cdots, x_i, \cdots, x_n)$$

Boolean Derivative

Captures change in the function w.r.t change in a variable

$$\frac{\partial f(\mathbf{x})}{\partial x_i} = f(x_1, x_2, \cdots, x_i = 0, \cdots, x_n) \bigoplus f(x_1, x_2, \cdots, x_i = 1, \cdots, x_n)$$

[PS04] C. Posthoff and B. Steinbach. *Logic functions and equations. Binary models for computer science.*

Computing the derivative

Example (ANF-Unknown)

$$f(x_1, \cdots, x_6) \equiv \texttt{Algorithm Known}$$

$$\frac{\partial f(\mathbf{x})}{\partial x_3} = \left[f(\mathbf{x})_{x_3=0} \oplus f(\mathbf{x})_{x_3=1}\right]$$

Where, $\{x_1, x_2, x_4, x_5, x_6\} = \mathbf{const} \in \{0,1\}^5$

Note that the free variables take a constant value

Example (Higher Order Derivative)

$$\frac{\partial^2 f(\mathbf{x})}{\partial x_2 \partial x_3} = \left[f(\mathbf{x})_{x_2=0,x_3=0}\right] \oplus \left[f(\mathbf{x})_{x_2=0,x_3=1}\right] \oplus \left[f(\mathbf{x})_{x_2=1,x_3=0}\right] \oplus \left[f(\mathbf{x})_{x_2=1,x_3=1}\right]$$

Where, $\{x_1, x_4, x_5, x_6\} = \mathbf{const} \in \{0,1\}^4$

Simple Vs Vectorial Derivatives

$$\text{Simple} \rightarrow \frac{\partial f(\mathbf{x})}{\partial x_i}$$

$$\text{Vectorial} \rightarrow \frac{\partial f(\mathbf{x})}{\partial \mathbf{x_i}}$$

- Here $x_i \equiv$ Single Variable
- x_i takes two values 0 and 1

- Here $\mathbf{x_i} \equiv$ Multiple variables
- $\mathbf{x_i}$ also takes two values

Example (Computing Vec. Derivative)

- Let $\mathbf{x_i} = \{x_1, x_2\}$, Then

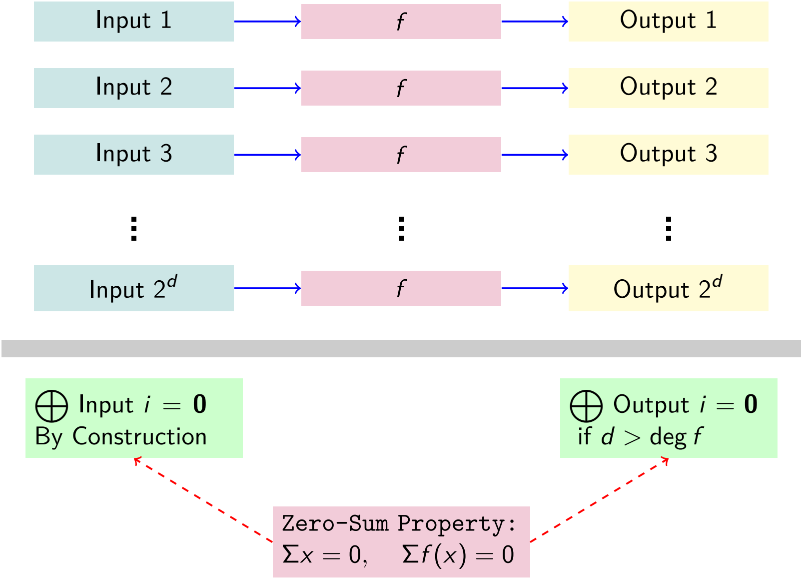
$$\frac{\partial f(\mathbf{x})}{\partial \mathbf{x_i}} = \left[f(\mathbf{x})_{\mathbf{x_i} \in \{0,1\}^2} \oplus f(\mathbf{x})_{\mathbf{x_i} = \overline{\mathbf{x_i}}} \right]$$

Where, other vars = **const**

0	0
0	1
1	0
1	1

- Say $\mathbf{x_i} \leftarrow \{0,1\}$ Compute $f(\mathbf{x})$ with $\mathbf{x_i} = \{0,1\}$ & $\mathbf{x_i} = \{1,0\}$

Zero-Sum Distinguisher



A new result on SHA3 [SKC16] IACR ToSC'16

Author's Prove

Round-constant dependent monomials **never** reach highest degree.

More precisely,

$$\deg \mathit{terms}_{rc} \le (\deg \mathtt{SHA3} - \deg \chi)$$

Implications for SHA3: $\deg \chi = 2$

$(d-1)^{th}$ order derivative of SHA3 $\Longrightarrow$ rc-independent function

$\Downarrow$

Preserves Symmetry

How to exploit this?

A new result on SHA3 [SKC16] IACR ToSC'16

Author's Prove

Round-constant dependent monomials **never** reach highest degree.

More precisely,

$$\deg \mathit{terms}_{rc} \leq (\deg \mathtt{SHA3} - \deg \chi)$$

Implications for SHA3: $\deg \chi = 2$

$(d-1)^{th}$ order derivative of SHA3 $\Longrightarrow$ rc-independent function

$\Downarrow$

Preserves Symmetry

How to exploit this?

Lemma

*For an iterated SPN round function ($\mathcal{G}$) if the ordering of the component transformations is such that the non-linear operation **precedes** the round constant addition, then highest-degree monomials are "**not affected**" by round-constants.*

$$\begin{aligned}\mathcal{G}^q &= (\mathcal{C}_q \circ \mathcal{N} \circ \mathcal{L}) \circ (\mathcal{C}_{q-1} \circ \mathcal{N} \circ \mathcal{L}) \circ \cdots \circ (\mathcal{C}_2 \circ \mathcal{N} \circ \mathcal{L}) \circ (\mathcal{C}_1 \circ \mathcal{N} \circ \mathcal{L}) \\ &= \Big[((\mathcal{C}_q \circ \mathcal{N} \circ \mathcal{L}) \circ \cdots \circ (\mathcal{C}_2 \circ \mathcal{N} \circ \mathcal{L})) \circ \mathcal{C}_1\Big] \circ (\mathcal{N} \circ \mathcal{L}) \qquad (1)\end{aligned}$$

Intuition

Notice effect of the first round non-linear operation

Proof Idea

- Segregate monomials in ANF based on dependence on round-constants

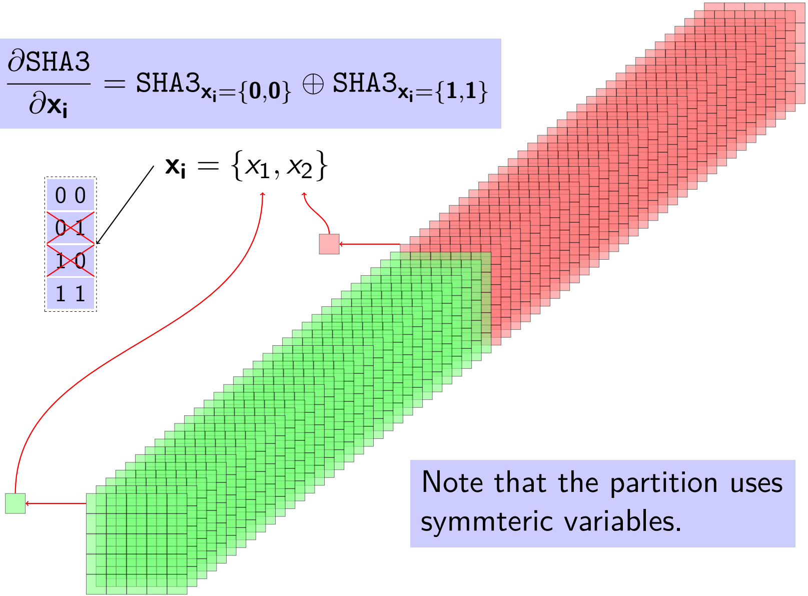
Example

$$
\begin{aligned}
f &= x_1x_2x_3 + c_1c_2x_2x_3 + x_3x_4 + c_2c_3 \\
&= (x_1x_2x_3 + x_3x_4) + (c_1c_2x_2x_3 + c_2c_3) \\
&= f_s + f_{s'}
\end{aligned}
$$

- Show difference in highest-degree attained

Special Vectorial Derivative of SHA3 [SKC16]

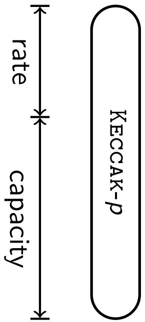
$$\frac{\partial \mathtt{SHA3}}{\partial \mathbf{x_i}} = \mathtt{SHA3}_{\mathbf{x_i}=\{\mathbf{0,0}\}} \oplus \mathtt{SHA3}_{\mathbf{x_i}=\{\mathbf{1,1}\}}$$



Note that the partition uses symmteric variables.

Self-Symmetric Inputs In Practice [SKC16] SHA3-512

8cd812d28cd812d2
****0*9b****0*9b
0000000000000000



Zeros at end indicate value of capacity bits

4a36ea584a36ea58	8cd812d28cd812d2	88e61fc788e61fc7	f3372eaff3372eaf	ea3f0b51ea3f0b51
ce168c02ce168c02	****0*9b****0*9b	b934cb9fb934cb9f	866ac262866ac262	0000000000000000
0000000000000000	0000000000000000	0000000000000000	0000000000000000	0000000000000000
0000000000000000	0000000000000000	0000000000000000	0000000000000000	0000000000000000
0000000000000000	0000000000000000	0000000000000000	0000000000000000	0000000000000000

Experimental Results [SKC16] 4-Round SHA3-512

|MsgSet|	Output-Sum	Remark

2^{17}	`000000000000000000000000000000000000000000000000`
	`000000000000000000000000000000000000000000000000`
	`00000000000000000000000000000000`
		Zero-Sum

Experimental Results [SKC16] 4-Round SHA3-512

$\lvert$MsgSet$\rvert$	Output-Sum	Remark
2^{17}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{16}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum

Experimental Results [SKC16] 4-Round SHA3-512

|MsgSet|	Output-Sum	Remark
2^{17}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{16}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{15}	000001000000010000000000000000000000200000002000 000000000000000000000000000000000000000000000000 00000000000000000000004000000040	Symmetric-Sum

Experimental Results [SKC16] 4-Round SHA3-512

|MsgSet|	Output-Sum	Remark
2^{17}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{16}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{15}	000001000000010000000000000000000000200000002000 000000000000000000000000000000000000000000000000 00000000000000000000004000000040	Symmetric-Sum
2^{14}	243f4942243f4942528c98d5528c98d57300b0d17300b0d1 c0585999c0585999147b20a3147b20a3083a3900083a3900 09225588092255886302671c6302671c	Symmetric-Sum

Experimental Results [SKC16] 4-Round SHA3-512

|MsgSet|	Output-Sum	Remark
2^{17}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{16}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{15}	000001000000010000000000000000000000200000002000 000000000000000000000000000000000000000000000000 00000000000000000000004000000040	Symmetric-Sum
2^{14}	243f4942243f4942528c98d5528c98d57300b0d17300b0d1 c0585999c0585999147b20a3147b20a3083a3900083a3900 092255880922558863026 71c6302671c	Symmetric-Sum
2^{13}	81ed3fca81ed3dca15553dac15553dec25858e1125858e11 11c9af8b11c9af8b509927bf5099273f9276901992679019 ca92a3d5ca9223d54ffce7974ffc6797	Not Symmetric

Experimental Results [SKC16] 4-Round SHA3-512

|MsgSet|	Output-Sum	Remark
2^{17}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{16}	000000000000000000000000000000000000000000000000 000000000000000000000000000000000000000000000000 00000000000000000000000000000000	Zero-Sum
2^{15}	000001000000010000000000000000000000200000002000 000000000000000000000000000000000000000000000000 00000000000000000000004000000040	Symmetric-Sum
2^{14}	243f4942243f4942528c98d5528c98d57300b0d17300b0d1 c0585999c0585999147b20a3147b20a3083a3900083a3900 09225588092255886302671c6302671c	Symmetric-Sum
2^{13}	81ed3fca81ed3dca15553dac15553dec25858e1125858e11 11c9af8b11c9af8b509927bf5099273f9276901992679019 ca92a3d5ca9223d54ffce7974ffc6797	Not Symmetric
2^{12}	78f523d01479a153802f16a4c8bbb67116d502ea0495823a 71057dfbf18b25f22bba947d0ba094fd1240ee380a42df38 99eaa56698fa64e6a21ac1328138c126	Not Symmetric

Comparison with ZeroSum [SKC16]

		Complexity	
#Rounds (n_r)	Bound on d°SHA3	ZeroSum ($2^{d^\circ \mathtt{SHA3}+1}$)	SymSum ($2^{d^\circ \mathtt{SHA3}-1}$)
1	2	2^3	2^1
2	4	2^5	2^3
3	8	2^9	2^7
4	16	2^{17}	2^{15}
5	32	2^{33}	2^{31}
6	64	2^{65}	2^{63}
7	128	2^{129}	2^{127}
8	256	2^{257}	2^{255}
9	512	2^{513}	$2^{511\dagger}$
10	1024	$2^{1025\dagger}$	$\star$
11	1408 (*Boura et al.*)	$\star$	$\star$

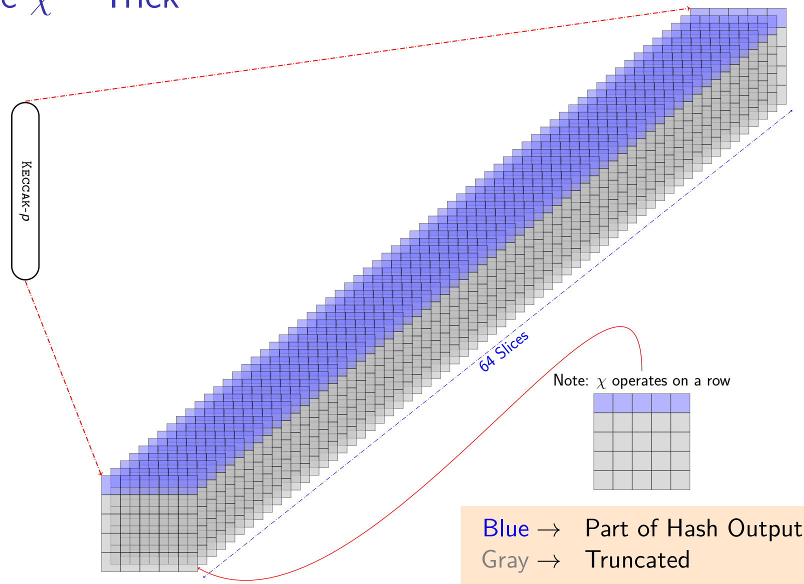
† Not applicable for SHA3-512 and SHA3-384

$\star$ Exceeds degrees of freedom

Can we do better?

Our Motivation

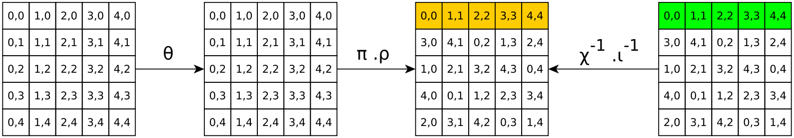
The χ^{-1} Trick



Blue $\rightarrow$ Part of Hash Output
Gray $\rightarrow$ Truncated

For Hash length $\geq$ 320-bits

Extending SymSum by applying χ^{-1} trick



Very simple idea:

- Invert the hash output for two operations:
- ι^{-1} followed by χ^{-1}
- Verify SymSum property
- Gives advantage of one-round
- Not applicable for SHA3-224/256

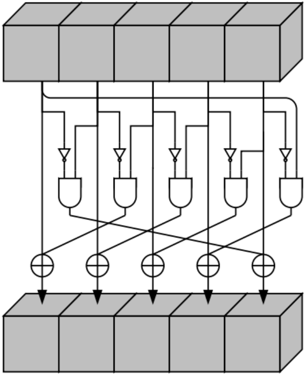
Linear Structures [GLS16]

- Introduced by Guo et al. in ASIACRYPT 2016
- For KECCAK-p permutation
- Basically a lane-wise restriction on the input space
- To handle the linear θ and non-linear χ operations of the round function

χ Mapping

Primary observation

If two consecutive variables never come together in a row then, then all output co-ordinate functions of χ become linear.



$$b \leftarrow \chi(a)$$

$$b_0 = a_0 \oplus (a_1 \oplus 1) \cdot a_2$$

$$b_1 = a_1 \oplus (a_2 \oplus 1) \cdot a_3$$

$$b_2 = a_2 \oplus (a_3 \oplus 1) \cdot a_4$$

$$b_3 = a_3 \oplus (a_4 \oplus 1) \cdot a_0$$

$$b_4 = a_4 \oplus (a_0 \oplus 1) \cdot a_1$$

Linearization of χ Mapping

$$a \to \chi \to b$$

$$b_0 = a_0 \oplus (a_1 \oplus 1) \cdot a_2$$

$$b_1 = a_1 \oplus (a_2 \oplus 1) \cdot a_3$$

$$b_2 = a_2 \oplus (a_3 \oplus 1) \cdot a_4$$

$$b_3 = a_3 \oplus (a_4 \oplus 1) \cdot a_0$$

$$b_4 = a_4 \oplus (a_0 \oplus 1) \cdot a_1$$

Let $a = 0a_1000$

$$\begin{aligned} b_0 &= 0 \\ b_1 &= a_1 \oplus 0 \\ b_2 &= 0 \\ b_3 &= 0 \\ b_4 &= 0 \oplus a_1 \end{aligned}$$

Linearization of χ Mapping

If $a = 0a_1a_2 00$

$$\begin{aligned} b_0 &= 0 \oplus (a_1 \oplus 1) \cdot a_2 \\ b_1 &= a_1 \oplus 0 \\ b_2 &= a_2 \oplus 0 \\ b_3 &= 0 \\ b_4 &= 0 \oplus a_1 \end{aligned}$$

Linearization Fails!

If $a = 0a_1 0a_3 0$

$$\begin{aligned} b_0 &= 0 \\ b_1 &= a_1 \oplus a_3 \\ b_2 &= 0 \\ b_3 &= 0 \\ b_4 &= a_3 \oplus a_1 \end{aligned}$$

Linearization Succeeds!

Linearization of χ Mapping

If $a = 0a_1a_2 00$

$$\begin{aligned} b_0 &= 0 \oplus (a_1 \oplus 1) \cdot a_2 \\ b_1 &= a_1 \oplus 0 \\ b_2 &= a_2 \oplus 0 \\ b_3 &= 0 \\ b_4 &= 0 \oplus a_1 \end{aligned}$$

Linearization Fails!

If $a = 0a_1 0 a_3 0$

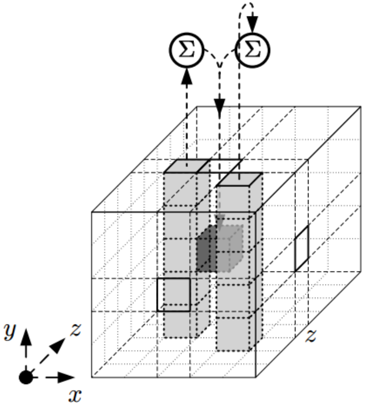
$$\begin{aligned} b_0 &= 0 \\ b_1 &= a_1 \oplus a_3 \\ b_2 &= 0 \\ b_3 &= 0 \\ b_4 &= a_3 \oplus a_1 \end{aligned}$$

Linearization Succeeds!

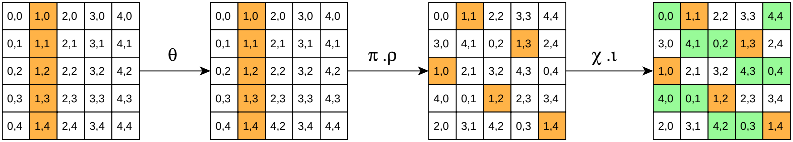
θ Mapping

Primary Observation

- θ relies on the **column parity** of spatially adjacent columns
- Does not diffuse the state if column parity is constants across calls to Keccak$-p$.



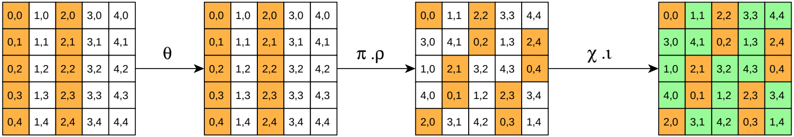
- KECCAK state configuration for 1-round linearization
- Degrees of freedom 256
- More such configurations possible



- Restrictions on the input space:

$$A[1,0] \oplus A[1,1] \oplus A[1,2] \oplus A[1,3] \oplus A[1,4] = \alpha_1$$

- Another example
- Degrees of freedom 512



white $\rightarrow$ Constants
Orange $\rightarrow$ Linear variable
Green $\rightarrow$ Variable that has at most degree 1

- Restrictions on the input space:

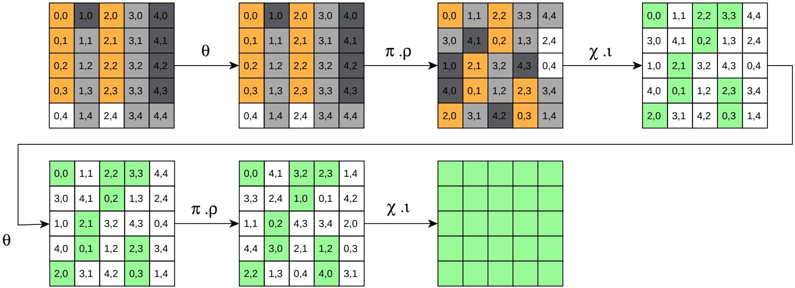
$$A[0,0] \oplus A[0,1] \oplus A[0,2] \oplus A[0,3] \oplus A[0,4] = \alpha_1$$

$$A[2,0] \oplus A[2,1] \oplus A[2,2] \oplus A[2,3] \oplus A[2,4] = \alpha_2$$

Linear Structures [GLS16] Two-rounds

- KECCAK state configuration for 2-round linearization
- Degrees of freedom 256

Lightgray → Zero
Darkgray → One
Orange → Linear variable
Green → Variable that has at most degree 1



Linear Structures [GLS16]

$$\begin{aligned} A[0,0] \oplus A[0,1] \oplus A[0,2] \oplus A[0,3] &= \alpha_1 \\ A[2,0] \oplus A[2,1] \oplus A[2,2] \oplus A[2,3] &= \alpha_2 \end{aligned}$$

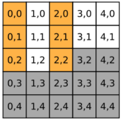
$$\begin{aligned} A[2,0]_{\lll 62} &= A[0,0] \oplus A[2,2]_{\lll 43} \\ A[2,1]_{\lll 6} &= S[0,1]_{\lll 36} \oplus A[2,3]_{\lll 15} \\ A[2,2]_{\lll 43} &= A[0,2]_{\lll 3} \\ A[2,3]_{\lll 15} &= A[0,3]_{\lll 41} \oplus A[2,0]_{\lll 62} \end{aligned}$$

- Adapt Linear structures on the hash function
- Introduce self-symmetry constraint
- Extend SymSum distinguisher to 1-round
  - Applying 1-round Linearization or
  - χ^{-1} trick
- Extend SymSum distinguisher up to 2-rounds
  - Applying 1-round Linearization and χ^{-1} trick
  - Applying 2-round Linearization
- Extend SymSum distinguisher up to 3-rounds
  - Applying 2-round Linearization and χ^{-1} trick

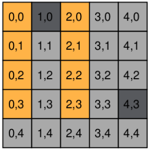
Adapting Linear structures on the hash function 1 Round

Variant	Slice Configuration	Restrictions on variables	Degree of Freedom
SHAKE128		$A[0,4] = \alpha_1 \oplus \sum_{i=0}^{3} A[0,i]$ $A[j,3] = \alpha_2 \oplus \sum_{i=0}^{2} A[j,i] \quad (j \in \{2,3\})$	2^{224}
SHAKE256		$A[0,3] = \alpha_1 \oplus \sum_{i=0}^{2} A[0,i]$ $A[j,2] = \alpha_2 \oplus \sum_{i=0}^{1} A[j,i] \quad (j \in \{2,3\})$	2^{160}
SHA3-224		$A[0,3] = \alpha_1 \oplus \sum_{i=0}^{2} A[0,i]$ $A[2,3] = \alpha_2 \oplus \sum_{i=0}^{2} A[2,i]$	2^{192}

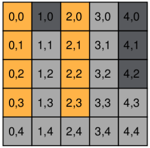
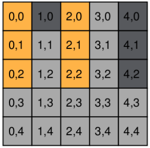
Adapting Linear structures on the hash function   1 Round

Variant	Slice Configuration	Restrictions on variables	Degree of Freedom
SHA3-256		$A[0,3] = \alpha_1 \oplus \sum_{i=0}^{2} A[0,i]$ $A[j,2] = \alpha_2 \oplus \sum_{i=0}^{1} A[j,i] \quad (j \in \{2,3\})$	2^{160}
SHA3-384		$A[0,2] = \alpha_1 \oplus \sum_{i=0}^{1} A[0,i]$ $A[2,2] = \alpha_2 \oplus \sum_{i=0}^{1} A[2,i]$	2^{128}
SHA3-512		$A[0,1] = \alpha_1 \oplus A[0,0]$ $A[j,1] = \alpha_2 \oplus A[j,0] \quad (j \in \{2,3\})$	2^{64}

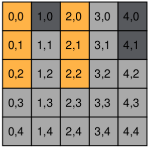
Adapting Linear structures on the hash function   2 Round

Variant	Slice Configuration	Restrictions on variables	Degree of Freedom
SHAKE128		$A[0,0] \oplus A[0,1] \oplus A[0,2] \oplus A[0,3] = \texttt{0xff...f}$ $A[2,0] \oplus A[2,1] \oplus A[2,2] \oplus A[2,3] = \texttt{0xff...f}$ $A[2,0]_{\lll 30} = A[0,0] \oplus A[2,2]_{\lll 11}$ $A[2,1]_{\lll 6} = A[0,1]_{\lll 4} \oplus A[2,3]_{\lll 15}$ $A[2,2]_{\lll 11} = A[0,2]_{\lll 3}$ $A[2,3]_{\lll 15} = A[0,3]_{\lll 9} \oplus A[2,0]_{\lll 30}$	2^{64}
SHAKE256		$A[i,0] \oplus A[i,1] \oplus A[i,2] = 0, \quad i = 0,2$ $A[2,0]_{\lll 30} = A[0,0] \oplus A[2,2]_{\lll 11}$ $A[2,1]_{\lll 6} = A[0,1]_{\lll 4}$ $A[2,2]_{\lll 11} = A[0,2]_{\lll 3}$	2^{32}

Adapting Linear structures on the hash function   2 Round

Variant	Slice Configuration	Restrictions on variables	Degree of Freedom
SHA3-224		$A[0,0] \oplus A[0,1] \oplus A[0,2] \oplus A[0,3] = A[0,4] \oplus 0$ $A[2,0] \oplus A[2,1] \oplus A[2,2] \oplus A[2,3] = 0$ $A[2,0]_{\lll 30} = A[0,0] \oplus A[2,2]_{\lll 11}$ $A[2,1]_{\lll 6} = A[0,1]_{\lll 4} \oplus A[2,3]_{\lll 15}$ $A[2,2]_{\lll 11} = A[0,2]_{\lll 3}$ $A[2,3]_{\lll 15} = A[0,3]_{\lll 9} \oplus A[2,0]_{\lll 30}$	2^{64}
SHA3-256		$A[i,0] \oplus A[i,1] \oplus A[i,2] = 0, \quad i = 0,2$ $A[2,0]_{\lll 30} = A[0,0] \oplus A[2,2]_{\lll 11}$ $A[2,1]_{\lll 6} = A[0,1]_{\lll 4}$ $A[2,2]_{\lll 11} = A[0,2]_{\lll 3}$	2^{32}

Adapting Linear structures on the hash function 2 Round

<table>
<tr><th>Variant</th><th>Slice Configuration</th><th>Restrictions on variables</th><th>Degree of Freedom</th></tr>
<tr><td>SHA3-384</td><td>
</td><td>$A[i,0] \oplus A[i,1] \oplus A[i,2] = 0, \quad i = 0, 2$
$A[2,0]_{\lll 30} = A[0,0] \oplus A[2,2]_{\lll 11}$
$A[2,1]_{\lll 6} = A[0,1]_{\lll 4}$
$A[2,2]_{\lll 11} = A[0,2]_{\lll 3}$</td><td>$2^{32}$</td></tr>
</table>

Adding Self-Symmetry to Linear Strucrture   For 1 Round

$$A[0,0] \oplus A[0,1] \oplus A[0,2] \oplus A[0,3] \oplus A[0,4] = \alpha_1$$

$$A[2,0] \oplus A[2,1] \oplus A[2,2] \oplus A[2,3] = \alpha_2$$

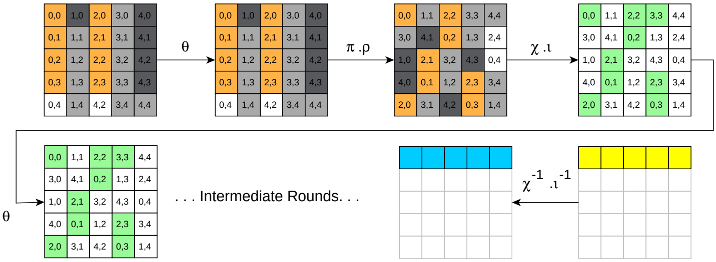
$$A[x,y,i] = A[x,y,i+32] \text{ where } i \in \{1,2\ldots 32\}$$

Adding Self-Symmetry to Linear Strucrture For 2 Round

$$\begin{aligned} A[0,0] \oplus A[0,1] \oplus A[0,2] \oplus A[0,3] &= \alpha_1 \\ A[2,0] \oplus A[2,1] \oplus A[2,2] \oplus A[2,3] &= \alpha_2 \end{aligned}$$

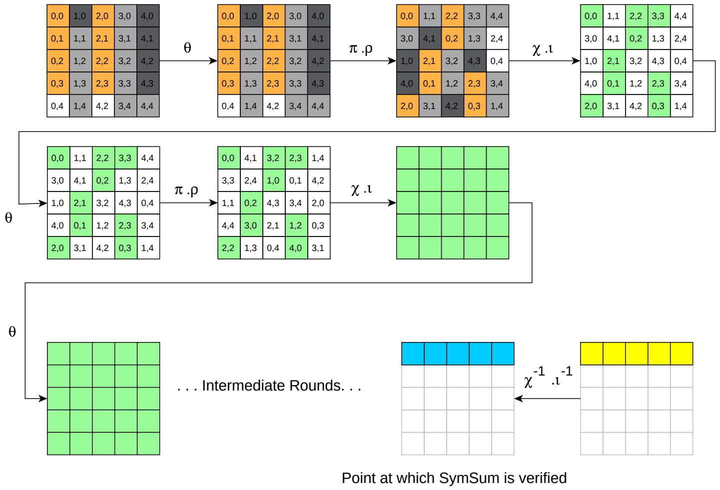
$$\begin{aligned} A[x,y,i] &= A[x,y,i+32] \text{ where } i \in \{1,2\ldots 32\} \\ A[2,0]_{\lll 30} &= A[0,0] \oplus A[2,2]_{\lll 11} \\ A[2,1]_{\lll 6} &= S[0,1]_{\lll 4} \oplus A[2,3]_{\lll 15} \\ A[2,2]_{\lll 11} &= A[0,2]_{\lll 3} \\ A[2,3]_{\lll 15} &= A[0,3]_{\lll 9} \oplus A[2,0]_{\lll 30} \end{aligned}$$

Extending SymSum 2 Rounds By 1-round Linearization and χ^{-1} trick



Point at which SymSum is verified

Extending SymSum 3 Rounds By 2-round Linearization and χ^{-1} trick



Effect of linearization on SymSum

- Classical SymSum has advantage of **4** in term of size of msgset over ZeroSum
- SymSum after applying Linearization has advantage of **2** in term of size of msgsetover ZeroSum

Observation

SymSum advantage no longer depend on degree of Non-Linear component χ

Effect of linearization on SymSum

Lemma

For any SPN round function $\mathcal{G}$ iterated for n_r rounds, if $l_r (\leq n_r)$ rounds are linearized, the degrees of the linearized version $(\mathbb{G})$ and nonlinearized versions $(\mathbb{G}')$ are related by the degree (λ) of the non-linear component function by the following relation:

$$d^\circ \mathbb{G} \leq \lambda^{l_r} \times d^\circ \mathbb{G}' \quad \textit{where} \quad \begin{cases} \mathbb{G} = \mathcal{G}^{n_r} \\ \mathbb{G}' = \mathcal{G}^{n_r - l_r} \circ \mathcal{G}'^{l_r} \\ \mathcal{G}' \leftarrow \textit{Linearized version of } \mathcal{G} \end{cases}$$

Here $d^\circ \mathbb{G}$, $d^\circ \mathbb{G}'$ are the upper bounds on the degrees of $\mathbb{G}, \mathbb{G}'$ respectively.

Effect of linearization on SymSum

Theorem

With at least one round linearized, the upper-bound on the degree of TYPE−II monomials in terms of TYPE−I monomials is given by:

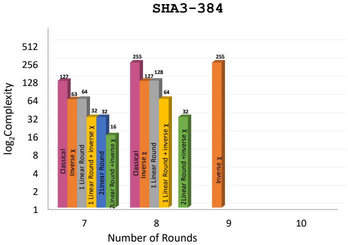
$$d^\circ \mathcal{F}_c^{n_r} \leq d^\circ \mathcal{F}_{c'}^{n_r} - 1$$

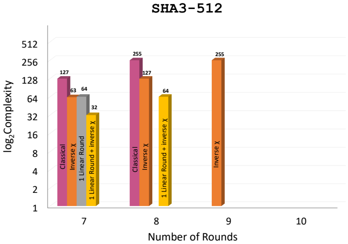
Monomials independent of round constants : (TYPE−I)
Monomials that involve round constants : (TYPE−II)

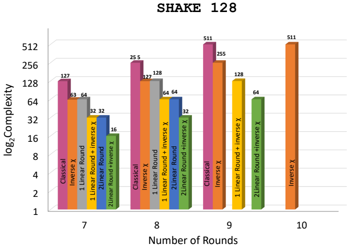
Corollary

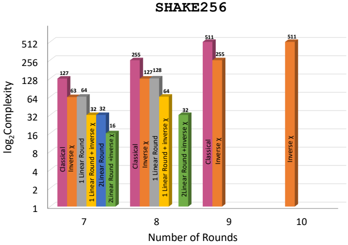
With l_r linearized rounds $\left(\frac{d^\circ \mathbb{G}}{\lambda^{l_r}}\right)$−fold vectorial derivative of $\mathbb{G}$ is a function which is independent of round constants.

Comparision of SHA-3 variants









The Results

SHA-3-variant	#Rounds	ZeroSum	SymSum	**Remarks**
SHA-3-224	8	2^{65}	2^{64}	2R Linear
SHA-3-256	7	2^{33}	2^{32}	2R Linear
SHA-3-384	8	2^{33}	2^{32}	2R Linear + χ^{-1}
SHA-3-512	8	2^{65}	2^{64}	1R Linear + χ^{-1}
SHAKE128	9	2^{65}	2^{64}	2R Linear + χ^{-1}
	10	2^{513}	2^{511}	χ^{-1}
SHAKE256	8	2^{33}	2^{32}	2R Linear + χ^{-1}
	9	2^{257}	2^{255}	χ^{-1}
	10	2^{513}	2^{511}	χ^{-1}

Summary

- Distinguishers
- Higher order Boolean derivatives
- `SymSum` property
- Linear Structures in KECCAK $-p$
- Applying linear structures to extend `SymSum`
- New observations on `SymSum` advantage over `ZeroSum`
- Best distinguisher on round-reduced variants

Thanks

get@.de.ci.phe.red