Update on SHA-1

Florian Mendel
Christian Rechberger
Vincent Rijmen

Crypto 2007 Rump Session

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

Faculty of Computer Science
Graz University of Technology

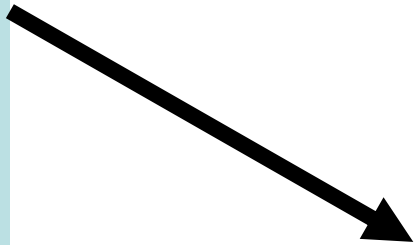
Prelude

CRYPTO rump session of last year…

Meaningful collision for 64-step SHA-1

I hereby solemnly promise to finish my PhD thesis by the end of 2005

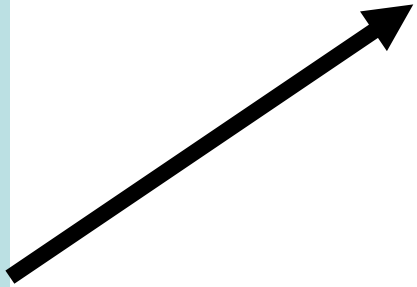
[Garbage]



Same Hash

I hereby solemnly promise to finish my PhD thesis by the end of 2006'

[Garbage]



The story continues…

Current status

This collision did not help ;-)

Christophe De Cannière finished in 2007

We need to do this again

Now for full (80-step) SHA-1

The problem:

How to get the necessary
degrees of freedom
for speed-ups?

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)

First attempt on full SHA-1

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

We just started a distributed computing effort:

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

The real problem:

How do we want the first SHA-1 collision to look like?

Update on SHA-1

Florian Mendel
Christian Rechberger
Vincent Rijmen

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