

**Rehashing Cryptographic Hash Functions:
 the SHA-3 Competition**

Bart Preneel
 COSIC – Katholieke Universiteit Leuven, Belgium
 bart.preneel(AT)esat.kuleuven.be

Journées Codage et Cryptographie
 October 2009

Outline

- definitions
- applications
- generic attacks
- attacks on iterated constructions: the rise and fall of MD
- MD4, MD5, SHA-0, SHA-1
- SHA-2
- SHA-3: the NIST AHS competition
- SHA-4
- conclusions

2

Hash functions

- MDC (manipulation detection code)
 - (MDC-2)
 - (MD5)
 - (SHA-1)
 - RIPEMD-160
 - SHA-256, SHA-512
- Protect short hash value rather than long text

This is an input to a cryptographic hash function. The input is a very long string, that is reduced by the hash function to a string of fixed length. There are additional security conditions: it should be very hard to find an input hashing to a given value (a preimage) or to find two colliding inputs (a collision).

3

Hash function flavours

cryptographic hash function

```

    graph TD
      CH[cryptographic hash function] --> MAC[MAC]
      CH --> MDC[MDC]
      MDC --> OWHF[OWHF]
      MDC --> UOWHF[UOWHF (TCR)]
      MDC --> CRHF[CRHF]
      this_talk[this talk] --> MDC
    
```

4

Informal definitions (1)

- no secret parameters
- input string x of arbitrary length \Rightarrow output $h(x)$ of fixed bitlength n
- computation “easy”
- One Way Hash Function (OWHF)
 - preimage resistance
 - 2nd preimage resistance
- Collision Resistant Hash Function (CRHF): OWHF +
 - collision resistant

5

Security requirements (n-bit result)

preimage	2 nd preimage	collision
2^n	2^n	$2^{n/2}$

6

Formal definition: (2nd) preimage resistance

Notation: $\Sigma = \{0, 1\}$, $l(n) > n$

A **one-way hash function (OWFH)** H is a function with domain $D = \Sigma^{l(n)}$ and range $R = \Sigma^n$ that satisfies the following conditions:

- preimage resistance:** let x be selected uniformly in D and let M be an adversary that on input $h(x)$ uses time $\leq t$ and outputs $M(h(x)) \in D$. For each adversary M ,

$$\Pr_{x \in D} \{ h(M(h(x))) = h(x) \} < \epsilon$$
 Here the probability is also taken over the random choices of M .
- 2nd preimage resistance:** let x be selected uniformly in $D = \Sigma^{l(n)}$ and let M' be an adversary who on input x uses time $\leq t$ and outputs $x' \in D$ with $x' \neq x$. For each adversary M' ,

$$\Pr_{x \in D} \{ h(M'(x)) = h(x) \} < \epsilon$$
 Here the probability is taken over the random choices of M' .

7

Formal definitions: collision resistance

A **collision-resistant hash function (CRHF)** H is a function family $\{h_s\}$ with domain $D = \Sigma^{l(n)}$ and range $R = \Sigma^n$ that satisfies the following conditions:

- the functions h_s are preimage resistant and second preimage resistant)
- collision resistance:** let F be a collision string finder that on input $S \in \Sigma^s$ uses time $\leq t$ and outputs either "?" or a pair $x, x' \in \Sigma^{l(n)}$ with $x' \neq x$ such that $h_s(x) = h_s(x')$. For each F ,

$$\Pr_S \{ F(H) \neq "?" \} < \epsilon$$
 Here the probability is also taken over the random choices of F .

8

Formal definitions - continued

- For collision resistance: considering a **family** of hash functions indexed by a parameter ("key") is essential for formalization (but see [Rogaway'06]: "formalizing human ignorance")
- For (2nd) preimage resistance, one can choose the challenge (x) and/or the key that selects the function.
- This gives three flavors [Rogaway-Shrimpton'04]
 - random challenge, random key (Pre and Sec)
 - random key, fixed challenge (ePre and eSec everywhere) (eSec=UOWHF)
 - fixed key, random challenge (aPre and aSec - always)
- Complex relationship (see figure on next slide).

9

Relation between formal definitions

[Rogaway-Shrimpton'04]

Figure 1: Summary of the relationships among seven notions of hash-function security. Solid arrows represent conventional implications, dotted arrows represent provisional implications (their strength depends on the relative size of the domain and range), and the lack of an arrow represents a separation.

10

Applications

- digital signatures: OWHF/CRHF, "destroy algebraic structure"
- information authentication: protect authenticity of hash result
- protection of passwords: preimage resistant
- confirmation of knowledge/commitment: OWHF/CRHF
- pseudo-random string generation/key derivation
- micropayments (e.g., micromint)
- construction of MAC algorithms, stream ciphers, block ciphers
- (redundancy: hash result appended to data before encryption)

Until recently: 800 uses of MD5 in Windows

11

Applications (2)

- Collision resistance is not always necessary
- Other properties are needed:
 - pseudo-randomness if keyed (with secret key)
 - near-collision resistance
 - partial preimage resistance
 - multiplication freeness
 - indifferentiable from random oracle
- how to formalize these requirements and the relation between them?

12

Summary



13

Brute force (2^{nd}) preimage

- If one can attack 2^t simultaneous targets, the effort to find a single preimage is 2^{n-t}
 - note for $t = n/2$ this is $2^{n/2}$
- [Hellman'80] if one has to find (second) preimages for many targets, one can use a time-memory trade-off with $\Theta(2^n)$ precomputation and storage $\Theta(2^{2n/3})$
 - inversion of one message in time $\Theta(2^{2n/3})$
- [Wiener'02] if $\Theta(2^{3n/5})$ targets are attacked, the full cost per (2^{nd}) preimage decreases from $\Theta(2^n)$ to $\Theta(2^{2n/5})$
- answer: randomize hash function
 - salt, spice, "key": parameter to index family of functions

14

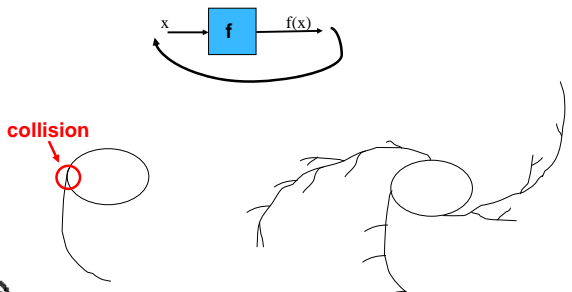
The birthday paradox for collisions

- Given a set with S elements
- Choose r elements at random (with replacements) with $r \ll S$
- The probability p that there are at least 2 equal elements (a collision) is $1 - \exp(-r(r-1)/2S)$
- S large, $r = \sqrt{S}$, $p = 0.39$: finding a collision takes computation and memory \sqrt{S}
 - for birthdays: $S = 365$, $r = 23$, $p = 0.50$

15

Brute force collision search: low memory

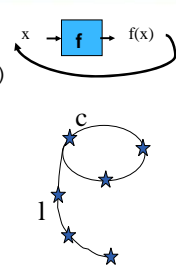
- Consider the functional graph of f



16

Brute force collision search: low memory

- Efficient implementation of the birthday attack [Pollard'78][Quisquater'89]
 - very little memory (cycle finding algorithm)
 - full parallelism [Wiener-van Oorschot'94]
- Distinguished point (d bits)
 - $\Theta(e^{2n/2} + e^{2^{d+1}})$ steps
 - $\Theta(n2^{n/2-d})$ memory
 - with e the cost of one function evaluation
- [Wiener'02] full cost: $\Theta(e n^{2n/2})$



$$l = c = (\pi/8) 2^{n/2}$$

17

Brute force attacks in practice

- (2^{nd}) preimage search
 - $n = 128$: 90 M\$ for 1 year if one can attack 2^{48} targets in parallel
 - $n = 128$: 90 B\$ for 1 year if one can attack 2^{38} targets in parallel
- parallel collision search
 - $n = 128$: 1 M\$ for 12 hours (or 1 year on 60K PCs)
 - $n = 160$: 90 M\$ for 1 year
 - need 256-bit result for long term security (25 years or more)

18

Can we get rid of collision resistance?

- collision resistance
 - requires double output lengths
 - requires family of functions for formalization
 - is hard to achieve (e.g., not by black box reduction from one-wayness)
- UOWHF (TCR, eSec) **randomize** hash function after choosing the message
- [Halevi-Krawczyk'05] randomized hashing = RMX mode:

$$H(r \parallel x_1 \oplus r \parallel x_2 \oplus r \parallel \dots \parallel x_t \oplus r)$$
 - needs e-SPR (not met by MD5 and SHA-1 reduced to 53 steps)
 - issues with **insider attacks** (i.e. attacks by the signer)
 - birthday attack for signatures [Gauravaram-Knudsen+09]

19

Outline

- definitions
- applications
- generic attacks
- attacks on iterated constructions: the rise and fall of MD
- MD4, MD5, SHA-0, SHA-1
- SHA-2
- SHA-3: the NIST AHS competition
- SHA-4
- conclusions

20

Hash function: iterated structure

Split messages into blocks of fixed length and hash them block by block with a compression function f

Efficient and elegant
 But many problems...

21

Security relation between f and h

- Iterating f can degrade its security
 - trivial example: 2nd preimage

22

Security relation between f and h

- Solution: Merkle-Damgård (MD) strengthening (popular!)
 fix IV, use unambiguous padding and insert length at the end
- [MD'89] f is collision resistant \Rightarrow h is collision resistant
- [Lai-Massey'92] f is 2nd preimage resistant \Leftrightarrow h is 2nd preimage resistant ?

23

Construction: relation between f and h (2)

[Damgård-Merkle'89]

Let f be a collision resistant function mapping l to n bits (with $l > n$).

- If the padding contains the length of the input string, and if f is preimage resistant, the iterated hash function h based on f will be a CRHF.
- If an unambiguous padding rule is used, the following construction will yield a CRHF ($l-n > 1$):

$$H_1 = f(H_0 \parallel 0 \parallel x_1)$$

$$H_i = f(H_{i-1} \parallel 1 \parallel x_i) \quad i=2,3,\dots,t.$$

24

Comment: tree structure

already suggested by Damgård in 1989; further work by Sarkar et al.

25

Construction: relation between f and h (3)

[Lai-Massey'92]

Assume that the padding contains the length of the input string, and that the message x (without padding) contains at least two blocks.

Then finding a second preimage for h with a fixed IV requires 2^n operations **iff** finding a second preimage for f with arbitrarily chosen H_{i-1} requires 2^n operations.

- this theorem is not quite right (see below)
- very few hash functions have a strong compression function
- very few hash functions are designed based on a strong compression function in the sense that they treat x_i and H_{i-1} in the same way.

26

Security relation between f and h (4)

- MD with envelope method (prepend and append secret key) works for pseudo-randomness/MAC [BCK'96]
 - but there are some problems and HMAC is a better construction
- MD preserves Preimage Awareness [Dodis-Ristenpart-Shrimpton'09]
- MD needs output transformation for pseudo-random oracle (PRO) property [Coron+05]
 - if one knows $h(x)$, easy to compute $h(x || y)$ without knowing x

- MD does **not** work for UOWHF [Bellare-Rogaway'97]

27

Attacks on MD: 1999-2006

- long message 2^{nd} preimage attack [Dean-Felten-Hu'99], [Kelsey-Schneier'05]
 - if one hashes 2^t message blocks with an iterated hash function, the effort to find a second preimage is only $2^{n+t-1} + t \cdot 2^{n/2+1}$
- multi-collision attack and impact on concatenation [Joux'04]
 - the concatenation of 2 iterated hash functions ($g(x) = h_1(x) || h_2(x)$) is as **most as strong as the strongest** of the two (even if both are independent)
 - cost of collision attack against g at most $n_1 \cdot 2^{n_2/2} + 2^{n_1/2} \ll 2^{(n_1+n_2)/2}$
- herding attack [Kelsey-Kohn'06]
 - reduces security of commitment using a hash function from 2^n
 - on-line $2^{n_1} + \text{precomputation } 2 \cdot 2^{(n_1+t)/2} + \text{storage } 2^t$

28

Improving MD iteration

- degradation with use: salting (family of functions, randomization)
- extension attack + PRO preservation: strong output transformation g (which includes total length and salt)
- long message 2^{nd} preimage: preclude fix points
 - counter $f \rightarrow f_i$ [Biham-Dunkelman] or dithering [Rivest]
- multi-collisions, herding: avoid breakdown at $2^{n/2}$ with larger internal memory: known as wide pipe
 - e.g., extended MD4, RIPEMD, [Lucks'05]

Many concrete proposals in the SHA-3 competition

29

Sponge functions

Examples

- Panama
- RadioGatun
- Keccak

30

Summary

- Growing theory to reduce security properties of hash function to that of compression function (MD) or permutation (sponge)
 - Preservation of large range of properties
 - Relation between properties
- It is very nice to assume multiple properties of the compression function f , but unfortunately it is very hard to verify these
- Still no single comprehensive theory

31

Outline

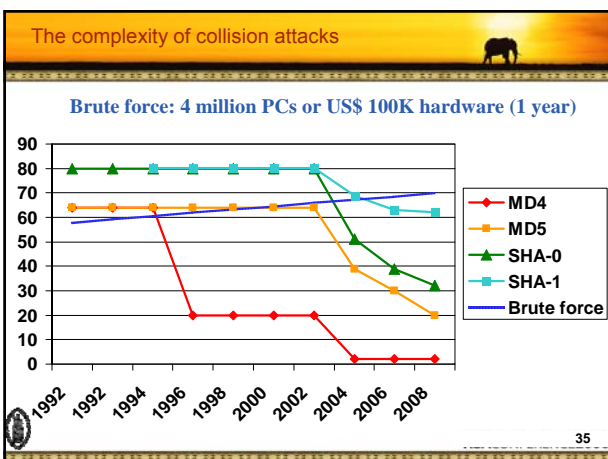
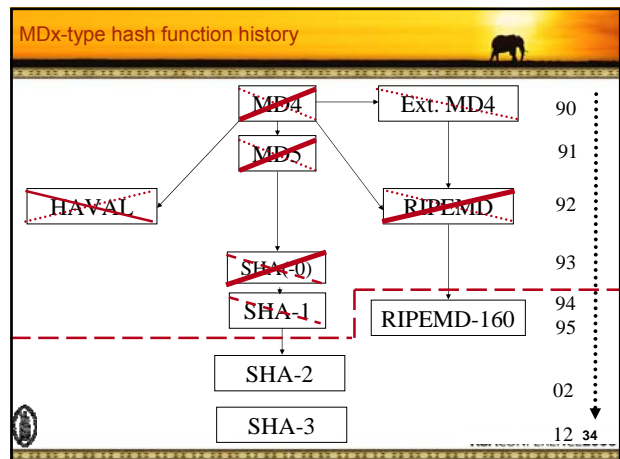
- definitions
- applications
- generic attacks
- attacks on iterated constructions: the rise and fall of MD
- MD4, MD5, SHA-0, SHA-1
- SHA-2
- SHA-3: the NIST AHS competition
- SHA-4
- conclusions

32

Hash function constructions

- block cipher based**
 - well studied but need very strong assumption on block cipher
 - due to key schedule for every encryption at least 3-4 times slower than AES
 - 30 proposals, more than half broken
 - some constructions use codes over $GF(2^8)$
- based on algebraic constructions with security proof**
 - factoring, discrete log, ECC: very slow
 - additive: lattices
 - multiplicative: matrices
- dedicated hash functions**
 - >40 designs until 2008
 - about 30 broken: X.509 Annex D, FFT-hash I,II, N-hash, Snefru, MD2, ...

33



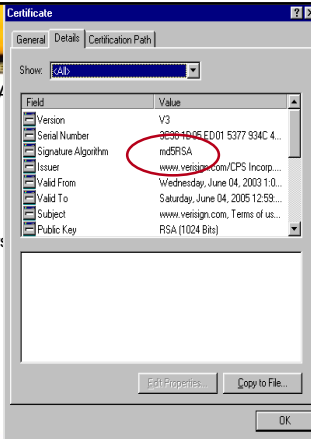
MD4

- designed by Rivest in 1990
- 3 rounds
- collisions for 2 rounds [Merkle'90, denBoerBosselaers'91]
- collisions for full MD4 in 2^{20} steps [Dobbertin'96]
- (second) preimage for 2 rounds [Dobbertin'97]
- collisions for full MD4 **by hand** [Wang+'04]
- practical preimage attack for 1 in 2^{56} messages [Wang+'05]
- abandoned since 1993 (except for HMAC-MD4?)

36

MD5

- Advice (RIPE since '92, RSA since '96): **stop using MD5**
- Largely ignored by industry (click on a cert...)
- Collisions for MD5
 - brute force (2^{64}): 1M\$ 10 hours in '09
 - [Wang+04] collision in 15 minutes on a PC
 - [Stevens+09] collisions in milliseconds
- 2nd preimage:
 - 2^{123} [Asaki-Aoki'09]



SHA(-0)

- SHA designed by NIST (NSA) in '92
 - now called SHA-0, because of '94 of publication SHA-1
- very similar to MD5:
 - 16 extra steps (from 64 to 80)
 - message expansion uses bitwise code rather than repetition

$$W_j \leftarrow (W_{j-3} \oplus W_{j-8} \oplus W_{j-14} \oplus W_{j-16}) \ggg j > 15$$
 - quasicyclic code with $d_{\min} = 23$
- 1994: withdrawn by NIST for unidentified flaw
- 2004: collisions for in 2^{51} [Joux+04]
- 2005: collisions in 2^{39} [Wang+05]
- 2007: collisions in 2^{32} [Joux+07]
- 2008: collisions in 1 hour [Manuel-Peyrin'08]
- 2008: preimages for 49 steps in 2^{159} [DeCannière+08]

SHA-1

- fix after 2 years ('94) to SHA-0
- add rotation to message expansion: quasicyclic code with $d_{\min} = 25$

$$W_j \leftarrow (W_{j-3} \oplus W_{j-8} \oplus W_{j-14} \oplus W_{j-16}) \ggg j > 15$$

collisions

- 53 steps [Oswald-Rijmen'04 and Biham-Chen'04]
- 58 steps [Wang+05]
- 64 steps in 2^{35} – highly structured [De Cannière-Rechberger'06-'07]:
- 70 steps in 2^{44} – highly structured [De Cannière-Rechberger'06-'07]:
- 70 steps 2^{39} (4 days on a PC) [Joux-Peyrin'07]
- 2^{69} [Wang+05]
- 2^{63} ? [Wang+05 - unpublished]
- 2^{62} ? [Mendel+08 - unpublished]
- 2^{52} ?? [McDonald+09 - unpublished]

- preimages for 49/80 steps in 2^{157} [DeCannière-Rechberger'08]

Prediction: collision for SHA-1 in the next 12-18 months

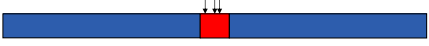


NIST's Policy on Hash Functions

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.

Impact of collisions (1)

- collisions for MD5, SHA-0, SHA-1
 - 2 messages differ in a few bits in 1 to 3 512-bit input blocks
 - limited control over message bits in these blocks
 - but arbitrary choice of bits before and after them



- what is achievable for MD5?
 - 2 colliding executables/postscript/gif/... [Luks-Daum'05]
 - 2 colliding RSA public keys – thus with colliding X.509 certificates [Lenstra+04]
 - chosen prefix attack: different IDs, same certificate [Stevens+07]
 - 2 arbitrary colliding files (no constraints) in 12 hours for 1 M\$

Impact of collisions (2)

- [Sotirov-Stevens-Appelbaum,-Lenstra-Molnar-Osvik-de Weger '08] MD5 considered harmful today
 - fake CA certificate.
 - results in a rogue CA: its certificates are trusted by all common browsers
 - need to predict serial number + validity period
- 6 CAs have issued certificates signed with MD5 in 2008:
 - Rapid SSL, Free SSL (free trial certificates offered by RapidSSL), TC TrustCenter AG, RSA Data Security, Verisign.co.jp

Impact of collisions (3)

- digital signatures: only an issue if for **non-repudiation**
- none** for signatures computed before attacks were public (1 August 2004)
- ~~**none** for certificates if public keys are generated at random in a controlled environment~~
- substantial** for signatures after 1 August 2005 (cf. traffic tickets in Australia)

43

And (2nd) preimages?

- security degrades with number of applications
- for large messages even with the number of blocks (cf. supra)
- specific results:
 - MD2: 2^{73} [Knudsen+09]
 - MD4: 2^{102} [Leurent'08]
 - MD5: 2^{123} [Asaki-Aoki'09]
 - SHA-0: 49 of 80 steps in 2^{159} [De Cannière-Rechberger'08]
 - SHA-1: 44 of 80 steps in 2^{157} [De Cannière-Rechberger'08]

44

HMAC

- HMAC keys through the IV (plaintext) [Kim+'06]
 - collisions for MD5 invalidate current security proof of HMAC-MD5
 - new attacks on reduced version of HMAC-MD5 and HMAC-SHA-1

	Rounds in f2	Rounds in f1	Data complexity
Haval-4	128	102 of 128	2^{254} CP
MD4	48	48	2^{72} CP + 2^{77} time
MD5	64	33 of 64	$2^{126.1}$ CP
MD5	64	64	2^{51} CP & 2^{100} time (RK)
SHA-0	80	80	2^{109} CP
SHA-1	80	53 of 80	$2^{98.5}$ CP

no problem yet for most widely used schemes

45

Fixes/Alternatives

- RIPEMD-160 seems more secure than SHA-1 ☺
- message precoding for SHA-1
- small patches to SHA-1

46

SHA-2 [01]

- SHA-224, SHA-256, SHA-384, SHA-512
 - non-linear message expansion
 - more complex operations
 - 64/80 steps
 - SHA-384 and SHA-512: 64-bit architectures
- collisions: 24 steps [Sanadhya-Sarkar'08]
- adoption
 - in spite of pedigree and analysis, industry migrates in the next 2-3 years to SHA-2
 - very slow for TLS/IPsec (no pressing need)
- alternative: Whirlpool (AES-based), in ISO standard
 - but attack at Asiacrypt 2009

47

Performance of hash functions - Bernstein (cycles/byte) AMD Intel Pentium D 2992 MHz (f64)

Function	Performance (cycles/byte)
MD4	~3
MD5	~5
SHA-1	~11
RMD-160	~16
SHA-256	~21
SHA-512	~31
Whirlp.	~41
AES-BC	~30
AES	~10

48

Outline

- definitions
- applications
- generic attacks
- attacks on iterated constructions: the rise and fall of MD
- MD4, MD5, SHA-0, SHA-1
- SHA-2
- SHA-3: the NIST AHS competition
- SHA-4
- conclusions

49

NIST AHS competition (SHA-3)

- SHA-3 must support 224, 256, 384, and 512-bit message digests, and must support a maximum message length of at least 2^{64} bits

Round	Number of Candidates	Deadline
Round 1	64	31/10/08
Round 2	51	9/12/08
Round 2	14	24/7/09
Round 2	5	-
Final	1	-

Standard: 2012

50

The Candidates

Slide credit: Christophe De Cannière

51

The Candidates

31/10/2008

Slide credit: Christophe De Cannière

52

Preliminary Cryptanalysis

16/06/2009

Slide credit: Christophe De Cannière

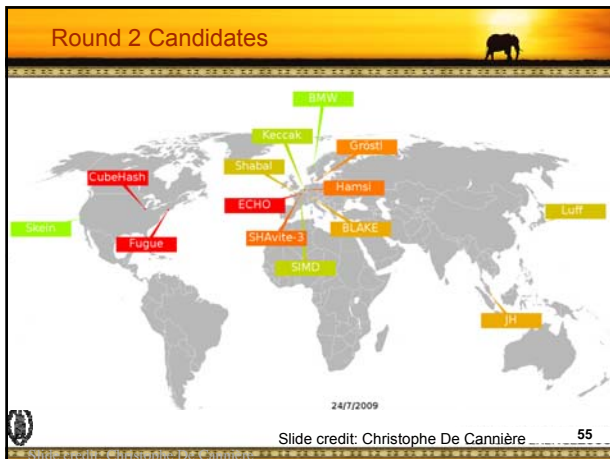
53

End of Round 1 Candidates

8/7/2009

Slide credit: Christophe De Cannière

54



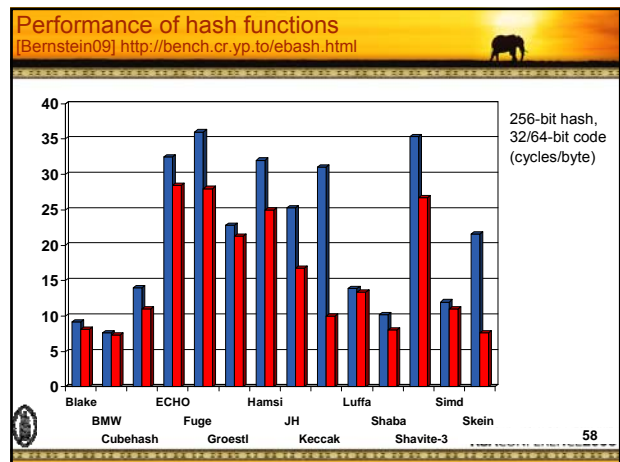
- ### Issues arisen during Round 1
- Security:
 - controversy around pseudo-collision attacks and memory requirements
 - proofs have not helped much to survive
 - Performance: roughly as fast or faster than SHA-2
 - tunable security/performance tradeoff: nominal parameters?
 - large memory (> 100 bytes) may be a problem for small devices
 - can we exploit 64 or 128 cores? Intel AES instruction?
 - 14 Round 2 candidates
 - Most are wide-pipe designs or sponge-like designs
 - Two main types: AES-based and AXR (addition/xor/rotate)
- 56

Security: SHA-3 Zoo

http://ehash.iak.tugraz.at/wiki/The_SHA-3_Zoo

Hash Name	Principal Submitter	Best Attack on Main	Best Attack on other
SHAKE	Jean-Philippe Aumasson	Best	Best
Blue Shabal Hash	Stavroullos Gouveias	Best	Best
CubeHash	Daniel J Bernstein	Best	Best
ECHO	Stavroullos Gouveias	Best	Best
Fugue	Changhae S. Jaffe	Best	Best
Groestl	Lars R. Knudsen	Best	Best
Hamsi	Dogan Husein	Best	Best

57



- ### SWIFFTX
- [Arbitman-Dogon-Lyubashevsky-Micciancio-Peikert-Rosen'08]
- compression function:
 - SWIFFT: FFT-like operation from $(\mathbb{Z}_2^{32})^{64}$ to \mathbb{Z}_{257}^{64}
 - sandwich: 3xSWIFFT - S-boxes - 1xSWIFFT
 - asymptotic proof of security: "it can be formally proved that finding a collision in a randomly-chosen compression function from the SWIFFTX family is at least as hard as finding short vectors in cyclic/ideal lattices over the ring $\mathbb{Z}[\alpha]/(\alpha^n+1)$ is in the worst case."
 - note: SWIFFT mapping is linear and some heuristics are needed to "kill" the linearity
 - speed: 57 cpb
- 59

- ### FSB [Augot-Finiasz-Gaborit-Manuel-Sendrier'08]
- compression function: multiplication of vector of Hamming weight w with a truncated quasi-cyclic binary matrix
 - can be interpreted as a syndrome computation of an error pattern with weight w
 - MD iteration with Whirlpool as output transformation
 - security can be reduced to:
 - (Computational Syndrome Decoding) Given a binary $r \times n$ matrix H , a word $s \in \{0,1\}^r$ and an integer $w > 0$, find a word $e \in \{0,1\}^n$ of Hamming weight $\leq w$ such that $eH^T = s$.
 - (Codeword Finding) Given a binary $r \times n$ matrix H and an integer $w > 0$, and a non-zero word $e \in \{0,1\}^n$ of Hamming weight $\leq w$ with an all zero H -syndrome.
 - 324 cpb (can be optimized)
- 60

SHA-4

- an open competition such as SHA-3 is bound to result in new insights between 2009-2012
- only few of these can be incorporated using "tweaks"
- the winner selected in 2012 will reflect the state of the art in October 2008
- nevertheless, it is unlikely that we will have a SHA-4 competition before 2030
- maybe everyone will use SHA-2 in 2020?
- for which applications will security proofs be relevant?

61

ZesT: a SHA-4 candidate?

- [Zémor-Tillich'04]: consider 2 generators of the group $SL(2; F_{2^n})$
$$A_0 = \begin{pmatrix} x & 1 \\ 1 & 0 \end{pmatrix} \quad A_1 = \begin{pmatrix} x & x+1 \\ 1 & 1 \end{pmatrix}$$

the hash value of a string x with elements $x[i]$ is $\prod_{i=1}^n A_{x[i]}$
- ZesT = vectorial version of the Zémor-Tillich function iterated $2x$
- security: ZesT is collision resistant if and only if the balance problem is hard and in particular if the representation problem is hard for the group $SL(2; F_{2^n})$ and the generators A_0 and A_1
- performance: 10-20 times slower than SHA-512 but parallelism

More details: PhD thesis of Christophe Petit, UCL, May 2009

Original ZT scheme recently broken
see IACR eprint [Grassl-Ilic-Magliveras-Steinwandt'09]

62

Hash functions: conclusions

- SHA-1 would have needed 128-160 steps instead of 80
- recent attacks are not dramatic for all applications, but they form a clear warning: upgrade asap
- theory is developing for more robust iteration modes and extra features; still early for building blocks
- use weaker security assumptions if possible (UOWHF?)
- Nirwana: efficient hash functions with security reduction

63

The end

Thank you for your attention



64

Hash³: Proofs, Analysis, and Implementation


ECRYPT II

<http://www.ecrypt.eu.org>

ECRYPT II Event
on Hash
Functions

November 16-20,
Tenerife, Spain

Registration opens
this week



65

Hash functions: further reading

- NIST <http://csrc.nist.gov/groups/ST/hash/index.html>
 - first SHA-3 candidate conference: February 25-28, 2009, Leuven
 - workshop October 31-November 1, 2005 and August 24-25, 2006
- ECRYPT: <http://www.ecrypt.eu.org>
 - SHA-3 Zoo http://ehash.iaik.tugraz.at/wiki/The_SHA-3_Zoo
 - workshops in May 2007 and June 2005 + statement on hash functions
- The IACR eprint server <http://eprint.iacr.org>
- My 1993 PhD thesis <http://homes.esat.kuleuven.be/~preneel>
- Overview paper from 1998 (LNCS 1528)
<http://www.cosic.esat.kuleuven.be/publications/article-246.pdf>

66