

# Impact of Recent Attacks on Hash Functions

Norbert Pramstaller

<http://www.iaik.tugraz.at/aboutus/people/pramstaller/index.php>

Hash&Stream, Salzburg, 2007/02/02

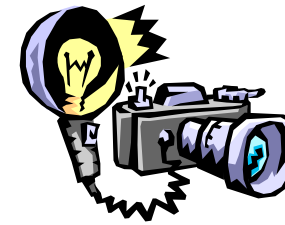
***Institute for Applied Information Processing  
and Communications (IAIK) - Krypto Group***

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



## A Legal Case in Australia

- „NSW speed cameras in doubt”  
(August, 2005)



- RTA's speed monitoring device uses MD5
  - picture taken by approved device
  - picture has not been altered
- Lawyer of defendant: MD5 is broken
- RTA: no expert to show authenticity of taken picture
- Magistrate: dismissed speeding case



security problem  
or  
smart lawyer

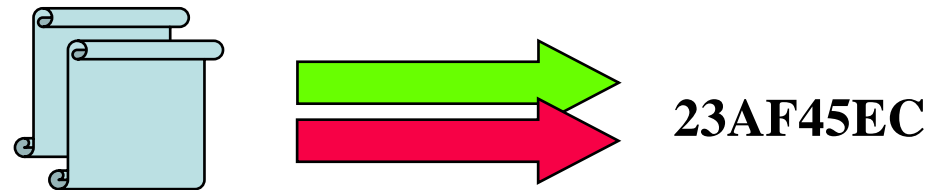


# Outline

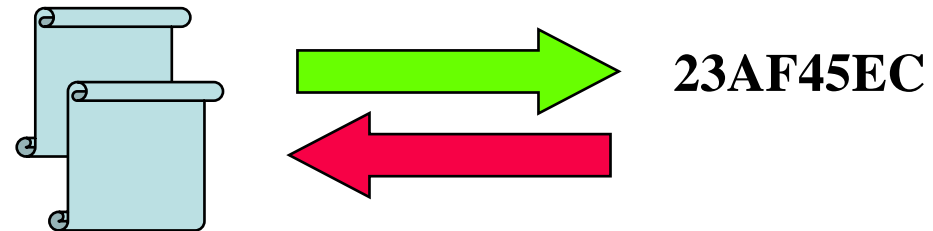
- Refresher
  - Requirements for cryptographic hash functions
- Application of hash functions and the impact of recent advances in cryptanalysis
  - electronic (digital) signatures
  - message authentication codes
  - password protection
  - some other applications and practical examples
    - colliding PS documents and colliding X.509 certificates
- Efforts in design and analysis of crypt. hash functions
  - NIST/ECRYPT

# Requirements for Cryptographic Hash Functions

- Collision resistance



- 2nd preimage resistance



- Preimage resistance



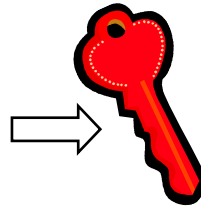
# Digital Signatures

CREATE



00110.....11001

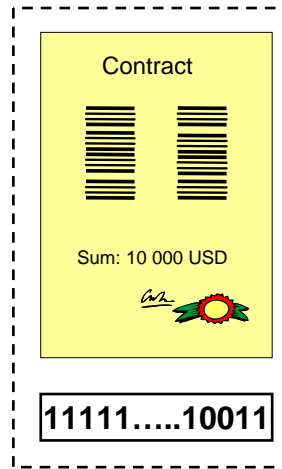
hash



private key sender

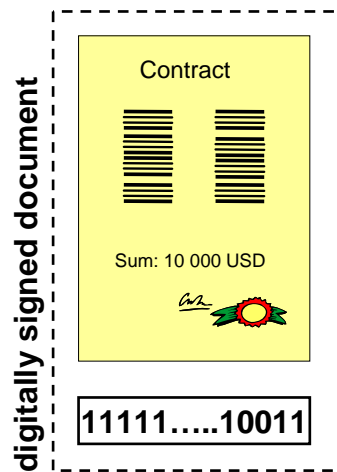
11111.....10011

signed hash



digitally signed document

VERIFY



digitally signed document



hash

00110.....11001



public key sender

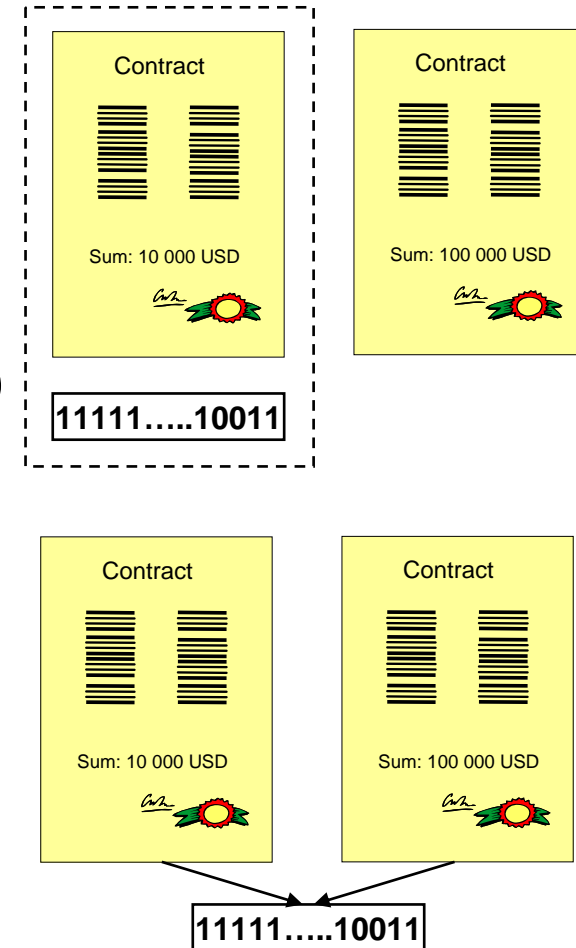
00110.....11001



compare

# Digital Signatures

- Second preimages
  - forgery
  - anybody can forge signature
  - can be done at anytime (after first signing)
- Collisions
  - allows signer to repudiate signature
  - must be done before signing
    - adversary needs to control both messages
    - old documents are not endangered
  - specifications demand collision resistance
- Preimages
  - second preimages (different message)

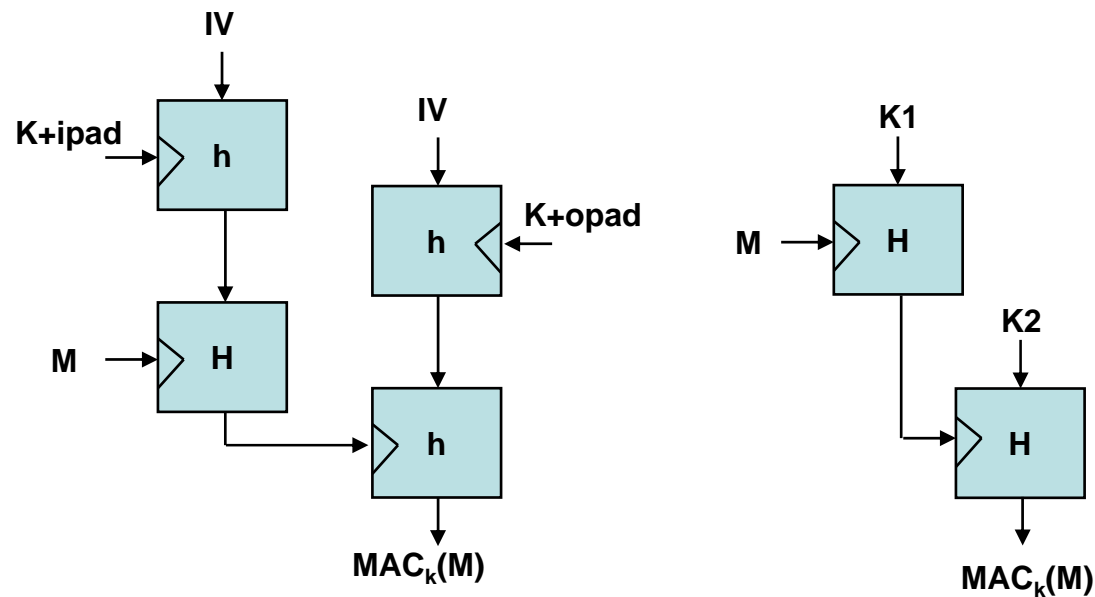


# Message Authentication Codes MACs

- Verify integrity and authenticity of information
- Must resist
  - forgery
  - key recovery

message  $M$ , key  $k$ : send  $MAC_k(M) || M$

- MACs based on hash functions
  - HMAC and NMAC
  - MD5/SHA-1



## Message Authentication Codes MACs

- Second preimage attacks: forgery

message  $M$ , key  $k$ :  $MAC_k(M) || M$   
 $M'$  is second preimage of  $M$   
 $MAC_k(M) = MAC_k(M')$

- Collision attacks have impact
  - distinguishing and forgery attacks  
(MD5 and round-reduced SHA-1)  
[CY2006, KBPH2006, RR2007]
  - other hash functions (e.g. SHA-2) no problem yet

# Password Protection

- Client authentication
  - password previously registered at server side
  - only save hash value (MD5) of password (+ salt)
- Preimages: crucial
  - */etc/passwd* root:Npg...pfz4wuk:503:100:Full root:/root:/bin/bash

```
-rw-r--r-- 1 root root 1366 2007-01-01 23:59 passwd
```

# Password Protection

- Client authentication

- password previously registered at server side
- only save hash value (MD5) of password (+ salt)

- Preimages: crucial

- */etc/passwd* root:Npg...pfz4wuk:503:100:Full root:/root:/bin/bash

```
-rw-r--r-- 1 root root 1366 2007-01-01 23:59 passwd
```

- */etc/passwd* & */etc/shadow*

```
Passwd: root:x:0:0:root:/root:/bin/bash
```

```
Shadow: root:$1$19TNpge08pfz4wukplkDBRSQoqwxKH1:13185:0:99999:7:::
```

```
-rw-r----- 1 root shadow 111 2007-01-01 23:59 shadow
```

# Meaningful Collisions

---

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

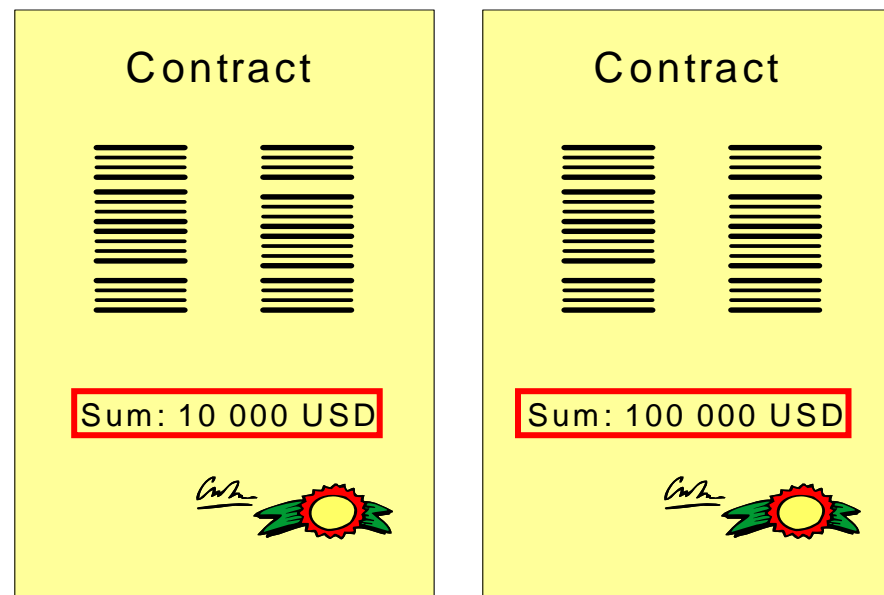
***Faculty of Computer Science  
Graz University of Technology***

---



# Meaningful Collisions

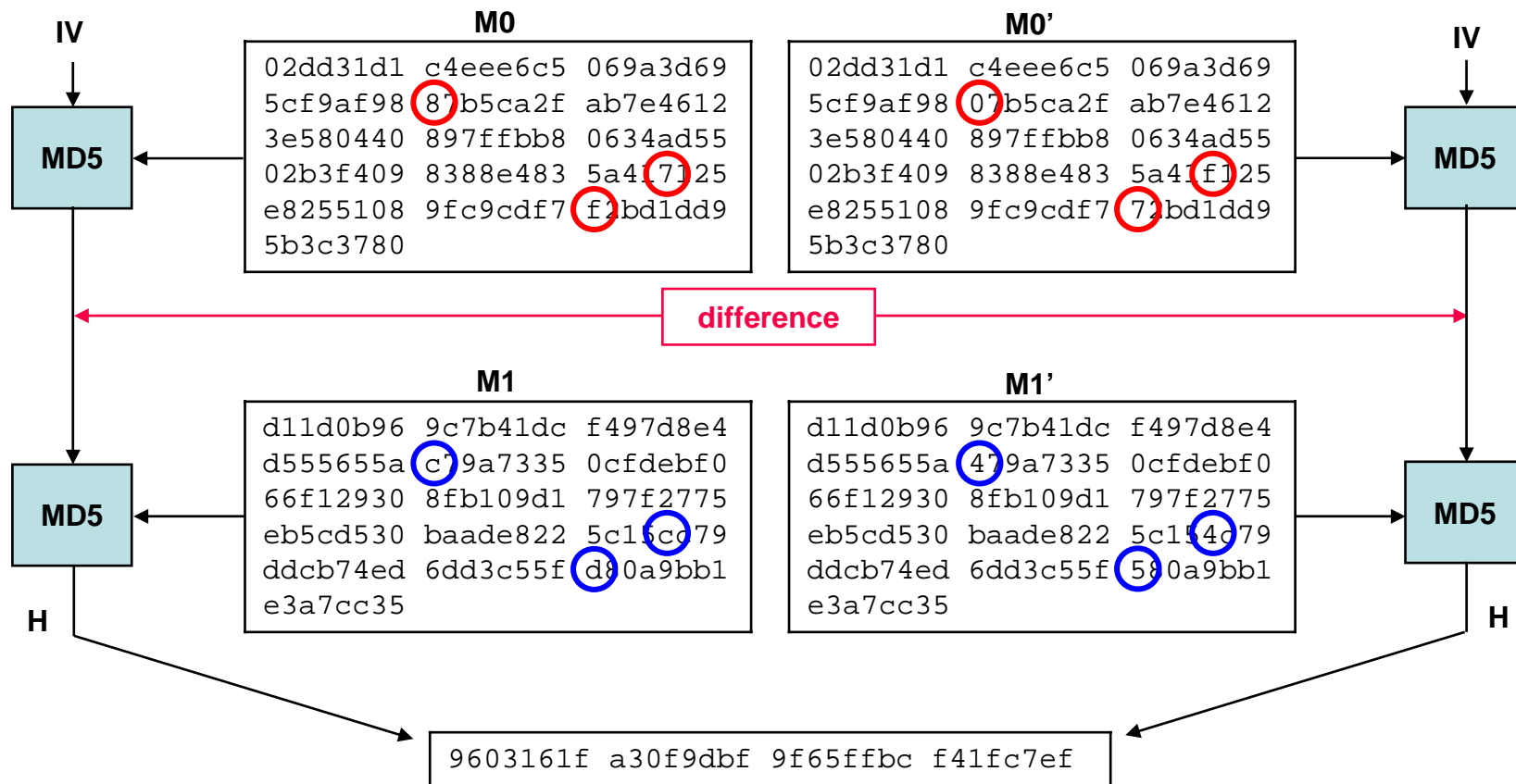
- Two documents with meaningful content that collide



- adversary does not have lot of freedom

# Meaningful Collisions

- Believed to be difficult



colliding message pairs for MD5 [WY2005]

# Meaningful Collisions

- Now some examples demonstrating the opposite
  - kind of meaningful
    - colliding PS documents (MD5) [DL2005]
    - colliding executables (MD5) [Sel2005]
    - etc
  - meaningful
    - colliding X.509 certificates (MD5) [SLdW2006]

## Colliding PS Documents [DL2005]

- Two different documents with same MD5 hash value

given target

... fulfilled all the requirements ... I highly recommend hiring her.  
  
Sincerely,  
Julius Caesar

colliding order

... full access to all confidential and secret information ...  
  
Sincerely,  
Julius Caesar

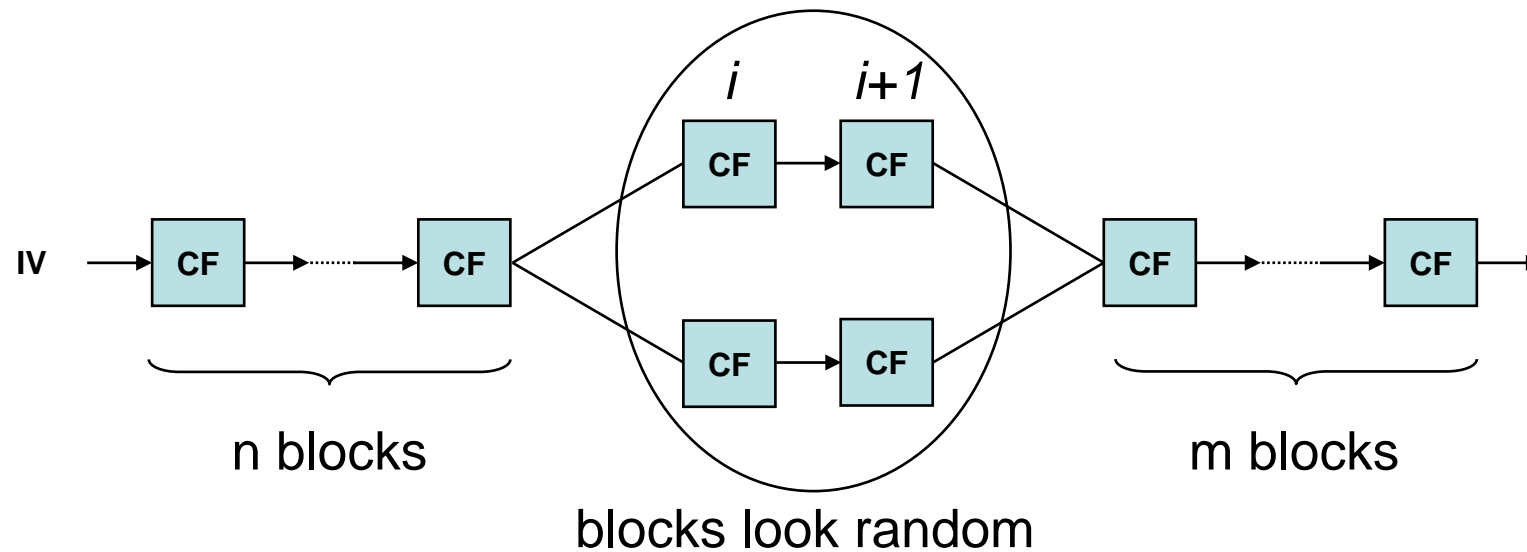
MD5

5421a523481fdc6a2a1c832e72c7b8a5

Source: <http://www.cits.rub.de/MD5Collisions/>

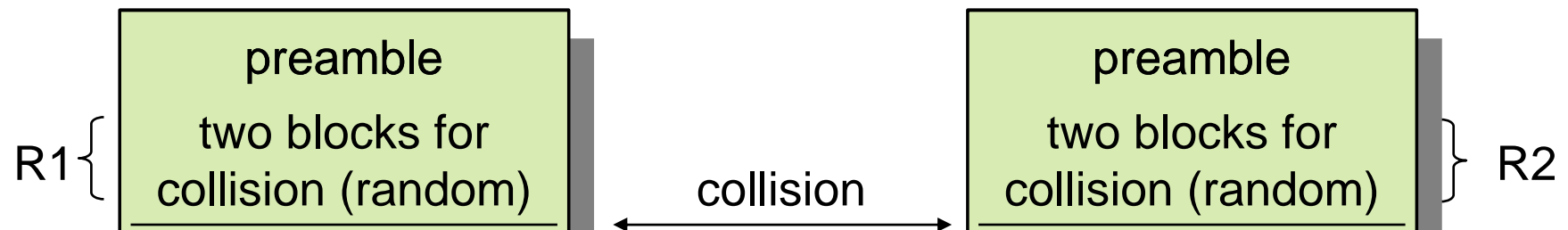
# Colliding PS Documents

- Basic idea
  - after collision we can append any string
  - if collision is independent of IV (MD5) then also append prefix



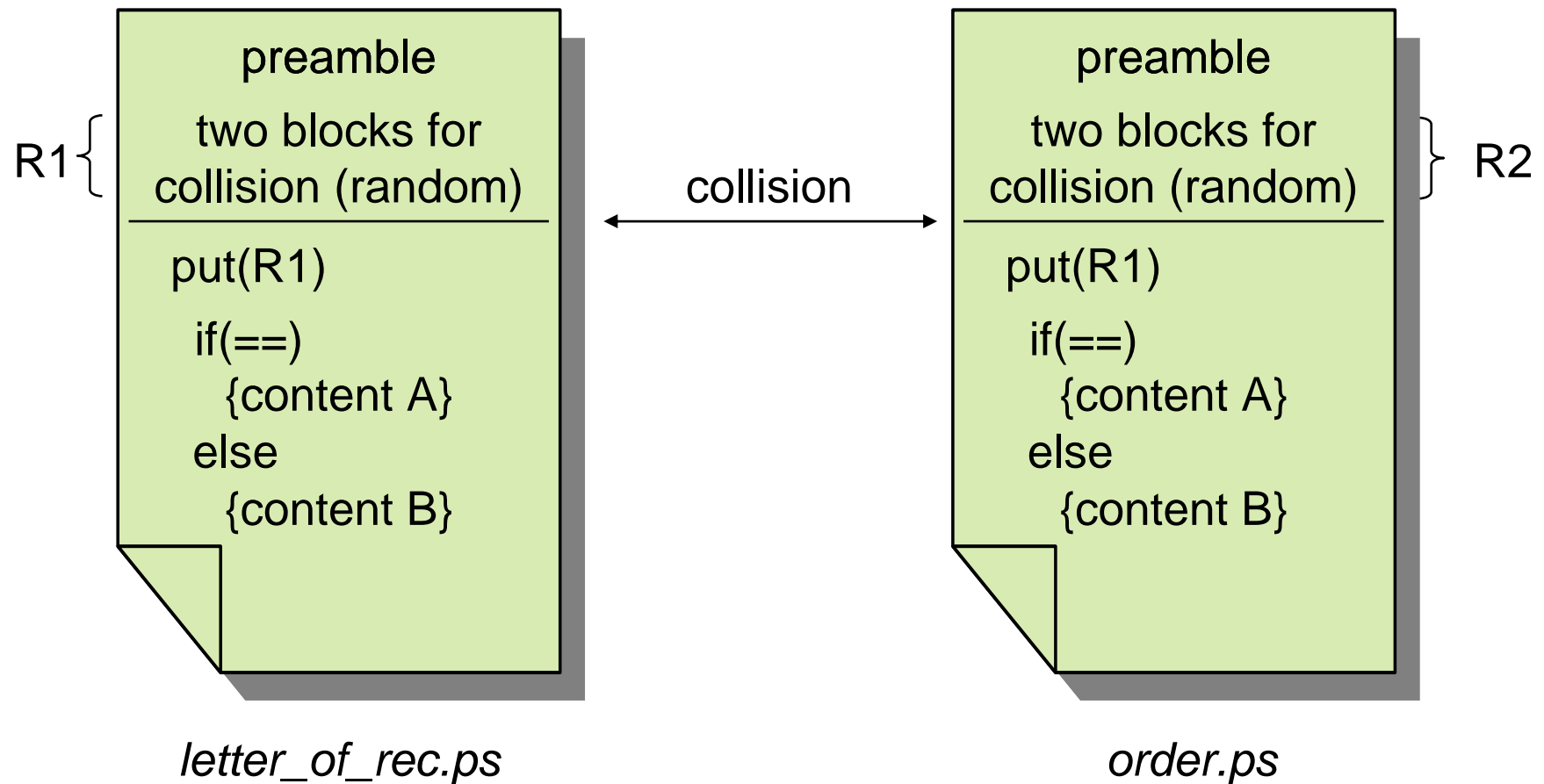
# Colliding PS Documents

- The working principle using postscript



# Colliding PS Documents

- The working principle using postscript

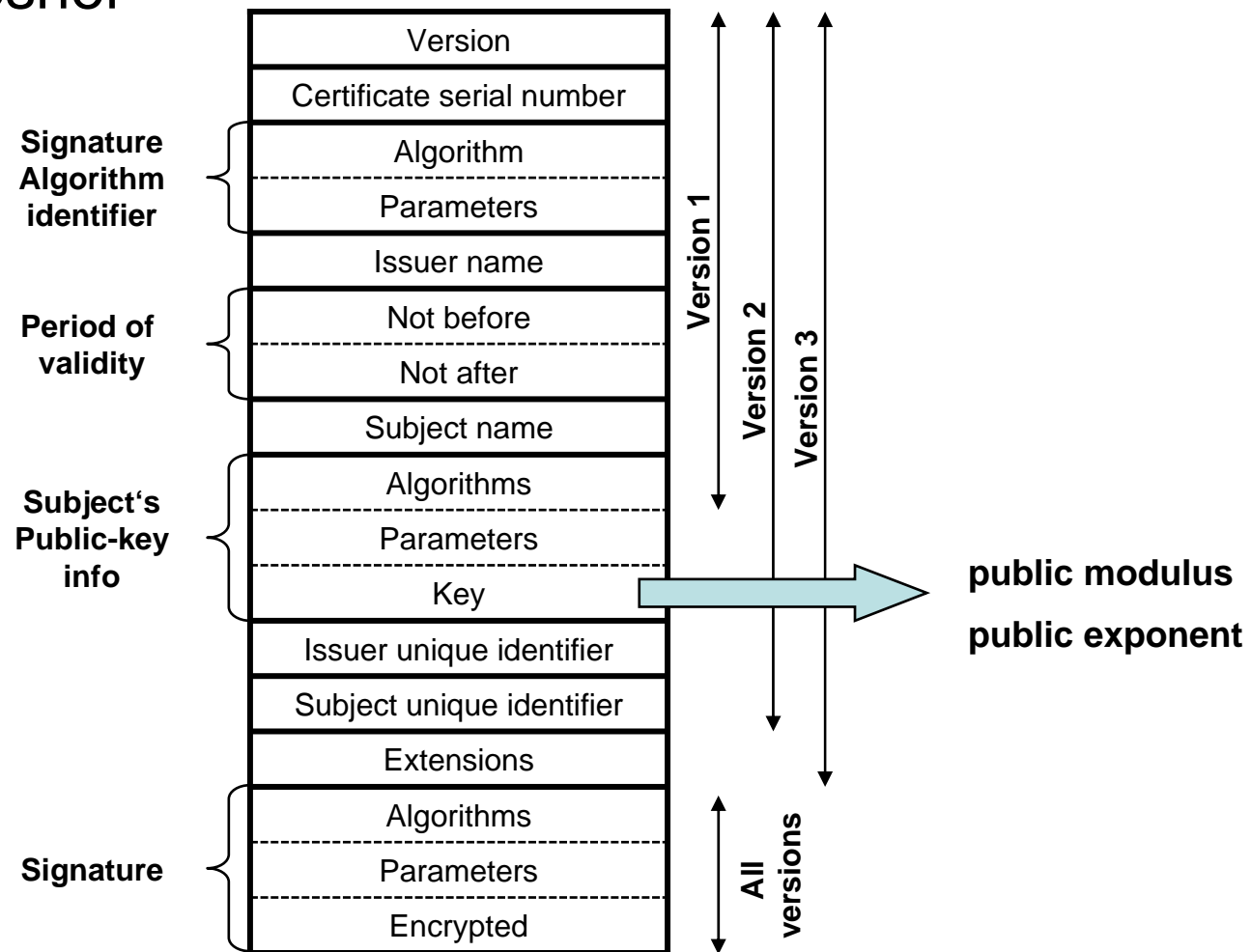


## From Random to Meaningful

- Previous example
  - colliding messages (random content) need to be hidden
  - can be counteracted by inspection (e.g. bit level)
- New approach [SLdW2006]
  - colliding X.509 certificates
  - <http://www.win.tue.nl/hashclash/>
  - <http://eprint.iacr.org/2006/360/>

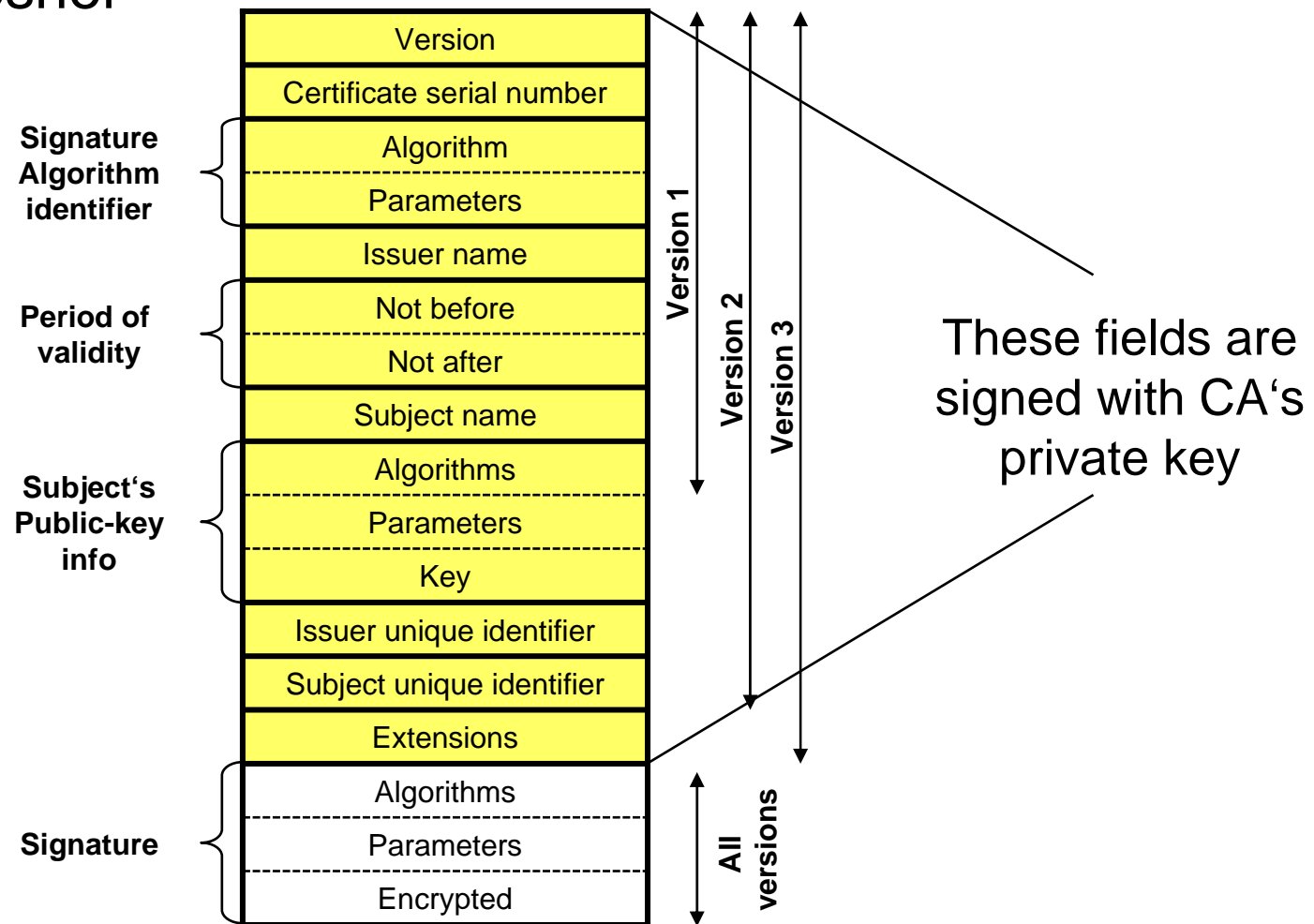
# Colliding X.509 Certificates

- X.509 refresher



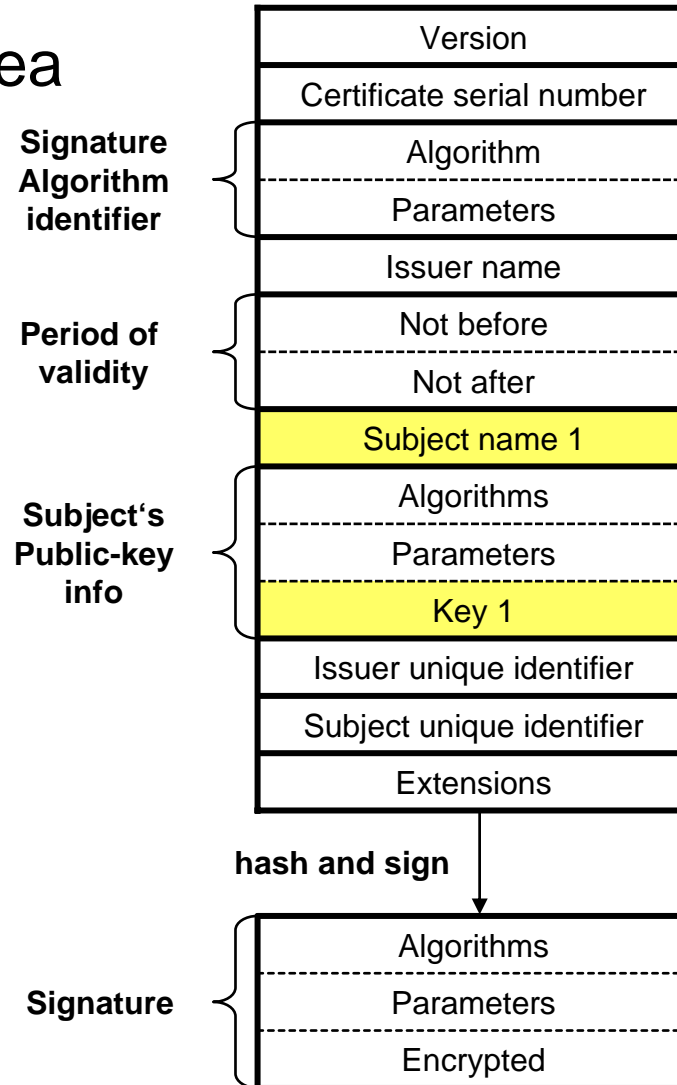
# Colliding X.509 Certificates

- X.509 refresher



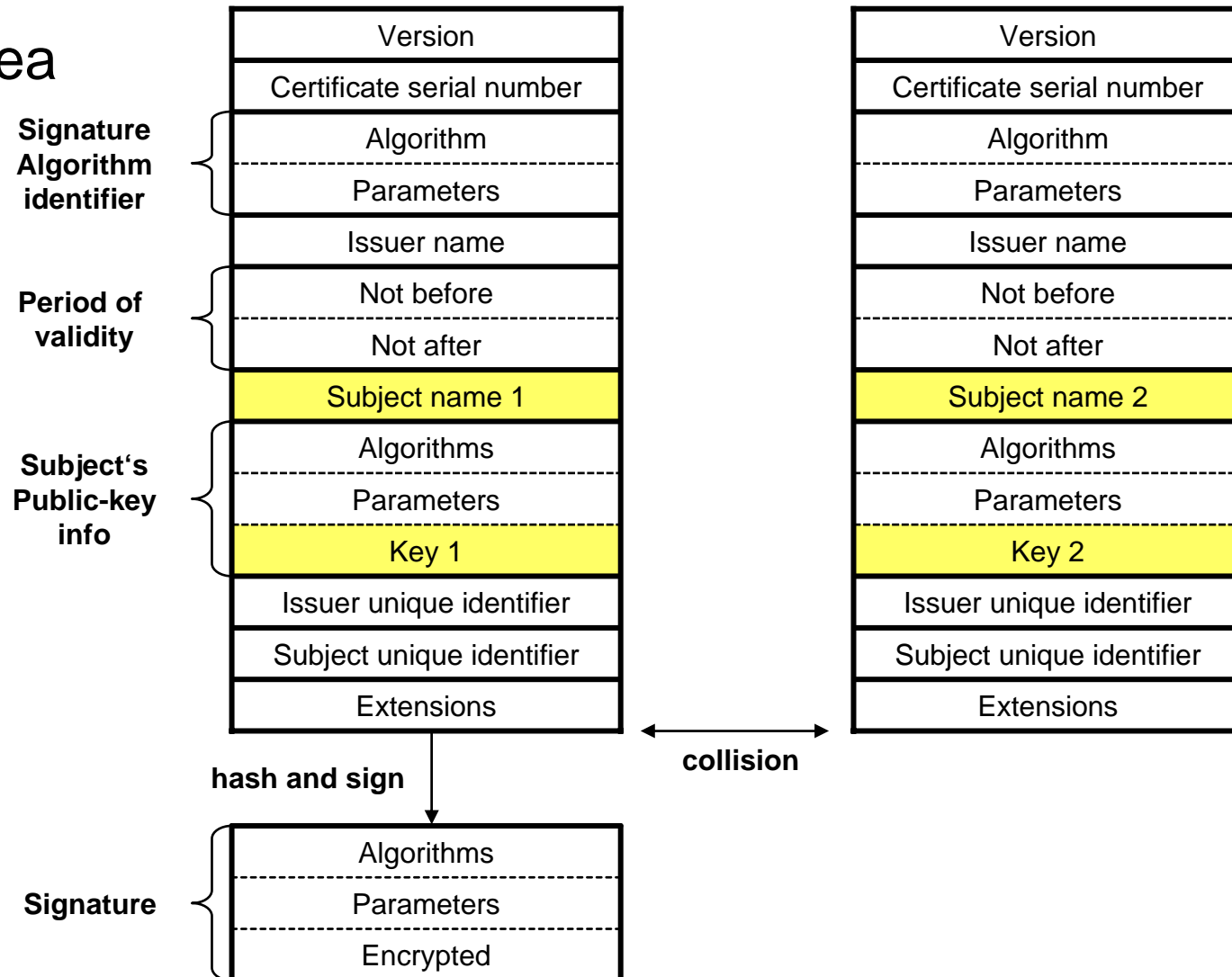
# Colliding X.509 Certificates

■ Basic idea



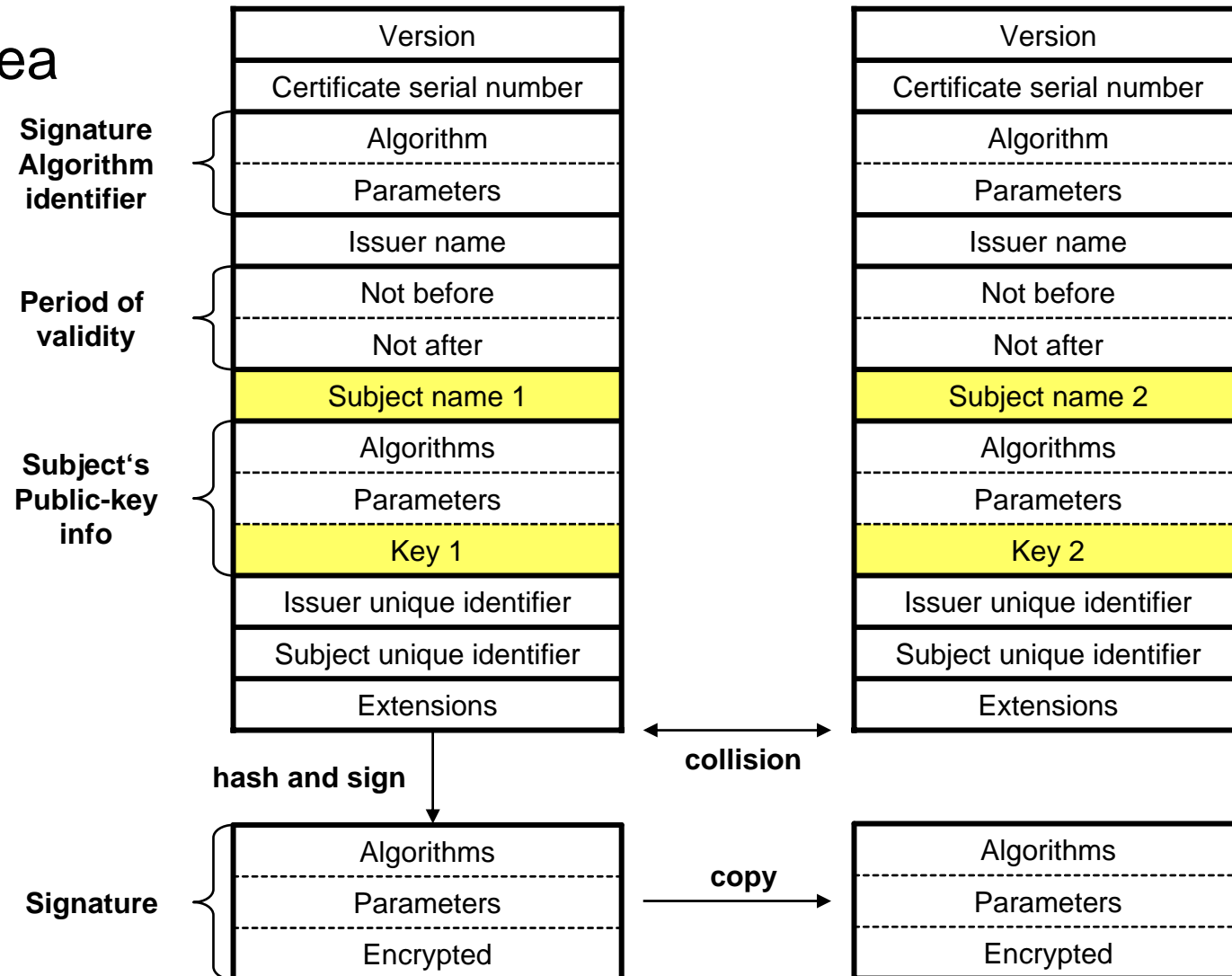
# Colliding X.509 Certificates

## Basic idea



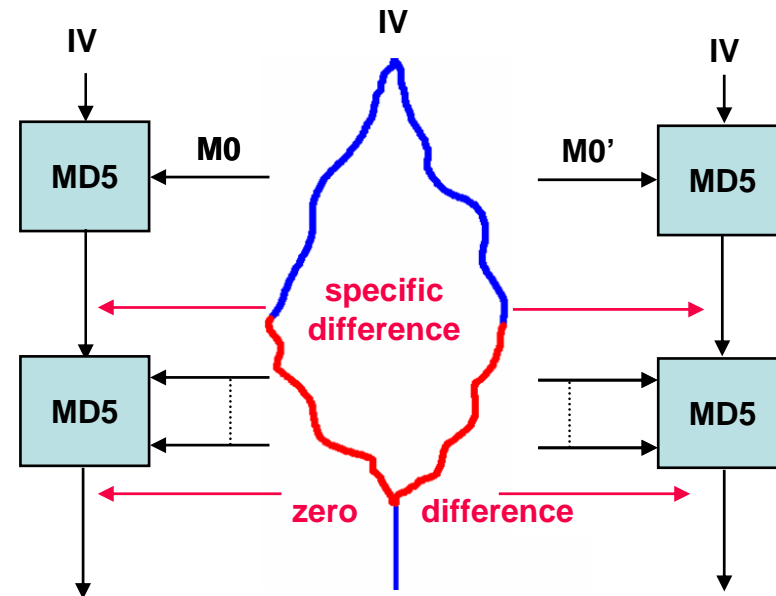
# Colliding X.509 Certificates

## Basic idea

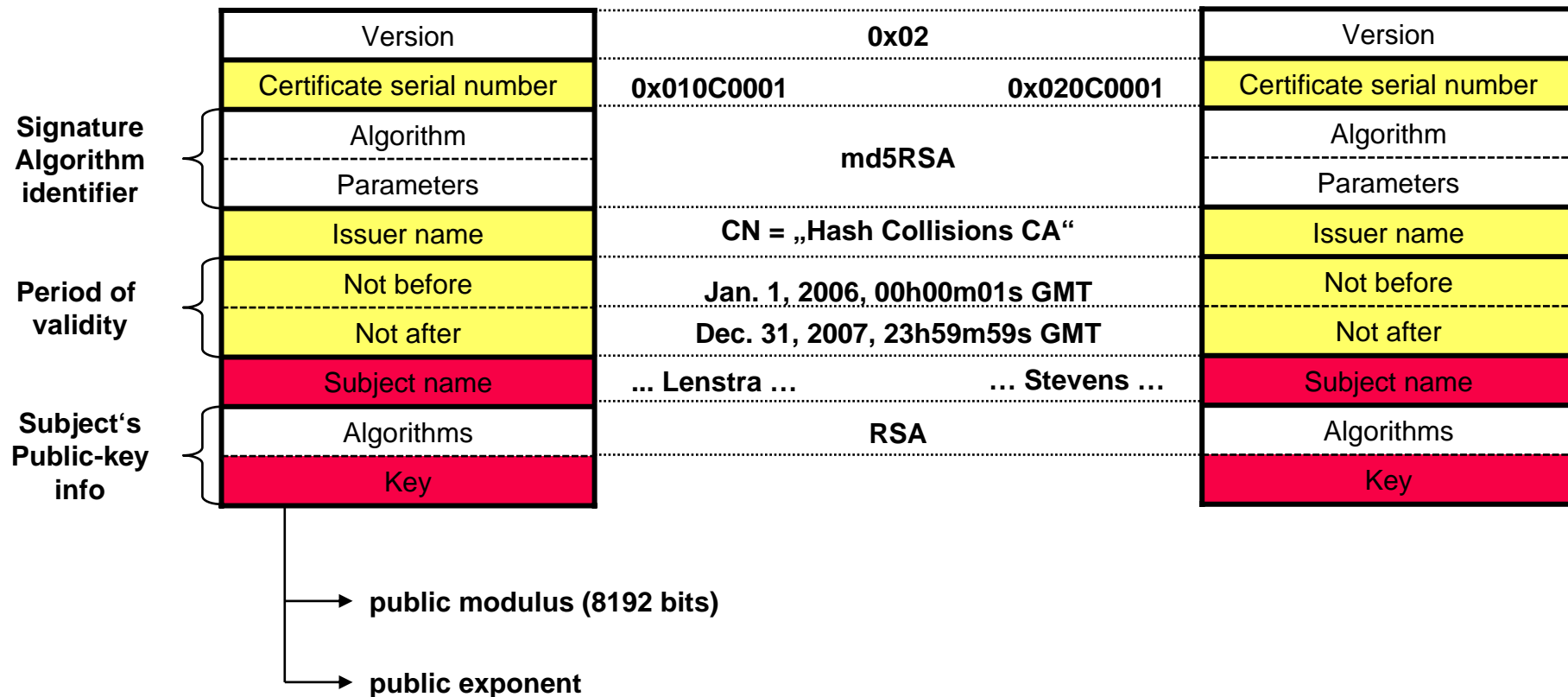


# Colliding X.509 Certificates

- Arbitrary  $M_0, M_0'$
- Bit-length  $416 \bmod 512$   
(96 bits of last block missing)
- Properly choose 96 bits to get specific difference
- Add certain number of blocks to cancel difference (for this example 8 blocks needed)
- Red part consists of
  - $96 + 8 \times 512 = 4192$  bits
- Estimated complexity for these steps:  $2^{52}$



# Colliding X.509 Certificates

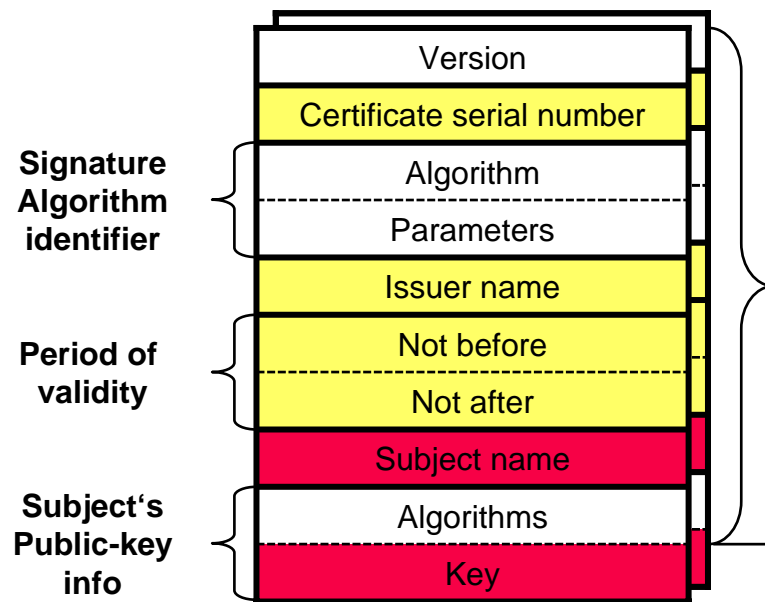


X.509 standard identical

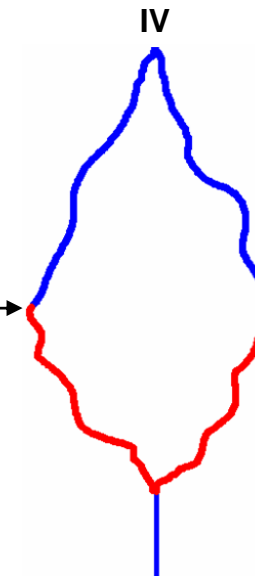
chosen by CA

chosen by adversary not identical

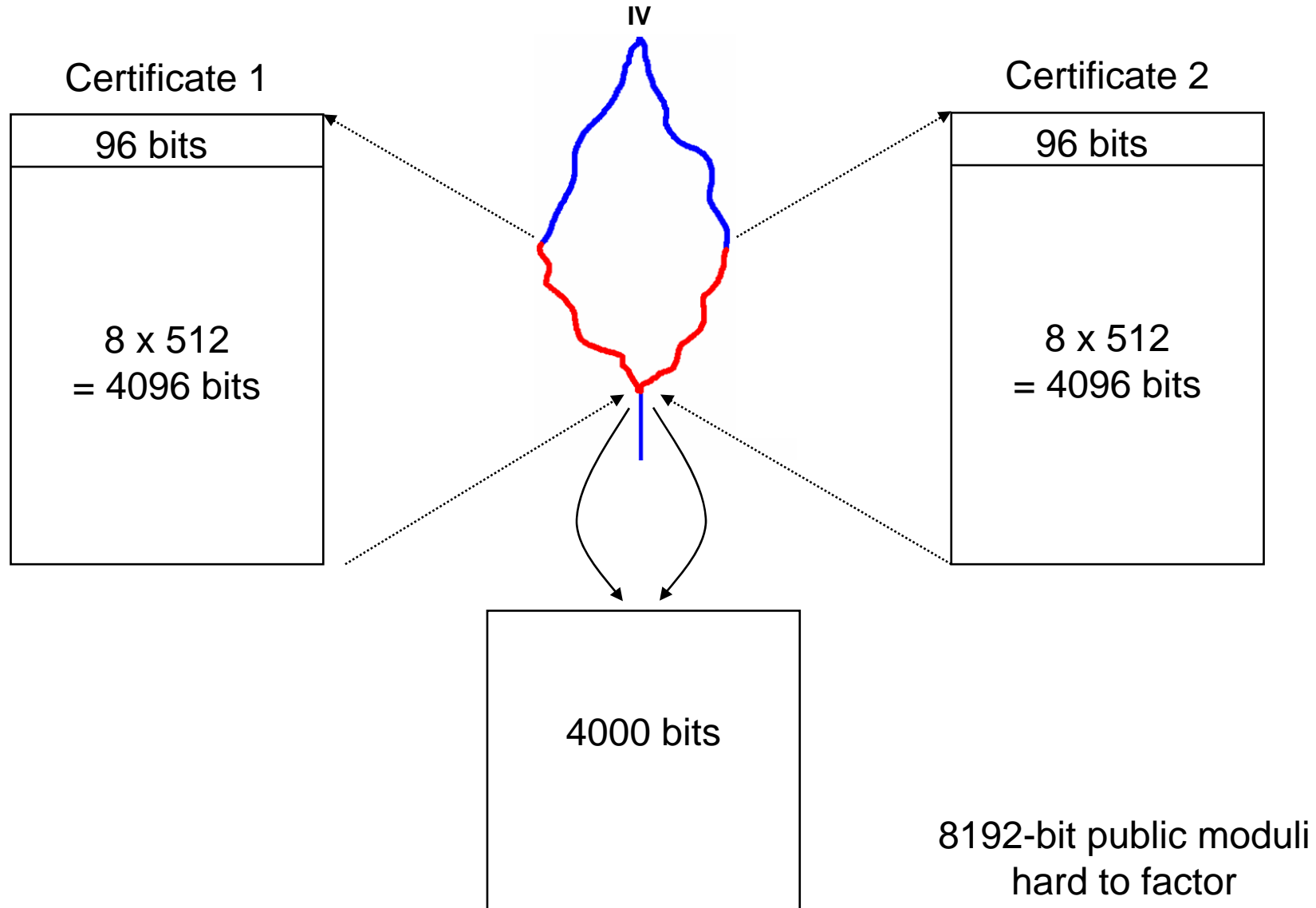
# Colliding X.509 Certificates



- Until subjects public-key modulus
  - both messages equal length
  - multiple of 512 bits
  - last block 416 bits
  - arbitrary difference



# Colliding X.509 Certificates

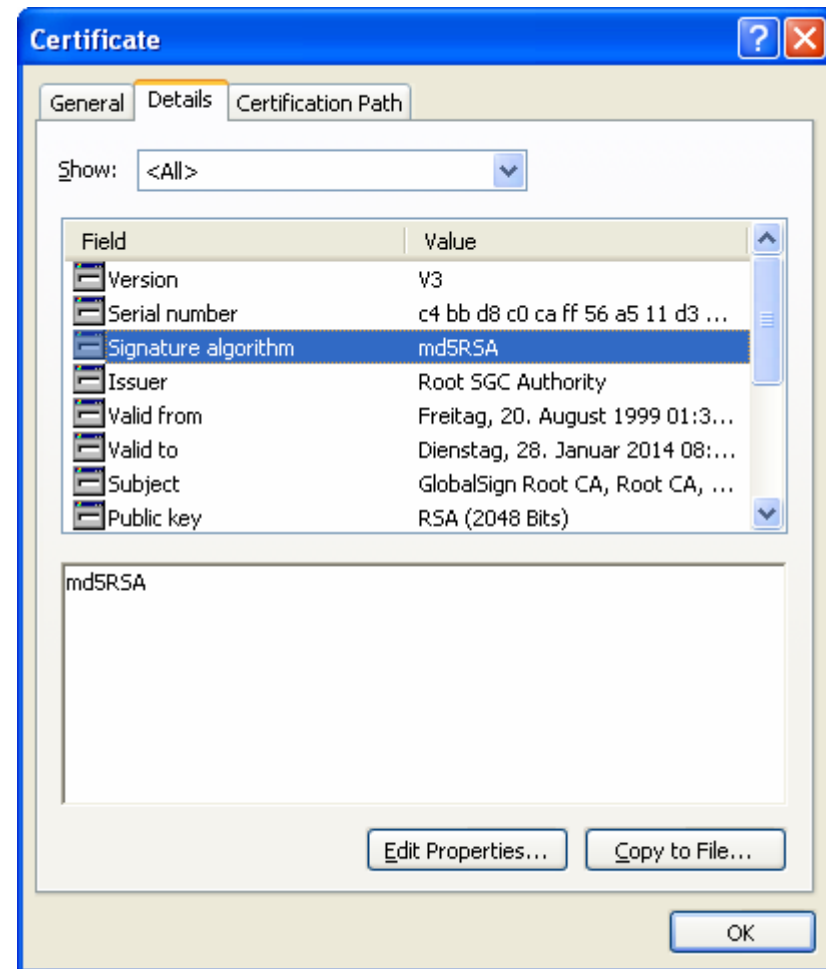


## Colliding X.509 Certificates

- Two colliding certificates with different subject name and different public keys
- First example of meaningful collision
- Certificates need to be generated simultaneously
- Assumptions:
  - need sufficient control over CA
    - predict all information prior to the public key info fields
  - attacker can be identified
- To summarize: **do not use MD5 anymore**
  
- Similar things for SHA-1
  - <http://www.iaik.tugraz.at/research/krypto/collision/>

## MD5 Based X.509 Certificates

- Advice: stop using MD5
  - RIPE since 1992
  - RSA since 1996 [1]
  
- Industry: largely ignored



[1] <ftp://ftp.rsasecurity.com/pub/pdfs/bulletn4.pdf>

# Design of New Hash Functions

---

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

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

---



# Efforts in Design and Cryptanalysis of Hash Functions

## ▪ NIST

- will launch similar public contest as for AES
- one or more hash algorithms to revise FIPS 180-2
- tentative timeline 2007-2012
  - define requirements and ask for hash function proposals
  - three *Hash Function Candidate Conferences*
  - 2011: announce new hash functions
  - 2012: standard and revise FIPS 180-2

## ▪ NoE ECRYPT

- working group within STVL
- Hash Workshop in Barcelona, May 24-25, 2007

<http://events.iaik.tugraz.at/hashworkshop07/>

# NIST

- **NIST's Policy on Hash Functions** March 15, 2006: **The SHA-2 family of hash functions (i.e., SHA-224, SHA-256, SHA-384 and SHA-512) may be used by Federal agencies for all applications using secure hash algorithms.** Federal agencies should stop using SHA-1 for digital signatures, digital time stamping and other applications that require collision resistance as soon as practical, and must use the SHA-2 family of hash functions for these applications after 2010. After 2010, Federal agencies may use SHA-1 only for the following applications: hash-based message authentication codes (HMACs); key derivation functions (KDFs); and random number generators (RNGs). Regardless of use, NIST encourages application and protocol designers to use the SHA-2 family of hash functions for all new applications and protocols.

<http://www.csrc.nist.gov/pki/HashWorkshop/index.html>

# ECRYPT

- Does not recommend
  - hash functions with less than 160 bits
  - HMAC-MD5
  - digital signatures with MD5
  - SHA-1 in new deployments
- Recommendations
  - RIPEMD-160 (next 3-5 years)
  - long term use: FIPS 180-2 or alternatives such as Whirlpool

[http://www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH\\_STMT-1.1.pdf](http://www.ecrypt.eu.org/documents/STVL-ERICS-2-HASH_STMT-1.1.pdf)

## Conclusion

- Real threat
  - second preimages and preimages
- Legally
  - collision resistance important (see speeding ticket case)
- Stop using MD5 and SHA-1
  - collisions for 80 steps expected sooner than later
  - old saying inside NSA:  
“Attacks always get better; they never get worse”
- New approaches and further details about hash functions required
  - NIST/ECRYPT

## References

- [WY2005] Wang and Yu, *How to Break MD5 and Other Hash Functions*, EUROCRYPT 2005 (LNCS 3494)
- [DL2005] Daum and Lucks, *Attacking Hash Functions by Poisoned Messages “The Story of Alice and her Boss”*  
<http://www.cits.rub.de/MD5Collisions/>
- [Sel2005] Selinger, *MD Collision Demo*  
<http://www.mscs.dal.ca/~selinger/md5collision/>
- [CY2006] Contini and Yin, *Forgery and Partial Key-Recovery Attacks on HMAC and NMAC Using Hash Collisions*, ASIACRYPT 2006 (LNCS 4284)
- [KBPH2006] Kim, Biryukov, Preneel, and Hong, *On the Security of HMAC and NMAC Based on HAVAL, MD4, MD5, SHA-0 and SHA-1*, SCN 2006 (LNCS 4116)
- [SLdW2006] Stevens, Lenstra, and de Weger, *Target Collisions for MD5 and Colliding X.509 Certificates for Different Identities*, Cryptology ePrint Archive, Report 2006/360, 2006 <http://eprint.iacr.org/2006/360>
- [RR2007] Rechberger and Rijmen, *On Authentication Using HMAC and Non-Random Properties*, FC 2007, to appear in LNCS