KATHOLIEKE UNIVERSITEIT LEUVEN

Security Analysis of the 3rd Round SHA-3 Candidates BLAKE, Grøstl, JH, Keccak and Skein

Elena Andreeva, Bart Mennink, Marjan Škrobot and Bart Preneel

COSIC, KU Leuven

The Third SHA-3 Candidate Conference
Washington, DC USA
22/03/2012

The Model

- **H** is SHA-3 candidate
- Security of **H** with **idealized**:
  - **F** compression f-n
  - **P, Q** permutations, **E** bl.cipher
- **This work**: ideal E, P, Q (lowest level primitive)

Upper bound maximal $Adv^{atk}_{H}(q)$ of any A in breaking some property **atk** of H with underlying primitives $\in$ {E, P, Q} after q queries.

- **atk** = NIST security requirements for SHA-3
- Security of **H** wrt atk $\in$ {**Col**, **Sec**, **Pre**} and **Indif**

Reminder

$$\mathrm{Adv}_{H}^{atk} \leq \mathrm{Pr}_{RO}^{atk} + \mathrm{Adv}_{H}^{Indif}$$

- $\mathrm{Adv}_{H}^{atk=\{Sec,\ Pre,\ Col\}} \leq \max\{\mathrm{Pr}_{RO}^{atk}, \mathrm{Adv}_{H}^{Indif}\}$
- Pr_{RO}^{atk} is success probability against atk generic attack on H, where H is viewed as a RO

Security Analysis of the 2nd Round SHA-3 Candidates [AMP10]

KATHOLIEKE UNIVERSITEIT LEUVEN

	type	sf	pf	(n,l,m)	$\mathbf{Adv}^{\mathrm{pre}}_{f}$	$\mathbf{Adv}^{\mathrm{sec}}_{f}$	$\mathbf{Adv}^{\mathrm{col}}_{f}$	$\mathbf{Adv}^{\mathrm{pre}}_{\mathcal{H}}$	$\mathbf{Adv}^{\mathrm{sec}}_{\mathcal{H}}$	$\mathbf{Adv}^{\mathrm{gcol}}_{\mathcal{H}}$	$\mathbf{Adv}^{\mathrm{ccl}}_{\mathcal{H}}$	$\mathbf{Adv}^{\mathrm{pro}}_{\mathcal{H}}$
BLAKE	HAIFA	✓	✓	$(256,256,512)$ or $(512,512,1024)$	PGV5-like E ideal		PGV5-like E ideal		$\Theta(q/2^n)$ f ideal	$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f}$	$\Theta(q^2/2^n)$ f ideal	$\Theta(Kq^2/2^n)$ f ideal
BMW	chop-(MD+FT)	✓	✗	$(256,512,512)$ or $(512,1024,1024)$	PGV3-like E ideal		PGV3-like E ideal			$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f} + \mathbf{Adv}^{\mathrm{gcol}}_{\mathrm{chop}\circ g}$		chopHMAC-like f ideal
CubeHash	chop-(MD+FT)	✗	✗	$(256,1024,256)$ or $(512,1024,256)$	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$O\left(\frac{q}{2^n}+\frac{q^2}{2^{l-n}}\right)$ P ideal	$O\left(\frac{q}{2^n}+\frac{q^2}{2^{l-n}}\right)$ P ideal	(no preservation)	$\Theta(q^2/2^n)$ P ideal	$O((Kq)^2/2^{l-n})$ P ideal
ECHO	chop-HAIFA	✓	✓	$(256,512,1536)$ or $(512,1024,1024)$	$\Theta(q/2^l)$ E ideal		$\Theta(q^2/2^l)$ E ideal		chop-HAIFA f ideal	$\leq \mathbf{Adv}^{\mathrm{gcol}}_{\mathrm{chop}\circ f}$	$\Theta(q^2/2^n)$ E ideal (proof by preservation)	chopMD construction
Fugue	chop-(MD+FT)	✓	✗	$(256,960,32)$ or $(512,1152,32)$	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal			(no preservation)		sponge-like P ideal
Grøstl	chop-(MD+FT)	✓	✗	$(256,512,512)$ or $(512,1024,1024)$	$\Theta(q^2/2^l)$ P,Q ideal		$\Theta(q^4/2^l)$ P,Q ideal			$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f} + \mathbf{Adv}^{\mathrm{gcol}}_{\mathrm{chop}\circ g}$	$\Theta(q^2/2^n)$ P,Q ideal (proof by preservation)	$O((Kq)^4/2^l)$ P,Q ideal
Hamsi	MD+FT	✓	✗	$(256,256,32)$ or $(512,512,64)$	$\Theta(q/2^n)$ P ideal		$\Theta(q^2/2^n)$ P ideal			$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f} + \mathbf{Adv}^{\mathrm{gcol}}_{g}$	$\Theta(q^2/2^n)$ $P,\tilde{P}$ ideal (proof by preservation)	NMAC-like f,g ideal
JH	chop-MD	✓	✗	$(256,1024,512)$ or $(512,1024,512)$	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$O\left(\frac{q}{2^n}+\frac{q^3}{2^{l-m}}\right)$ P ideal	$O\left(\frac{q}{2^n}+\frac{q^3}{2^{l-m}}\right)$ P ideal	(no preservation)	$O\left(\frac{q^2}{2^n}+\frac{q^3}{2^{l-m}}\right)$ P ideal	$O\left(\frac{q^3}{2^{l-m}}+\frac{Kq^3}{2^{l-n}}\right)$ P ideal
Keccak	chop-MD	✗	✗	$(256,1600,1088)$ or $(512,1600,576)$	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$\Theta(1)$ P ideal	$\Theta(q/2^n)$ P ideal	$\Theta(q/2^n)$ P ideal	(no preservation)	$\Theta(q^2/2^n)$ P ideal	$\Theta((Kq)^2/2^{l-m})$ P ideal
Luffa	chop-(MD+FT)	✗	✗	$(256,768,256)$ or $(512,1278,256)$	$\Theta(1)$ P_i ideal	$\Theta(1)$ P_i ideal	$\Theta(1)$ P_i ideal			(no preservation)		sponge-like P_i ideal
Shabal	chop-MD	✓	✓	$(256,1408,512)$ or $(512,1408,512)$			$O(q^2/2^{l-m})$ E ideal	$\Theta(q/2^n)$ E ideal	$O\left(\frac{q}{2^n}+\frac{q^2}{2^{l-m}}\right)$ E ideal	$\leq \mathbf{Adv}^{\mathrm{gcol}}_{\mathrm{chop}\circ f}$	$\Theta(q^2/2^n)$ E ideal	$O((Kq)^2/2^{l-m})$ E ideal
SHAvite-3	HAIFA	✓	✓	$(256,256,512)$ or $(512,512,1024)$	$\Theta(q/2^n)$ E ideal		$\Theta(q^2/2^n)$ E ideal		$\Theta(q/2^n)$ f ideal	$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f}$	$\Theta(q^2/2^n)$ E ideal (proof by preservation)	$O((Kq)^2/2^n)$ E ideal
SIMD	chop-(MD+FT)	✓	✗	$(256,512,512)$ or $(512,1024,1024)$	$\Theta(q/2^l)$ E ideal		$\Theta(q^2/2^l)$ E ideal			$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f} + \mathbf{Adv}^{\mathrm{gcol}}_{\mathrm{chop}\circ g}$	$\Theta(q^2/2^n)$ $E,\tilde{E}$ ideal (proof by preservation)	chopMD construction
Skein	chop-MD	✓	✓	$(256,512,512)$ or $(512,512,512)$	$\Theta(q/2^l)$ E ideal		$\Theta(q^2/2^l)$ E ideal	$O\left(\frac{q}{2^n}+\frac{q^2}{2^l}\right)$ E ideal	$O\left(\frac{q}{2^n}+\frac{q^2}{2^l}\right)$ E ideal	$\leq \mathbf{Adv}^{\mathrm{gcol}}_{f}$	$\Theta(q^2/2^n)$ E ideal (proof by preservation)	$O((Kq)^2/2^l)$ E ideal

NIST Requirements

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
BLAKE (256, 256, 512) **(512, 512, 1024)**								
Grøstl (256, 512, 512) **(512, 1024, 1024)**								
JH (256, 1024, 512) **(512,1024, 512)**								
Keccak (256, 1600, 1088) **(512, 1600, 576)**								
Skein (256, 512, 512) **(512, 512, 512)**								
NIST requirements				**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

KATHOLIEKE UNIVERSITEIT LEUVEN

Earlier Results for BLAKE, Grøstl, JH, Keccak and Skein

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
BLAKE (256, 256, 512) **(512, 512, 1024)**				256 **512**	256 **512**	128 **256**	128 **256**	**F**
Grøstl (256, 512, 512) **(512, 1024, 1024)**	512 **1024**	512 **1024**	256 **512**	256 **512**	128 **256**	128 **256**	128 **256**	**P, Q**
JH (256, 1024, 512) **(512,1024, 512)**	Insec Insec	Insec Insec	Insec Insec	170 **170**	170 **170**	128 **256**	170 **170**	**P**
Keccak (256, 1600, 1088) **(512, 1600, 576)**	Insec Insec	Insec Insec	Insec Insec	256 **512**	256 **512**	128 **256**	256 **512**	**P**
Skein (256, 512, 512) **(512, 512, 512)**	512 **512**	512 **512**	256 **256**	256 **512**	256 **256**	128 **256**	256 **256**	**E**
NIST requirements				**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

Our Objective

Provide “fair” security comparison for all H

- Focus on security analysis of H
- Security of all H based on ideal lower level primitives (E, P, Q, etc.)
- Tighten security results for H (where possible)
- Ideally: color uniformity in our previous table

BLAKE Old Results

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
BLAKE (256, 256, 512) **(512, 512, 1024)**				256 **512**	256 **512**	128 **256**	128 **256**	**F**
NIST requirements				**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- If **F** ideal
  - Indif $2^{n/2}$
  - Pre, Sec, Col (HAIFA design)
- If **F** Col and Pre ➔ BLAKE is Pre and Col (preservation)

BLAKE New Results

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre H	Sec H	Col H	Indif H	Ideal
BLAKE (256, 256, 512) **(512, 512, 1024)**	256 **512**	256 **512**	128 **256**	128 **256**	**E**
NIST requirements	**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- **F** differentiable in $2^{n/4} << 2^{n/2}$ queries
- New: if **E** ideal:
  - Indif $2^{n/2}$
  - F is Pre and Col ➔ BLAKE is Pre and Col (preservation)
  - BLAKE Sec direct proof

E. Andreeva, A. Luykx and B. Mennink, **"Provable Security of BLAKE with Non-Ideal Compression Function"**, *ePrint Archive, Report 2011/620.*
D. Chang, M. Nandi and M. Yung: **"Indifferentiability of the hash algorithm BLAKE"** , *ePrint Archive, Report 2011/623.*

Grøstl Old Results

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
Grøstl (256, 512, 512) **(512, 1024, 1024)**	512 1024	512 1024	256 512	256 **512**	128 **256**	128 **256**	128 **256**	**P, Q**
NIST requirements				**256** **512**	**256-L** **512-L**	**128** **256**	-	

- If **P, Q** ideal
  - Indif $2^{l/4} = 2^{n/2}$
  - Sec security implied by Indif (not optimal)
  - **F** is Col and Pre ➔ Grøstl is Pre and Col (preservation)

Grøstl New Result

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre H	Sec H	Col H	Indif H	Ideal
Grøstl (256, 512, 512) **(512, 1024, 1024)**	256 **512**	256 **512**	128 **256**	128 **256**	**P, Q**
NIST requirements	**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- New: if **P, Q** ideal
  - Sec direct proof: obtain **optimal** security

  Proof: shows similarities with Sec proof of BLAKE

JH Old Result

(n, l, m) n *output*, l *state*, m *msg.bl.*		Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
JH	(256, 1024, 512) **(512,1024, 512)**	- -	- -	- -	170 **170**	170 **170**	128 **256**	170 **170**	**P**
NIST requirements					**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- Based on **P** (**F** is Col, Sec and Pre insecure)
- If **P** ideal
  - Pre, Sec implied by Indif 2^{170} (not optimal)
  - Col direct proof by Lee and Hong 2011

JH New Result

(n, l, m) n *output*, l *state*, m *msg.bl.*		Pre H	Sec H	Col H	Indif H	Ideal
JH	(256, 1024, 512) **(512,1024, 512)**	256 **256**	256 **256**	128 **256**	170 **170**	**P**
NIST requirements		**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- New: if **P** ideal
  - Direct Pre proof (optimal for n = 256), (not optimal for n = 512)
  - Direct Sec proof (optimal for n = 256), (not optimal for n = 512)
- Proof
  - technical
  - graph-based: upper bound Pr to find a path from IV to final target hash value

Keccak

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
Keccak (256, 1600, 1088) **(512, 1600, 576)**	- -	- -	- -	256 **512**	256 **512**	128 **256**	256 **512**	**P**
NIST requirements				**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- Based on **P** (**F** is Col, Sec and Pre insecure)
- Known results: If **P** ideal
  - Pre, Sec and Col implied by Indif $2^{(l-m)/2}$

Skein Old Results

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre F	Sec F	Col F	Pre H	Sec H	Col H	Indif H	Ideal
Skein (256, 512, 512)	512	512	256	256	256	128	256	**E**
(512, 512, 512)	512	512	256	**512**	**256**	**256**	**256**	
NIST requirements				**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- Based on **E** (MMO type)
- Earlier: if **E** ideal
  - Indif $2^{l/2}$
  - F is Pre, Col ➔ Skein is Pre, Col secure (preservation)
  - Sec implied by Indif $2^{l/2}$ (not optimal Sec for 512-bit version)

Skein New Results

(n, l, m) n *output*, l *state*, m *msg.bl.*	Pre H	Sec H	Col H	Indif H	Ideal
Skein (256, 512, 512) **(512, 512, 512)**	256 **512**	256 **512**	128 **256**	256 **256**	**E**
NIST requirements	**256** **512**	**256-L** **512-L**	**128** **256**	**-**	

- New: if **E** is ideal
  - Direct Sec proof (optimal for both n = 256, 512)

  Proof: shows similarities with Sec proof of BLAKE

Security Results for 256-bit Versions

	l	m	Pre	Sec	Col	Indif
BLAKE-256	256	512	256	256	128	128
Grøstl-256	512	512	256	256-L	128	128
JH-256	1024	512	256	256	128	170
Keccak-256	1600	1088	256	256	128	256
Skein-256	512	512	256	256	128	256
NIST requirements			**256**	**256-L**	**128**	**-**

KATHOLIEKE UNIVERSITEIT LEUVEN

Security Results for 512-bit Versions

	l	m	Pre	Sec	Col	Indif
BLAKE-512	512	1024	512	512	256	256
Grøstl-512	1024	1024	512	512-L	256	256
JH-512	1024	512	256	256	256	170
Keccak-512	1600	576	512	512	256	512
Skein-512	512	512	512	512	256	256
NIST requirements			**512**	**512-L**	**256**	**-**

Open Questions

- Standard model security proofs
  (other than CoI preservation)
- Improved **Indif** bounds
- JH-512 optimality for Sec and Pre security in the ideal model

KATHOLIEKE UNIVERSITEIT LEUVEN

Thank you!