Nat McHugh

An important site on a minor internet.

Home | About | PGP Key

Wednesday, January 7, 2015

Hash Collisions Reading List

Lately in an effort to code up and properly understand the Wang attack on the MD4 family of hash functions I've been reading a lot of papers on the subject. Many of the papers have very similar names and the same authors. I found myself having to create a quick reference about each paper and it's contents.

Here they are with a brief summary of what I got from each:

Collision for Hash Functions MD4, MD5 HAVAL-128 and RIPEMD
Xiaoyun Wang, Dengguo Feng, Xuejia Lai and Hongbo Yu

https://eprint.iacr.org/2004/199.pdf

This is the original paper listing out some collisions for each of these functions. This must have been quite a blockbuster at the time.

Cryptanalysis of the Hash Functions MD4 and RIPEMD
Xiaoyun Wang, Xuejia Lai, Dengguo Feng, Hui Chen, and Xiuyuan Yu

https://s3-eu-west-1.amazonaws.com/md5collisions/CryptanalysisOftheHashFunctionsMD4andRIPEMD.pdf

This article details the attack that was used to generate the collisions of the previous paper and should be all you need to write a collision generating script for MD4 and RIPEMD.

Twitter

How to Break MD5 and Other Hash Functions
Xiaoyun Wang and Hongbo Yu

https://s3-eu-west-1.amazonaws.com/md5collisions/HowtoBreakMD5andOtherHashFunctions.pdf

MD5 is slightly harder to break than MD4 requiring 2 blocks and more muli-step message modifications. This article details the method used to generate MD5 collisions in the first.

Searching for Differential Paths in MD4
Martin Schälffer and Elisabeth Oswald

https://s3-eu-west-1.amazonaws.com/md5collisions/SearchingforDifferentialPathsInMD4.pdf

More detail on how the attacks work with a good description of how paths are calculated and an algorithm for finding them. Also contains a new path with fewer stage 2 required requirements.

Improved Collision Attack on MD5
Yu Sasaki, Yusuke Naito, Noboru Kunihiro and Kazuo Ohta

https://s3-eu-west-1.amazonaws.com/md5collisions/ImprovedCollisionAttackonMD5.pdf

The paper where I finally understood how the correction of second round collisions worked

Improved Collision Attack on MD4
Yusuke Naito, Yu Sasaki, Noboru Kunihiro, and Kazuo Ohta

https://eprint.iacr.org/2005/151.pdf

Some corrections to the Wang collision on MD4 speeds things up with good explanation.

Automatic Search of Differential Path in MD4
Pierre-Alain Fouque, Gaëtan Leurent, Phong Nguyen

http://www.di.ens.fr/~fouque/pub/md4.pdf

New Message Difference for MD4
Yu Sasaki, Lei Wang, Kazuo Ohta and Noboru Kunihiro

https://www.iacr.org/archive/fse2007/45930331/45930331.pdf

The best path I know of with a totally different message difference and explanation of the local collisions underlying the collisions.

Herding Hash Functions and the Nostradamus Attack
John Kelsey and Tadayoshi Kohno

http://homes.cs.washington.edu/~yoshi/papers/EC06/herding.pdf

Posted by Nathaniel McHugh at 3:10 PM

G+1 Recommend this on Google

Labels: Hash functions
Location: Sheffield, South Yorkshire, UK

No comments:

Post a Comment

Tweets by @natmchugh

natmchugh
@natmchugh

@katie_fenn ok 🔥🔥🔥

17 May

natmchugh
@natmchugh

@katie_fenn I have one if you need to borrow one.

17 May

natmchugh
@natmchugh

Ah yes short Weierstrass form versus Edwards form, very amusing.

12 May

natmchugh
@natmchugh

@katie_fenn Sadly not available beta.companieshouse.gov.uk/search/compani...+

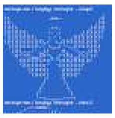
Embed View on Twitter

Popular Posts

Create your own MD5 collisions
A while ago a lot of people visited my site (~ 90,000) with a post about how easy it is to make two images with same MD5 by using a chos...

How I created two images with the same MD5 hash
I posted the following images the other day which although looking totally different have exactly the same MD5 hash (e06723d4961a0a3f950e...

How I made two PHP files with the same MD5 hash
I recently posted a link on twitter to two PHP scripts which have different behaviours but the same MD5 hash. To verify this download the fi...



How to make two binaries with the same MD5 hash
One question I was asked when I demo'd creating two PHP files with the same hash is; does it work on compiled binaries? Well the answ...

Three way MD5 collision
Previously I explained how I created two images one of James Brown the other of Barry White with the same MD5 hash. At the end of the post I...

Hash Collisions Reading List
Lately in an effort to code up and properly understand the Wang attack on the MD4 family of hash functions I've been reading a lot of pa...

The Magic Words are Squeamish Ossifrage - factoring RSA-129 using CADO-NFS