Introducing the **Banana Bound** and Beyond-Birthday-Barrier Security of the JH Mode

Dustin Moody[†], Souradyuti Paul[†‡], Daniel Smith-Tone[†]

[†]National Institute of Standards and Technology, US

[‡]KULeuven, Belgium

FSE 2012 Rump Session

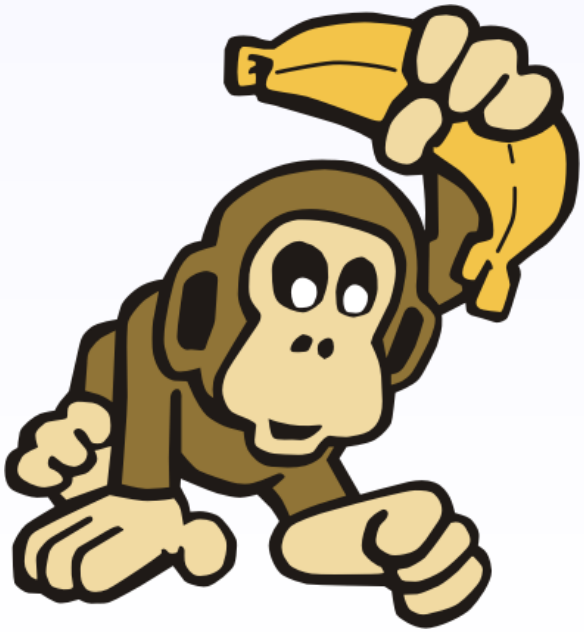
Presented by Souradyuti Paul

Banana Cryptography (I)

Not very well developed...

Banana Attacks

- Introduced by Aumasson in 2010 to capture the practise of presenting trivial crypto-attacks under the pretext that they are significant. Another name: pseudo-attacks.
- It is a powerful concept.

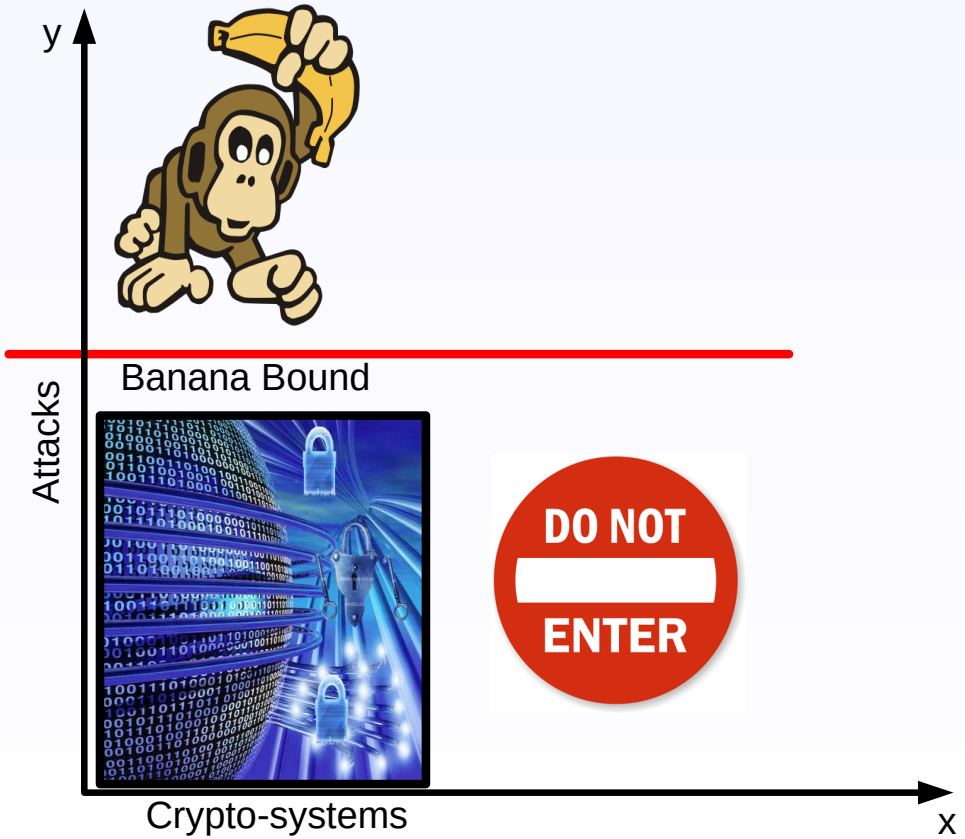


Banana Cryptography (II)

We extend the notion ....

Definition (Banana Bound)

The security bound below which no banana attack is possible.



Skepticism on Indifferentiability Framework

- Indifferentiability Attacks are Banana Attacks
- Indifferentiability Security Bounds are Banana Bounds

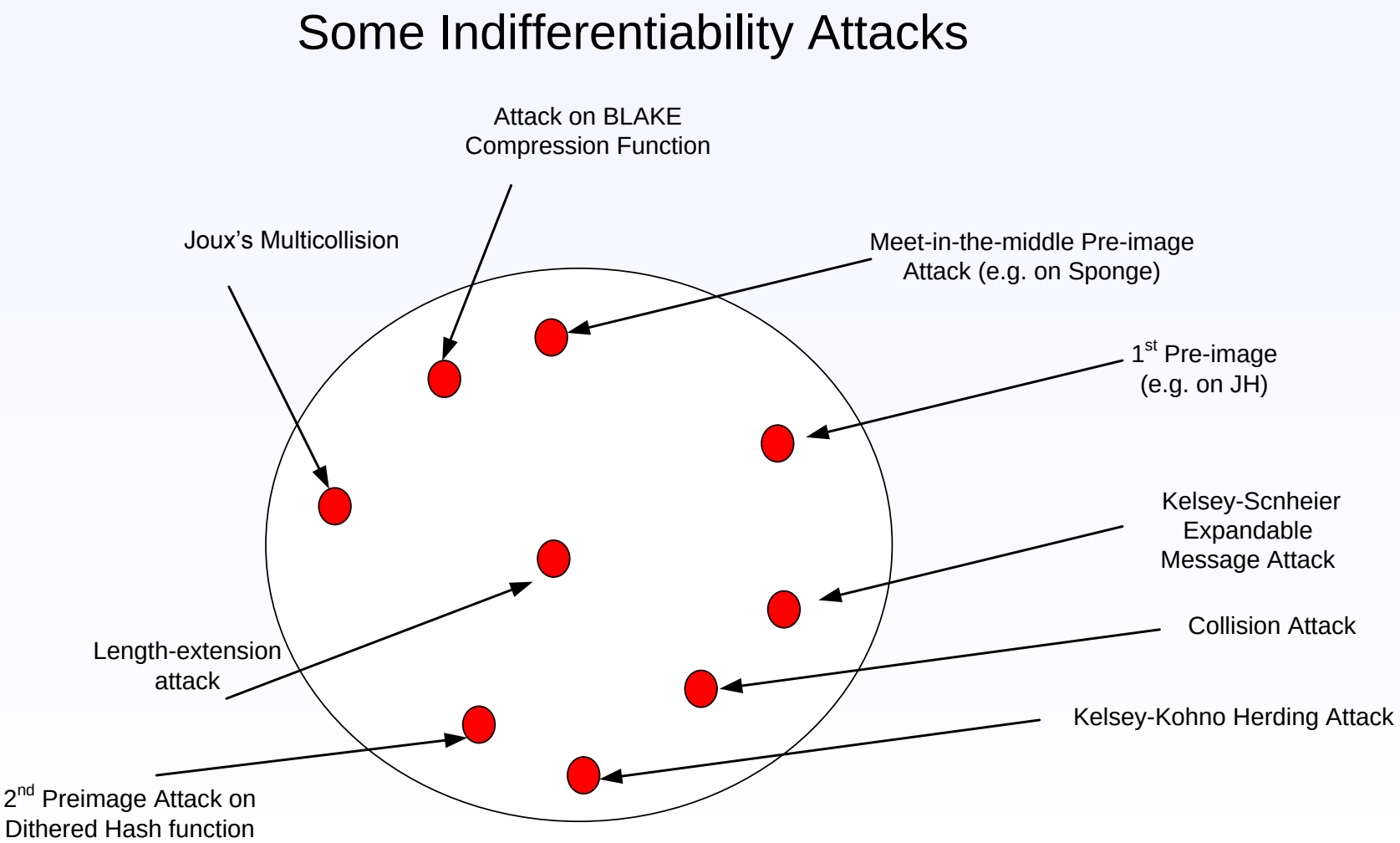
Some Retrospection

Influential Attacks that Changed Our Outlook on Hash function Security

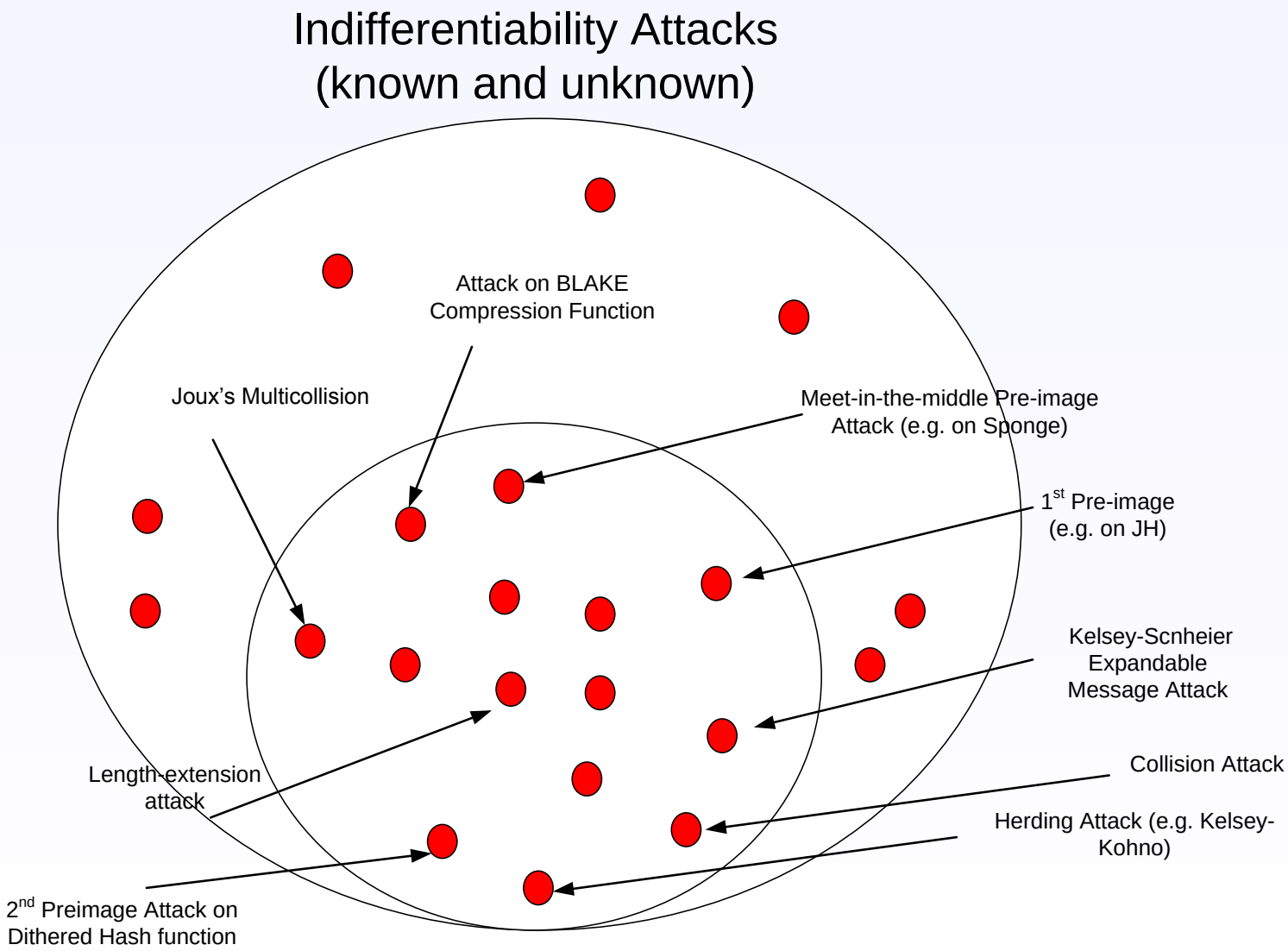
- Joux's Multi-collision
- Kelsey-Schneier Expandable Message
- Kelsey-Kohno Herding Attack
- Length extension attack
- ...
- ...

All the above attacks assume that the underlying primitive is a random oracle.

Indifferentiability attacks are not from far-away galaxies (I)

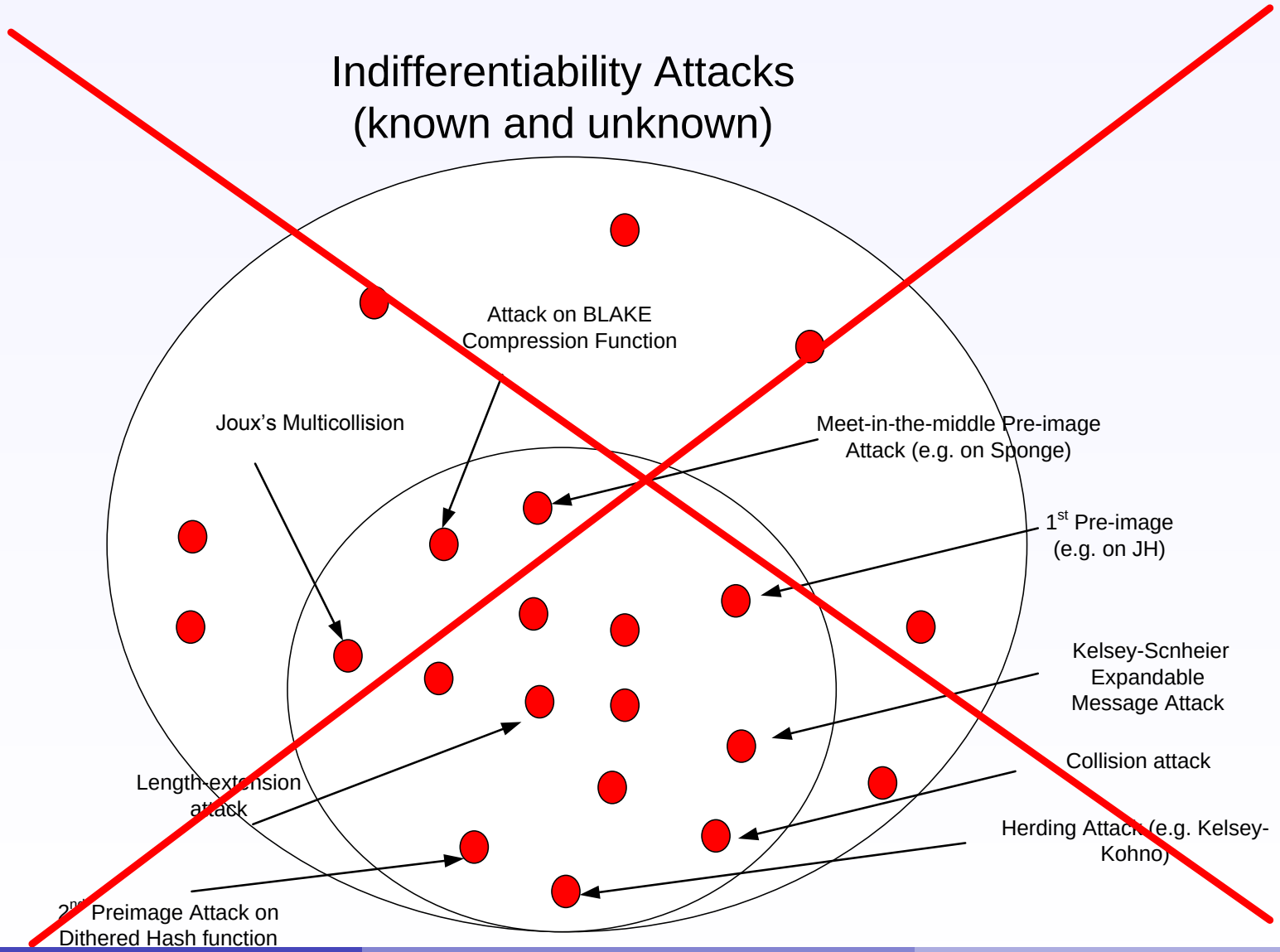


Indifferentiability attacks are not from far-away galaxies (II)



What does Indifferentiability Security Mean?

Resistance to all Indifferentiability Attacks.

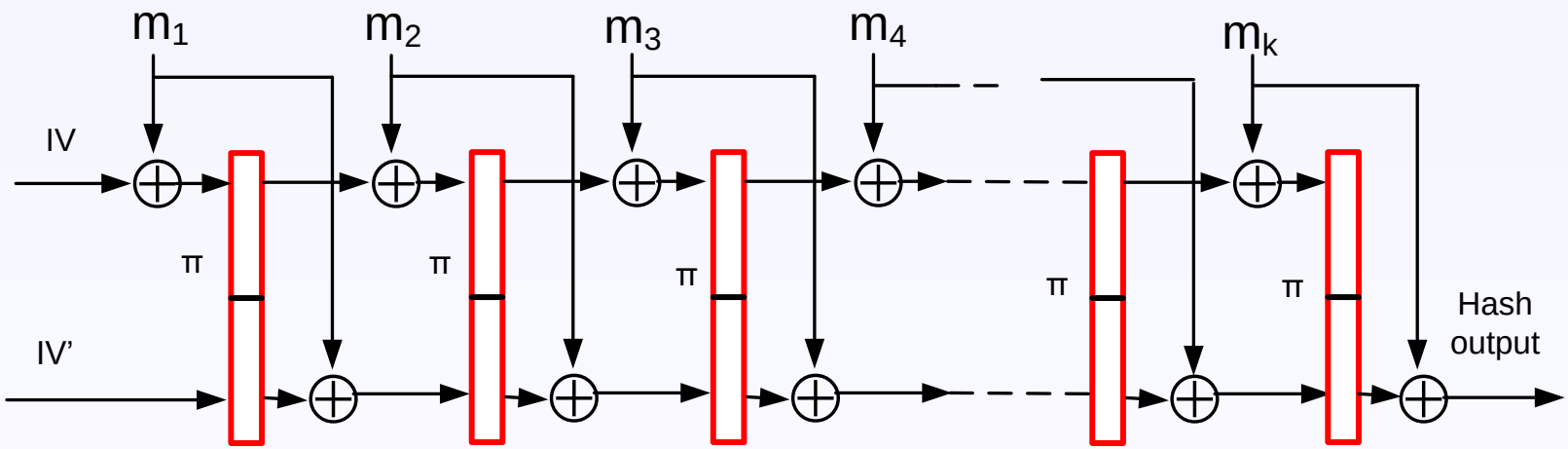


Bounds for popular hash modes of operation

Mode of operation	Message block-length per call (b)	Primitive input-length per call (a)	Rate = $\frac{b}{a-b}$	Primitive Output-length per call	Indiff. bound
MD	n	$2n$	1	n	0
MDP	n	$2n$	1	n	$n/2^*$
EMD	n	$2n$	1	n	$n/2^*$
JH	n	$2n$	1	$2n$	$\boldsymbol{n/3}$
Sponge	n	$2n$	1	$2n$	$\boldsymbol{n/2^*}$
Grøstl	n	$2n$	1	$2n$	$\boldsymbol{n/2}$
Parazoa	n	$2n$	1	$2n$	up to $n/2$
FWP	n	$2n$	1	$2n$	$2n/3$
HAIFA	n	$3n$	1/2	n	$n/2^*$
Skein	n	$3n$	1/2	n	$\boldsymbol{n/2^*}$
WP,chopMD	n	$3n$	1/2	$2n$	$n - \log n^{**}$
Shabal	n	$4n$	1/3	$2n$	n^*
BLAKE	$2n$	$4n$	1	$2n$	$\boldsymbol{n/2^*}$

- For each case the hash-output is n-bit.
- The symbols * and ** denote optimal and close to optimal.

The JH mode



- $M \xrightarrow{pad} m_1 m_2 m_3 \cdots m_k$
- π is a permutation
- All wires are n bits
- Variants: Chop n output bits to hash-size h
- Value $n = 512$, $h = 512, 384, 256$ and 224 bits

Results on the JH mode of operation

- Previous Results.

Mode of operation	Message block-length per call	Primitive input-length per call	1st preimage resistance	2nd preimage resistance	Collision bound	Indiff. bound
JH-n	n	$2n$	$n/2$	$n/2$	$n/2^*$	$n/3$
JH-512	512	1024	256	256	256*	170
JH-256	512	1024	256*	256*	128*	170

- Results to be presented at the SHA3 Conference.

Mode of operation	Message block-length per call	Primitive input-length per call	1st preimage resistance	2nd preimage resistance	Collision bound	Indiff. bound
JH-n	n	$2n$	$n/2$	$n/2$	$n/2^*$	$\mathbf{n/2}$
JH-512	512	1024	256	256	256*	**256**
JH-256	512	1024	256	256*	128*	**256***

- New results for the rump session .

Mode of operation	Message block-length per call	Primitive input-length per call	1st preimage resistance	2nd preimage resistance	Collision bound	Indiff. bound
JH-n	n	$2n$	$2n/3$	$2n/3$	$n/2^*$	$\mathbf{2n/3}$
JH-512	512	1024	**342**	**342**	256*	**342**
JH-256	512	1024	256*	256*	128*	256*

Attack Technique

- Almost the same set of *Bad* events as in FWP: Two-phase framework.
- Additional *Bad* events for reverse queries.