Security Reductions of the Second Round SHA-3 Candidates

Bart Mennink (K.U.Leuven)

Joint work with: Elena Andreeva and Bart Preneel (K.U.Leuven)

Information Security Conference
Florida, USA

October 26, 2010

Overview

NIST's SHA-3 Hash Function Competition

2004: Attacks by Wang et al. exposed vulnerabilities in several widely employed hash functions (incl. MD5 and SHA-1)

2007: US NIST launched a public competition for the design of a new hash function: SHA-3

Dec 2008: NIST announced 51 first round candidates

Jul 2009: NIST announced 14 second round candidates

End of 2010: NIST will announce 4 - 6 finalists

$\pm$ 2012: NIST will announce new hash function

NIST's SHA-3 Hash Function Competition

2004: Attacks by Wang et al. exposed vulnerabilities in several widely employed hash functions (incl. MD5 and SHA-1)

2007: US NIST launched a public competition for the design of a new hash function: SHA-3

Dec 2008: NIST announced 51 first round candidates

Jul 2009: NIST announced 14 second round candidates

End of 2010: NIST will announce 4 - 6 finalists

$\pm$ 2012: NIST will announce new hash function

SHA-3 must be efficient and secure

NIST's Security Requirements

Hash function must provide message digests of 224, 256, 384 and 512 bits

(i) At least one variant must support HMAC and randomized hashing

For all n-bit digest values, the hash function must provide

(ii) preimage resistance

(iii) second preimage resistance

(iv) collision resistance

(v) resistance to the length-extension attack

(vi) For any $m \leq n$, the hash function specified by taking a fixed subset of m bits of the function's output is required to satisfy properties (ii)-(v) with n replaced by m

NIST's Security Requirements

Hash function must provide message digests of $224, 256, 384$ and 512 bits

(i) At least one variant must support HMAC and randomized hashing

For all n-bit digest values, the hash function must provide

- (ii) preimage resistance
- (iii) second preimage resistance
- (iv) collision resistance
- (v) resistance to the length-extension attack

(vi) For any $m \leq n$, the hash function specified by taking a fixed subset of m bits of the function's output is required to satisfy properties (ii)-(v) with n replaced by m

NIST's Security Requirements

Hash function must provide message digests of 224, 256, 384 and 512 bits

For all n-bit digest values, the hash function must provide

(ii) preimage resistance

(iii) second preimage resistance

(iv) collision resistance

(vi) For any $m \leq n$, the hash function specified by taking a fixed subset of m bits of the function's output is required to satisfy properties (ii)-(v) with n replaced by m

NIST's Security Requirements

Hash function must provide message digests of 224, 256, 384 and 512 bits

For all n-bit digest values, the hash function must provide

(ii) preimage resistance

(iii) second preimage resistance

(iv) collision resistance

(vi) For any $m \leq n$, the hash function specified by taking a fixed subset of m bits of the function's output is required to satisfy properties (ii)-(v) with n replaced by m

NIST's Security Requirements

Hash function must provide message digests of 256 and 512 bits

For all *n*-bit digest values, the hash function must provide

(ii) preimage resistance

(iii) second preimage resistance

(iv) collision resistance

NIST's Security Requirements

Hash function must provide message digests of 256 and 512 bits

For all n-bit digest values, the hash function must provide

(ii) preimage resistance

(iii) second preimage resistance

(iv) collision resistance

(vii) Additionally, we analyze the indifferentiability

Outline

Security in the Ideal Model

Security in the Ideal Model

Assumption: design is built on one or more ideal underlying primitives

Security in the Ideal Model

Assumption: design is built on one or more ideal underlying primitives

pre/sec/col security

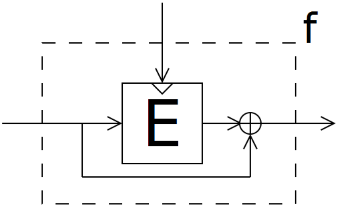
Advantage of an adversary (with query access to these primitives) in finding preimages, second preimages or collisions

Security in the Ideal Model

Assumption: design is built on one or more ideal underlying primitives

pre/sec/col security

Advantage of an adversary (with query access to these primitives) in finding preimages, second preimages or collisions



- Davies-Meyer construction
- Preimage and collision resistant if E is assumed to be an ideal block cipher

Security in the Ideal Model

Indifferentiability (indiff)

Advantage of a distinguisher to differentiate $\mathcal{H}$ from a RO

Security in the Ideal Model

Indifferentiability (indiff)

Advantage of a distinguisher to differentiate $\mathcal{H}$ from a RO

Indifferentiability bound implies security bounds for pre/sec/col/...

Security in the Ideal Model

Indifferentiability (indiff)

Advantage of a distinguisher to differentiate $\mathcal{H}$ from a RO

Indifferentiability bound implies security bounds for pre/sec/col/...

$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{col}}$: advantage of a collision finding adversary for $\mathcal{H}$

$\mathbf{Pr}_{RO}^{\mathrm{col}}$: success probability of finding collision for $\mathcal{H}$ generically

$\mathbf{Adv}_{\mathcal{H}}^{\mathrm{indiff}}$: indifferentiability bound of $\mathcal{H}$

Security in the Ideal Model

Indifferentiability (indiff)

Advantage of a distinguisher to differentiate $\mathcal{H}$ from a RO

Indifferentiability bound implies security bounds for pre/sec/col/...

$\mathbf{Adv}^{\mathrm{col}}_{\mathcal{H}}$: advantage of a collision finding adversary for $\mathcal{H}$

$\mathbf{Pr}^{\mathrm{col}}_{RO}$: success probability of finding collision for $\mathcal{H}$ generically

$\mathbf{Adv}^{\mathrm{indiff}}_{\mathcal{H}}$: indifferentiability bound of $\mathcal{H}$

$$\mathbf{Adv}^{\mathrm{col}}_{\mathcal{H}} \leq \mathbf{Pr}^{\mathrm{col}}_{RO} + \mathbf{Adv}^{\mathrm{indiff}}_{\mathcal{H}}$$

(formal proof in the full version of the paper)

Security in the Standard Model

Security in the Standard Model

Generic collision security of $\mathcal{H}$ (gcol)

Advantage of an *efficient* adversary in finding collisions for $\mathcal{H}$

Security in the Standard Model

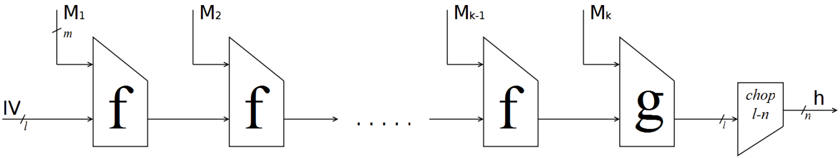
Generic collision security of $\mathcal{H}$ (gcol)

Advantage of an *efficient* adversary in finding collisions for $\mathcal{H}$

Strengthened Merkle-Damgård

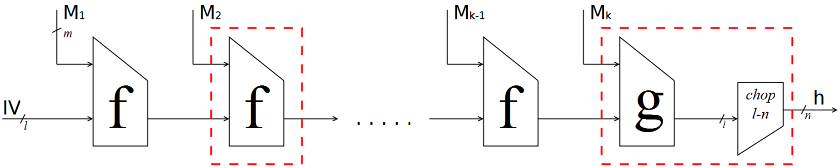
- Strengthened Merkle-Damgård *preserves* collision resistance: collisions for the hash function imply collisions for the compression function
- Extension: *all* SHA-3 candidates with a suffix-free padding preserve collision resistance

Security in the Standard Model



- All SHA-3 candidates follow this 'generalized Merkle-Damgård design', where g may equal f, and the chopping is optional

Security in the Standard Model



- All SHA-3 candidates follow this 'generalized Merkle-Damgård design', where g may equal f, and the chopping is optional
- Generalized MD with suffix-free padding preserves collision-resistance
  - Collisions for this design imply collisions for f or $\text{chop}_{l-n} \circ g$
- Formal proof in the full version of the paper

Outline

Security Comparison

	padding	
	sf	pf
BLAKE	✓	✓
BMW	✓	✗
CubeHash	✗	✗
ECHO	✓	✓
Fugue	✓	✗
Grøstl	✓	✗
Hamsi	✓	✗
JH	✓	✗
Keccak	✗	✗
Luffa	✗	✗
Shabal	✓	✓
SHAvite-3	✓	✓
SIMD	✓	✗
Skein	✓	✓

Security Comparison

	padding sf	padding pf
BLAKE	✓	✓
BMW	✓	✗
CubeHash	✗	✗
ECHO	✓	✓
Fugue	✓	✗
Grøstl	✓	✗
Hamsi	✓	✗
JH	✓	✗
Keccak	✗	✗
Luffa	✗	✗
Shabal	✓	✓
SHAvite-3	✓	✓
SIMD	✓	✗
Skein	✓	✓

Explanation of the Table:

- (green) Optimal security upper bound
- (yellow) Non-optimal security upper bound
- (red) Efficient attack known
- (white) No non-trivial security bound known
- ? Design is similar to a secure design, but no non-trivial security bound known

Security Comparison

	padding	
	sf	pf
BLAKE	✓	✓
BMW	✓	✗
CubeHash	✗	✗
ECHO	✓	✓
Fugue	✓	✗
Grøstl	✓	✗
Hamsi	✓	✗
JH	✓	✗
Keccak	✗	✗
Luffa	✗	✗
Shabal	✓	✓
SHAvite-3	✓	✓
SIMD	✓	✗
Skein	✓	✓

Explanation of the Table:

- (green) Optimal security upper bound
- (yellow) Non-optimal security upper bound
- (red) Efficient attack known
- (white) No non-trivial security bound known
- ? Design is similar to a secure design, but no non-trivial security bound known

Bounds and underlying assumptions are summarized in the paper!

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓			
BMW	✓	✗			
CubeHash	✗	✗			
ECHO	✓	✓			
Fugue	✓	✗			
Grøstl	✓	✗			
Hamsi	✓	✗			
JH	✓	✗			
Keccak	✗	✗			
Luffa	✗	✗			
Shabal	✓	✓			
SHAvite-3	✓	✓			
SIMD	✓	✗			
Skein	✓	✓			

Optimal | Non-optimal | Insecure | No bound | ? Similarity

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓			
BMW	✓	✗			
CubeHash	✗	✗			
ECHO	✓	✓			
Fugue	✓	✗			
Grøstl	✓	✗			
Hamsi	✓	✗			
JH	✓	✗			
Keccak	✗	✗			
Luffa	✗	✗			
Shabal	✓	✓			
SHAvite-3	✓	✓			
SIMD	✓	✗			
Skein	✓	✓			

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(Collisions and preimages in constant time; sponge-like designs)

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓			
BMW	✓	✗			
CubeHash	✗	✗			
ECHO	✓	✓			
Fugue	✓	✗			
Grøstl	✓	✗			
Hamsi	✓	✗			
JH	✓	✗			
Keccak	✗	✗			
Luffa	✗	✗			
Shabal	✓	✓			
SHAvite-3	✓	✓			
SIMD	✓	✗			
Skein	✓	✓			

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(PGV compression function [BRS02])

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓			
BMW	✓	✗			
CubeHash	✗	✗			
ECHO	✓	✓			
Fugue	✓	✗			
Grøstl	✓	✗			
Hamsi	✓	✗			
JH	✓	✗			
Keccak	✗	✗			
Luffa	✗	✗			
Shabal	✓	✓			
SHAvite-3	✓	✓			
SIMD	✓	✗			
Skein	✓	✓			

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(Generalized PGV compression function [Sta09])

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓	?		?
BMW	✓	✗	?		?
CubeHash	✗	✗			
ECHO	✓	✓			
Fugue	✓	✗			
Grøstl	✓	✗			
Hamsi	✓	✗			
JH	✓	✗			
Keccak	✗	✗			
Luffa	✗	✗			
Shabal	✓	✓			
SHAvite-3	✓	✓			
SIMD	✓	✗			
Skein	✓	✓			

Optimal   Non-optimal   Insecure   No bound   ? Similarity

(Similar to the generalized PGV compression function)

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓	?		?
BMW	✓	✗	?		?
CubeHash	✗	✗			
ECHO	✓	✓			
Fugue	✓	✗			
Grøstl	✓	✗			
Hamsi	✓	✗			
JH	✓	✗			
Keccak	✗	✗			
Luffa	✗	✗			
Shabal	✓	✓			
SHAvite-3	✓	✓			
SIMD	✓	✗			
Skein	✓	✓			

Optimal   Non-optimal   Insecure   No bound   ? Similarity

(Security of compression function of Grøstl and Shabal proven differently)

Security Comparison: Security of f

	padding		compression fn.		
	sf	pf	pre	sec	col
BLAKE	✓	✓	?		?
BMW	✓	✗	?		?
CubeHash	✗	✗	Insecure	Insecure	Insecure
ECHO	✓	✓	Optimal		Optimal
Fugue	✓	✗	Insecure	Insecure	Insecure
Grøstl	✓	✗	Non-optimal		Non-optimal
Hamsi	✓	✗	Optimal		Optimal
JH	✓	✗	Insecure	Insecure	Insecure
Keccak	✗	✗	Insecure	Insecure	Insecure
Luffa	✗	✗	Insecure	Insecure	Insecure
Shabal	✓	✓			Non-optimal
SHAvite-3	✓	✓	Optimal		Optimal
SIMD	✓	✗	Optimal		Optimal
Skein	✓	✓	Optimal		Optimal

Optimal — Non-optimal — Insecure — No bound — ? Similarity

General remarks:

- Insecure compression function $\Rightarrow$ ideality cannot be assumed
- Non-optimal bounds for f do not imply insecurity of $\mathcal{H}$

Security Comparison: Indifferentiability of $\mathcal{H}$

	padding		compression fn.			$\mathcal{H}$
	sf	pf	pre	sec	col	indiff
BLAKE	✓	✓	?		?	
BMW	✓	✗	?		?	
CubeHash	✗	✗				
ECHO	✓	✓				
Fugue	✓	✗				
Grøstl	✓	✗				
Hamsi	✓	✗				
JH	✓	✗				
Keccak	✗	✗				
Luffa	✗	✗				
Shabal	✓	✓				
SHAvite-3	✓	✓				
SIMD	✓	✗				
Skein	✓	✓				

Optimal | Non-optimal | Insecure | No bound | ? Similarity

Security Comparison: Indifferentiability of $\mathcal{H}$

	padding		compression fn.			$\mathcal{H}$
	sf	pf	pre	sec	col	indiff
BLAKE	✓	✓	?		?	
BMW	✓	✗	?		?	
CubeHash	✗	✗				
ECHO	✓	✓				
Fugue	✓	✗				
Grøstl	✓	✗				
Hamsi	✓	✗				
JH	✓	✗				
Keccak	✗	✗				
Luffa	✗	✗				
Shabal	✓	✓				
SHAvite-3	✓	✓				
SIMD	✓	✗				
Skein	✓	✓				

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(Hash function indifferentiable for ideal permutation(s)/block cipher)

Security Comparison: Indifferentiability of $\mathcal{H}$

	padding		compression fn.			$\mathcal{H}$
	sf	pf	pre	sec	col	indiff
BLAKE	✓	✓	?		?	
BMW	✓	✗	?		?	
CubeHash	✗	✗				
ECHO	✓	✓				
Fugue	✓	✗				
Grøstl	✓	✗				
Hamsi	✓	✗				
JH	✓	✗				
Keccak	✗	✗				
Luffa	✗	✗				
Shabal	✓	✓				
SHAvite-3	✓	✓				
SIMD	✓	✗				
Skein	✓	✓				

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(Hash function indifferentiable for ideal compression function)

Security Comparison: Indifferentiability of $\mathcal{H}$

	padding		compression fn.			$\mathcal{H}$
	sf	pf	pre	sec	col	indiff
BLAKE	✓	✓	?		?	
BMW	✓	✗	?		?	?
CubeHash	✗	✗				
ECHO	✓	✓				?
Fugue	✓	✗				?
Grøstl	✓	✗				
Hamsi	✓	✗				?
JH	✓	✗				
Keccak	✗	✗				
Luffa	✗	✗				?
Shabal	✓	✓				
SHAvite-3	✓	✓				
SIMD	✓	✗				?
Skein	✓	✓				

Optimal Non-optimal Insecure No bound ? Similarity

(Hash function similar to an indifferentiable design)

Security Comparison: Indifferentiability of $\mathcal{H}$

	padding		compression fn.			$\mathcal{H}$
	sf	pf	pre	sec	col	indiff
BLAKE	✓	✓	?		?	
BMW	✓	✗	?		?	?
CubeHash	✗	✗				
ECHO	✓	✓				?
Fugue	✓	✗				?
Grøstl	✓	✗				
Hamsi	✓	✗				?
JH	✓	✗				
Keccak	✗	✗				
Luffa	✗	✗				?
Shabal	✓	✓				
SHAvite-3	✓	✓				
SIMD	✓	✗				?
Skein	✓	✓				

Optimal | Non-optimal | Insecure | No bound | ? Similarity

General remarks:

- Eight designs are proven indifferentiable
- Yellow boxes only: the bounds are not optimal

Security Comparison: (Second) Preimage Resistance of $\mathcal{H}$

	padding		compression fn.			hash function		
	sf	pf	pre	sec	col	indiff	pre	sec
BLAKE	✓	✓	?		?			
BMW	✓	✗	?		?	?		
CubeHash	✗	✗						
ECHO	✓	✓				?		
Fugue	✓	✗				?		
Grøstl	✓	✗						
Hamsi	✓	✗				?		
JH	✓	✗						
Keccak	✗	✗						
Luffa	✗	✗				?		
Shabal	✓	✓						
SHAvite-3	✓	✓						
SIMD	✓	✗				?		
Skein	✓	✓						

Optimal Non-optimal Insecure No bound ? Similarity

Security Comparison: (Second) Preimage Resistance of $\mathcal{H}$

	padding		compression fn.			hash function		
	sf	pf	pre	sec	col	indiff	pre	sec
BLAKE	✓	✓	?		?			
BMW	✓	✗	?		?	?		
CubeHash	✗	✗						
ECHO	✓	✓				?		
Fugue	✓	✗				?		
Grøstl	✓	✗						
Hamsi	✓	✗				?		
JH	✓	✗						
Keccak	✗	✗						
Luffa	✗	✗				?		
Shabal	✓	✓						
SHAvite-3	✓	✓						
SIMD	✓	✗				?		
Skein	✓	✓						

Optimal   Non-optimal   Insecure   No bound   ? Similarity

(Preimage resistance derived from indifferentiability)

Security Comparison: (Second) Preimage Resistance of $\mathcal{H}$

	padding		compression fn.			hash function		
	sf	pf	pre	sec	col	indiff	pre	sec
BLAKE	✓	✓	?		?			
BMW	✓	✗	?		?	?		
CubeHash	✗	✗						
ECHO	✓	✓				?		
Fugue	✓	✗				?		
Grøstl	✓	✗						
Hamsi	✓	✗				?		
JH	✓	✗						
Keccak	✗	✗						
Luffa	✗	✗				?		
Shabal	✓	✓						
SHAvite-3	✓	✓						
SIMD	✓	✗				?		
Skein	✓	✓						

Optimal   Non-optimal   Insecure   No bound   ? Similarity

(Preimage resistance of Shabal proven differently)

Security Comparison: (Second) Preimage Resistance of $\mathcal{H}$

	padding		compression fn.			hash function		
	sf	pf	pre	sec	col	indiff	pre	sec
BLAKE	✓	✓	?		?			
BMW	✓	✗	?		?	?		
CubeHash	✗	✗						
ECHO	✓	✓				?		
Fugue	✓	✗				?		
Grøstl	✓	✗						
Hamsi	✓	✗				?		
JH	✓	✗						
Keccak	✗	✗						
Luffa	✗	✗				?		
Shabal	✓	✓						
SHAvite-3	✓	✓						
SIMD	✓	✗				?		
Skein	✓	✓						

Optimal · Non-optimal · Insecure · No bound · ? Similarity

(Second preimage resistance derived from indifferentiability)

Security Comparison: (Second) Preimage Resistance of $\mathcal{H}$

	padding		compression fn.			hash function		
	sf	pf	pre	sec	col	indiff	pre	sec
BLAKE	✓	✓	?		?			
BMW	✓	✗	?		?	?		
CubeHash	✗	✗						
ECHO	✓	✓				?		?
Fugue	✓	✗				?		
Grøstl	✓	✗						
Hamsi	✓	✗				?		
JH	✓	✗						
Keccak	✗	✗						
Luffa	✗	✗				?		
Shabal	✓	✓						
SHAvite-3	✓	✓						
SIMD	✓	✗				?		
Skein	✓	✓						

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(HAIFA designs are second preimage resistant)

Security Comparison: (Second) Preimage Resistance of $\mathcal{H}$

	padding		compression fn.			hash function		
	sf	pf	pre	sec	col	indiff	pre	sec
BLAKE	✓	✓	?		?	Non-optimal		Optimal
BMW	✓	✗	?		?	?		
CubeHash	✗	✗	Insecure	Insecure	Insecure	Non-optimal	Non-optimal	Non-optimal
ECHO	✓	✓	Optimal		Optimal	?		?
Fugue	✓	✗	Insecure	Insecure	Insecure	?		
Grøstl	✓	✗	Non-optimal		Non-optimal	Non-optimal		
Hamsi	✓	✗	Optimal		Optimal	?		
JH	✓	✗	Insecure	Insecure	Insecure	Non-optimal	Non-optimal	Non-optimal
Keccak	✗	✗	Insecure	Insecure	Insecure	Non-optimal	Optimal	Optimal
Luffa	✗	✗	Insecure	Insecure	Insecure	?		
Shabal	✓	✓			Non-optimal	Non-optimal	Optimal	Non-optimal
SHAvite-3	✓	✓	Optimal		Optimal	Non-optimal		Optimal
SIMD	✓	✗	Optimal		Optimal	?		
Skein	✓	✓	Optimal		Optimal	Non-optimal	Non-optimal	Non-optimal

Optimal | Non-optimal | Insecure | No bound | ? Similarity

General remarks:

- MD design does *not* preserve (second) preimage resistance
- Possible direction for proofs: graph based approach

Security Comparison: Collision Resistance of $\mathcal{H}$

	padding		compression fn.			hash function				
	sf	pf	pre	sec	col	indiff	pre	sec	gcol	col
BLAKE	✓	✓	?		?	Non-optimal		Optimal		
BMW	✓	✗	?		?	?				
CubeHash	✗	✗	Insecure	Insecure	Insecure	Non-optimal	Non-optimal	Non-optimal		
ECHO	✓	✓	Optimal		Optimal	?		?		
Fugue	✓	✗	Insecure	Insecure	Insecure	?				
Grøstl	✓	✗	Non-optimal		Non-optimal	Non-optimal				
Hamsi	✓	✗	Optimal		Optimal	?				
JH	✓	✗	Insecure	Insecure	Insecure	Non-optimal	Non-optimal	Non-optimal		
Keccak	✗	✗	Insecure	Insecure	Insecure	Non-optimal	Optimal	Optimal		
Luffa	✗	✗	Insecure	Insecure	Insecure	?				
Shabal	✓	✓			Non-optimal	Non-optimal	Optimal	Non-optimal		
SHAvite-3	✓	✓	Optimal		Optimal	Non-optimal		Optimal		
SIMD	✓	✗	Optimal		Optimal	?				
Skein	✓	✓	Optimal		Optimal	Non-optimal	Non-optimal	Non-optimal		

Optimal | Non-optimal | Insecure | No bound | ? Similarity

Security Comparison: Collision Resistance of $\mathcal{H}$

	padding		compression fn.			hash function				
	sf	pf	pre	sec	col	indiff	pre	sec	gcol	col
BLAKE	✓	✓	?		?					
BMW	✓	✗	?		?	?				
CubeHash	✗	✗								
ECHO	✓	✓				?		?		
Fugue	✓	✗				?				
Grøstl	✓	✗								
Hamsi	✓	✗				?				
JH	✓	✗								
Keccak	✗	✗								
Luffa	✗	✗				?				
Shabal	✓	✓								
SHAvite-3	✓	✓								
SIMD	✓	✗				?				
Skein	✓	✓								

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(Collision resistance preservation for all designs with sf padding)

Security Comparison: Collision Resistance of $\mathcal{H}$

	padding		compression fn.			hash function				
	sf	pf	pre	sec	col	indiff	pre	sec	gcol	col
BLAKE	✓	✓	?		?					
BMW	✓	✗	?		?	?				
CubeHash	✗	✗								
ECHO	✓	✓				?		?		
Fugue	✓	✗				?				
Grøstl	✓	✗								
Hamsi	✓	✗				?				
JH	✓	✗								
Keccak	✗	✗								
Luffa	✗	✗				?				
Shabal	✓	✓								
SHAvite-3	✓	✓								
SIMD	✓	✗				?				
Skein	✓	✓								

Optimal   Non-optimal   Insecure   No bound   ? Similarity

(Collision resistance in the ideal model due to preservation)

Security Comparison: Collision Resistance of $\mathcal{H}$

	padding		compression fn.			hash function				
	sf	pf	pre	sec	col	indiff	pre	sec	gcol	col
BLAKE	✓	✓	?		?					
BMW	✓	✗	?		?	?				
CubeHash	✗	✗								
ECHO	✓	✓				?		?		
Fugue	✓	✗				?				
Grøstl	✓	✗								
Hamsi	✓	✗				?				
JH	✓	✗								
Keccak	✗	✗								
Luffa	✗	✗				?				
Shabal	✓	✓								
SHAvite-3	✓	✓								
SIMD	✓	✗				?				
Skein	✓	✓								

Optimal | Non-optimal | Insecure | No bound | ? Similarity

(Collision resistance derived from indifferentiability)

Security Comparison: Collision Resistance of $\mathcal{H}$

	padding		compression fn.			hash function				
	sf	pf	pre	sec	col	indiff	pre	sec	gcol	col
BLAKE	✓	✓	?		?					
BMW	✓	✗	?		?	?				
CubeHash	✗	✗								
ECHO	✓	✓				?		?		
Fugue	✓	✗				?				
Grøstl	✓	✗								
Hamsi	✓	✗				?				
JH	✓	✗								
Keccak	✗	✗								
Luffa	✗	✗				?				
Shabal	✓	✓								
SHAvite-3	✓	✓								
SIMD	✓	✗				?				
Skein	✓	✓								

Optimal | Non-optimal | Insecure | No bound | ? Similarity

General remarks:

- For 10 candidates, optimal collision resistance
- For others, graph based approach may be fruitful

Outline

Conclusions

- Classification of the provable security results of the SHA-3 candidates
  - Preimage, second preimage and collision resistance
  - Indifferentiability
- Classification is based on security results in the ideal model

- We extended the standard proof of Merkle-Damgård collision resistance to cover *all* candidates with a suffix-free padding
- We formalized security implications of indifferentiability

Conclusions

- Classification of the provable security results of the SHA-3 candidates
  - Preimage, second preimage and collision resistance
  - Indifferentiability
- Classification is based on security results in the ideal model

- We extended the standard proof of Merkle-Damgård collision resistance to cover *all* candidates with a suffix-free padding
- We formalized security implications of indifferentiability

- Several observations and open problems
  - Most of the designs satisfy collision resistance and indifferentiability
  - Few results known on (second) preimage resistance

Thank you for your attention!

SUPPORTING SLIDES!!!

Security in the Ideal Model: Indifferentiability

- Indifferentiability of the hash function from a random oracle (indiff)
- Extension of indistinguishability: distinguisher may know the underlying structure of a hash function
- Hash function $\mathcal{H}$ built on π is indifferentiable from RO if there exists a simulator S such that for any distinguisher these games are indistinguishable