

Dedicated Collision Search

Christian Rechberger

Special-purpose Hardware for Attacking Cryptographic Systems
SHARCS 2007

SHA-1 Collision Search: <http://boinc.iaik.tugraz.at>

***Institute for Applied Information Processing
and Communications (IAIK) - Krypto Group***

***Faculty of Computer Science
Graz University of Technology***



Supported by the Austrian Science Fund (FWF), project P18138.

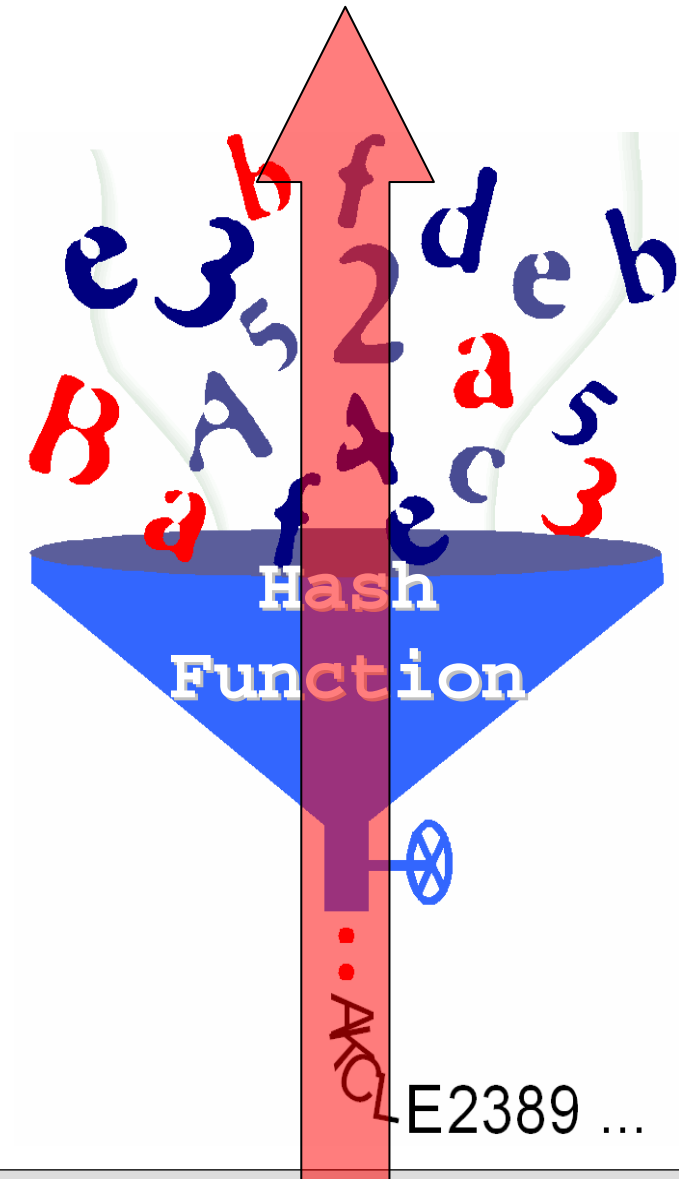
Motivation

- Browse SSL-secured websites
 - Administer your server via `ssh`
 - Console login
 - Digitally sign something
 - Integrity checks of p2p traffic
 - ...
-
- What do they have in common?

Some properties of hash functions

- Efficient to compute
- One-wayness
- Collision resistance

One-wayness



One-wayness

Applications:

Storing a password

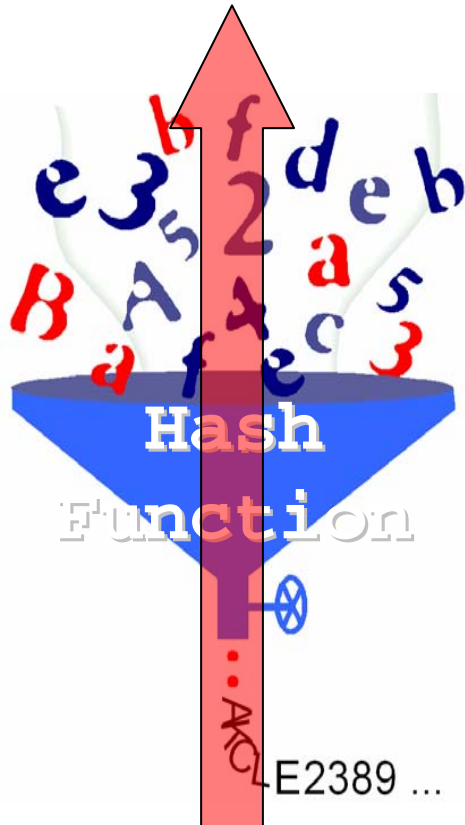
Payment schemes (e.g. Hashcash)

Key derivation

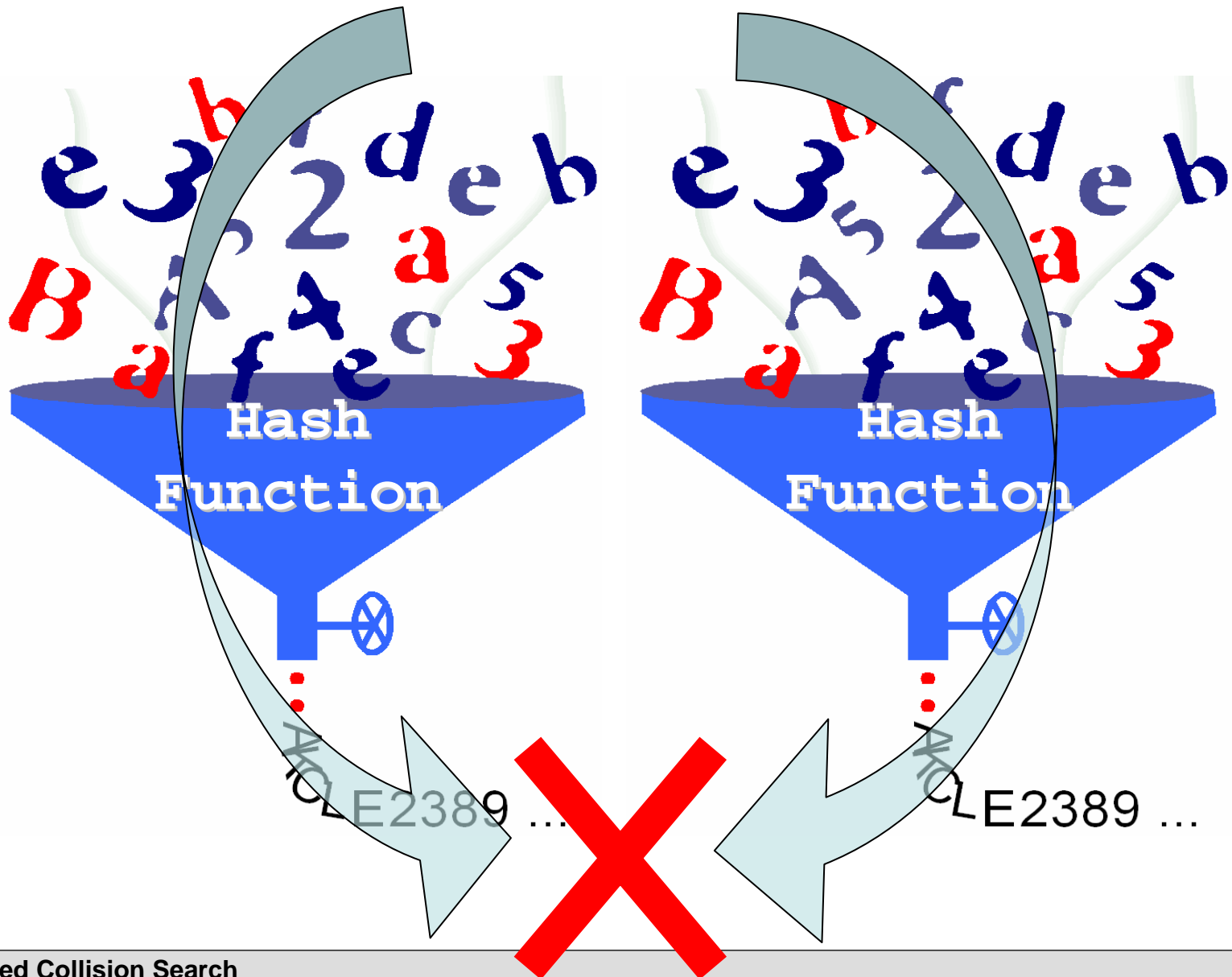
Commitment schemes

Random number generation

...

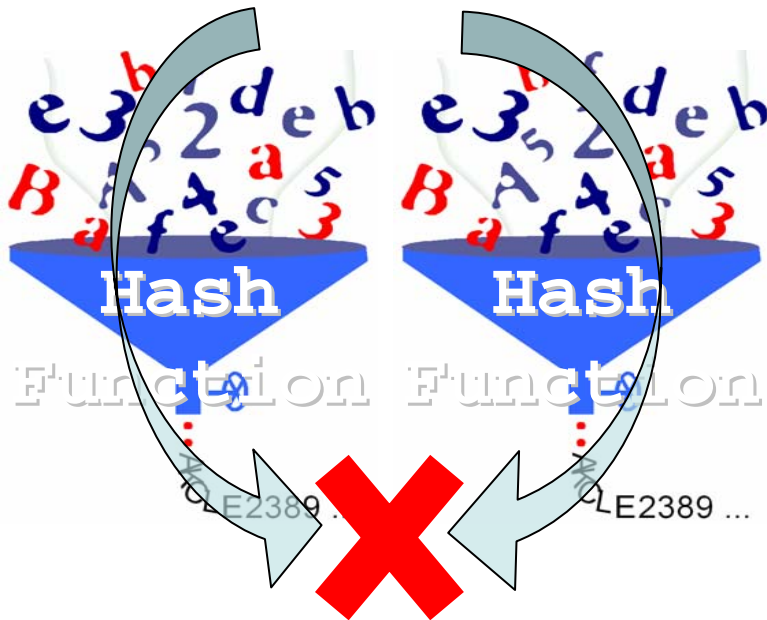


Collision resistance



Collision resistance

Applications:

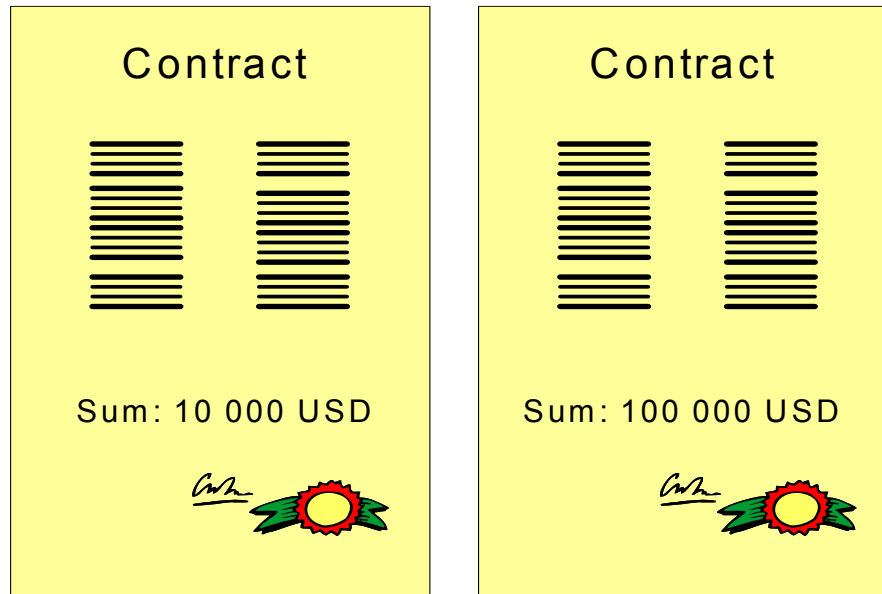


Integrity checks

Authentication
(Digital signatures,
MAC, ...)

Often required by law

Application requiring collision resistance

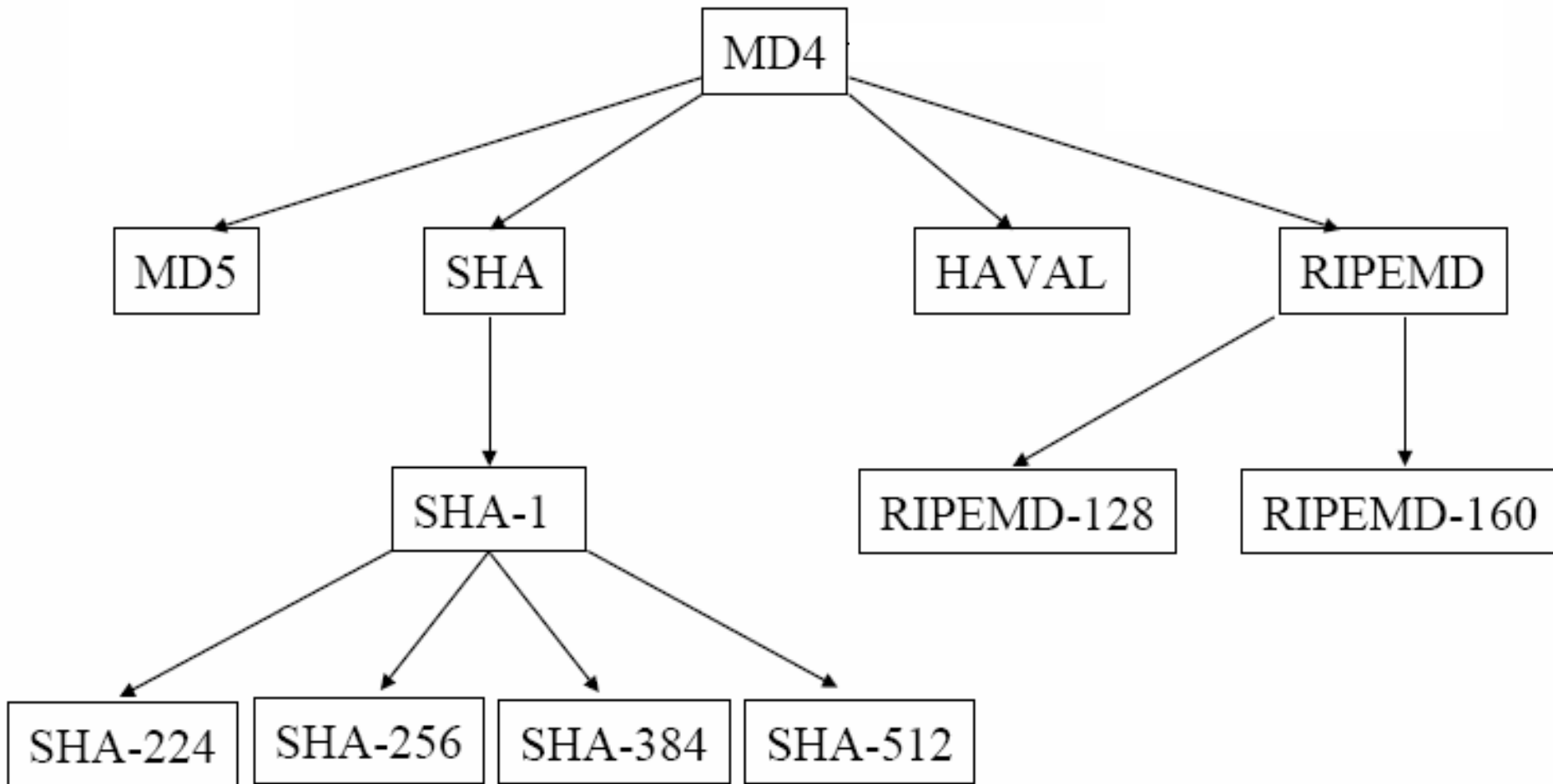


Two documents producing the same fingerprint.

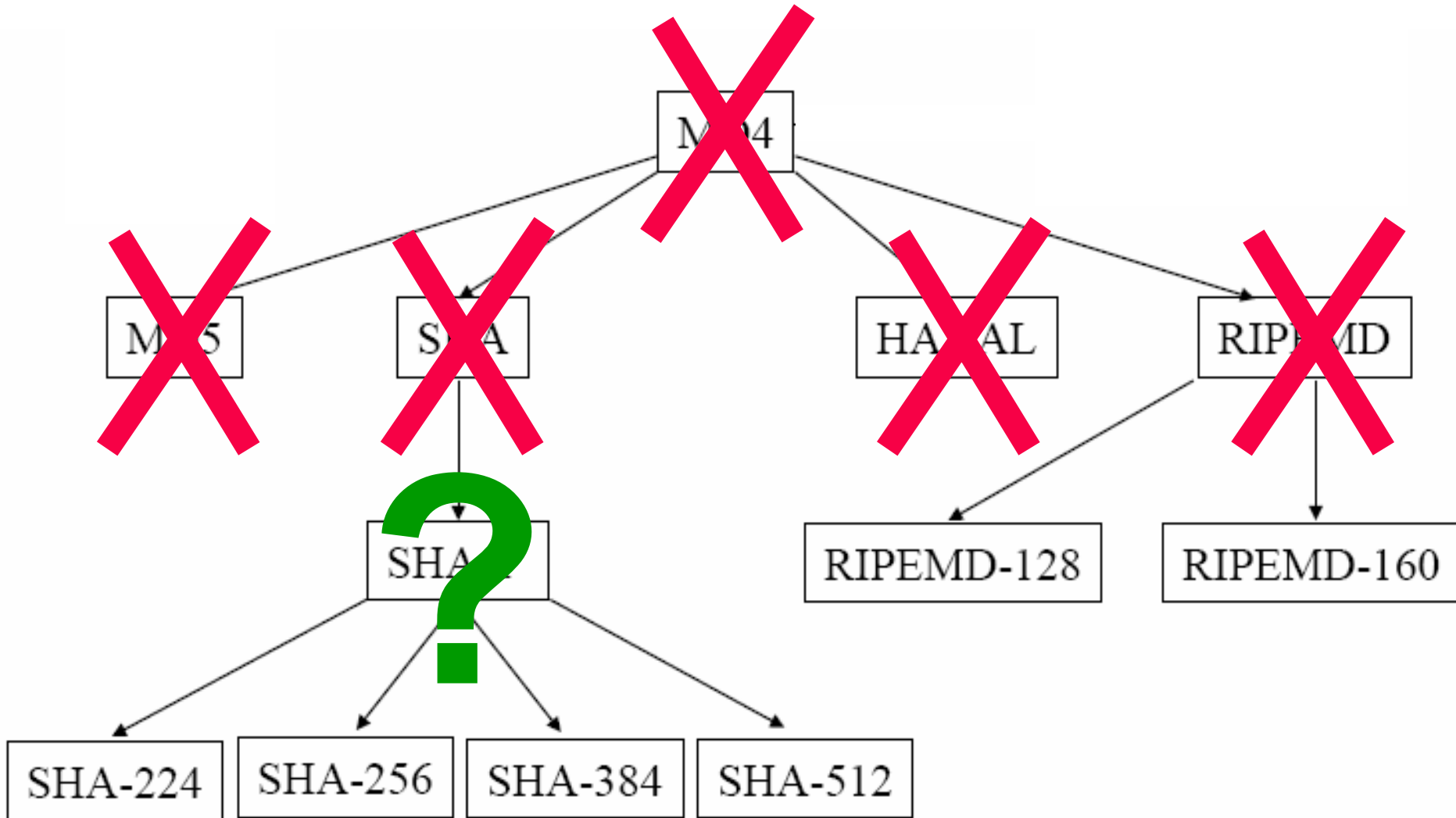
Same fingerprints \Rightarrow same signatures.

Signature verifier can not detect replacing of document

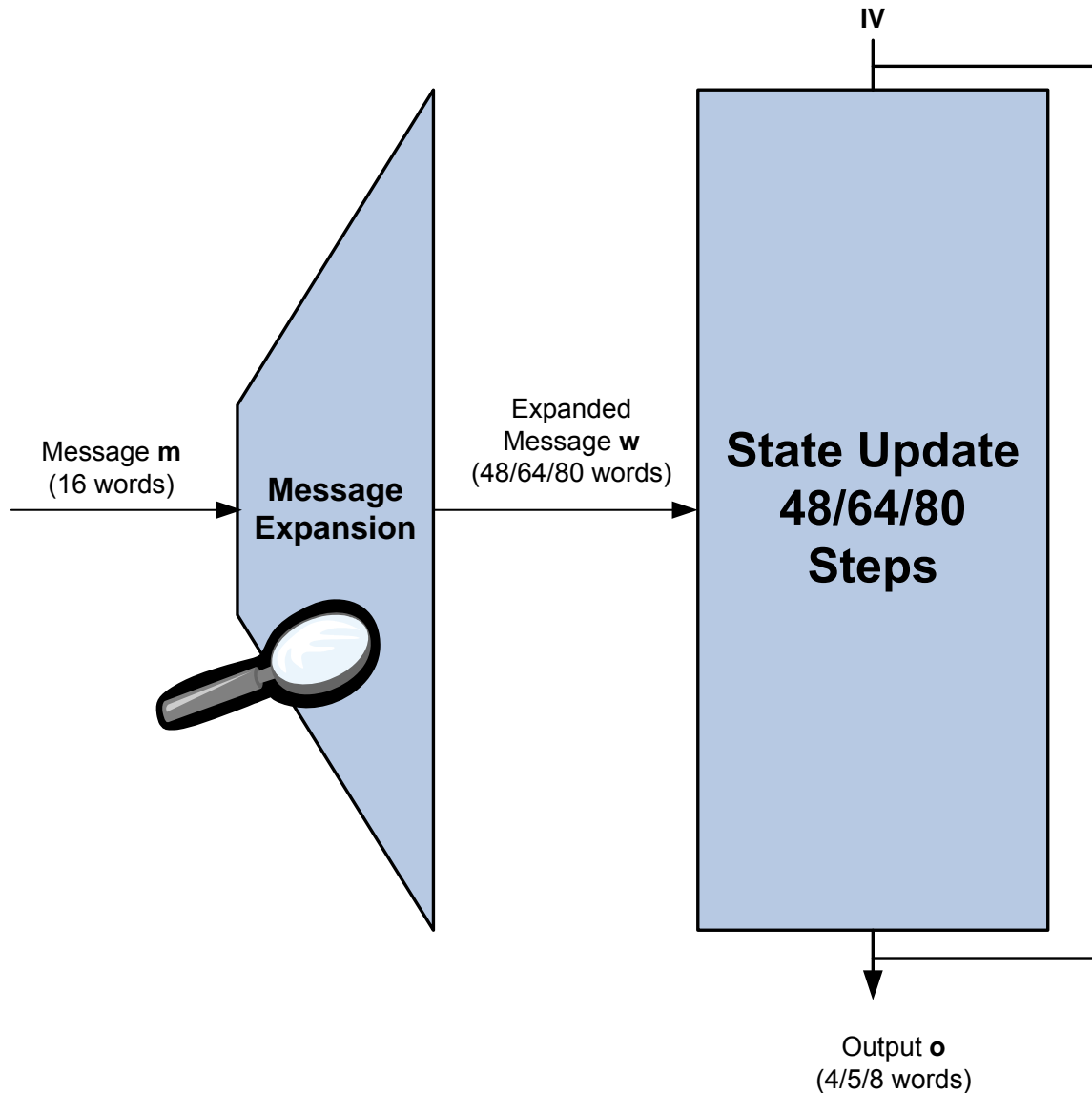
What happened so far?



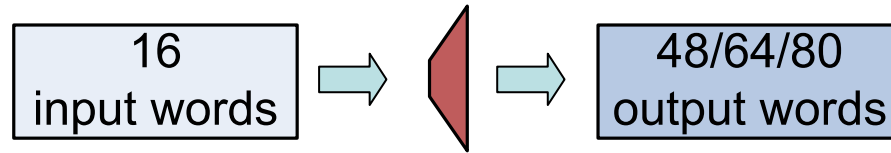
What happened so far?



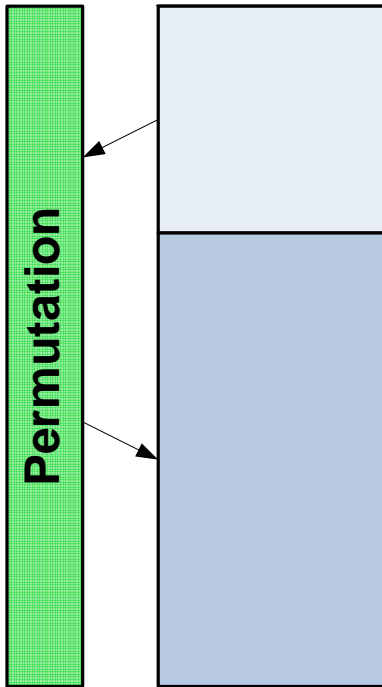
Outline of MD4-style Hash Functions



Message Expansions in the MD4 family



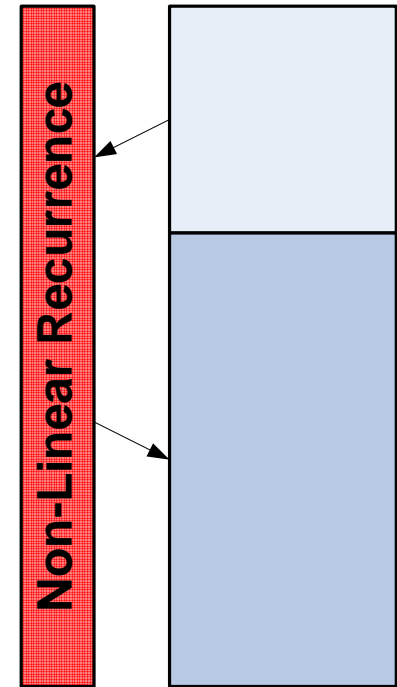
MD4/5, RIPEMD



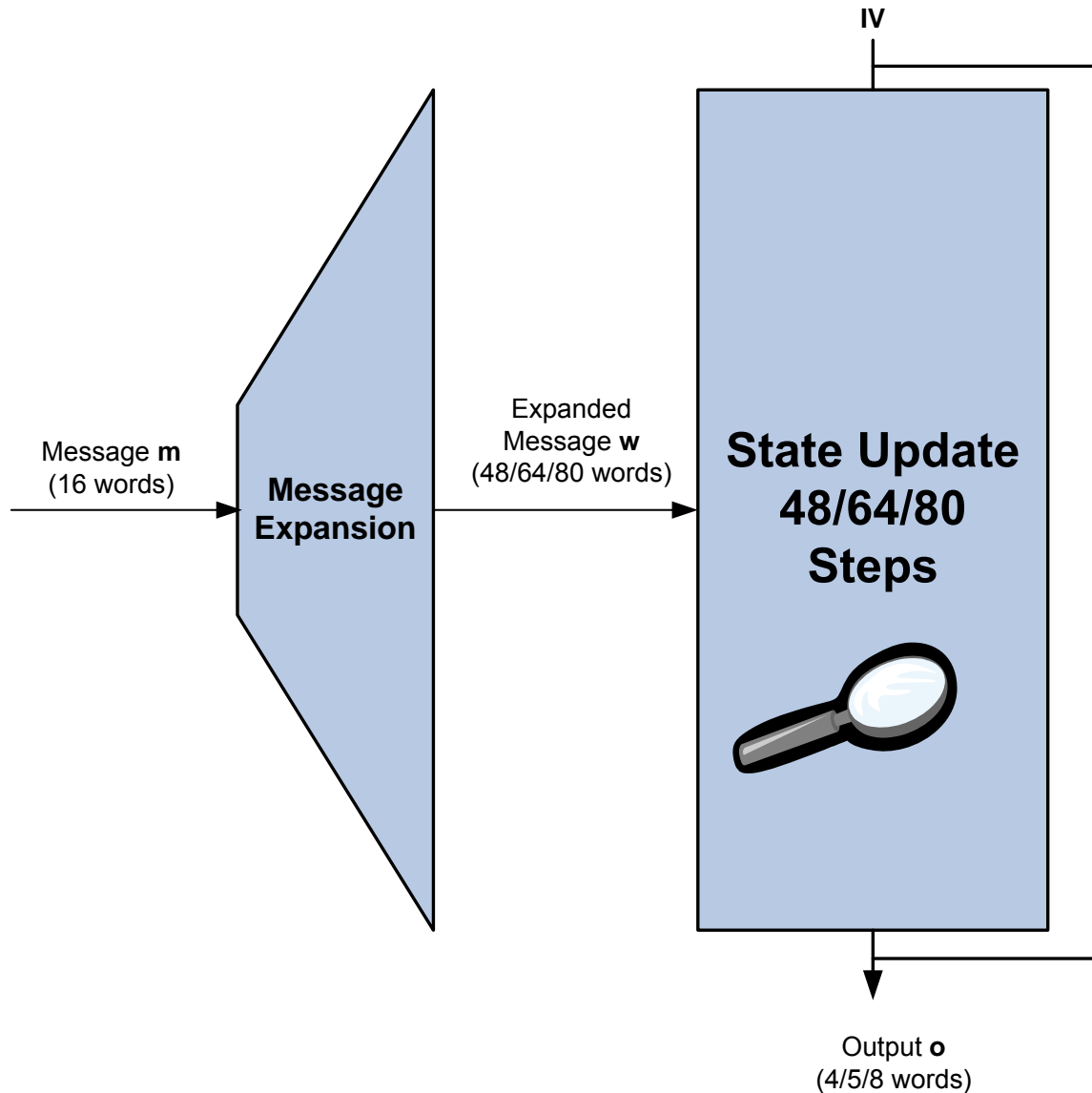
SHA / SHA-1



SHA-2 members

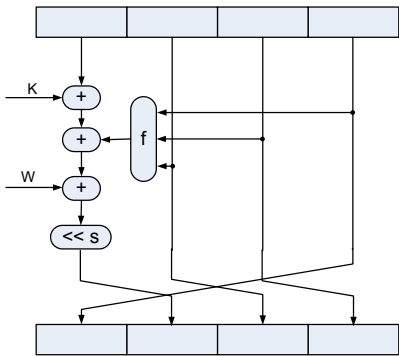


Outline of MD4-style Hash Functions

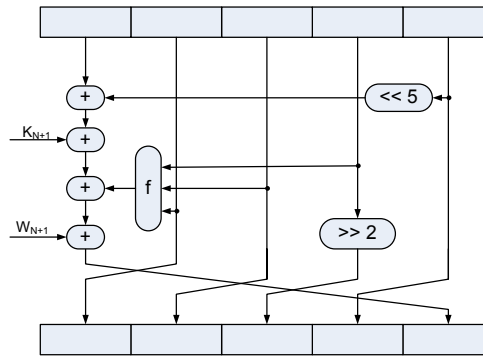


Evolution of the State Updates in the MD4 Family

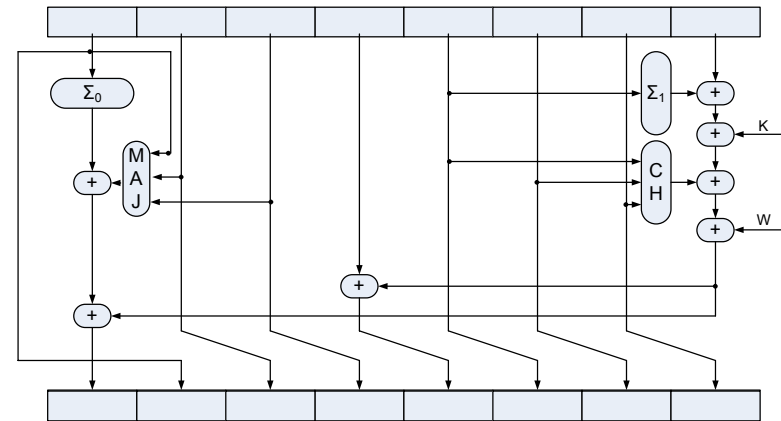
MD4



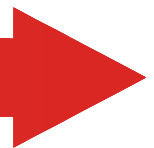
SHA/SHA-1



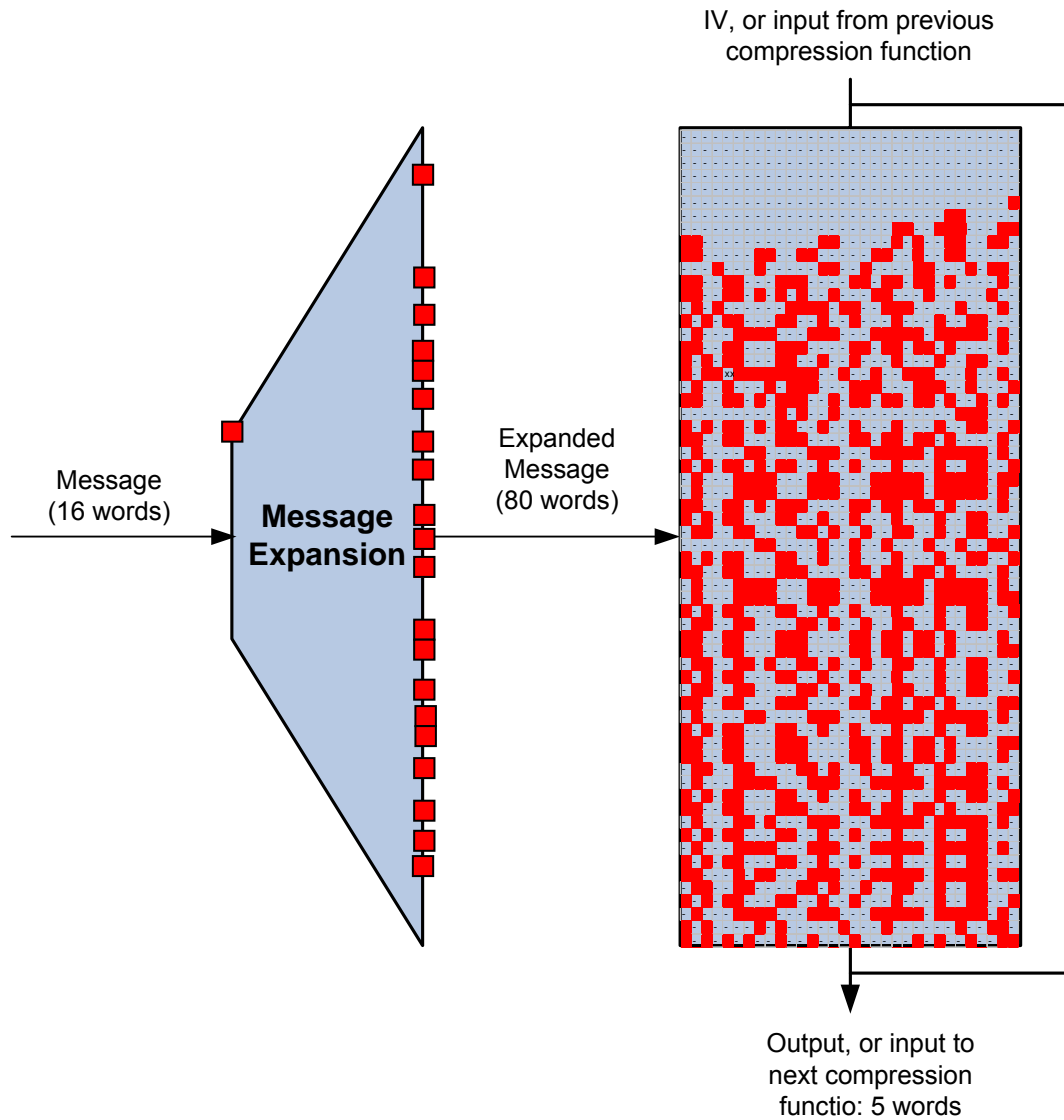
SHA-2 members



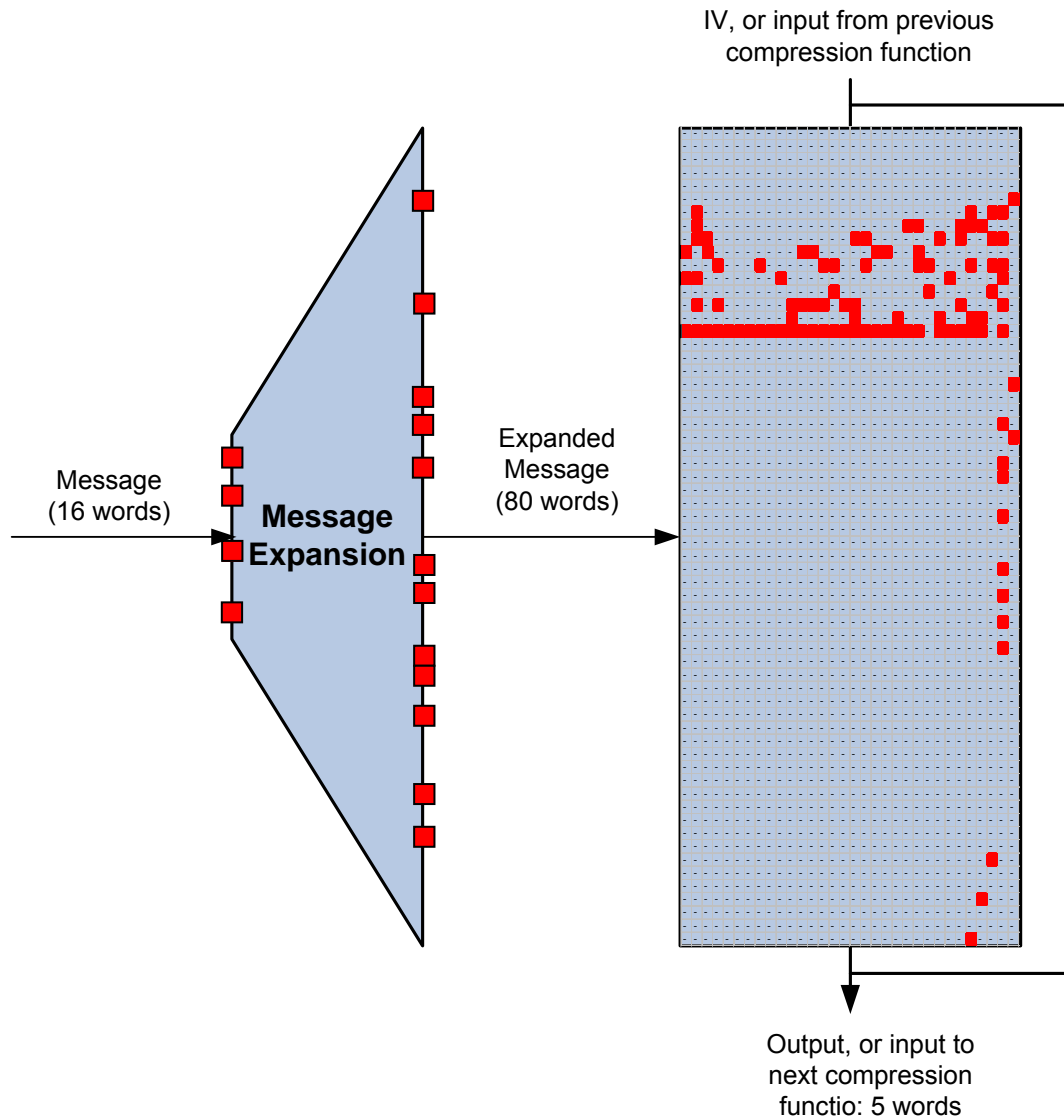
Design Complexity



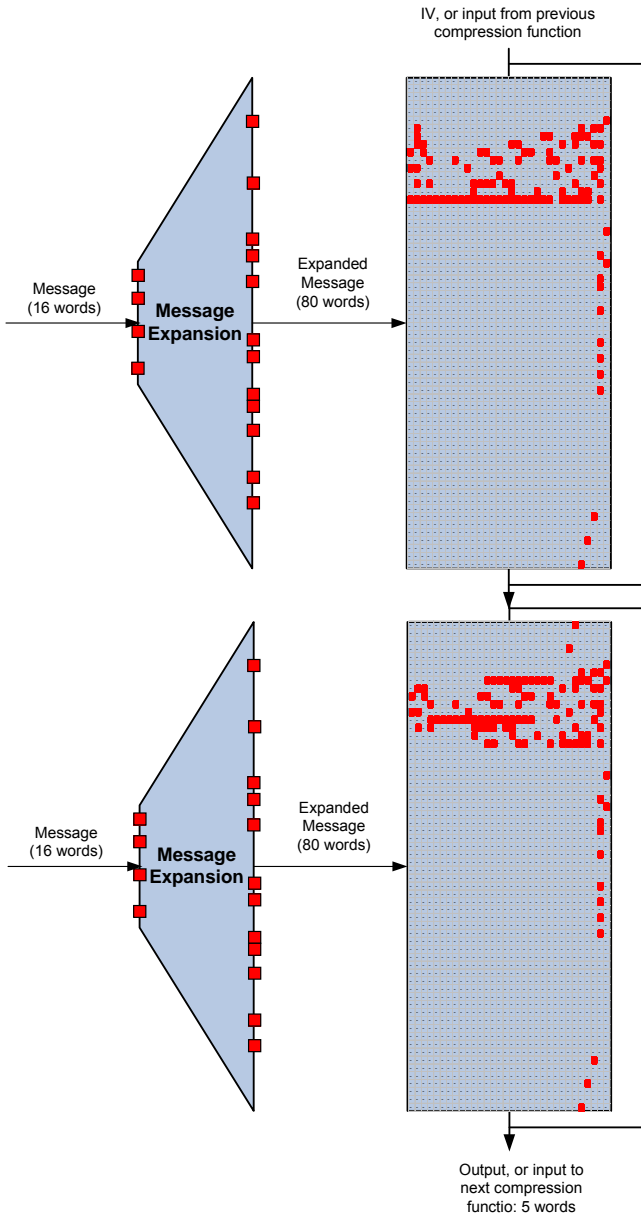
Effect of a single bit flip



Differential Attack on SHA-1



Attack on SHA-1



1st block:

- Near collision

2nd block:

- Same message difference
- Same near collision

2xnear collision cancels out →
Collision

Anatomy of a collision search attack on SHA-1

- Message difference
- Sequence of differences with high probability
- Speed-up methods
- Actual search (search space large enough?)

Anatomy of a collision search attack on SHA-1

- **Message difference**
- Sequence of differences with high probability
- Speed-up methods
- Actual search (search space large enough?)

XOR-Approx → Search for candidate characteristic

Several proposals: [RO05], [WYY05], [PRR05]

Precise evaluation of candidates: [DR06]

(no counting of Hamming weight, no ad-hoc rules)

Anatomy of a collision search attack on SHA-1

- Message difference
- **Sequence of differences with high probability**
- Speed-up methods
- Actual search (search space large enough?)

Introduction of “Signed-bit differences”,

First solution by [WYY05], manual

Introduction of “Generalized characteristics”,

Automated Method: [DR06]

Generalized conditions

x_i	x_i^*
0	0
0	1
1	0
1	1

Type	Possibilities
XOR	2
Signed-bit	4-6
Generalized:	16

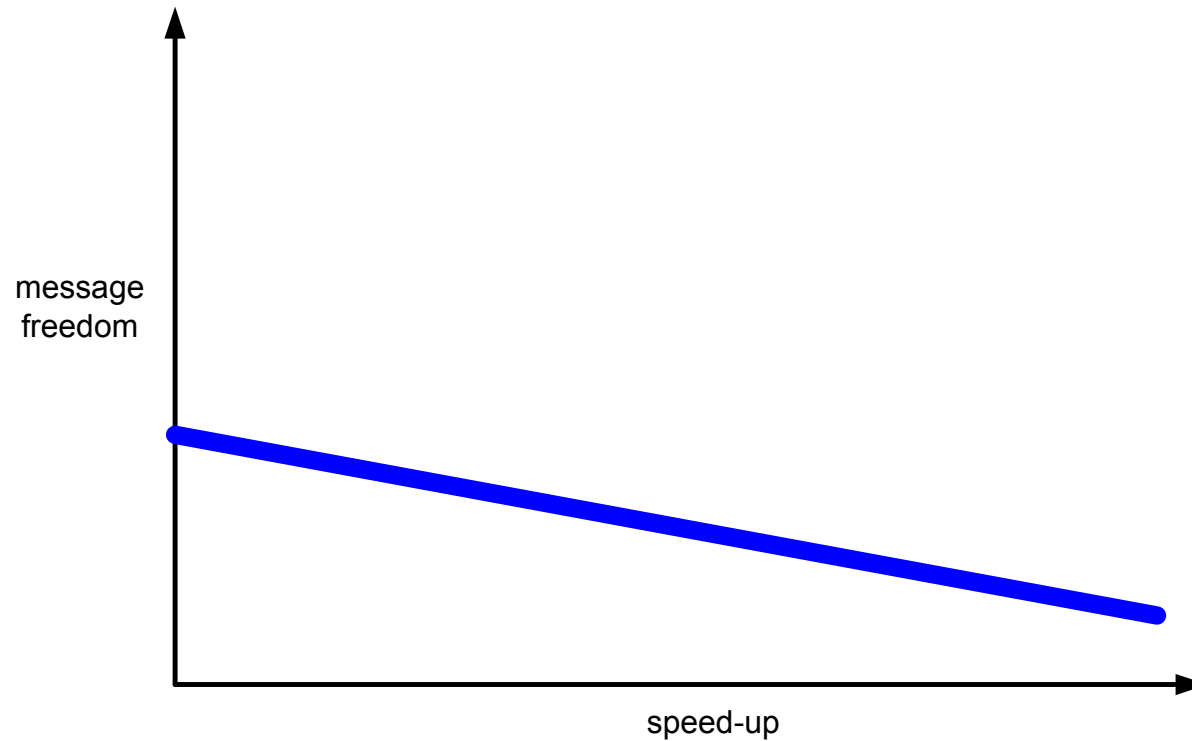
Anatomy of a collision search attack on SHA-1

- Message difference
- Sequence of differences with high probability
- **Speed-up methods**
- Actual search (search space large enough?)

- **New method:** (Almost) deterministically toggle single bits up to more than 30 steps
 - Efficient in terms of computations needed
 - Efficient use of degrees of freedom

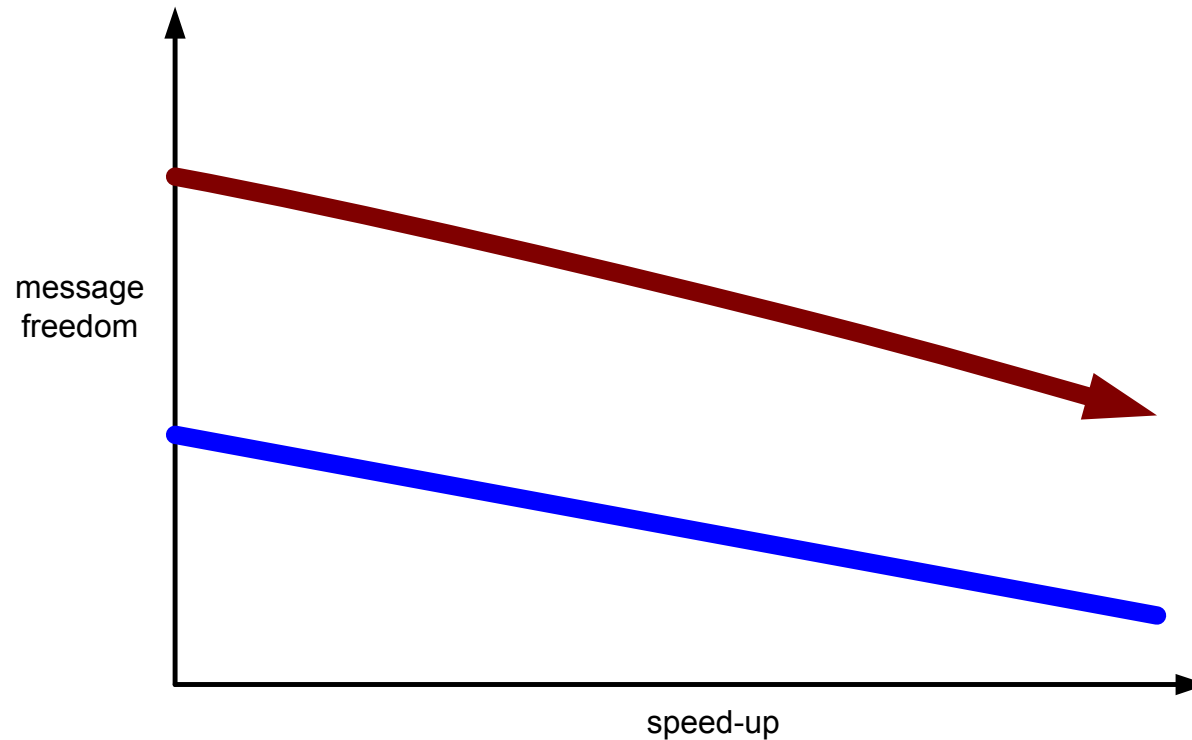
Cost of speed-up

2) Loss of degrees of freedom



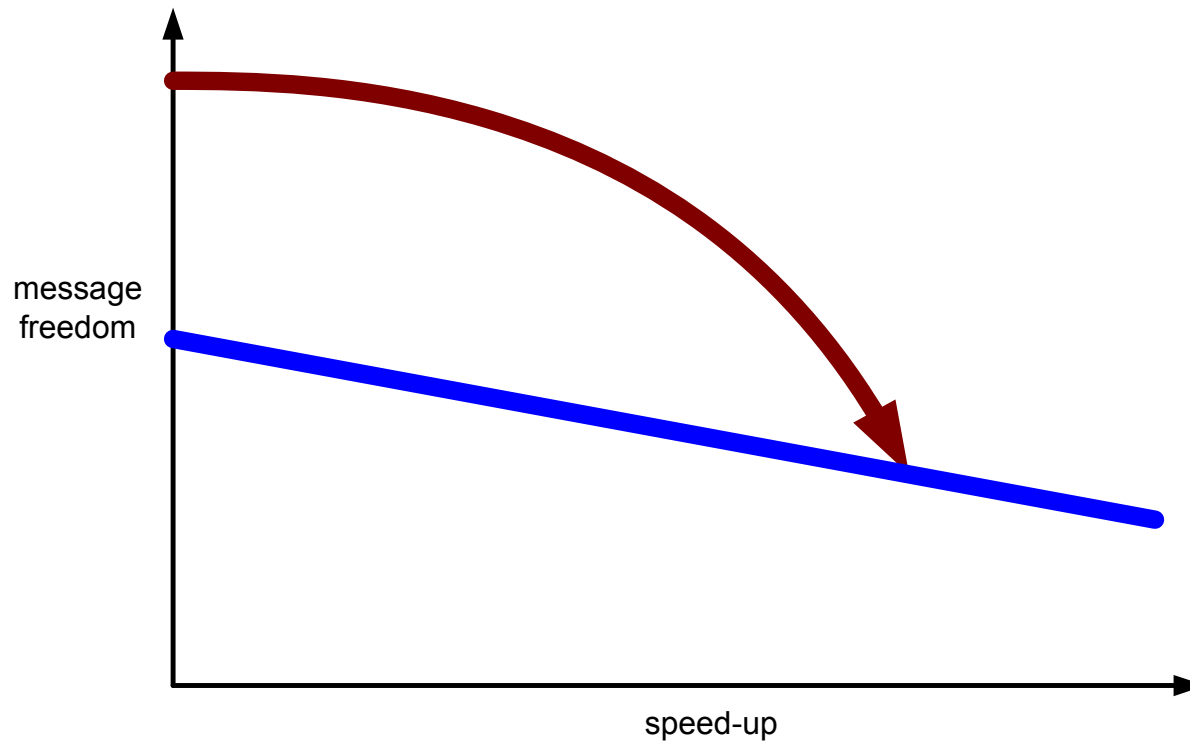
Cost of speed-up

2) Loss of degrees of freedom case MD4/MD5/SHA



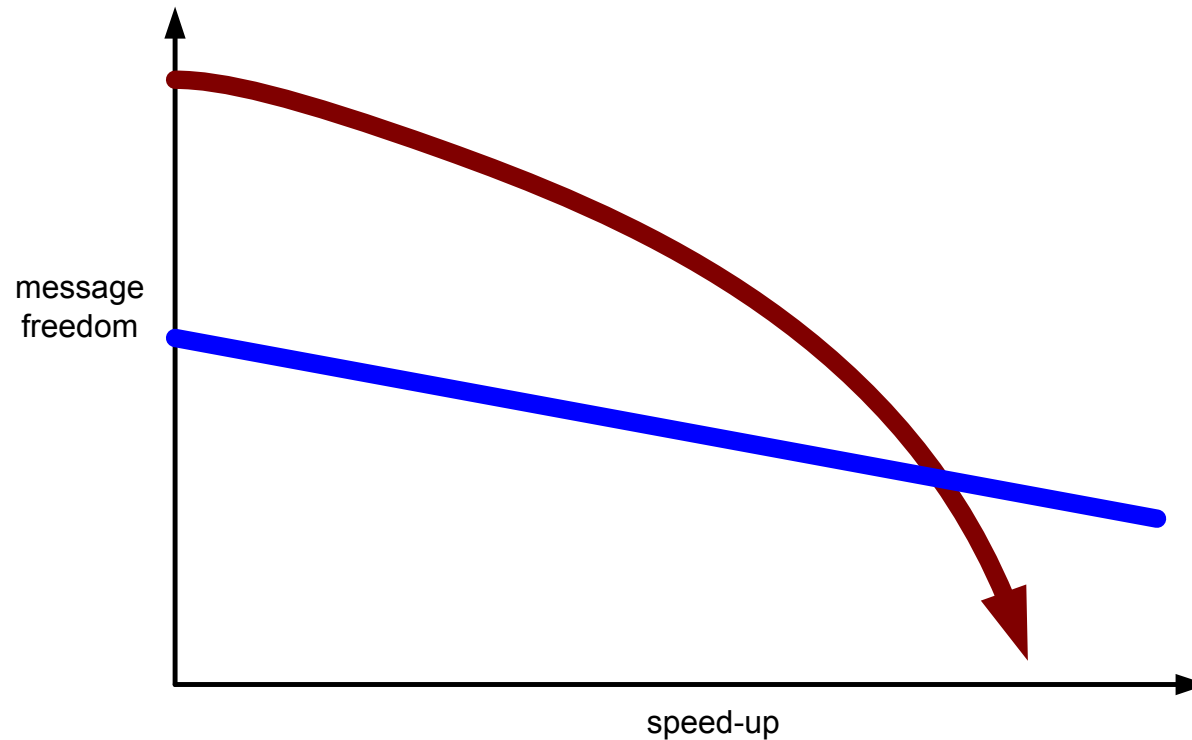
Cost of speed-up

2) Loss of degrees of freedom case SHA-1



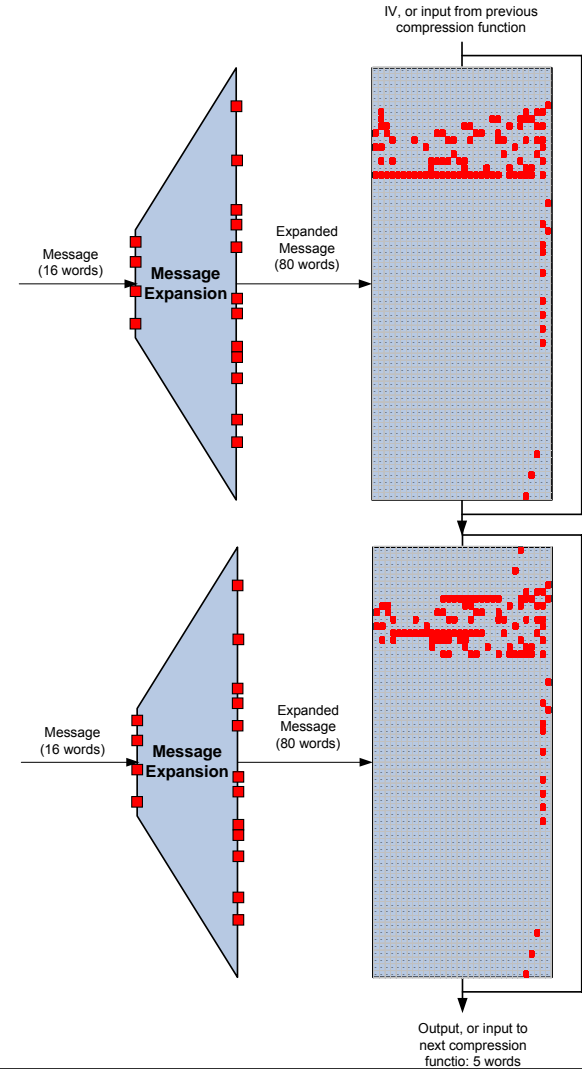
Cost of speed-up

2) Loss of degrees of freedom case SHA-1



Source of degrees of freedom

512



160

512

Summary of new techniques

- **Distribute workload**
3 blocks (instead of 2 blocks)
- **Efficiently control bits in state**
up to step 31 (best before was 25)
- **Number of distinct attacks**
millions of attacks (instead of a single one)
- **Fine grained optimization model**
#steps (instead of #trials)

Effort for dedicated collision search

- $2^x * C$

- Constant C depends on
 - details of actual collision-search algorithm
 - the used platform / architecture

First attempt on full SHA-1

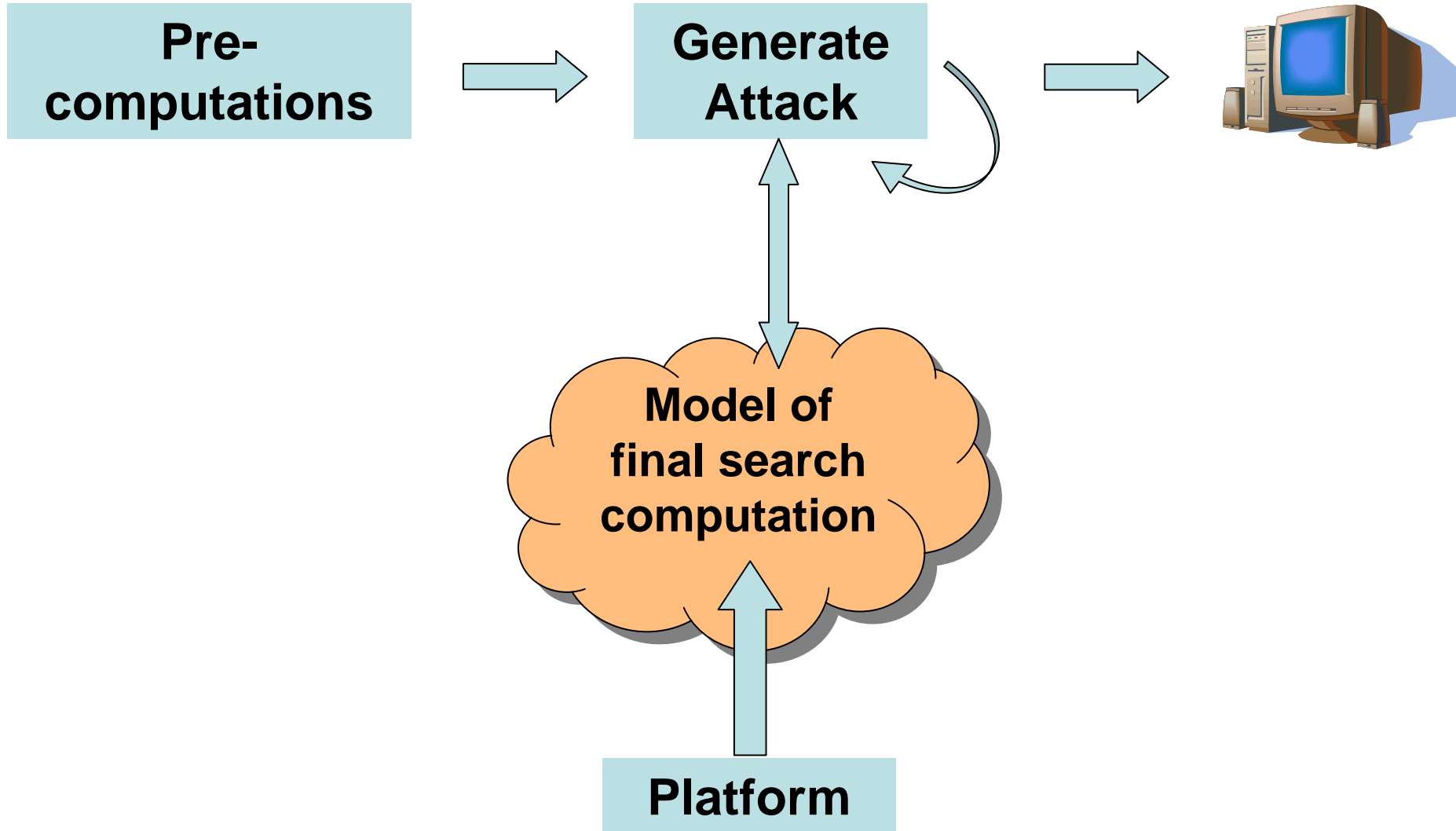
Current rough estimate: $\sim 2^{60.x}$ compress

We recently started a
distributed computing effort:



URL: <http://boinc.iaik.tugraz.at>

Workflow



Candidate Platforms

- Standard PCs
- GPUs
- New platforms: Cell / PS3, ...
- FPGA
- ASIC

Open Problems

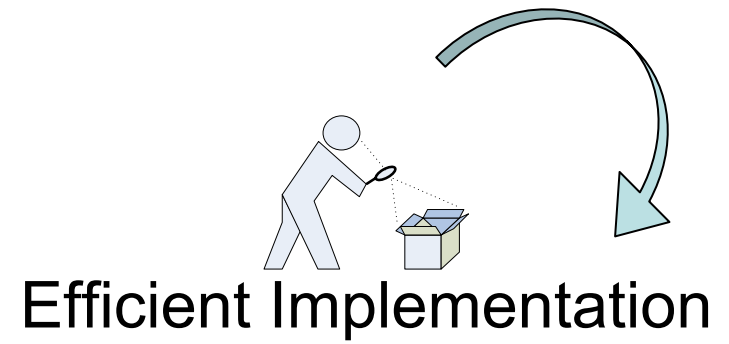
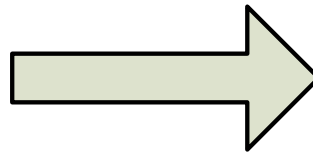
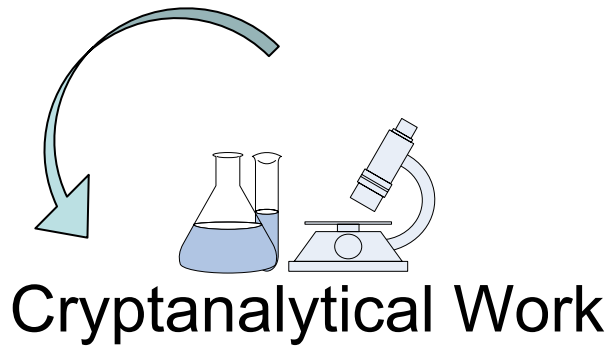
“we are in particular interested in exploring the interaction between cryptanalytical algorithms and computer hardware”

www.sharcs.org

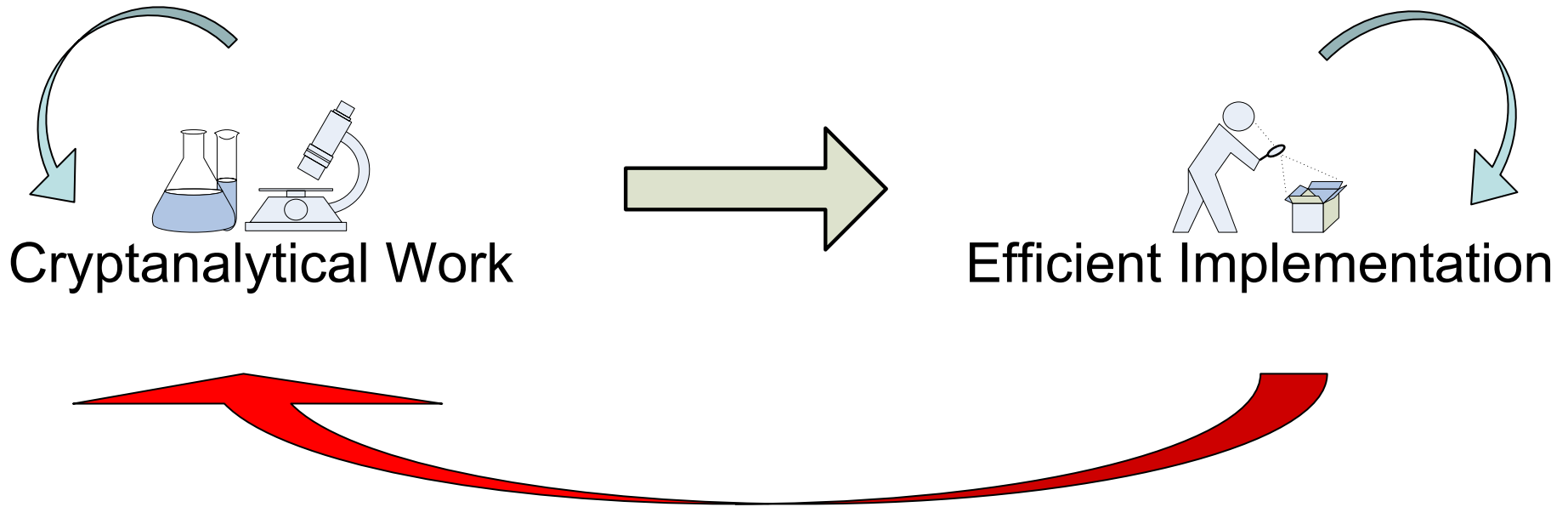
Explore design space spanned by

- * different/custom architectures and their
- * interaction between different cryptanalytic methods

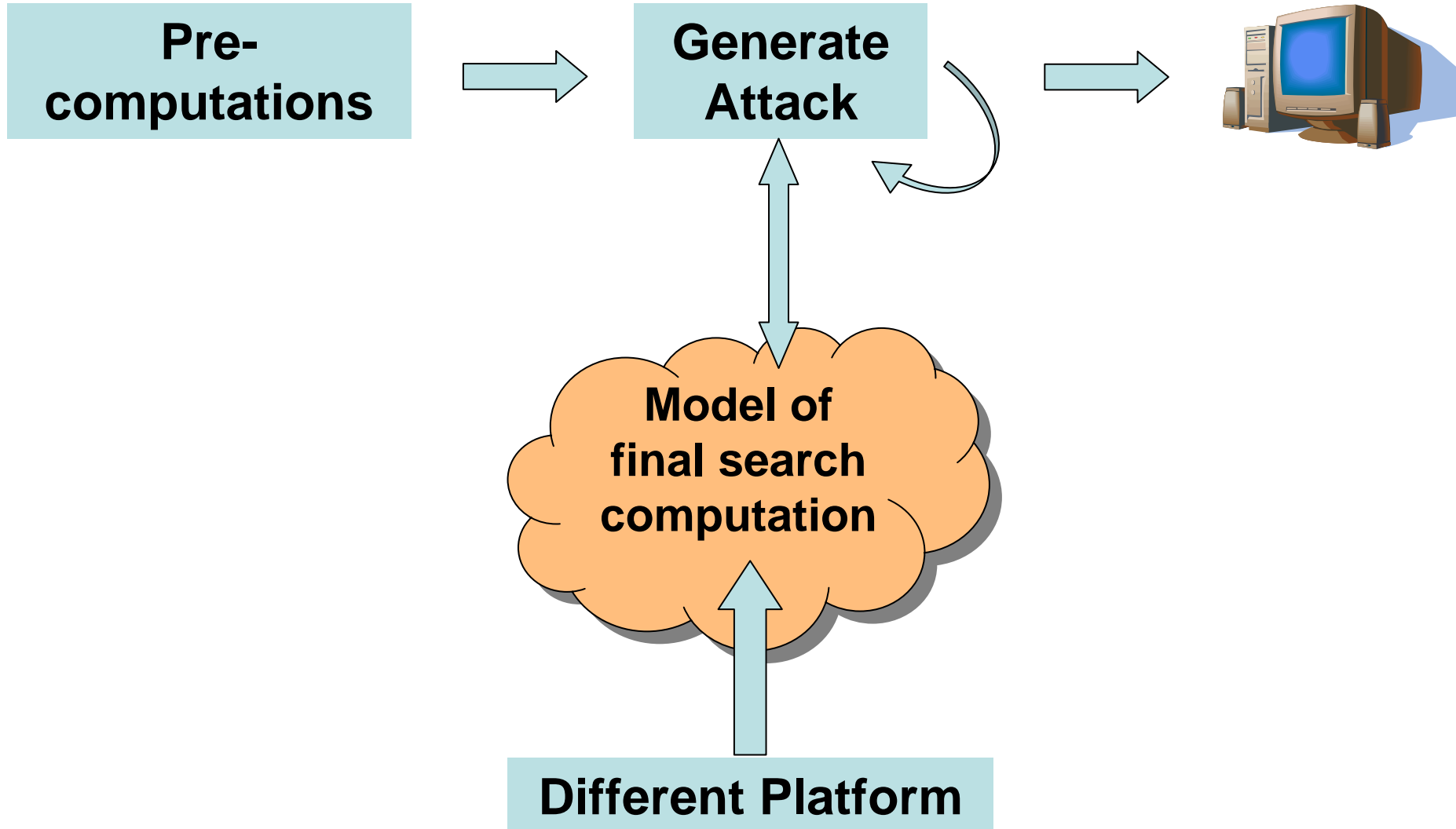
Typical workflow



Typical workflow



Workflow



Wrap-up

- The challenge: finding the first SHA-1 collision
- New method
 - exploit more degrees of freedom
 - use them more efficiently
 - many different attacks are generated on demand
- Open Problem
 - Exploit interaction between client architecture and cryptanalytic method

Dedicated Collision Search

Christian Rechberger

SHA-1 Collision Search: <http://boinc.iaik.tugraz.at>

***Institute for Applied Information Processing
and Communications (IAIK) - Krypto Group***

***Faculty of Computer Science
Graz University of Technology***



Supported by the Austrian Science Fund (FWF), project P18138.