Towards SHA-3

Christian Rechberger, KU Leuven

Fundamental questions in CS theory

Do oneway functions exist?

Do collision-intractable functions exist?

We don't know.

Do we care?

What we care about: computational properties

For cryptographic hash functions, it should be sufficiently hard to

- find preimages
- find collisions
- ...

Secure? What properties?

Collision resistance

Preimage resistance

2nd preimage resistance

Near-collision resistance

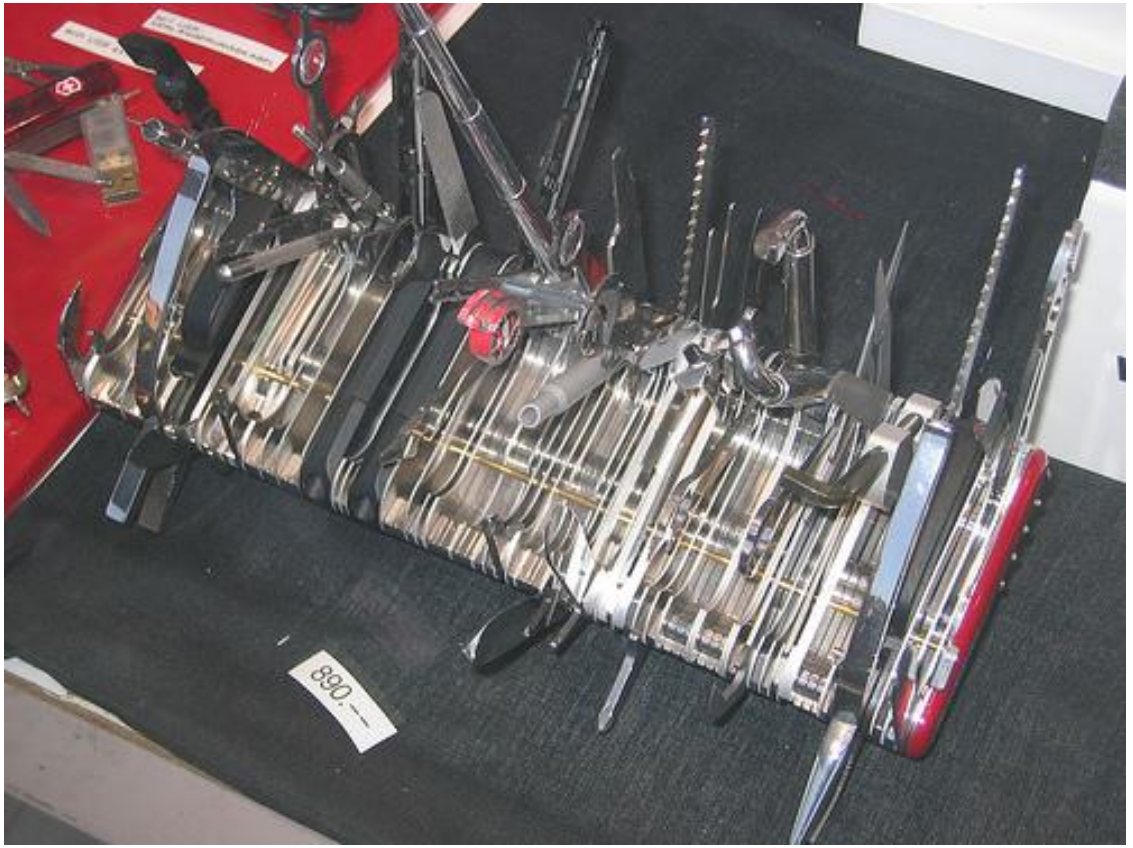
Pseudorandom generator

Pseudorandom function

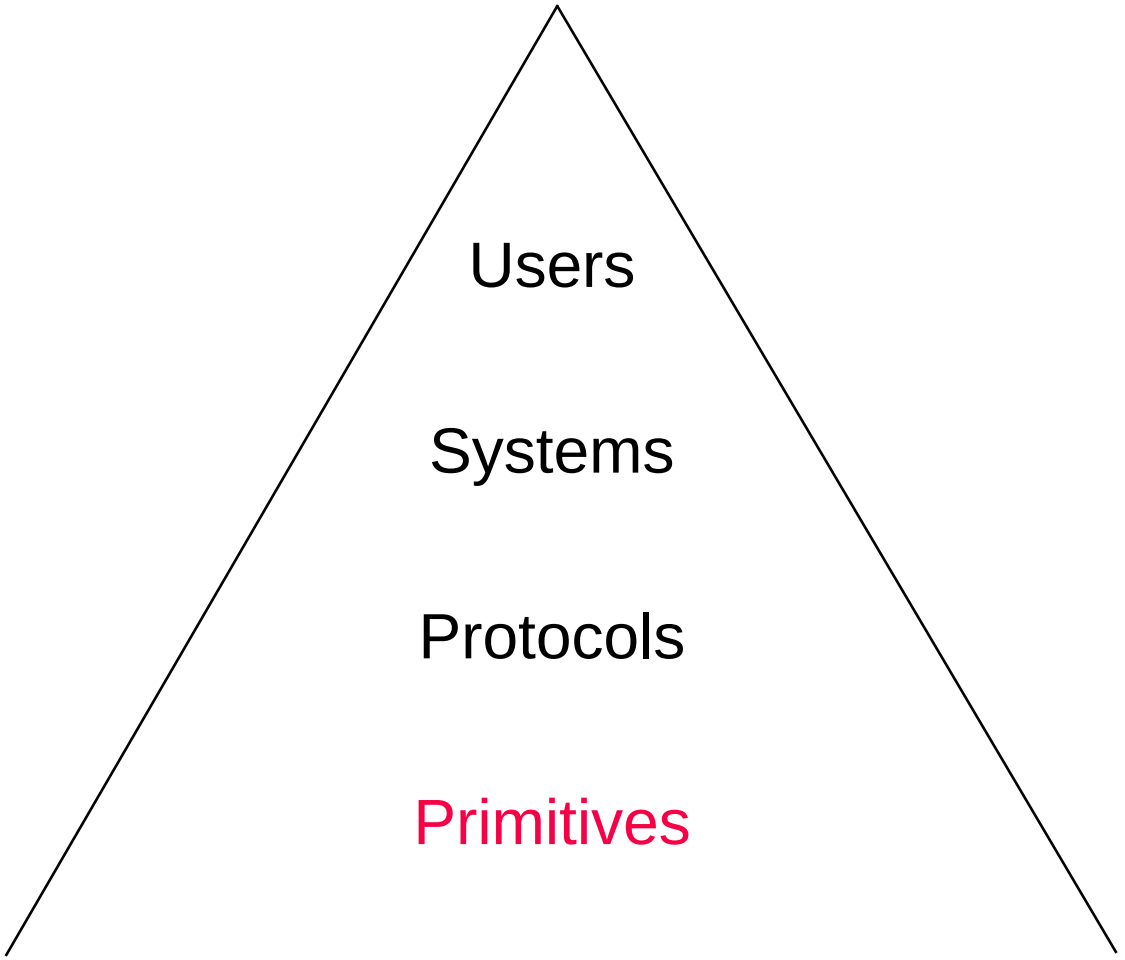
Key derivation function

Random oracle

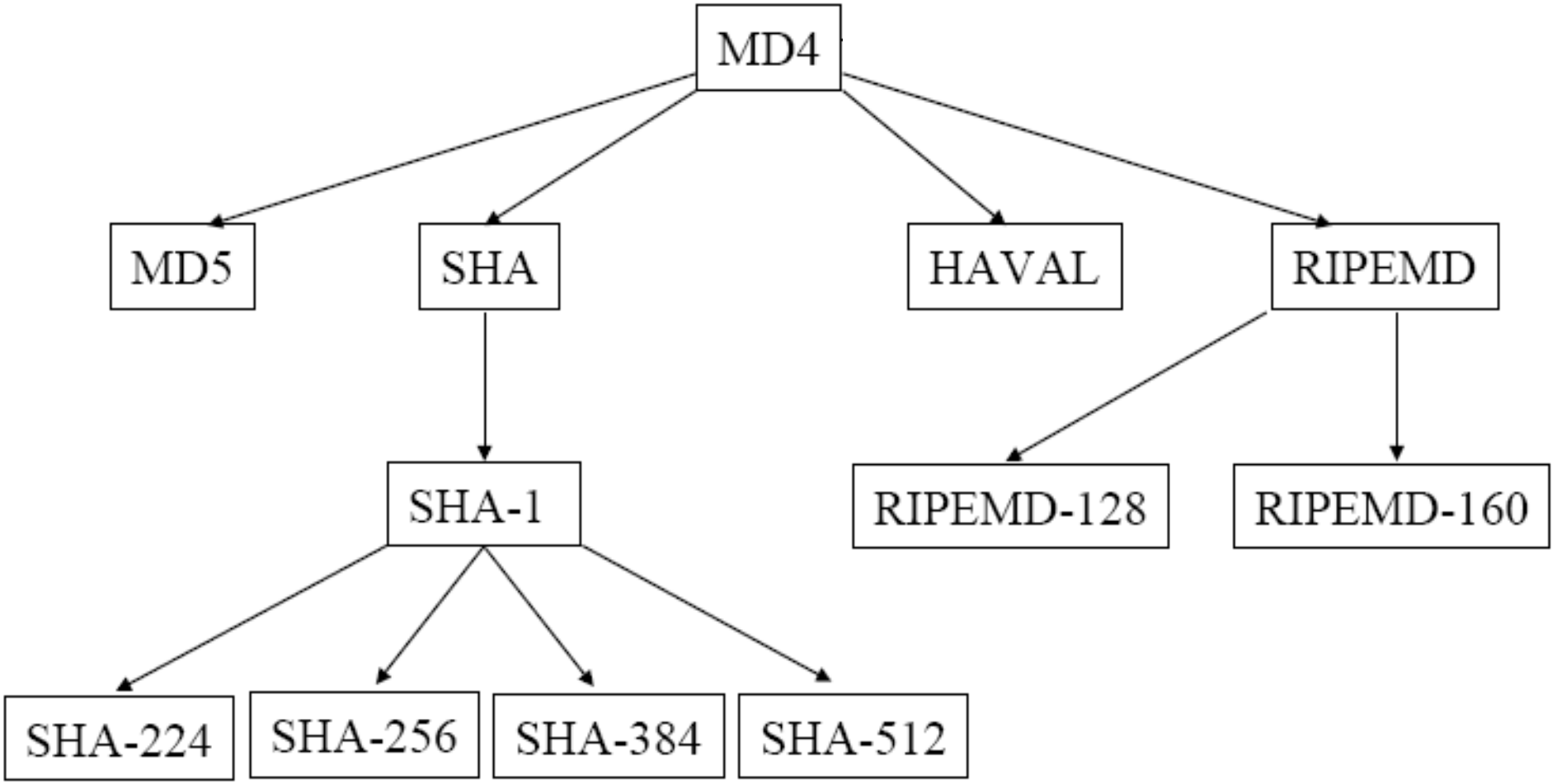
…



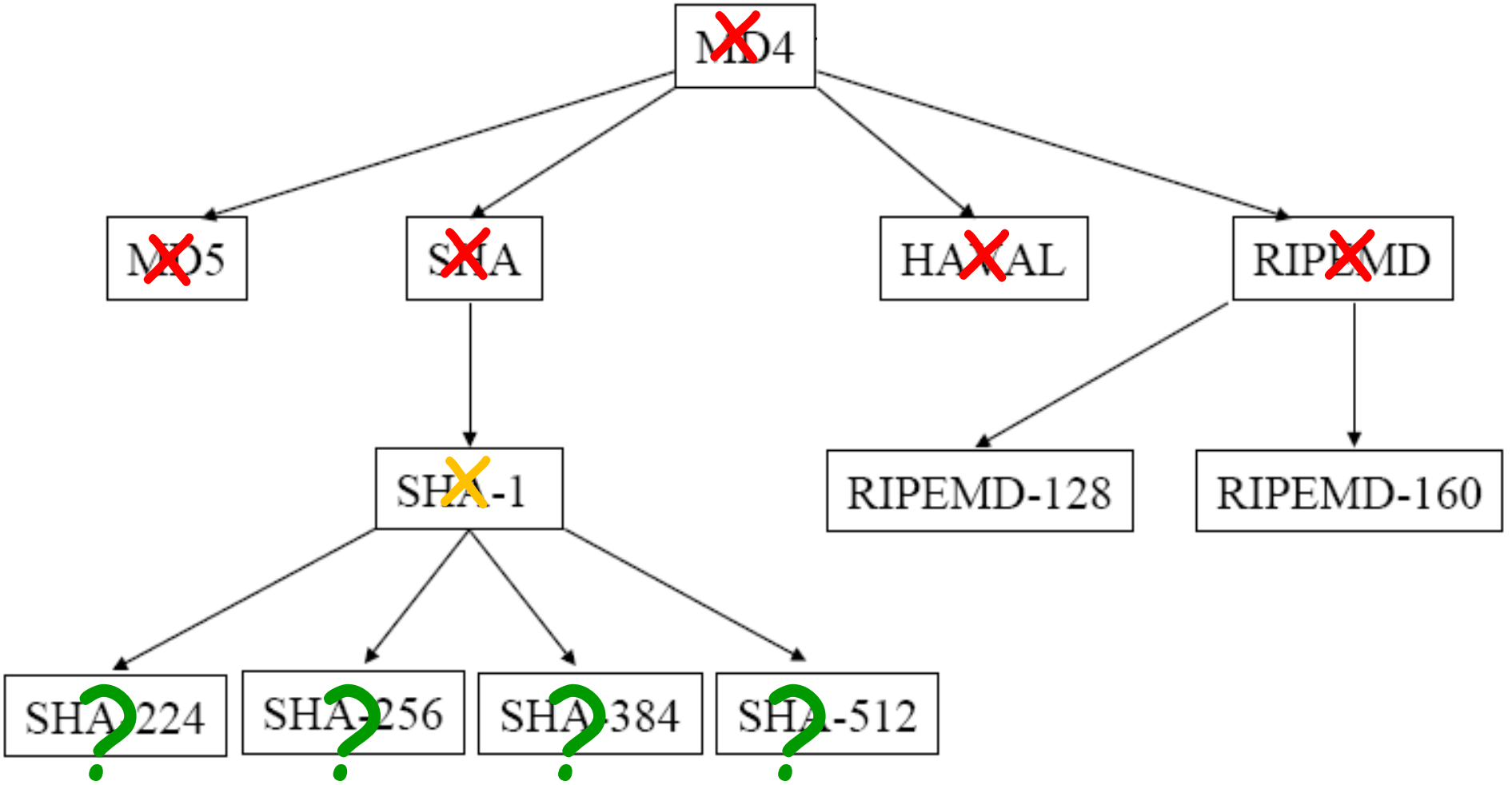
Hash functions as a fundamental primitive



MD4 family


MD4
MD5
SHA
HAVAL
RIPEMD
SHA-1
RIPEMD-128
RIPEMD-160
SHA-224
SHA-256
SHA-384
SHA-512

MD4 family


MD4
MD5
SHA
HAVAL
RIPEMD
SHA-1
RIPEMD-128
RIPEMD-160
SHA-224
SHA-256
SHA-384
SHA-512

Collisions for reduced SHA-1

40 rounds: Biham, Chen, 2005

58 rounds: Wang, Yu, Yin, 2005

64 rounds: De Cannière, R., 2006

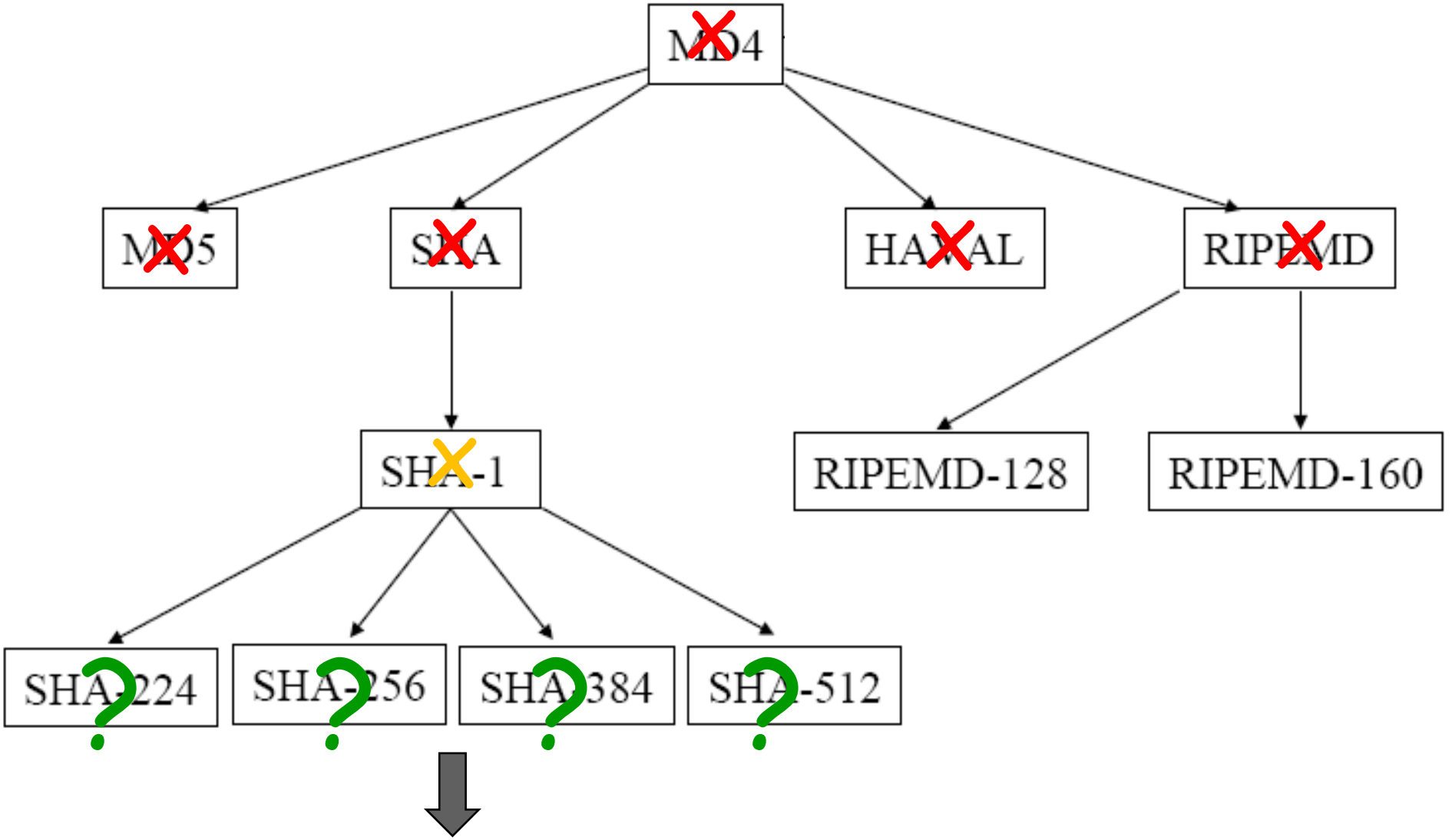
70 rounds: De Cannière, Mendel, R., 2007

Full 80 rounds?

What are the problems

- Too fast?
- Designers too optimistic
- New powerful variants of differential cryptanalysis

Road towards SHA-3



SHA-3 (selected in an open competition)

Design challenges for SHA-3

Faster than SHA-2 on many platforms

More secure than SHA-2, confidence

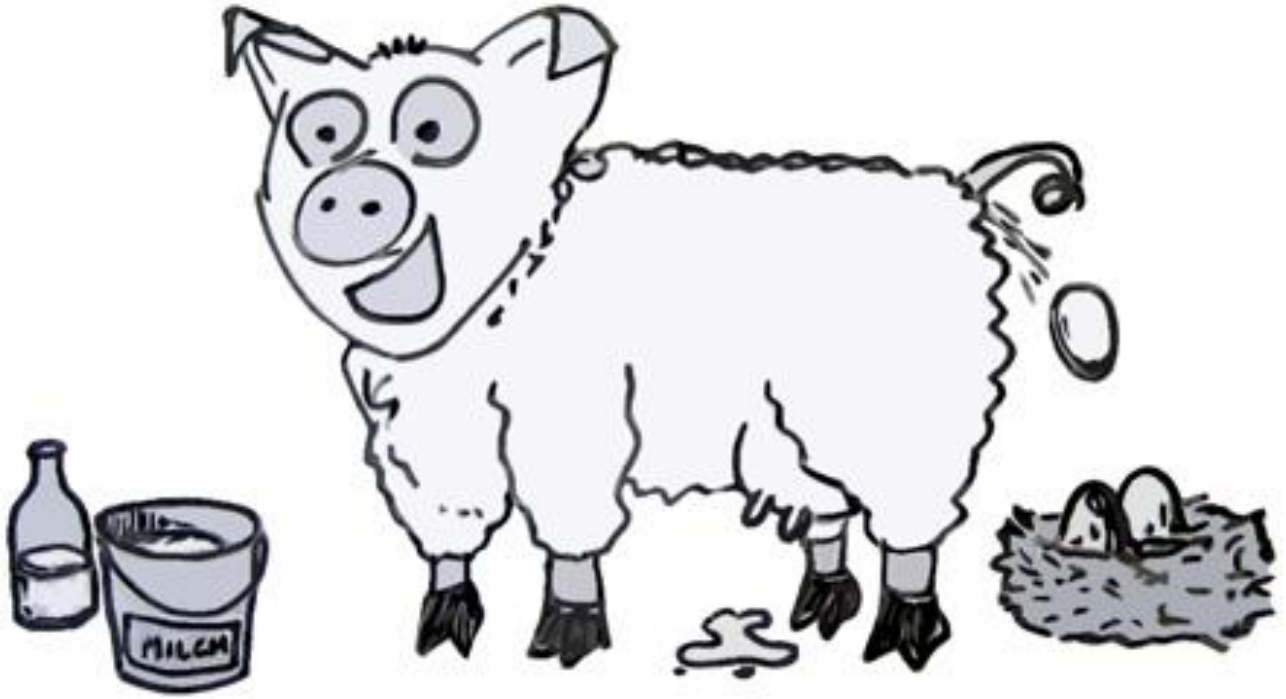
All the properties that you could think of now and in the years to come

Design challenges for SHA-3

Faster than SHA-2 on many platforms

More secure than SHA-2, confidence

All the properties that you could think of now and in the years to come



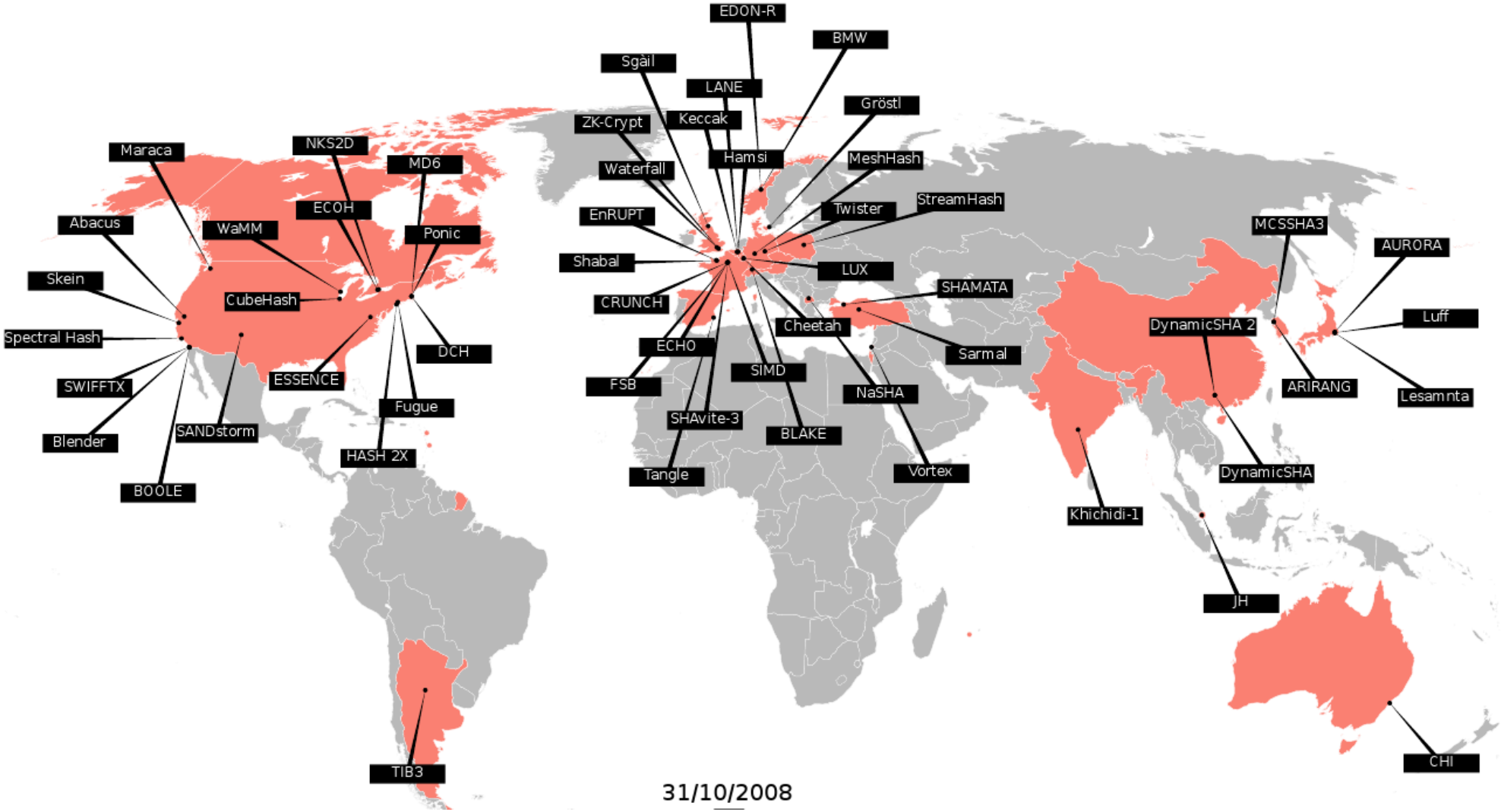
Outline

- Motivation
- SHA-3 competition
- Grøstl and the rebound attack
- SHA-3 candidates through the rebound lens
- Concluding discussions

SHA-3 competition

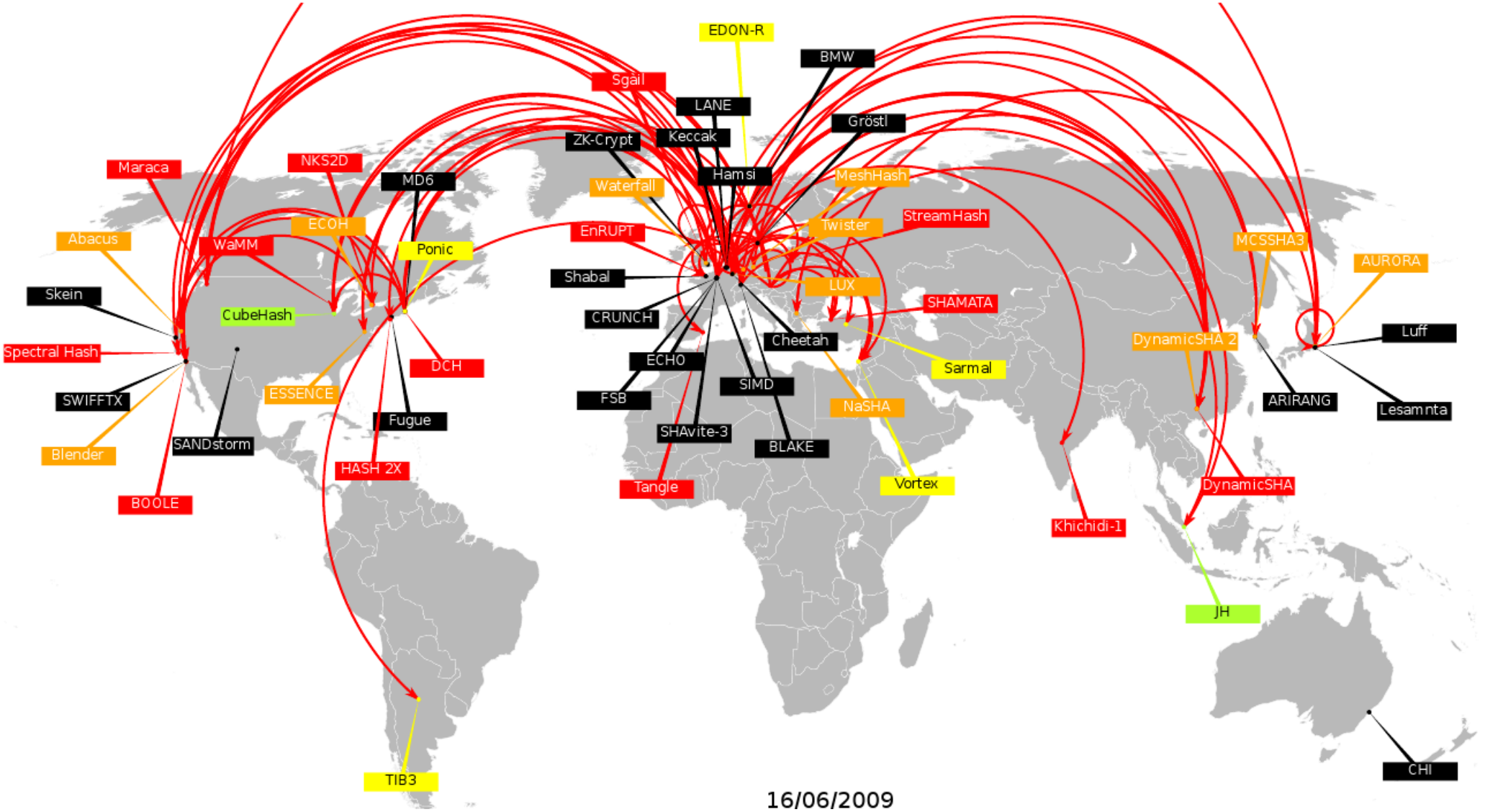
- 2006/2007: NIST drafts requirements and calls for submissions
- 10/2008: 64 submissions, >200 designers
- 12/2008: 51 round-1 candidates announced
- 07/2009: 14 round-2 candidates announced
- 12/2010: Five finalists announced
- Q2 2012: Final selection

The candidates



Slides credits: Christophe De Cannière

Preliminary cryptanalysis



ECRYPT II

navigation
- The eHash Main Page
- Hash Function Zoo
- SHA-3 Zoo
- Recent changes
- Random page
- Help

search
Go Search

toolbox
- What links here
- Related changes
- Special pages
- Printable version
- Permanent link

The SHA-3 Zoo

The SHA-3 Zoo (work in progress) is a collection of cryptographic hash functions (in alphabetical order) submitted to the SHA-3 contest (see also here). It aims to provide an overview of design and cryptanalysis of all submissions. A list of all SHA-3 submitters is also available. For a software performance related overview, see eBASH. At a separate page, we also collect hardware implementation results of the candidates. Another categorization of the SHA-3 submissions can be found here.

The idea of the SHA-3 Zoo is to give a good overview of cryptanalytic results. We try to avoid additional judgement whether a submission is broken. The answer to this question is left to NIST. However, we categorize the cryptanalytic results by their impact from very theoretic to practical attacks. A detailed description is given in Cryptanalysis Categories.

At this time, 56 out of 64 submissions to the SHA-3 competition are publicly known and available. 51 submissions have advanced to round 1 and 14 submissions have made it into round 2.

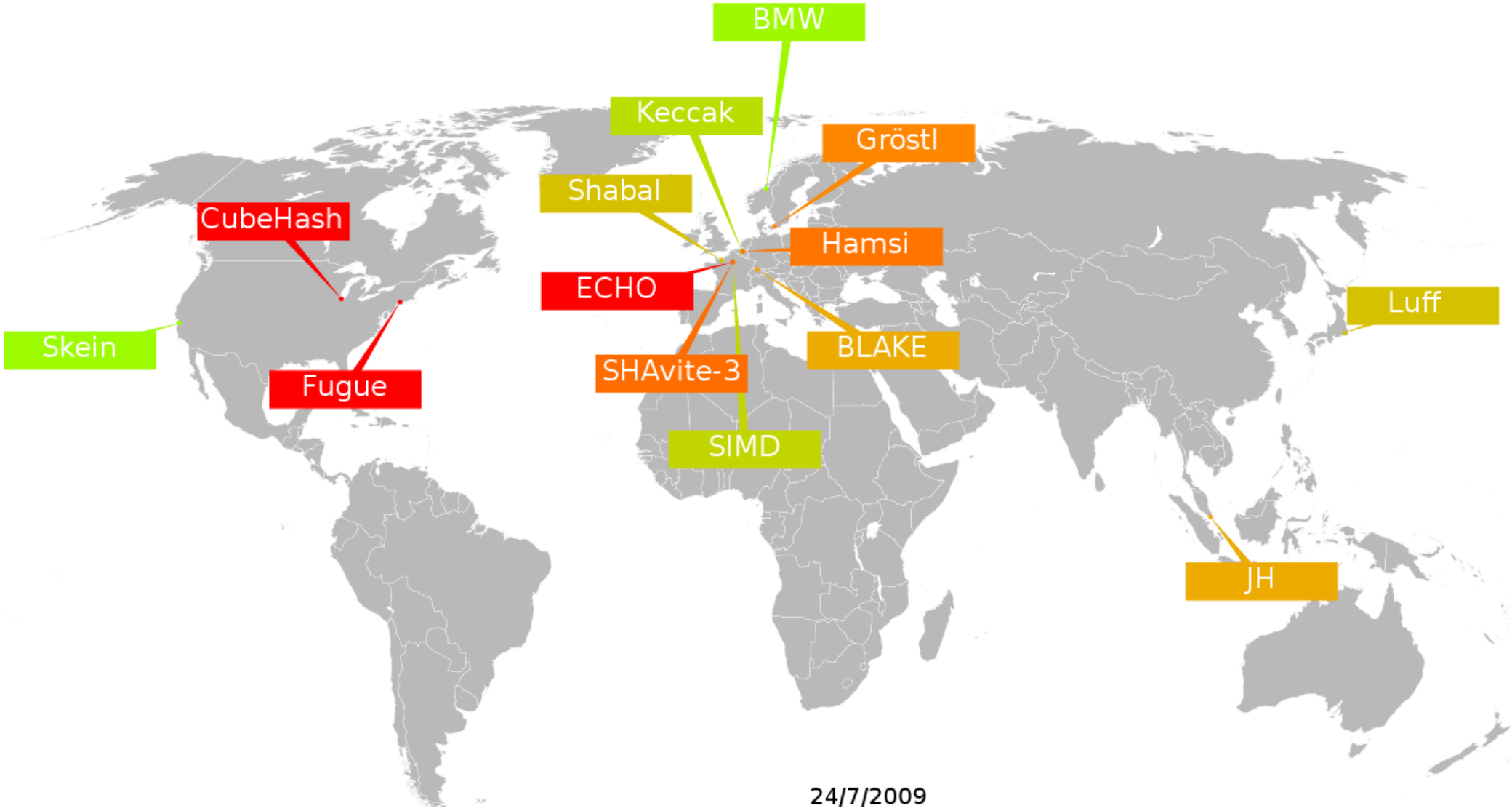
The following table should give a first impression on the remaining SHA-3 candidates. It shows only the best known attack, more detailed results are collected at the individual hash function pages. A description of the main table is given here.

Recent updates of the SHA-3 Zoo

The 5 finalists of the SHA-3 competition are:

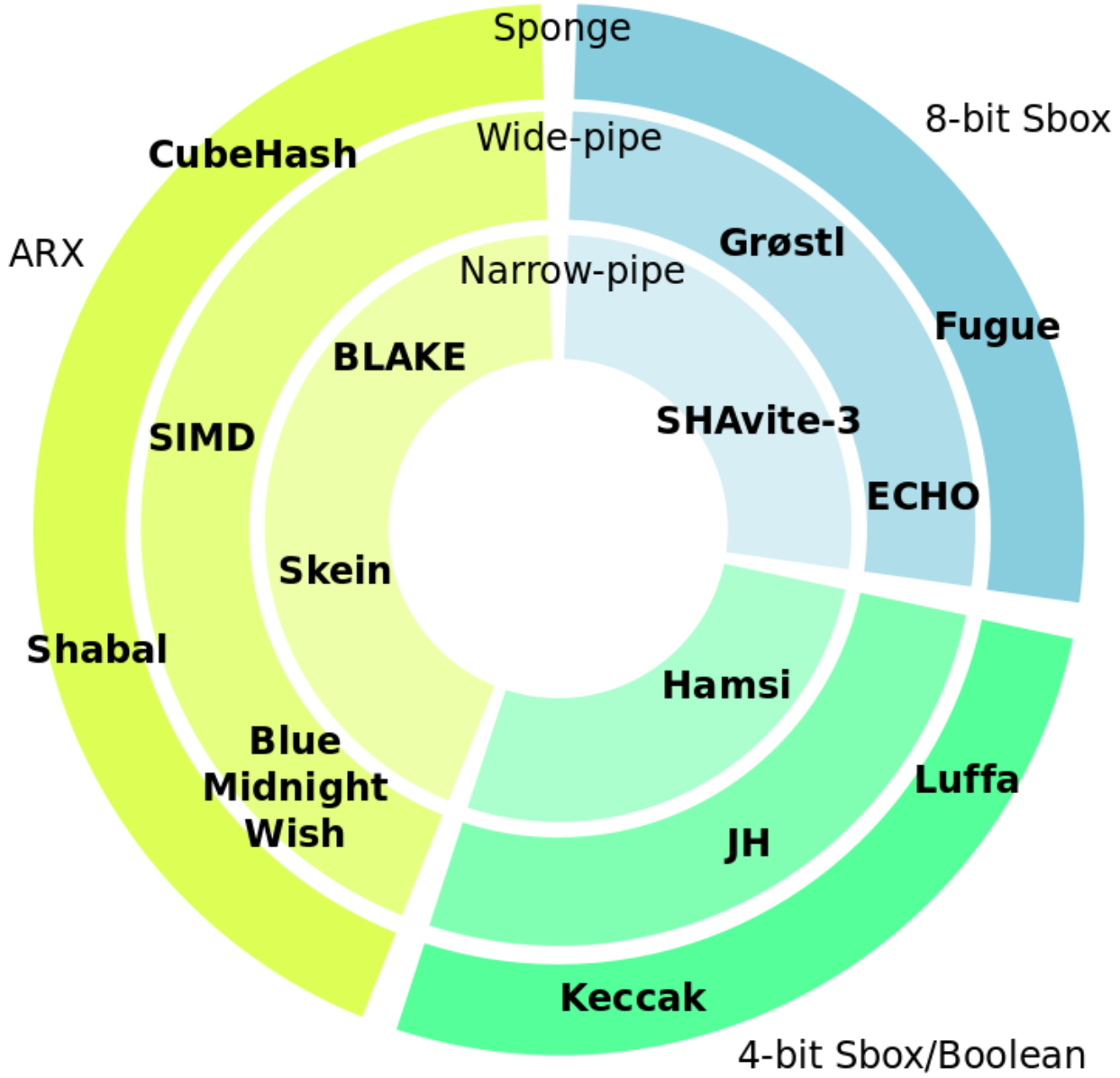
Hash Name	Principal Submitter	Best Attack on Main NIST Requirements	Best Attack on other Hash Requirements
BLAKE	Jean-Philippe Aumasson		
Grøstl	Lars R. Knudsen		
JH	Hongjun Wu	preimage	
Keccak	The Keccak Team		
Skein	Bruce Schneier		

Round-2 candidates



How to categorize them?

How to categorize them?



Credits to

Dai Watanabe

How to compare them?

- Security
- Performance/Implementation costs
  - Software (code size, speed, ...)
  - Hardware (lowest gate count, highest throughput, power consumption characteristics, …)
  - Side-Channel countermeasures
- Confidence?

Grøstl

Grøstl is inspired by

- Rijndael/AES (Daemen, Rijmen, 1997)
- SMASH (Knudsen, 2005)
- Grindahl (Knudsen, R., Thomsen, 2007)

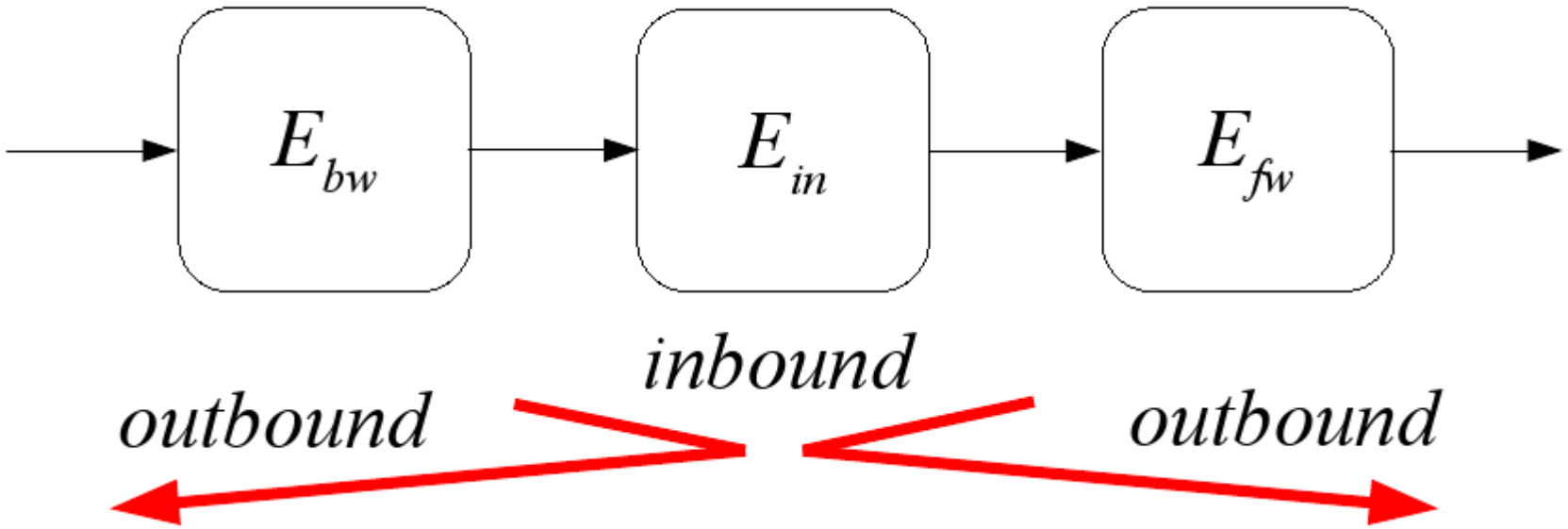
Proofs against differential attacks

Proofs against generic shortcut attacks

Rebound attack

New variant of differential cryptanalysis, FSE 2009

Developed during the design of Grøstl



Origins of the rebound attack

Differential attack, Biham and Shamir, 1989

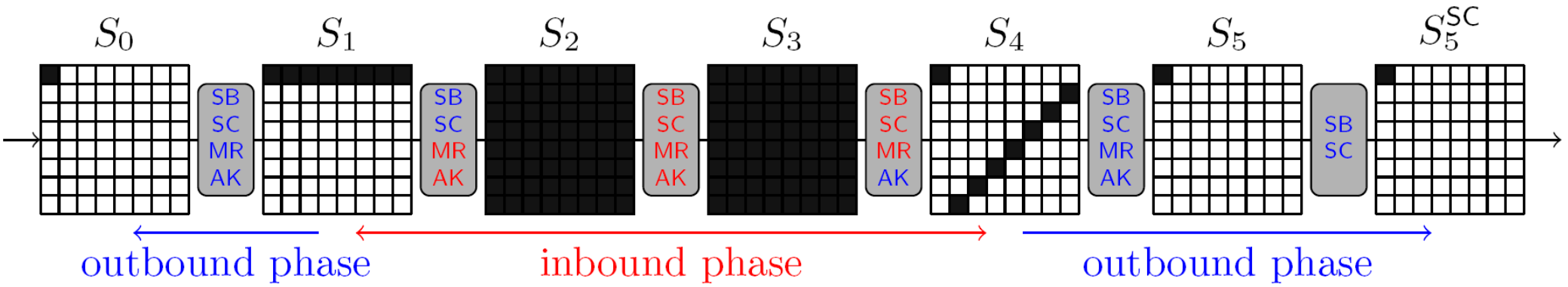
Inside-out approach, Dobbertin 1995, Wagner 1998

Truncated differential, Knudsen, 1994

Original Goal:

Get a good estimate of the security margin of Grøstl

Example of a rebound attack



Within a few months, others became a “victim”:

- Twister (round-1 SHA-3 candidate)
- LANE (round-1 SHA-3 candidate)
- Whirlpool (ISO standard, unbroken since 2001)
- …

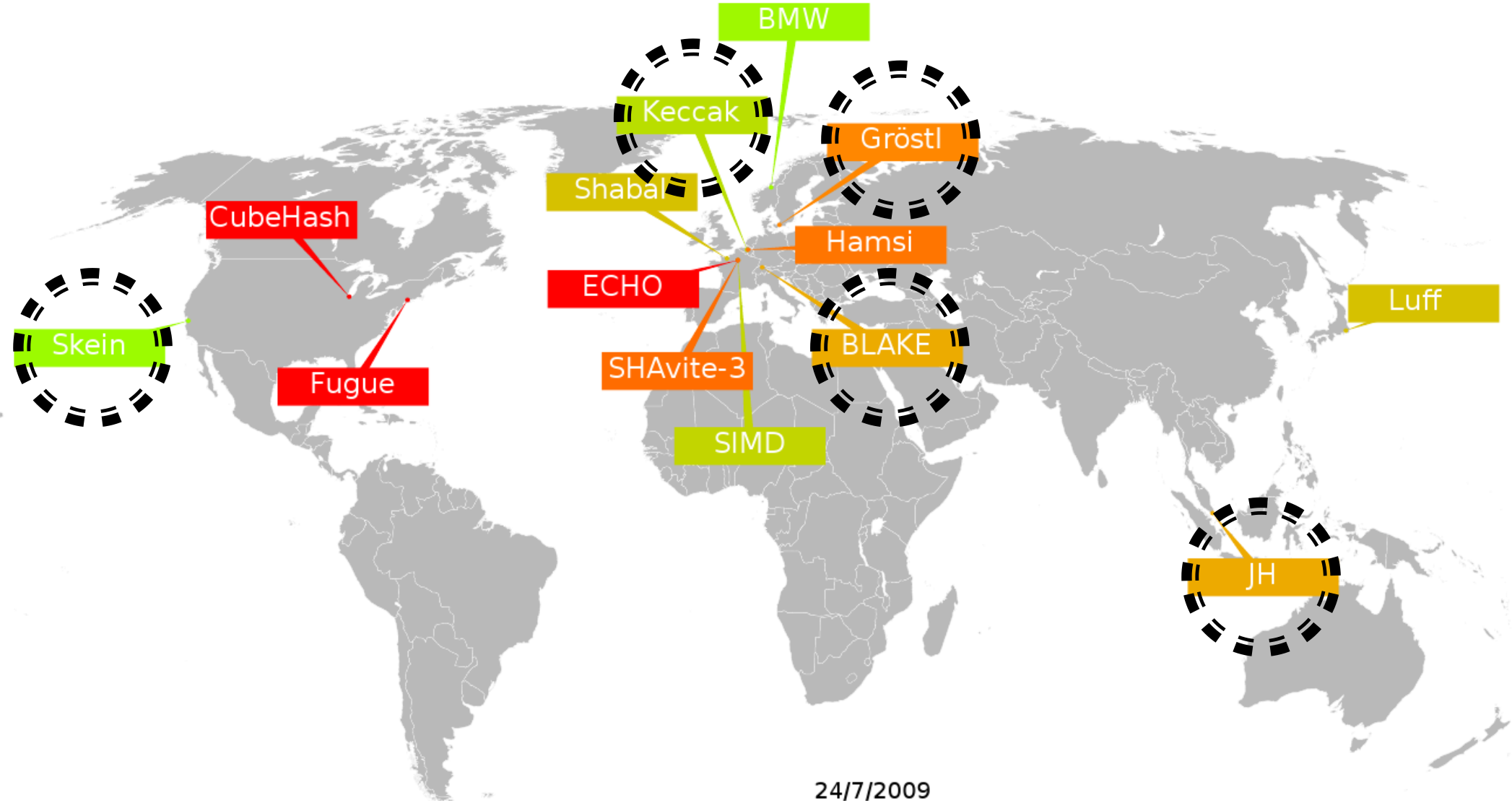
Further technical developments

The

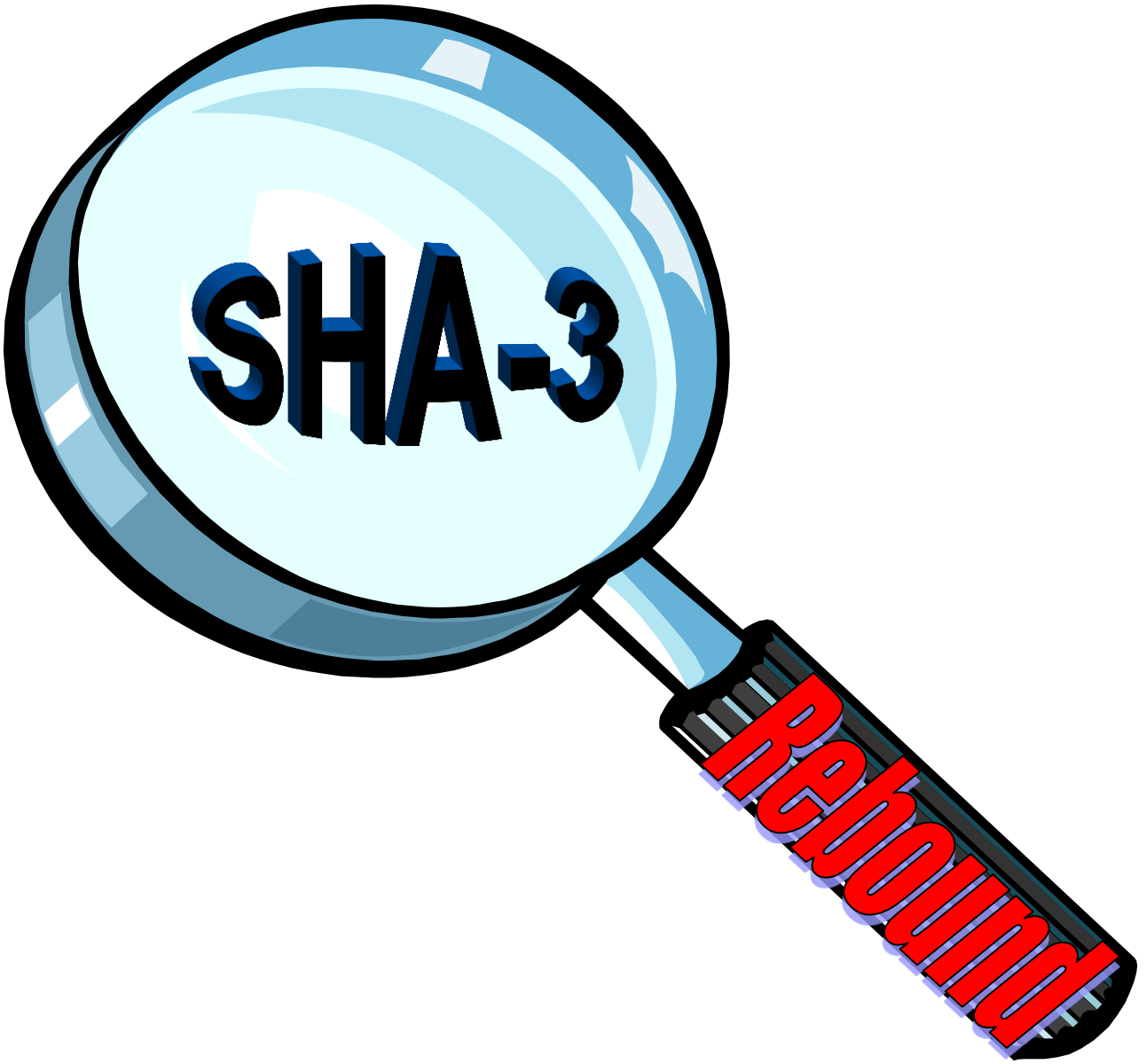
- Linear solving variant (SAC 2009)
- Start-in-the-middle variant (SAC 2009)
- Super(S)box variant (Asiacrypt 2009 and FSE 2010)
- Multiple-inbound phase variant (Asiacrypt 2009)
- Rotational variant (Asiacrypt 2010)

...of the rebound attack

SHA-3 finalists




Rehind


SHA-3
Rebound

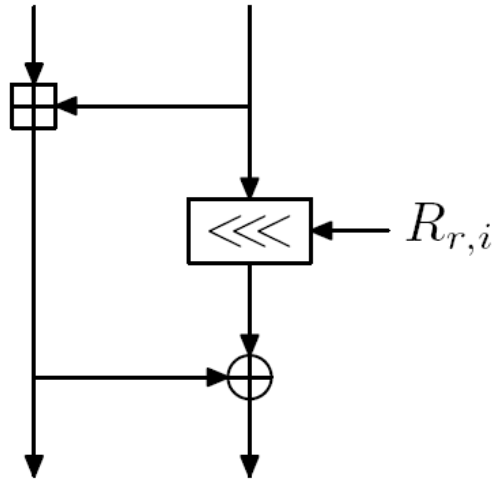
SHA-3 round-2 candidates through the rebound lens

4 or 8-bit S-box based	*Others*
Grøstl	Skein
ECHO	BMW
JH	Blake
Luffa	Cubehash
Shavite-3	Keccak
Fugue	SIMD
Hamsi	Shabal

SHA-3 round-2 candidates through the rebound lens

4 or 8-bit S-box based		*Others*	
Grøstl	✓✓✓✓✓✓	Skein	✓
ECHO	✓✓✓✓	BMW	
JH	✓✓	Blake	
Luffa	✓✓	Cubehash	
Shavite-3	✓	Keccak	
Fugue		SIMD	
Hamsi		Shabal	

Most recent case: Skein



- Recent analysis by Khovratovich, Nikolic, R. in 2010
- Rebound idea for the first time applied to ARX construction
- Results in perspective:
  - 2009: Related-key differential attack: 34 rounds
  - 2010: Rotational attack: 42 rounds
  - **New:** Rebound rotational attack: 57 rounds

SHA-3 **finalists** through the rebound lens

4 or 8-bit S-box based		*Others*	
Grøstl	✓✓✓✓✓✓✓	Skein	✓
ECHO	✓✓✓✓	BMW	
JH	✓✓	Blake	
Luffa	✓✓	Cubehash	
Shavite-3	✓	Keccak	
Fugue		SIMD	
Hamsi		Shabal	

SHA-3 finalists in numbers

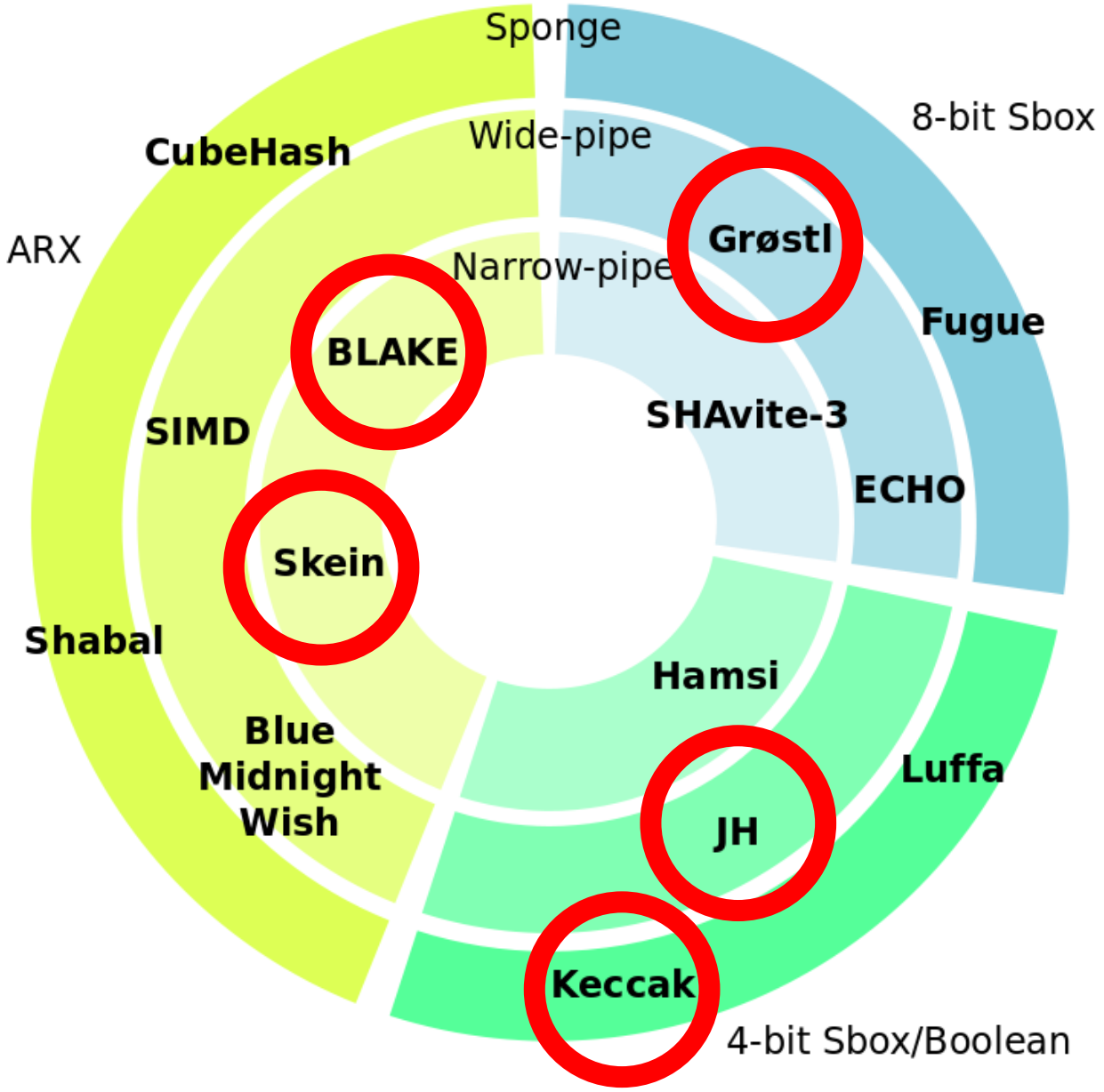
Geography:
3 from Europe, 1 from Asia, 1 from America

Tweaks:
|all 5 got tweaked, 2 got tweaked twice

Team members also AES finalist: 3

Teams that designed a hash function before: 2

How to categorize them?



Credits to

Dai Watanabe

SHA-3 finalists

Compression strategy:

- Single Permutation: Blake (with finalization), JH, Keccak
- Two Permutations: Grøstl
- Large family of permutations (block cipher): Skein

Source of non-linearity:

- 64-bit: Skein
- 32/64-bit: Blake
- 8-bit: Grøstl
- 4/5-bit: JH
- 3-bit: Keccak

Conclusion (1/2) Assurance?

Very complicated attacks against MD5 and SHA-1

(1) Differential trail with complicated carry interactions

(2) Degrees of freedom utilization for speedup

Level of assurance provided by finalists against this class of attacks:

Blake, Skein: ARX, issues similar to SHA-1/SHA-2

Grøstl: both (1) and (2) done by **rebound attacks**

JH: (1) and (2) may be possible, open problem

Keccak: seems infeasible

Conclusion (2/2)

Building confidence in a new cryptographic primitive takes time

A lot remains to be done for a final SHA-3 selection by 2012

Upcoming: ECRYPT Hash Workshop 2011, May 19-20, Tallinn

The road ahead

- Application of new cryptanalytic techniques to other areas, examples
  - Internal fixed points:
    - Collision and preimage attack on GOST hash: 2008
    - Key recovery attack on GOST block cipher: 2011
  - Local collisions:
    - Collisions in SHA-0: 1998
    - Related-key attacks on AES: 2009
- New lightweight algorithms, where designers cut corners

Towards SHA-3

Q&A

Christian Rechberger, KU Leuven

Backup slides

Addendum: Grøstl?

Call for input

Name	Country
Gröstl	Austria
Hash	USA
Bubble and squeak	United Kingdom
Rumbledethumps/Stovies	Scotland
Colcannon	Ireland
Bauernfrühstück	Germany
Stamppot	Netherlands
Pyttipanna	Finland, Norway, Sweden
Biksemad	Denmark
Roupa Velha	Portugal
Bergerdil	Malaysia
Ha'DIBaH 'ay'mey 'oQqar je	Qo'noS (Klingon)