Hash Functions and Cryptographic Competitions

Christian Rechberger

TU Graz
Taceo

Fundamental questions in CS theory

Do oneway functions exist?

Do collision-intractable functions exist?

New: Do equivocal hash 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

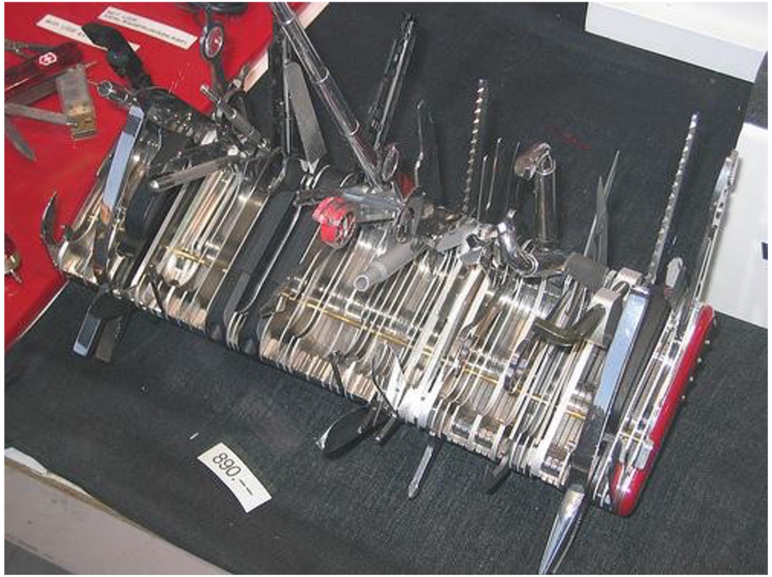
Near-collision resistance

Pseudorandom generator

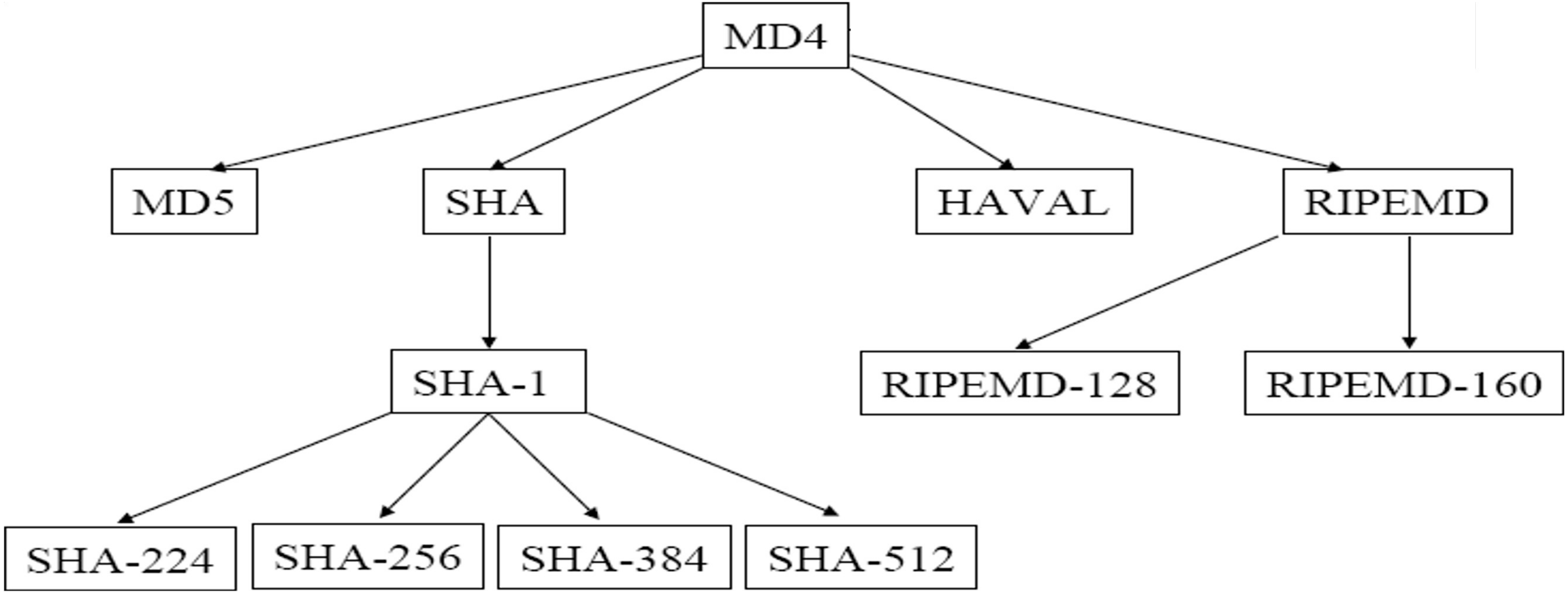
Pseudorandom function

Key derivation function

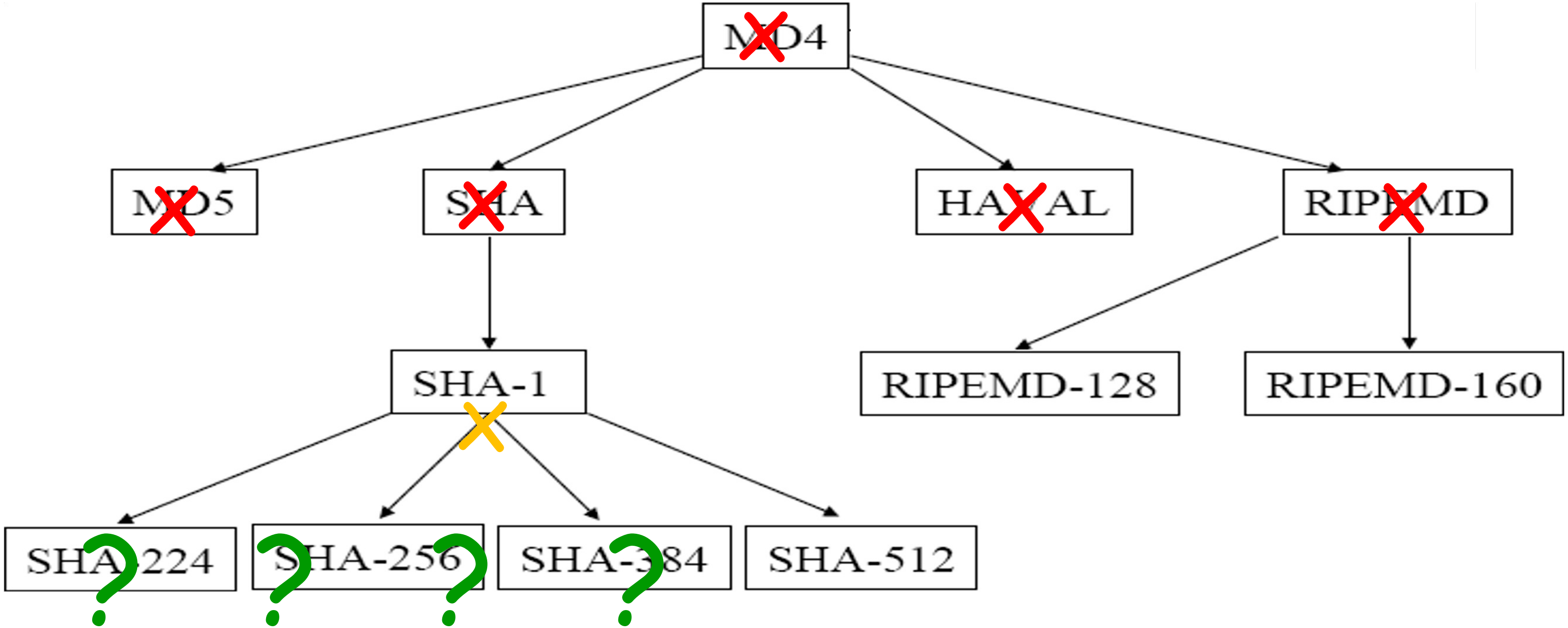
Random oracle



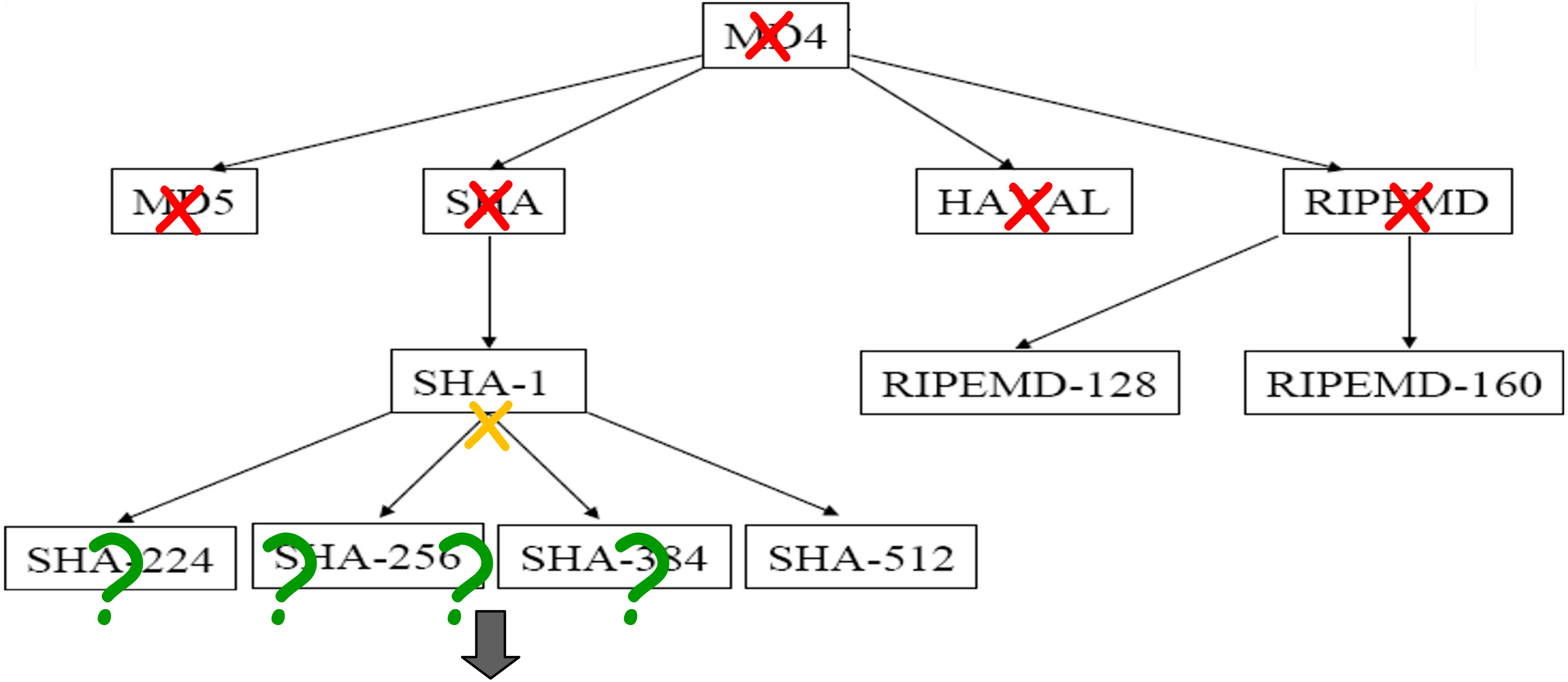
A bit of history: MD4 family



Cryptanalysis status in 2005



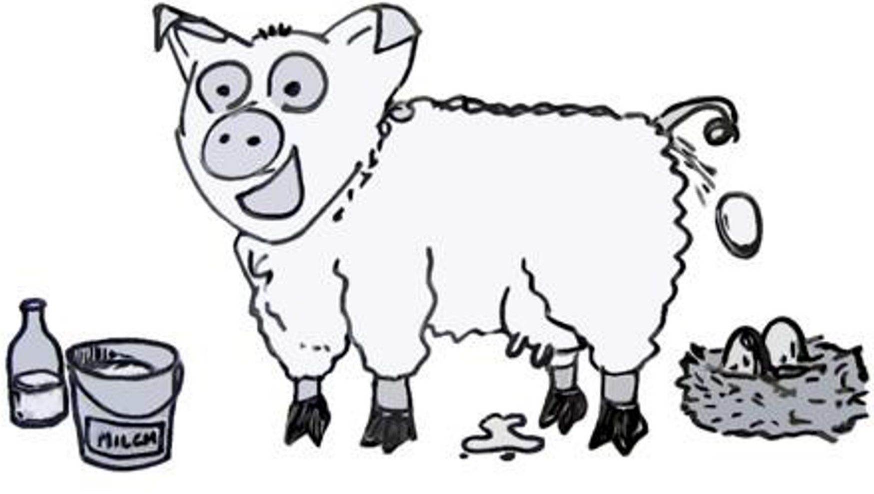
Road towards SHA-3



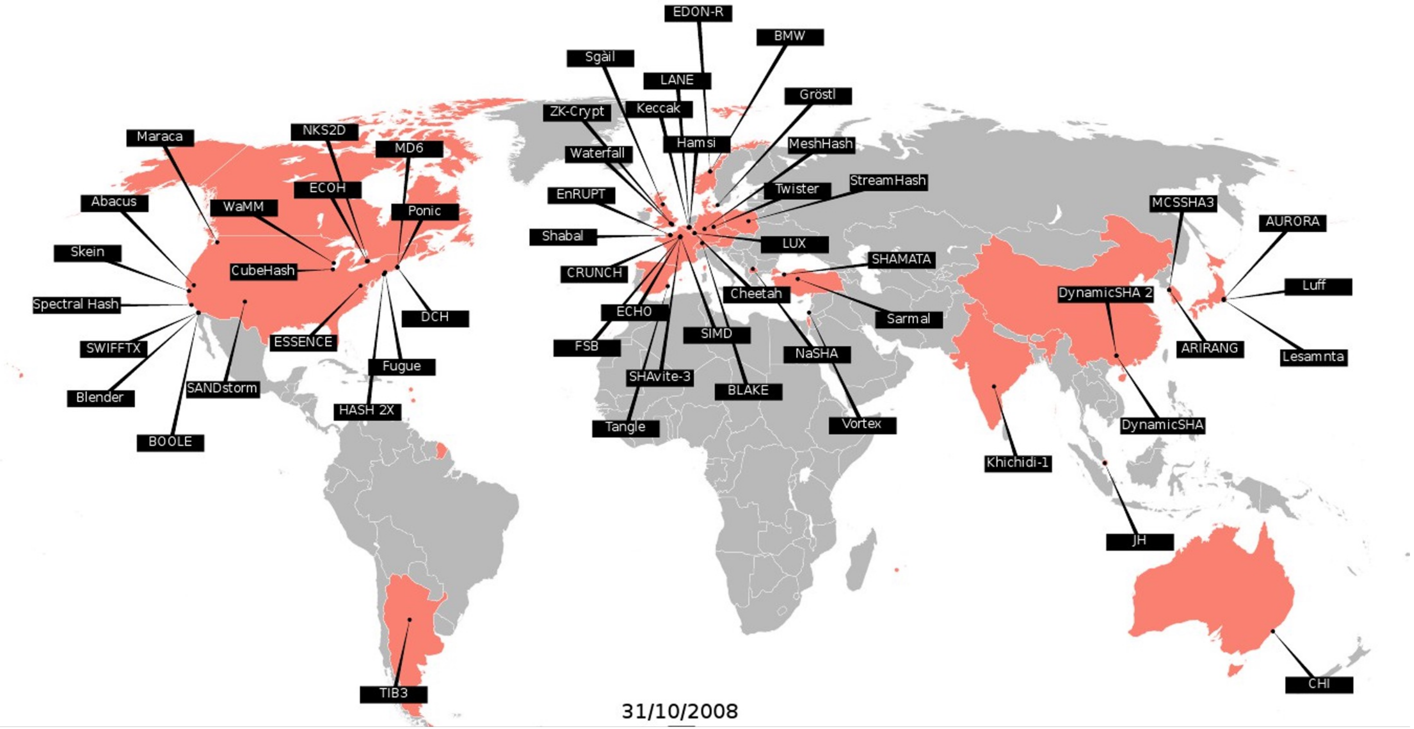
SHA-3 (open competition 2006-2012)

Usual requirements for “hash functions”

All the properties that you could think of now and in the y



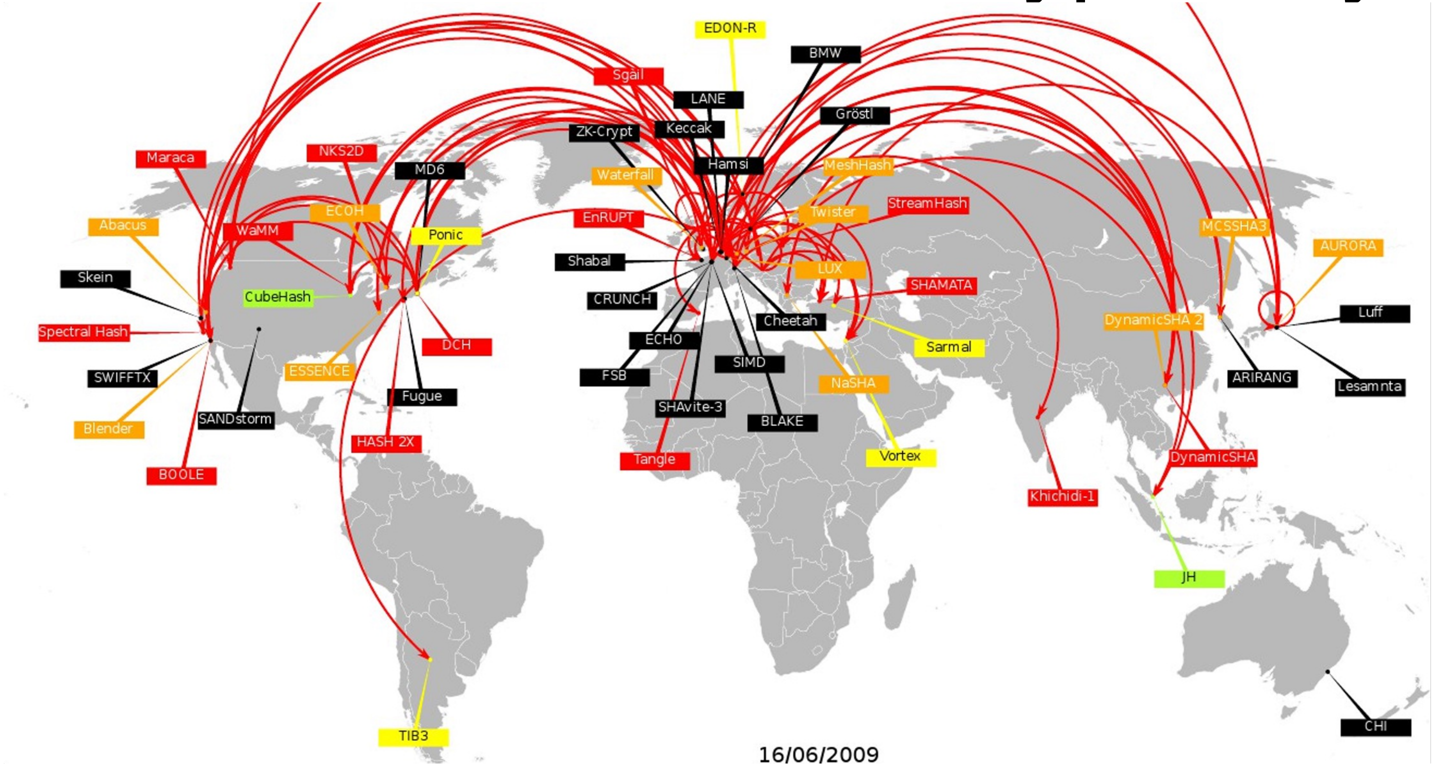
The SHA-3 candidates



31/10/2008

Slides credits: Christophe De Cannière

First 6 months of cryptanalysis



16/06/2009

More recent competitions

Ecrypt Lightweight Crypto □ NIST Lightweight Crypto

NIST Post-Quantum Crypto

A long shot:

practical, but super-adhoc and fragile realization of notions similar to iO: White-box cryptography

Research gap: quantum-secure white-box

My conclusion

Building confidence in a new cryptographic primitive takes time