Security Reductions of the SHA-3 Candidates

On the Indifferentiability of the Grøstl Hash Function

Bart Mennink (K.U.Leuven)

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

Second SHA-3 Candidate Conference, UCSB

August 24, 2010

NIST's Securit 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 Securit 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 Securit 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 Securit 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 Securit 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 Securit 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

Security in the Ideal Model

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

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 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

Securit Comparison

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

Securit Comparison

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

Explanation of the Table:

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

Securit Comparison

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

Explanation of the Table:

- Optimal security upper bound
- Non-optimal security upper bound
- Efficient attack known
- 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!

Securit Comparison: Securit 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

Securit Comparison: Securit 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)

Securit Comparison: Securit 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])

Securit Comparison: Securit 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])

Securit Comparison: Securit 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)

Securit Comparison: Securit 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)

Securit Comparison: Securit 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

General remarks:

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

Securit Comparison: Indifferentiabilit 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

Securit Comparison: Indifferentiabilit 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 design is proven indifferentiable [CDMP05])

Securit Comparison: Indifferentiabilit 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 a design proven indifferentiable in [CDMP05])

Securit Comparison: Indifferentiabilit 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 proven indifferentiable separately)

Securit Comparison: Indifferentiabilit 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:

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

Securit 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

Securit 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)

Securit 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)

Securit 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)

Securit 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)

Securit 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

General remarks:

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

Securit 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

Securit 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)

Securit 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)

Securit 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)

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

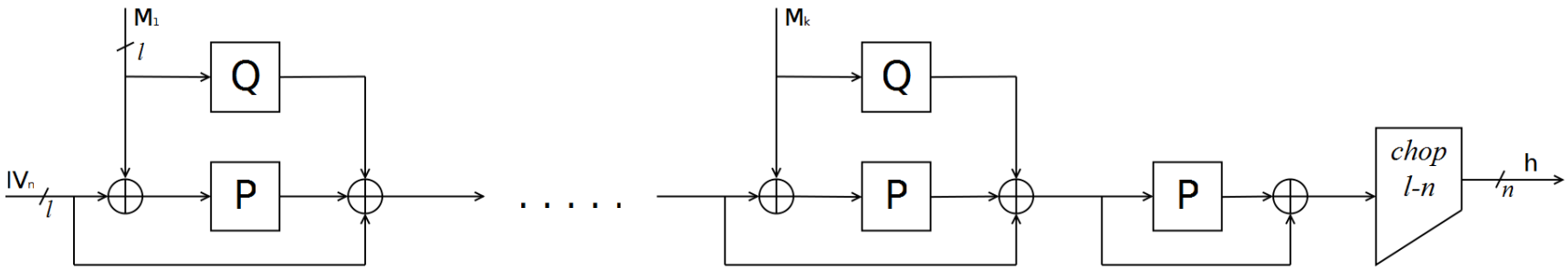
	padding		compression fn.			hash function				
	sf	pf	pre	sec	col	indiff	pre	sec	gcol	col
BLAKE	✓	✓	?		?					
BMW	✓	✗	?		?	?				
CubeHash	✗	✗								
ECHO	✓	✓						?		
Fugue	✓	✗				?				
Grøstl	✓	✗								
Hamsi	✓	✗				?				
JH	✓	✗								
Keccak	✗	✗								
Luffa	✗	✗				?				
Shabal	✓	✓								
SHAvite-3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

Indifferentiabilit of Grøstl



- Grøstl: based on two independent random l-bit permutations P, Q
- State size l larger than output size n: $l \geq 2n$

- Grøstl behaves like a random oracle up to $2^{n/2}$ queries
- Implies optimal collision resistance bound $\Theta(q^2/2^n)$

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 proved indifferentiability of Grøstl

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

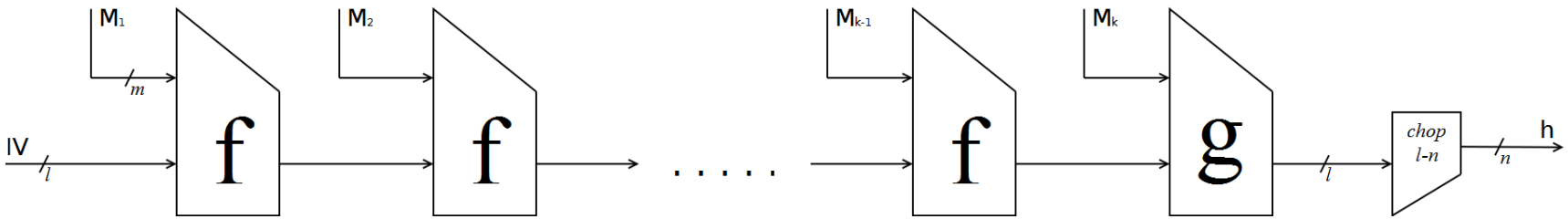
- We extended the standard proof of Merkle-Damgård collision resistance to cover *all* candidates with a suffix-free padding
- We proved indifferentiability of Grøstl

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

Questions?

SUPPORTING SLIDES!!!

Hash unction Design



- All SHA-3 candidates follow this 'generalized Merkle-Damgård design', where the final transformation (FT) and chopping are optional

- Generalized MD with suffix-free padding preserves collision-resistance
  - Collisions for this design imply collisions for f or $\mathrm{chop}_{l-n} \circ g$