New SHA-1 Collision Attacks, and Applications

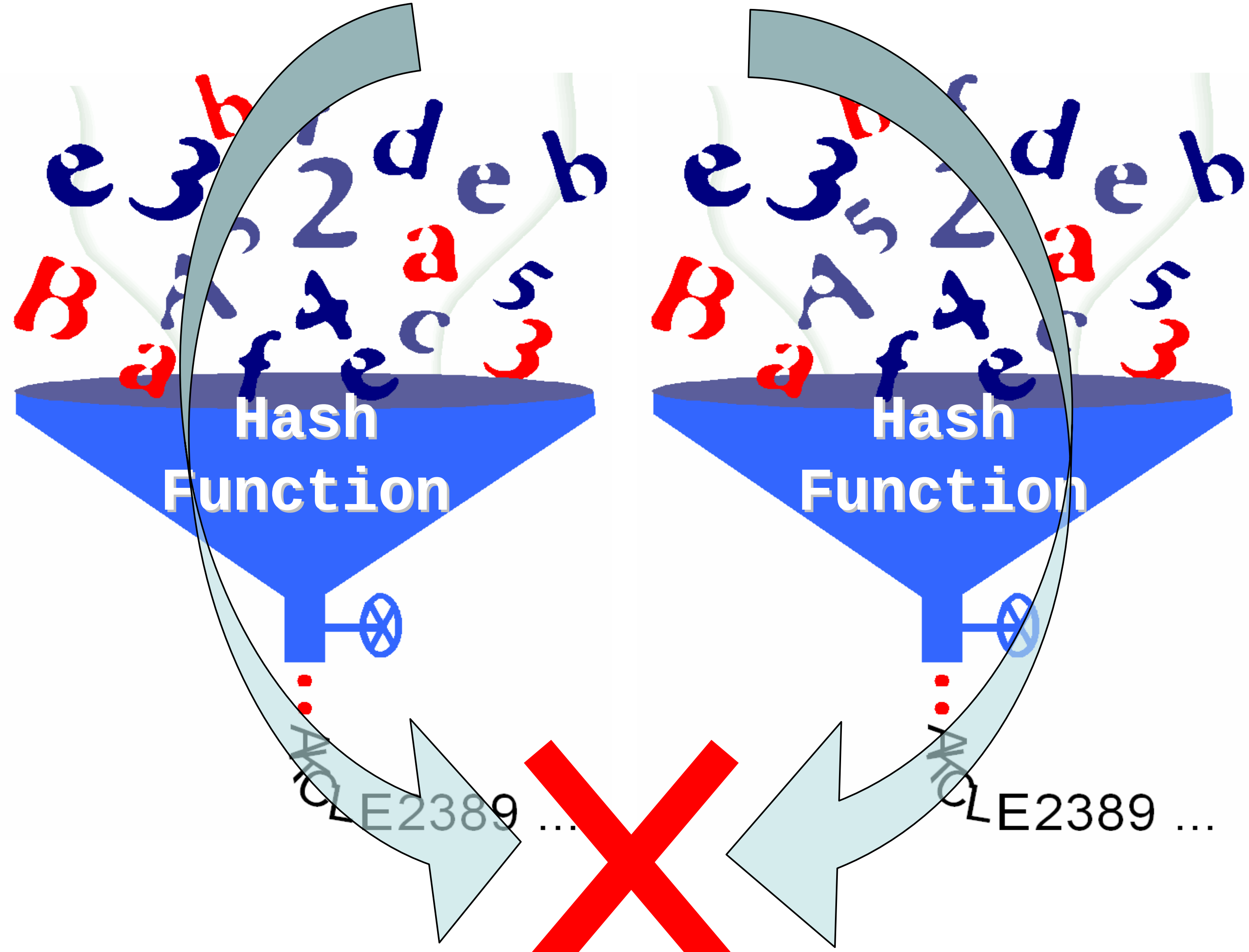
Florian Mendel, Christian Rechberger, Vincent Rijmen

Echternach, 01/2008

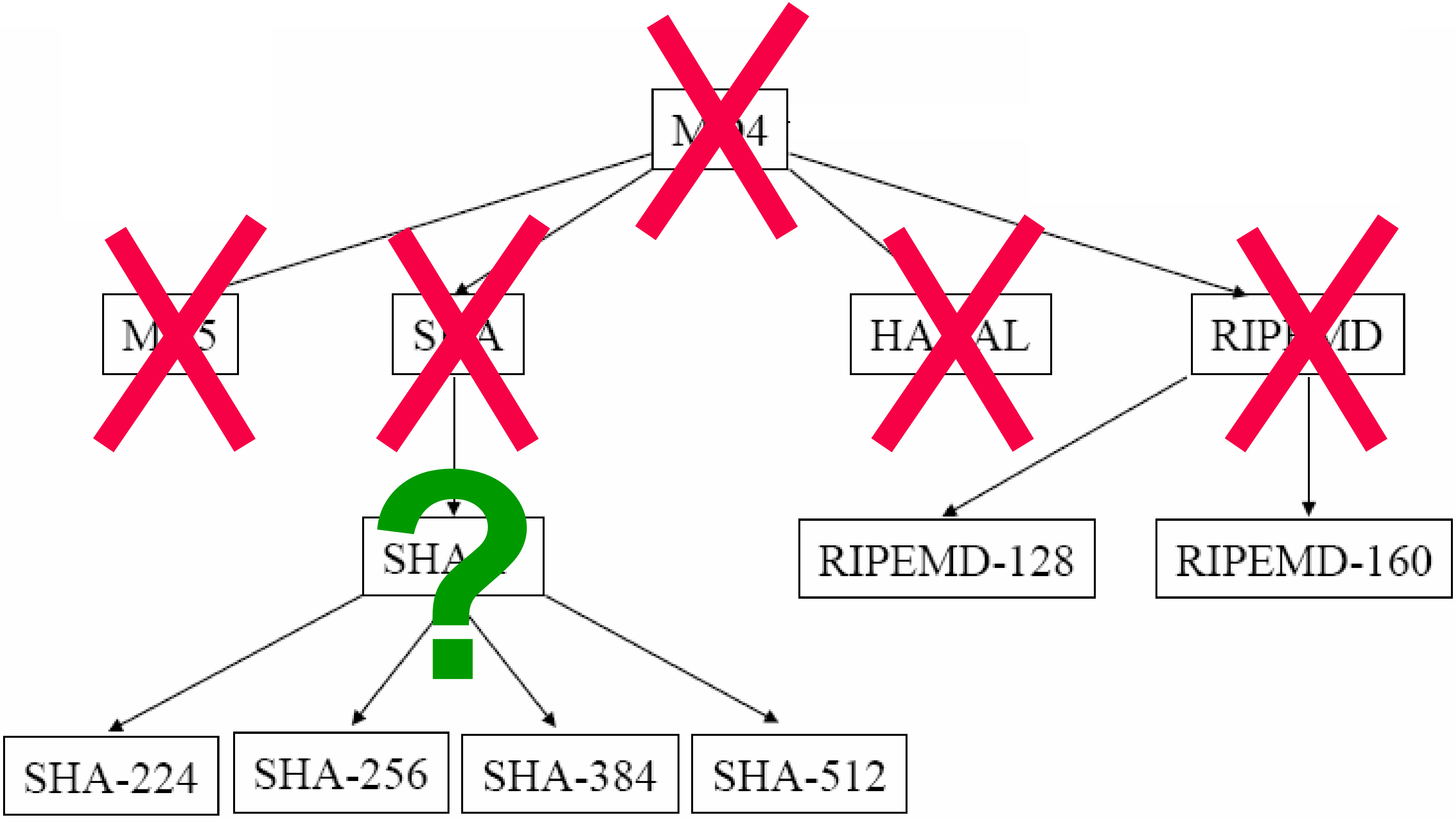
Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Collision resistance



What happened so far?



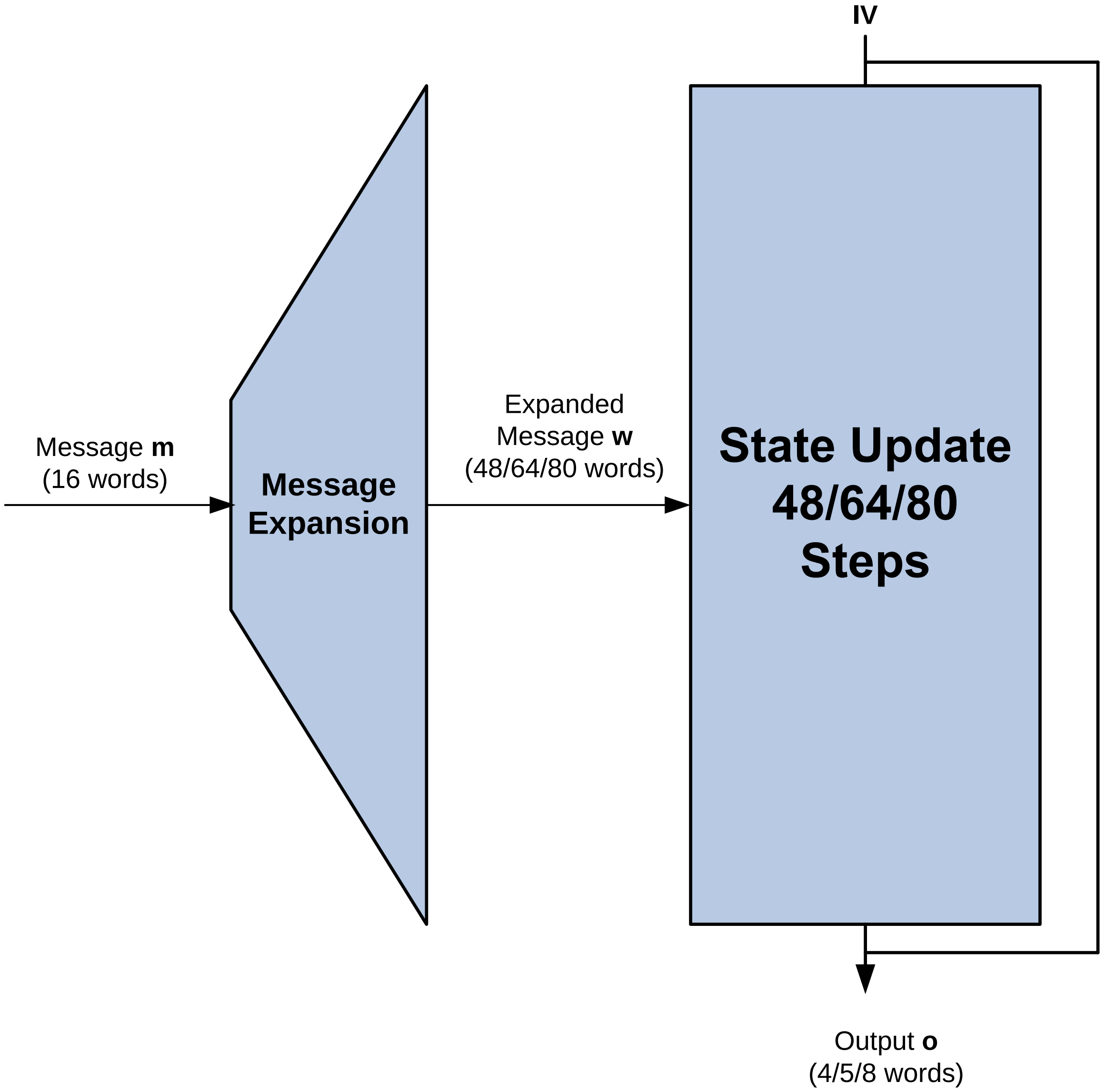
Current Status of SHA-1

- Differential collision attacks
  - Wang et al., 2005: 2^{69}
  - Joux and Peyrin, 2007: claim 2^{5} improvement over x
  - Wang et al.: 2^{63}, (2^{62}?), unpublished
  - Mendel, Rechberger, Rijmen: $2^{60.x}$, unpublished
- Preimage Attacks
  - Reuse of collision attacks?
  - Dedicated attacks?

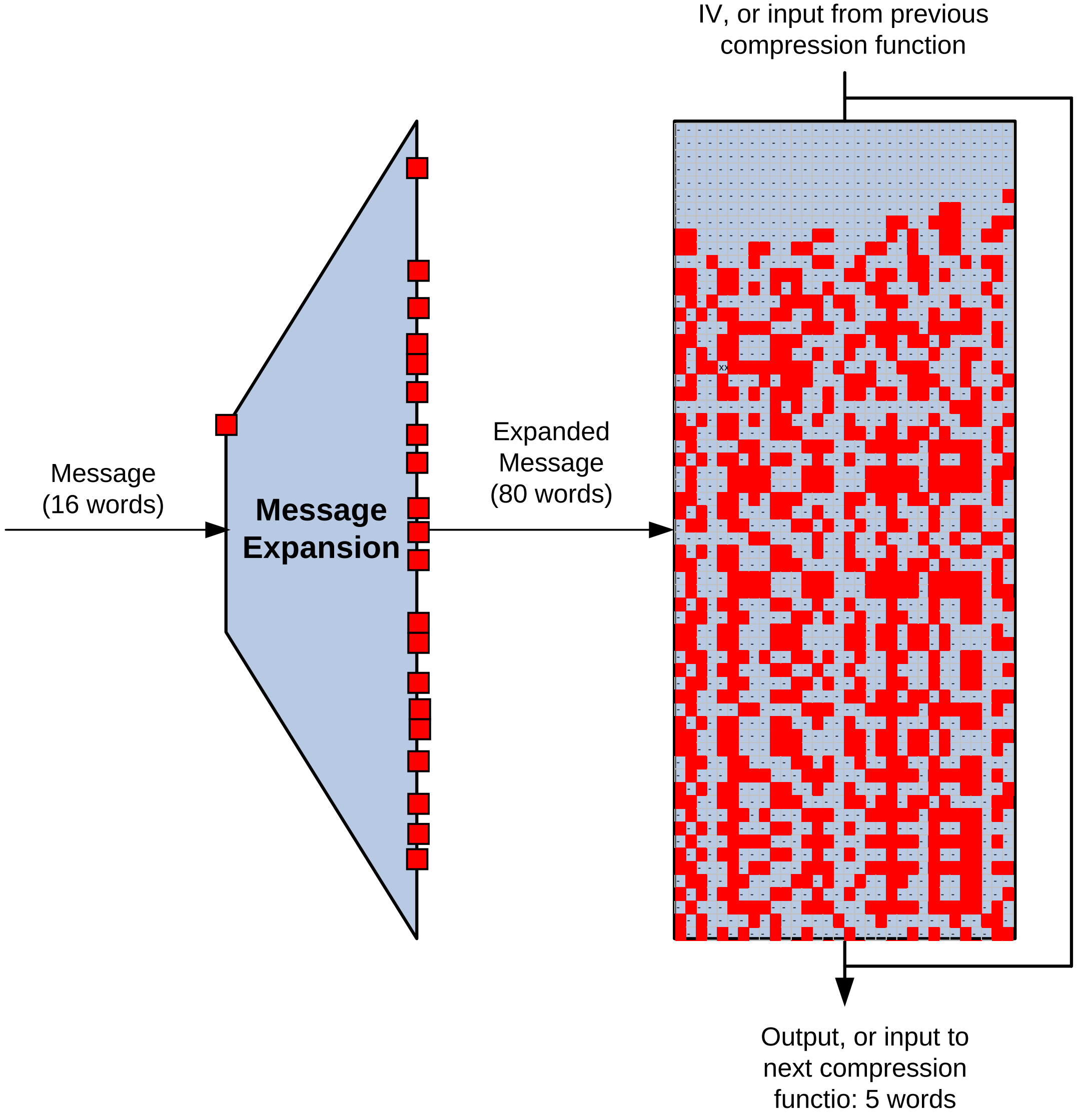
Current Status of SHA-1

- Differential collision attacks
  - Wang et al., 2005: 2^{69}
  - Joux and Peyrin, 2007: claim 2^{5} improvement over x
  - Wang et al.: 2^{63}, (2^{62}?), unpublished
  - *Mendel, Rechberger, Rijmen: $2^{60.x}$, unpublished*
- Preimage Attacks
  - *Reuse of collision attacks?*
  - Dedicated attacks?

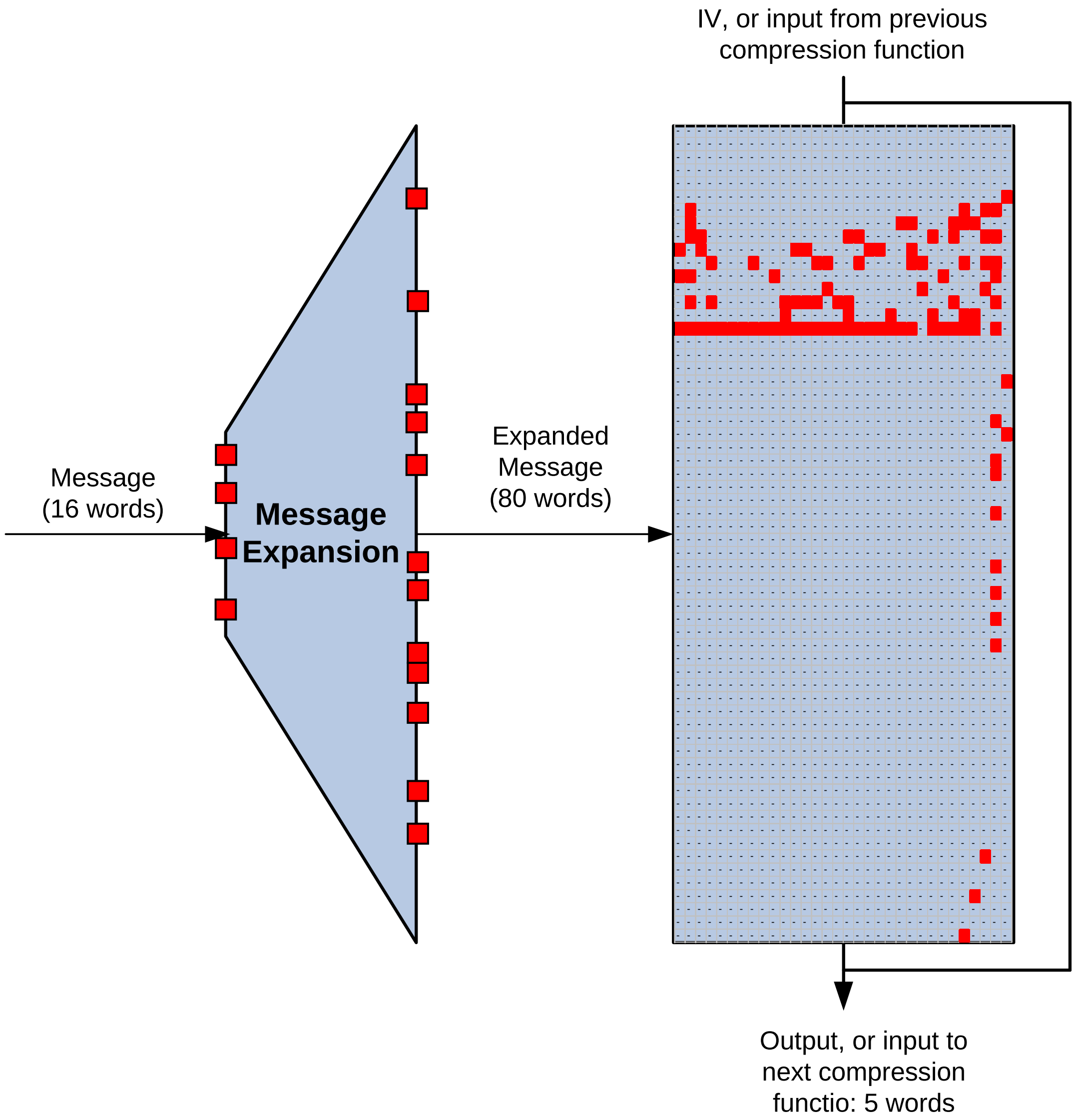
Outline of SHA-style Hash Functions



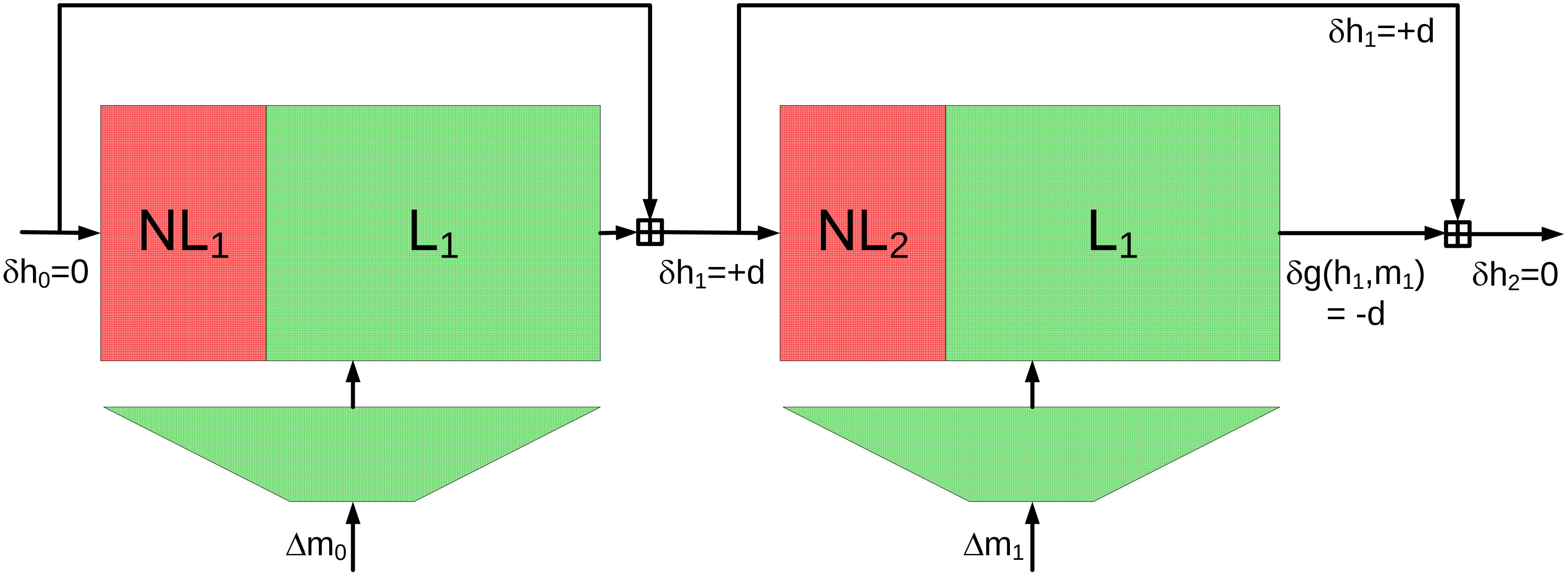
Effect of a single bit flip


IV, or input from previous compression function
Message (16 words)
Message Expansion
Expanded Message (80 words)
Output, or input to next compression functio: 5 words

Differential Attack on SHA-1


IV, or input from previous compression function
Message (16 words)
Message Expansion
Expanded Message (80 words)
Output, or input to next compression functio: 5 words

Standard 2-block approach



Summary of our new techniques

- **Efficiently control bits in state**

  up to step 31 (best before was 25)

- **Distribute workload**

  3 blocks (instead of 2 blocks)

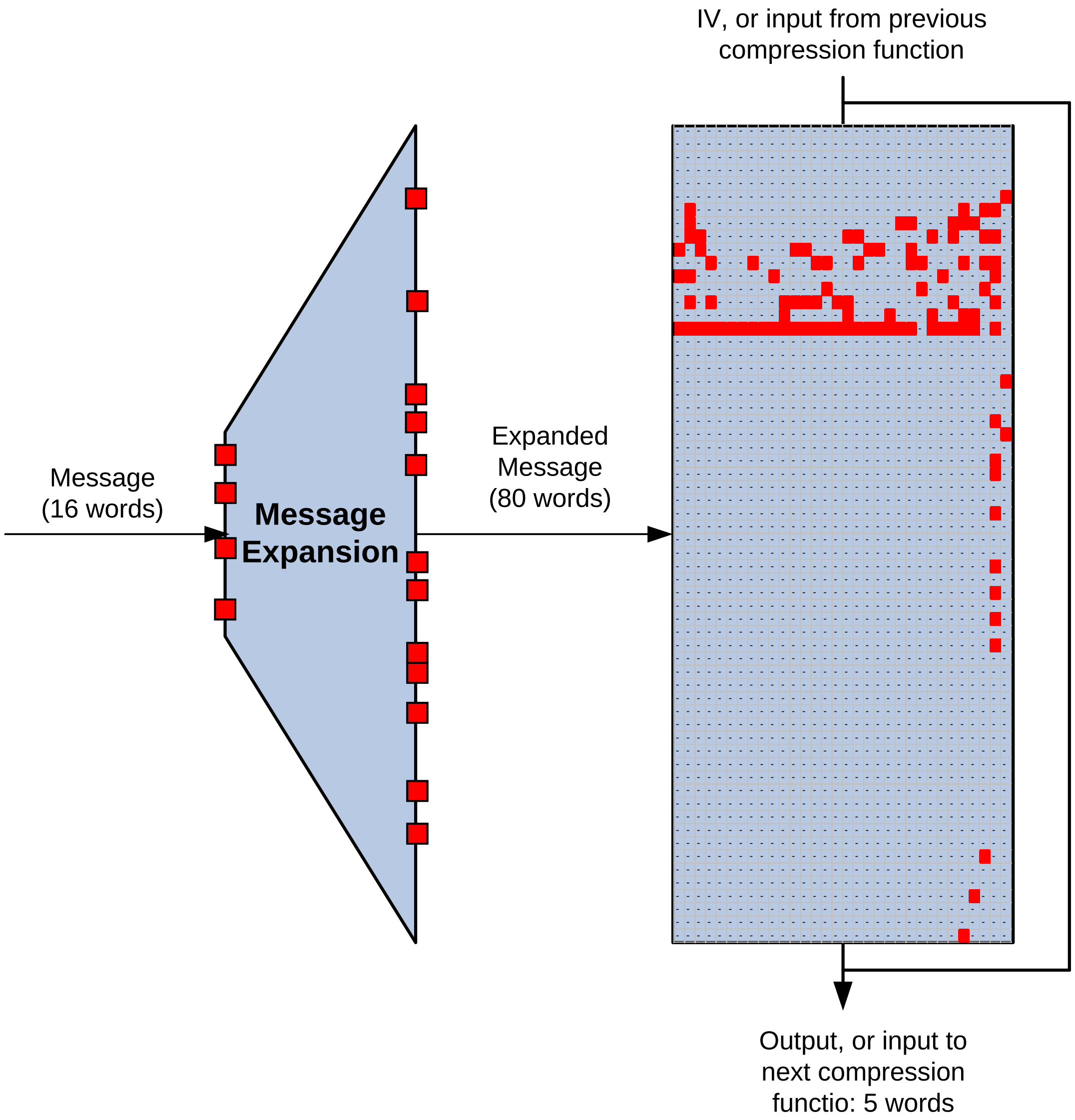
- **Number of distinct attacks**

  millions of attacks (instead of a single one)

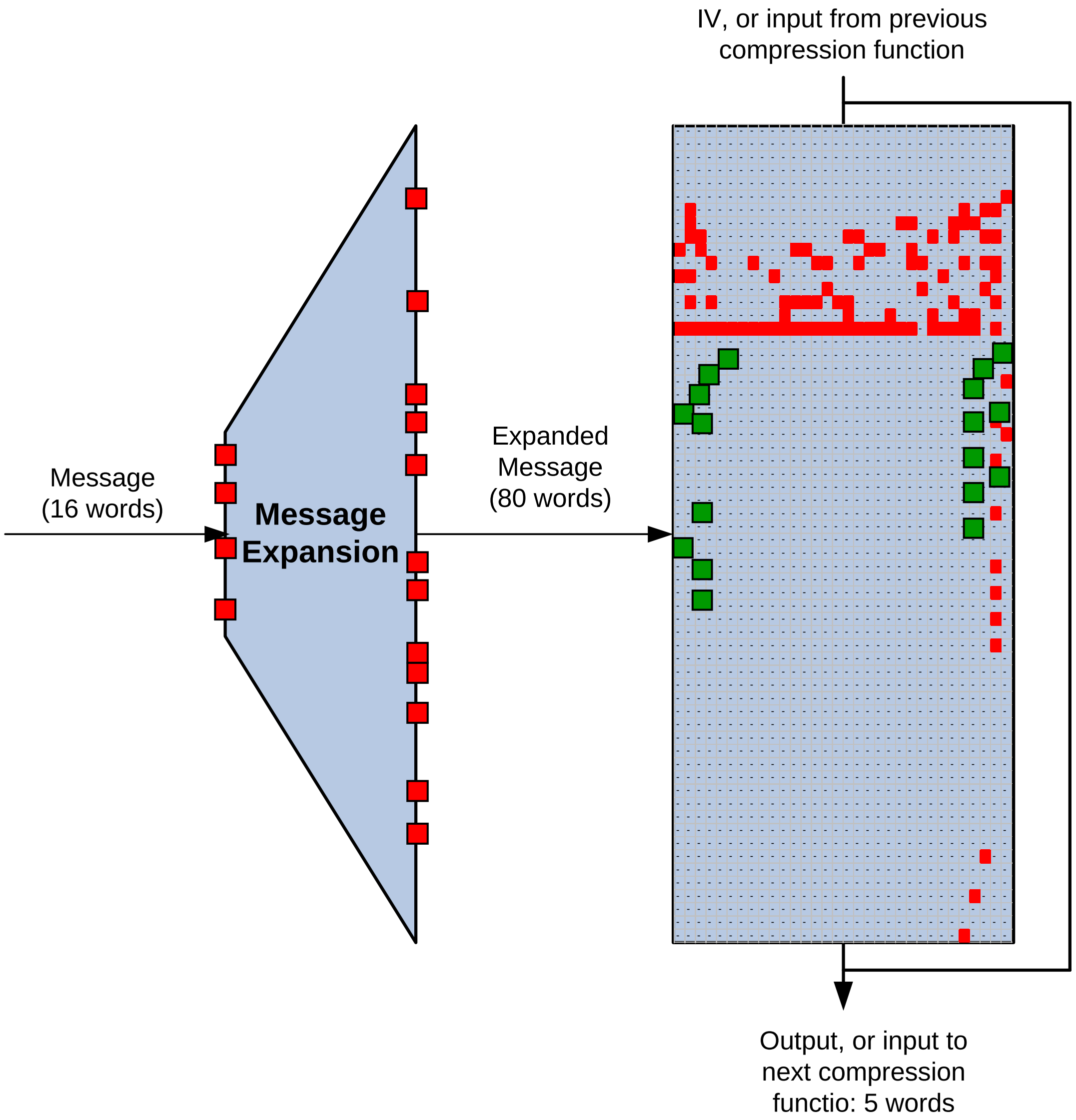
- **Fine grained optimization model**

  #steps (instead of #trials)

Differential Attack on SHA-1



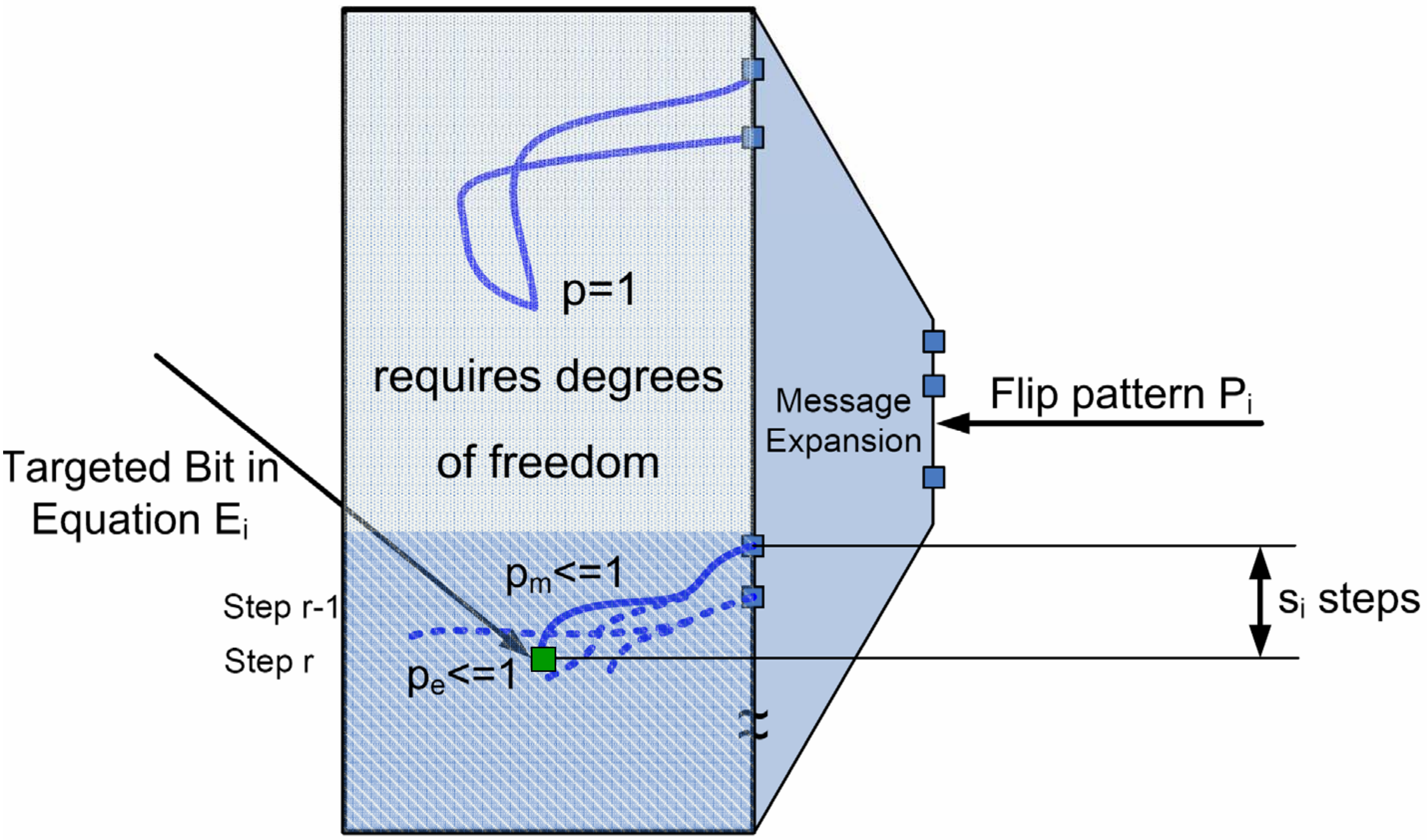
Differential Attack on SHA-1



🟩 Equations in:

Message bits

State bits


p=1
requires degrees
of freedom
Message
Expansion
Flip pattern P_i
Targeted Bit in
Equation E_i
$p_m<=1$
Step r-1
Step r
$p_e<=1$
s_i steps

Using these patterns in practice

- Compatible with main differential, and also to each other

How?

- Using the flexibility of the characteristic generator of De Cannière and Rechberger:
  - Used to demonstrate meaningful collisions [DR06]
  - Used in the boomerang approach [JP07]
  - Also here.

Summary of our new techniques

- **Efficiently control bits in state**

  up to step 31 (best before was 25)

- **Distribute workload**

  3 blocks (instead of 2 blocks)

- **Number of distinct attacks**

  millions of attacks (instead of a single one)

- **Fine grained optimization model**

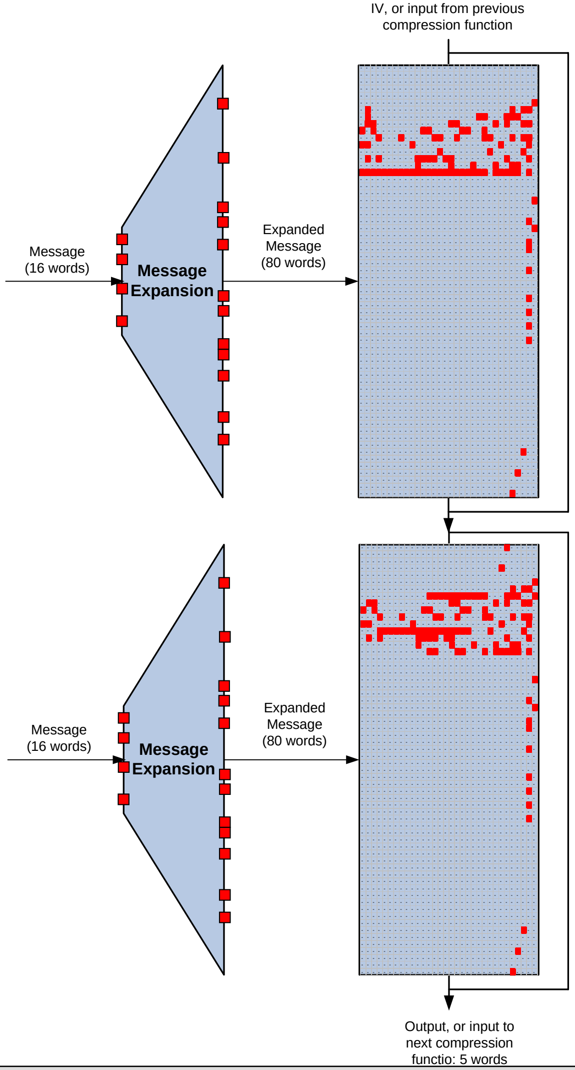
  #steps (instead of #trials)

Source of degrees of freedom

160

512

512


IV, or input from previous compression function
Message (16 words)
Message Expansion
Expanded Message (80 words)
Message (16 words)
Message Expansion
Expanded Message (80 words)
Output, or input to next compression functio: 5 words

Summary of our new techniques

- **Efficiently control bits in state**

  up to step 31 (best before was 25)

- **Distribute workload**

  3 blocks (instead of 2 blocks)

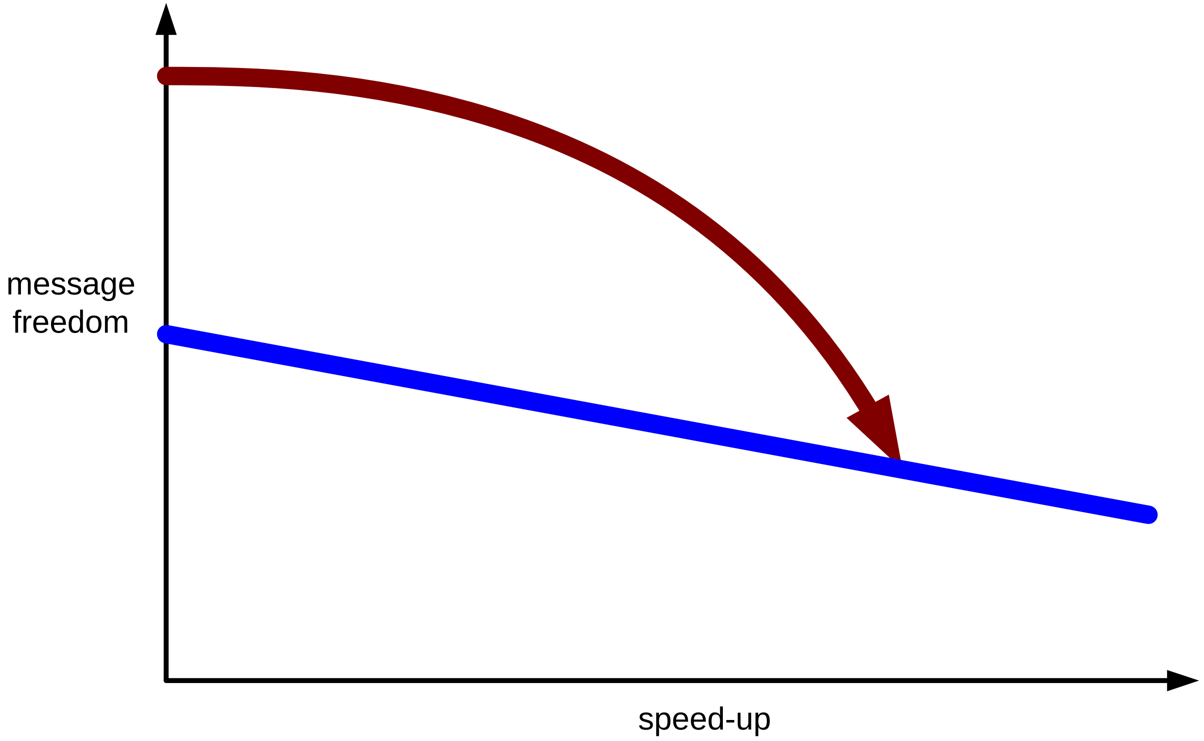
- **Number of distinct attacks**

  millions of attacks (instead of a single one)

- **Fine grained optimization model**

  #steps (instead of #trials)

Degrees of freedom

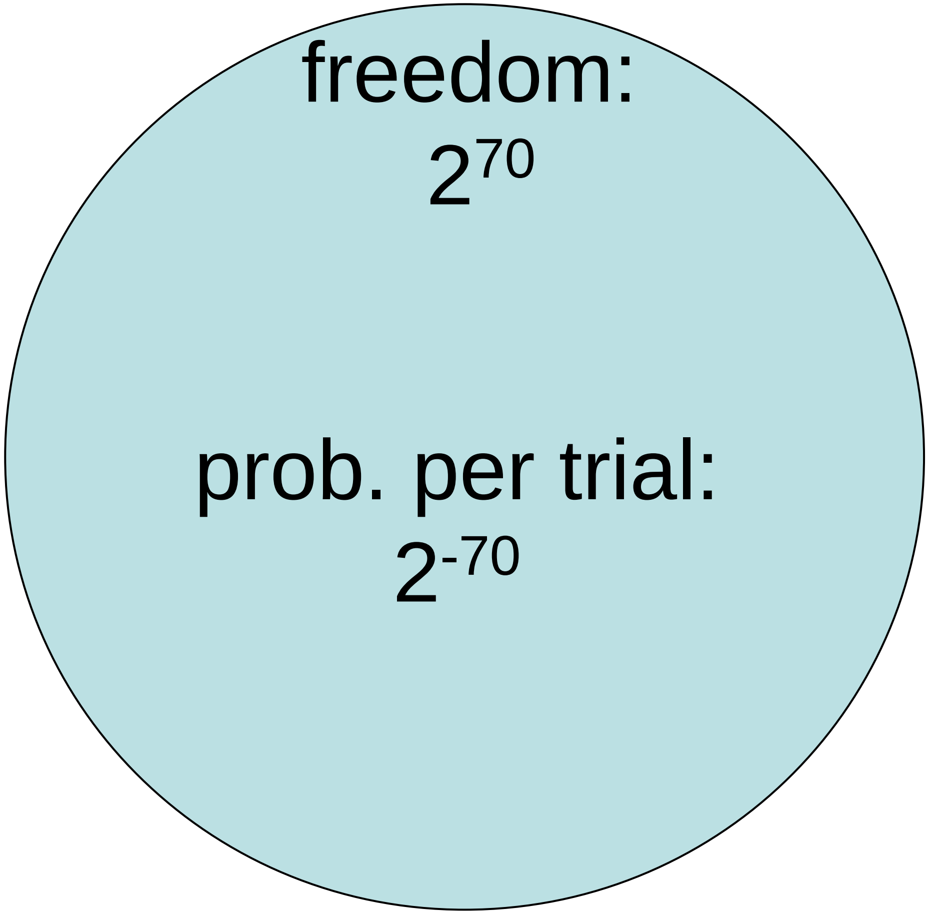


Piling up collision attacks

Generic principle, applicable if
degrees of freedom are limiting factor for improvements

Resulting performance is the average performance
weighted with the respective search space size

Piling up collision attacks: Example



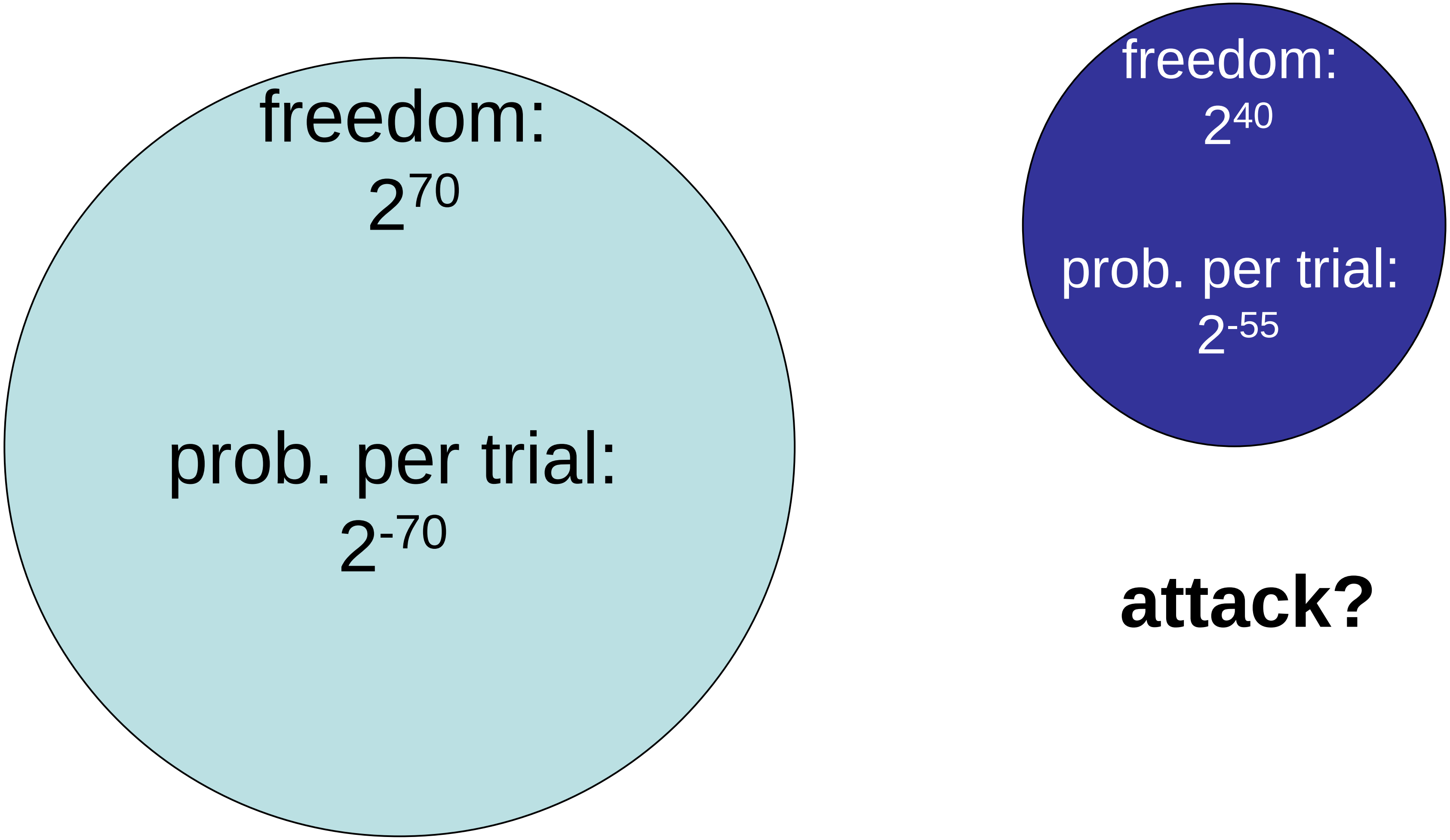
freedom:

2^{70}

prob. per trial:

2^{-70}

Piling up collision attacks: Example



freedom:
2^{70}

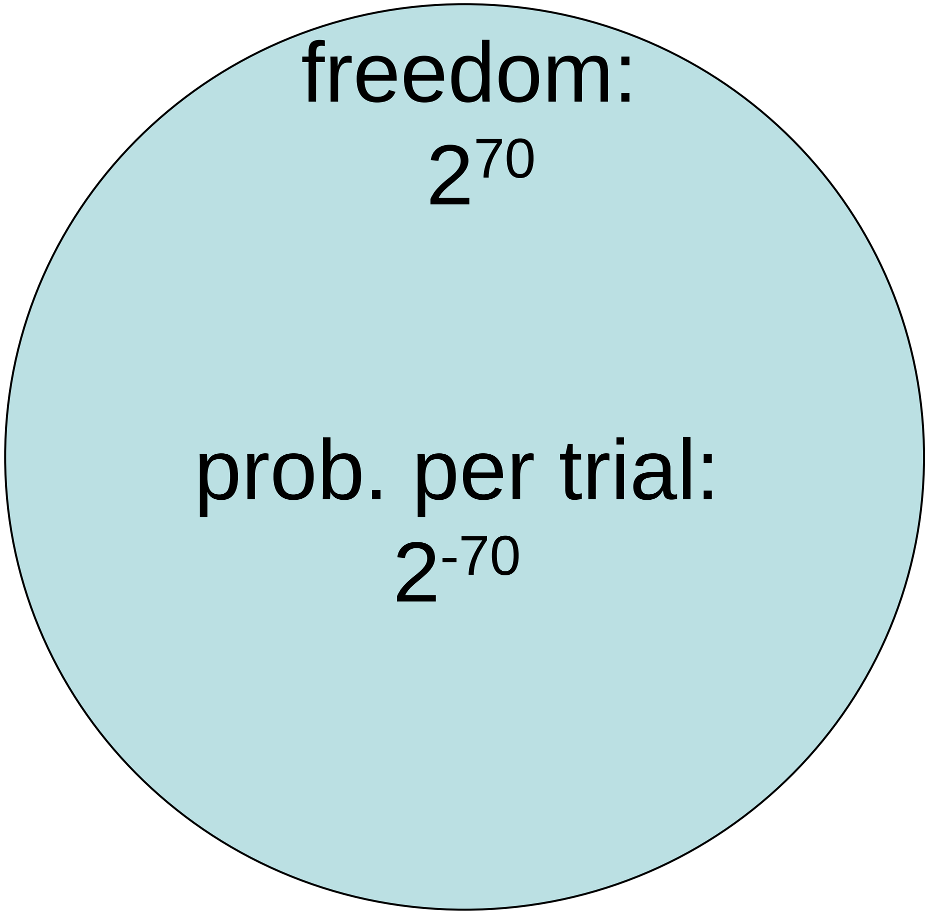
prob. per trial:
2^{-70}

freedom:
2^{40}

prob. per trial:
2^{-55}

attack?

Piling up collision attacks: Example

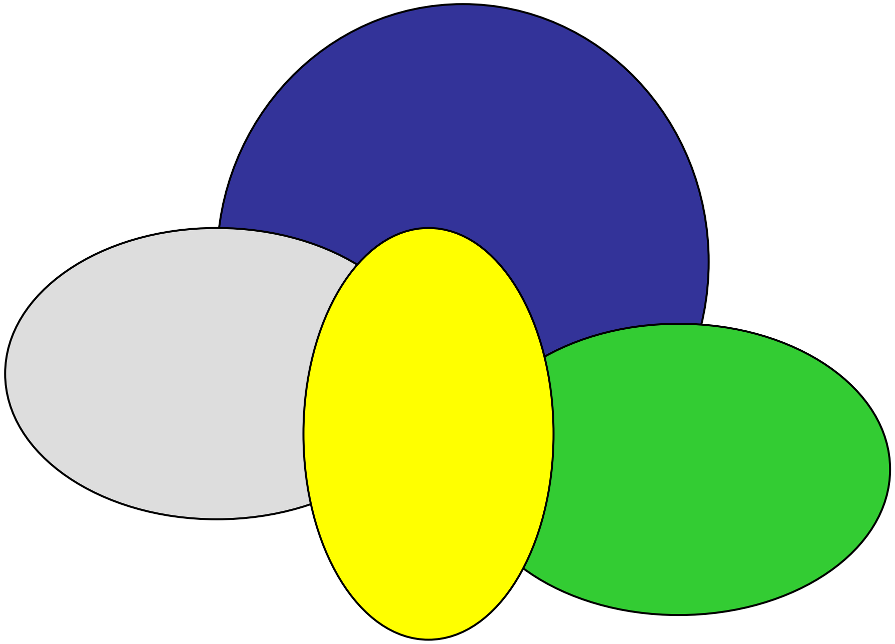


freedom:

2^{70}

prob. per trial:

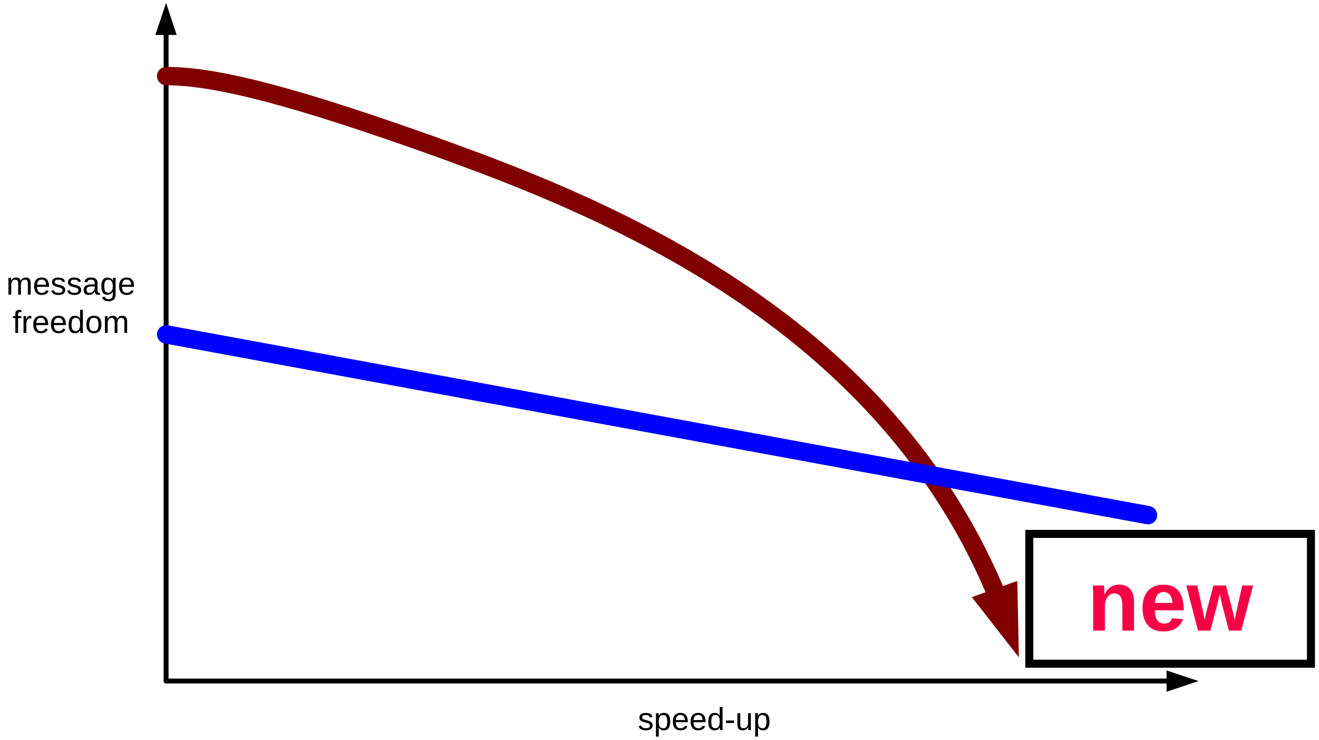
2^{-70}



Sum of freedom: 2^{60}

Weighted average probability per trial: 2^{-60}

Degrees of freedom



Summary of our 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)

Implementation of attacks

- Attack details are very intricate and complicated
- Only an actual implementation can rule out oversights

Reduced variants of SHA-1 considered in the past:

  - 2005: 40 steps [BC05]
  - 2005: 58 steps [WYY05,SPI07]
  - 2006: 64 steps [DR06]
  - 2007: 70 steps [DMR07,JP07]

First attempt on full SHA-1

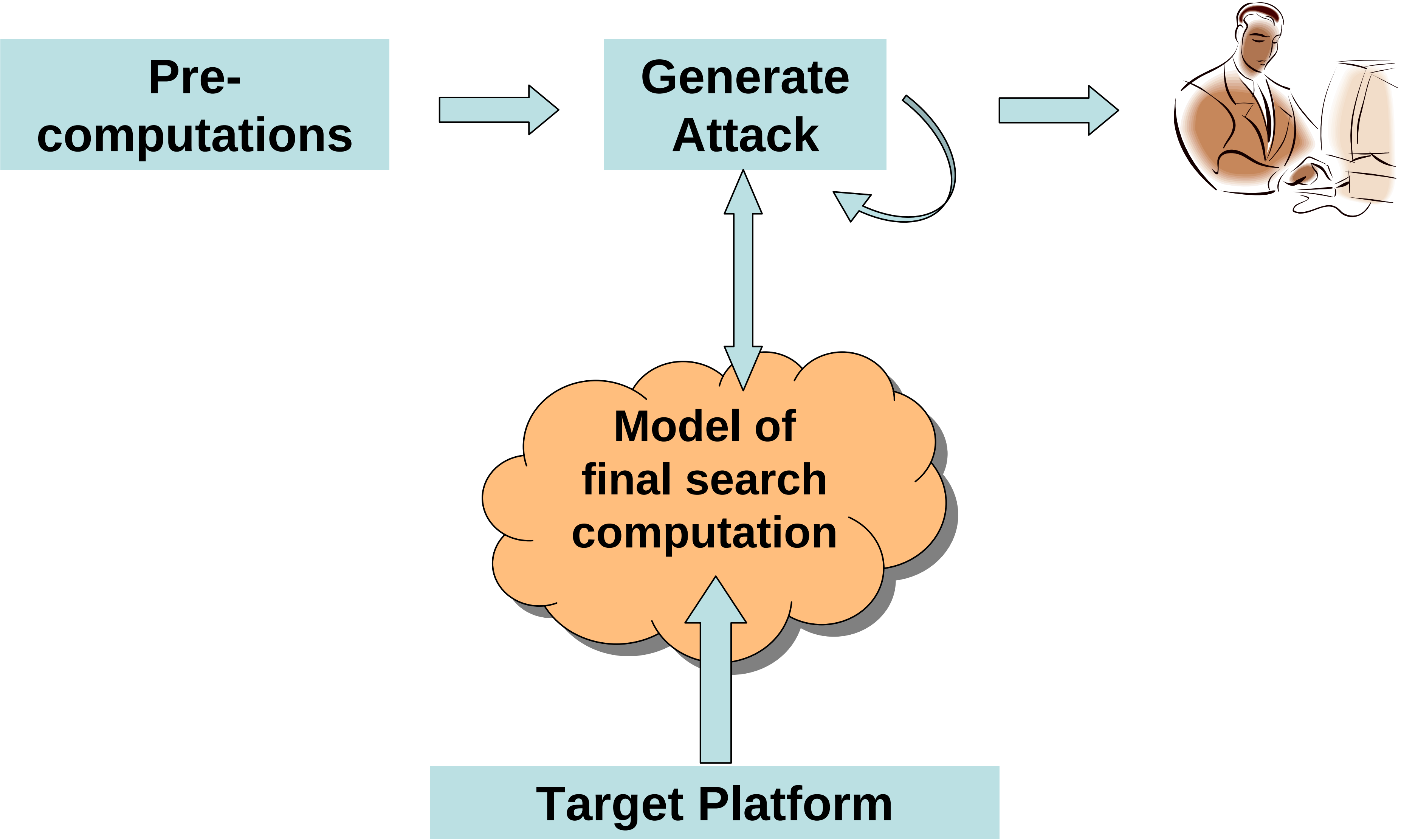
New rough estimate: ~$2^{60.x}$ simple hash

We recently started a distributed computing effort:

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

Measures to prevent misuse are in place

Workflow

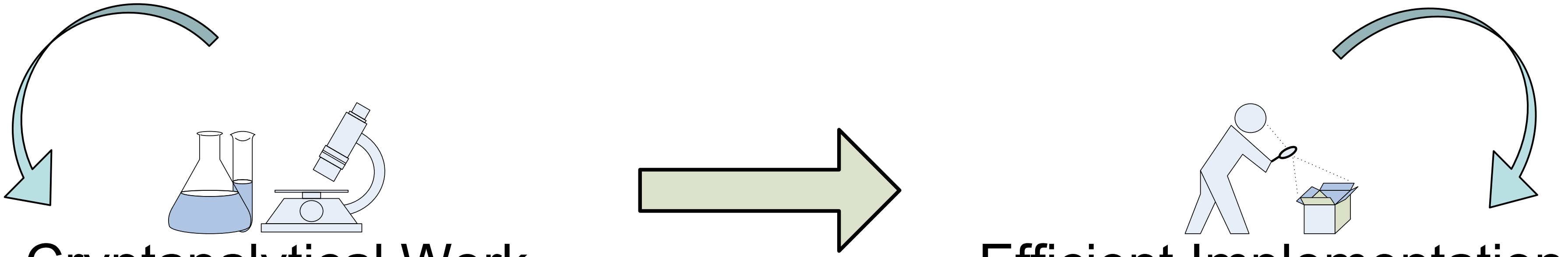


Pre-computations

Generate Attack

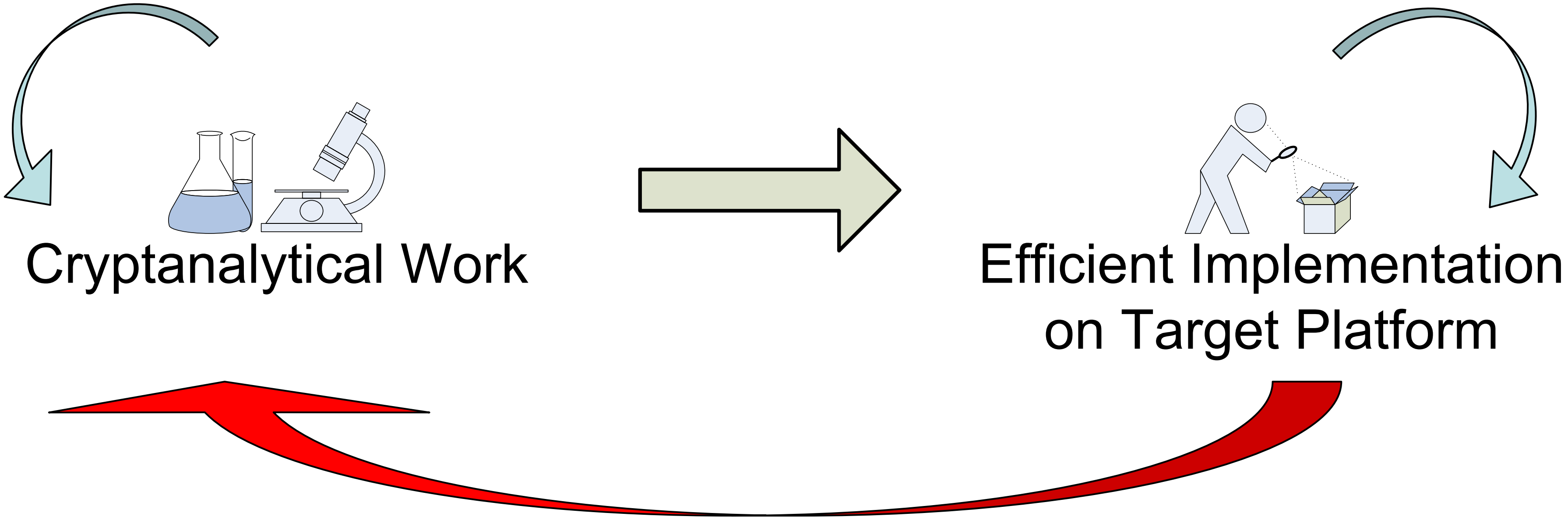
Model of final search computation

Target Platform



Cryptanalytical Work

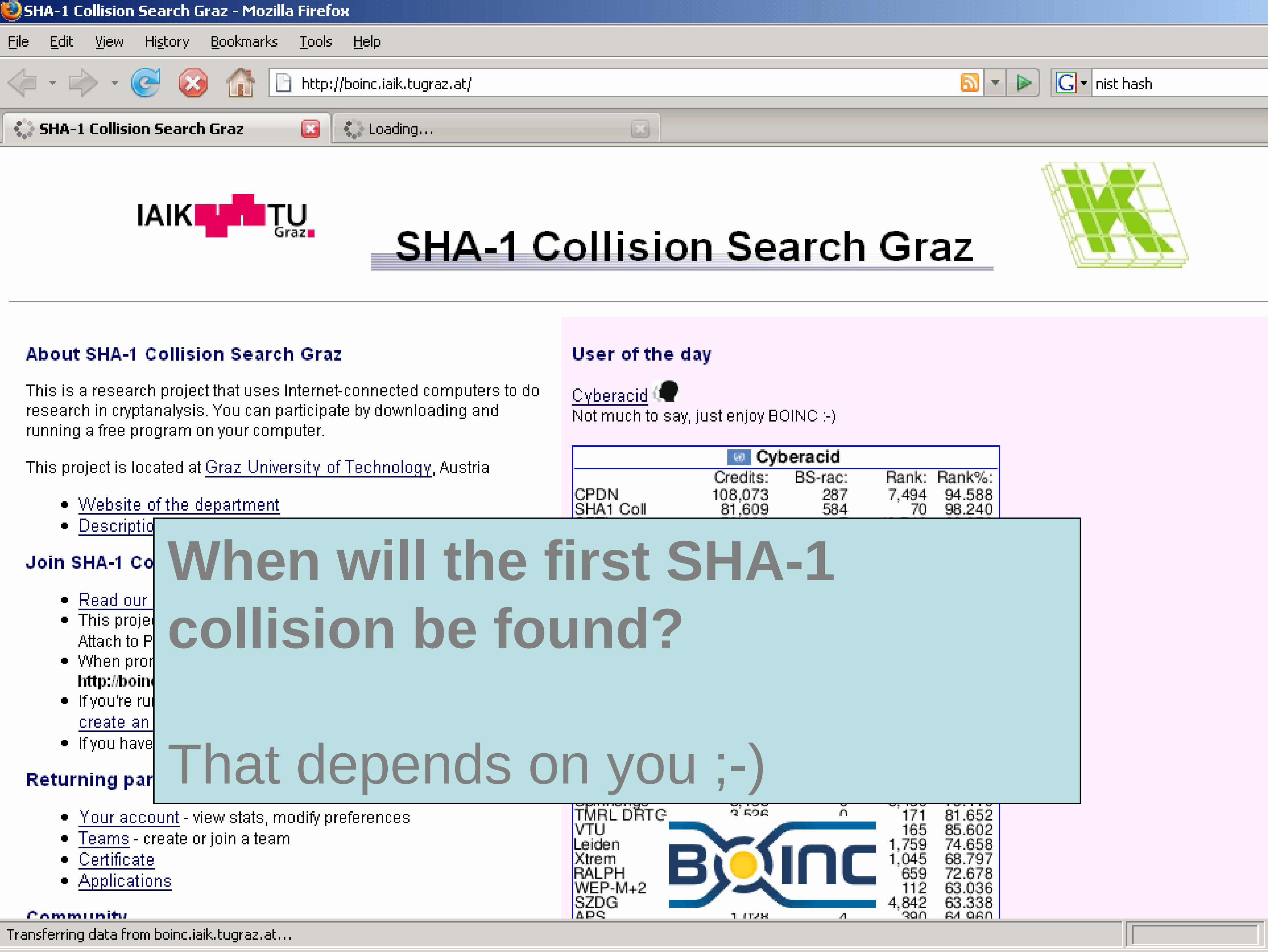
Efficient Implementation on Target Platform



Cryptanalytical Work

Efficient Implementation on Target Platform

New possibility: exploit this feedback loop during single attack


SHA-1 Collision Search Graz - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://boinc.iaik.tugraz.at/
nist hash
SHA-1 Collision Search Graz
Loading...
IAIK TU Graz

SHA-1 Collision Search Graz

About SHA-1 Collision Search Graz

This is a research project that uses Internet-connected computers to do research in cryptanalysis. You can participate by downloading and running a free program on your computer.

This project is located at Graz University of Technology, Austria

- Website of the department
- Descriptio

Join SHA-1 Co

- Read our
- This proje
  Attach to P
- When pro
  http://boin
- If you're ru
  create an
- If you have

Returning par

- Your account - view stats, modify preferences
- Teams - create or join a team
- Certificate
- Applications

Community

User of the day

Cyberacid
Not much to say, just enjoy BOINC :-)

Cyberacid	Credits:	BS-rac:	Rank:	Rank%:
CPDN	108,073	287	7,494	94.588
SHA1 Coll	81,609	584	70	98.240
TMRL DRTG	3,526	0	171	81.652
VTU			165	85.602
Leiden			1,759	74.658
Xtrem			1,045	68.797
RALPH			659	72.678
WEP-M+2			112	63.036
SZDG			4,842	63.338
APS	1,078	4	390	64.960

Transferring data from boinc.iaik.tugraz.at...

When will the first SHA-1 collision be found?

That depends on you ;-)

Application to (2nd) preimage attacks

Application to (2nd) preimage attacks

- One is well known [Yu, Wang 2005]:
  - Any collision differential with high enough probability 2^{-p} can be used for one out of 2^p messages to find a 2nd preimage
  - On average, the resulting speedup over brute force search is negligible

- Surprisingly, there is another link between collision attacks and **preimage** and **2nd preimage** attacks

- no constraints on 1st preimage or target hash

Application to (2nd) preimage attacks: Idea

Start with candidate message, hash it

In case message is not a preimage

Use **(collection of) fast near-collision attacks** to

Toggle collection of bits at the output of the hash
(→ advantage over brute force search)

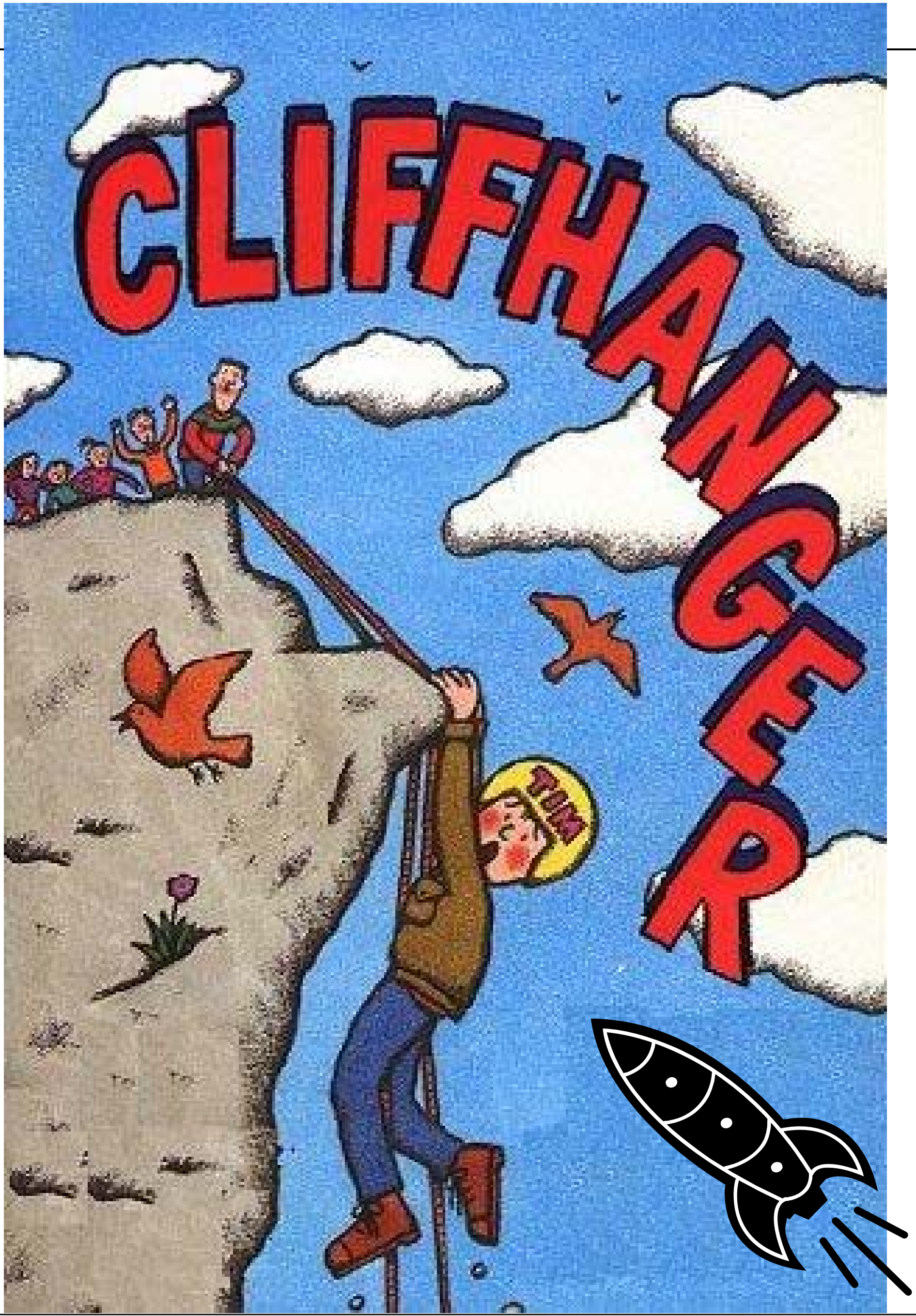
Repeat

Explored for MD4, HAVAL, reduced SHA/SHA-1

Even on average, noticeable improvement over brute force search

Summary

- SHA-1 collisions finally within reach
- 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
- Link between near-collision attacks and preimage attacks


CLIFFHANGER
TIM

Collision attack

SHA-1

Preimage Attacks