Improving the Indifferentiability Security Bounds for the Fast Wide-pipe and the JH Modes

Dustin Moody[†] Souradyuti Paul[†‡]

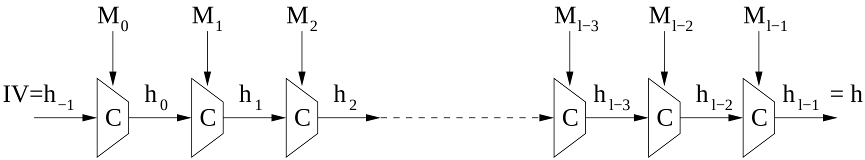
National Institute of Standards and Technology, US[†] and Katholieke Universiteit Leuven, Belgium[†‡]

16th August 2011, Rump Session Crypto 2011

How to build a Sequential Hash function

- Iterating a primitive C in a mode of operation H to build a hash function H^C.
- Typical Example is the Classical Merkle-Damgärd mode of operation.

Figure: The Classical Merkle-Damgärd Mode.



Stages of Improvement on Merkle-Damgärd Mode

- **Additional postprocessing and/or counters** in the Merkle-Damgärd mode to eliminate the length-adjustment related attacks. Examples: HAIFA, EMD, MDP.
- **Widen the output length** of the primitive C to $2n$-bits (or more) to eliminate Joux's multi-collision type attacks. Examples: chopMD, JH, Groestl, Sponge, Shabal.
- **Multiple applications** of the primitive C on the same message-block. Example: Doublepipe MD.
- **Widen the output length of C, and, also, increase the rate** of the hash function. Example: Fast Wide-pipe (FWP).

Status of Many Popular Hash Functions

Mode of operation	Message block length (b)	Primitive input length (a)	Primitive output length	Indiff. bound	rate $(b/(a-b))$
MD	ℓ	$\ell+n$	n	0	1
MDP	ℓ	$\ell+n$	n	$n/2^*$	1
EMD	ℓ	$\ell+n$	n	$n/2^*$	1
HAIFA	ℓ	$\ell+n$	n	$n/2^*$	1
chopMD	ℓ	$\ell+2n$	$2n$	n^{**}	1/2
Shabal	n	$4n$	$2n$	n^*	1/3
JH	n	$2n$	$2n$	$n/3$	1
Sponge	n	$2n$	$2n$	$n/2^*$	1
Grøstl	$2n$	$2n$ $(\times 2)$	$2n$ $(\times 2)$	$n/2$	1
FWP	ℓ	$\ell+n$	$2n$	$n/2$	1

Table: Hash output n bits. For fair comparison, we chose $\ell = n$. * and ** denote optimal and close to optimal.

The Fast Wide-pipe Mode of Operation

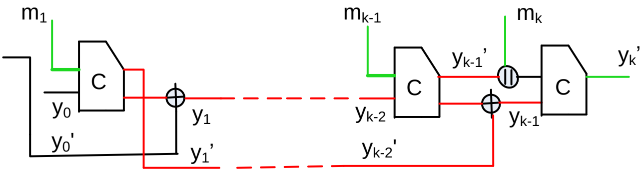


Figure: All wires are n bits except for the m_i $(1 \leq i \leq k)$.
$|m_1| = \cdots = |m_{k-1}| = \ell, |m_k| = \ell - n$.

- Proposed by Nandi and Paul in Indocrypt 2010.
- The earlier indifferntiability bound was $\frac{n}{2}$-bit.
- We improve the bound to $\frac{2n}{3}$-bit.

What we basically claim ...

To the best of our knowledge, this is the first time the indifferentiability security of a hash mode with rate 1 has been shown to be better than the birthday bound.[1]

[1] Assumption: The message-block length is equal to the hash-output length, and the primitive output length is not more than twice as large as the hash-output, otherwise the entire problem is meaningless.

The Basic Components of The Proof

- Code-based game playing technique.
- Designing a simulator that augments a tree in just two phases on each fresh query: first, it checks for $2n$-bit collisions, and, in the second phase, it checks for n-bit collisions in tree nodes.
- Usage of a special "Balls and Bins" problem – where the numbers of balls and bins increase every round, following a "special" pattern – to finally estimate the collision probability.
- Employing a correction factor to get a better estimate on the statistical distance between two random variables.

Application to JH

- The technique can be used to extend the indifferentiability security of JH from $\frac{n}{3}$-bit to $\frac{n}{2}$-bit.
- It **seems** possible to further extend the JH bound beyond the birthday barrier.

Thanks!