

Improved Indifferentiability Security Bound for the JH Mode

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

[†]National Institute of Standards and Technology, US

[‡]KULeuven, Belgium

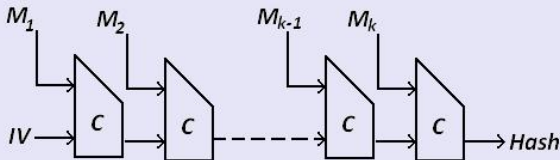
Third SHA3 Candidate Conference

Presented by Souradyuti Paul

Hash function design

- Iterative hash functions are usually composed of two parts:
 - ▶ A compression function $C : \{0, 1\}^{m+n} \rightarrow \{0, 1\}^n$
 - ▶ A mode of operation H to extend C
- We denote the hash function by $H^C : \{0, 1\}^* \rightarrow \{0, 1\}^n$.

Example: classical Merkle-Damgård mode MD



- If C is collision-resistant then so is MD^C .

New modes of operation

- Flaws in Merkle-Damgård
 - ▶ Length-extension attack
 - ▶ Joux's multi-collision attack
 - ▶ Herding attack
 - ▶ Kelsey-Schneier 2nd preimage attack
- # of SHA-3 submissions using *MD* mode: 0
- Improved ideas
 - ▶ Additional postprocessing
 - ▶ Adding counters
 - ▶ Widening output length of C
 - ▶ Multiple applications of C on the same message block

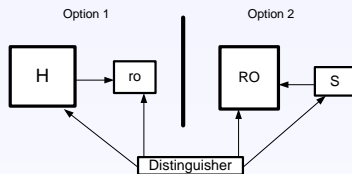
Indifferentiability framework (I)

- The *indifferentiability framework* was introduced in 2004 by Maurer et al. and applied to hash modes of operation by Coron et al. in 2005.
- Indifferentiability focuses on the mode H and not C .
- C is assumed to be ideal, i.e. a random oracle, ideal permutation, or an ideal cipher.
- If H^C is indifferentiable from a random oracle RO , then we can replace RO by H^C in any cryptosystem and the result is as least as secure in the ideal compression model as in the random oracle model.
- Indifferentiability guarantees resistance against all generic attacks, including the ones given in the previous slide. (Refer to our FSE 2012 Rump session talk.)

Indifferentiability framework (I)

- The *indifferentiability framework* was introduced in 2004 by Maurer et al. and applied to hash modes of operation by Coron et al. in 2005.
- Indifferentiability focuses on the mode H and not C .
- C is assumed to be ideal, i.e. a random oracle, ideal permutation, or an ideal cipher.
- If H^C is indifferentiable from a random oracle RO , then we can replace RO by H^C in any cryptosystem and the result is as least as secure in the ideal compression model as in the random oracle model.
- **Indifferentiability guarantees resistance against all generic attacks, including the ones given in the previous slide. (Refer to our FSE 2012 Rump session talk.)**

Indifferentiability framework (II)



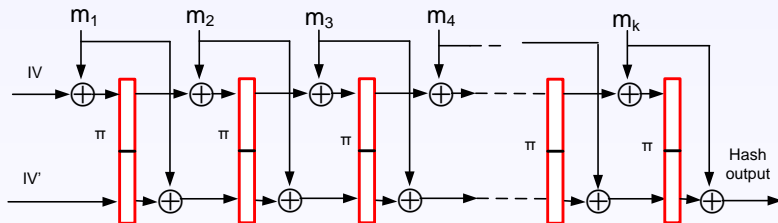
- Indifferentiability measures the extent to which a Distinguisher can tell the difference between Option 1 and Option 2
- Option 1 implements a hash mode H with primitive ro , a random oracle
- Option 2 consists of a random oracle RO , and a simulator s

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	$2n$	$n/3$
Sponge	n	$2n$	1	$2n$	$n/2^*$
Grøstl	n	$2n$	1	$2n$	$n/2$
Parazoa	n	$2n$	1	$2n$	up to $n/2$
FWP	n	$2n$	1	$2n$	$2n/3$
Skein	n	$2.25n$	$4/5$	n	$n/2^*$
HAIFA	n	$3n$	$1/2$	n	$n/2^*$
WP,chopMD	n	$3n$	$1/2$	$2n$	$n - \log n^{**}$
Shabal	n	$4n$	$1/3$	$2n$	n^*
BLAKE	$2n$	$4n$	1	$2n$	$n/2^*$

- 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

Previous results on the JH mode of operation

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

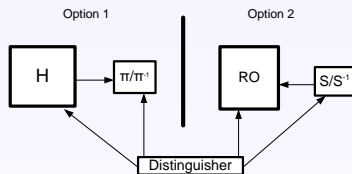
- Our indistinguishability results subsume all previous results
- In addition, it pushes bounds for all known and unknown attacks to $n/2$ bits

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	$2n$	$n/2$	$n/2$	$n/2^*$	$n/2$
JH-512	512	1024	256	256	256^*	256
JH-256	512	1024	256^*	256^*	128^*	256^*

Concrete security of JH-256 and JH-512

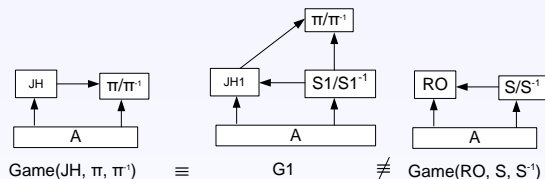
- We have improved the indistinguishability security bound for JH-512 (and JH-256) from **170 to 256 bits**: increase of **86 bits** of security
- This bound is the **optimal** for JH-256, and the **best** for JH-512
- This means JH-512 (and JH-256) **cannot be attacked** nontrivially with work less than 2^{256} , unless there are weaknesses in the underlying permutation

Indifferentiability framework (with permutations)



- Indifferentiability measures the extent to which a Distinguisher can tell the difference between Option 1 and Option 2
- Option 1 implements the JH hash mode with primitive π , an ideal permutation
- Option 2 consists of a random oracle RO , and a pair of simulators s and s^{-1}

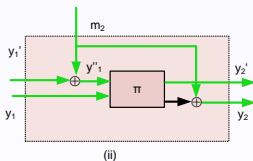
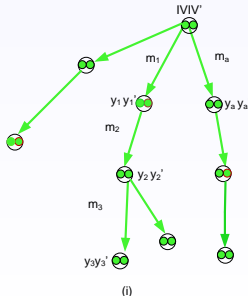
Security games



- Game $G1$ is an intermediate step, allowing us to more easily compare the games
- Game $G1$ is *equivalent* to $\text{Game}(\text{JH}, \pi, \pi^{-1})$
- Game $G1$ has the same code as $\text{Game}(\text{RO}, S, S^{-1})$, except when certain *BAD* events occur

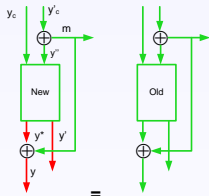
The simulator

- (1) The simulator outputs as if it is a random permutation. (2) The simulator “tries her level best” to ensure that the RO output is indistinguishable from JH output.
- To accomplish the above, it builds a graph from the queries and responses. See the paper for complete description.



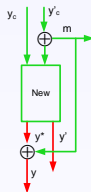
The *BAD* events

- The simulator fails on *BAD* events.



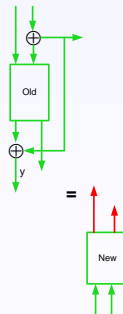
Node-collision
(n bits)

Type1-a



Forward-query-collision
(n bits)

Type1-b



Reverse-query-collision
(n bits)

Type1-c

Conclusion

- We extended the indistinguishability security bound for JH from $n/3$ to $n/2$ bits: concretely from **170 to 256 bits** for both JH-256 and JH-512.
- It seems possible to improve the bound even to $2n/3$ bits, that is, **to 342 bits**. We are presently working on it (refer to our FSE 2012 rump session presentation).