MegoSAT project

Differential cryptanalysis with SAT solvers

Today: “master thesis presentation”

Lukas Prokop
Advisors: Florian Mendel, Maria Eichlseder
Institute of Applied Information Processing and Communications

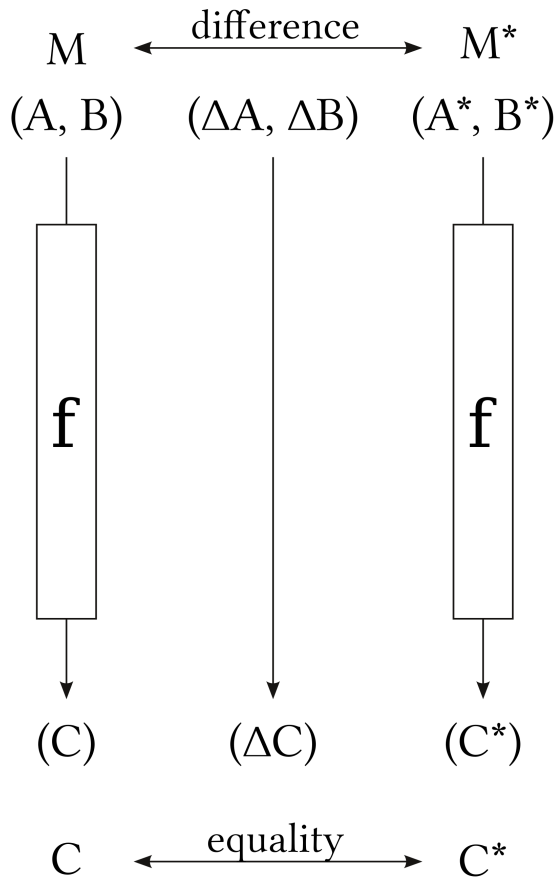
Goal

- Find hash collisions . . .
- for MD4 and SHA-256 . . .
- using SAT solvers

Outline

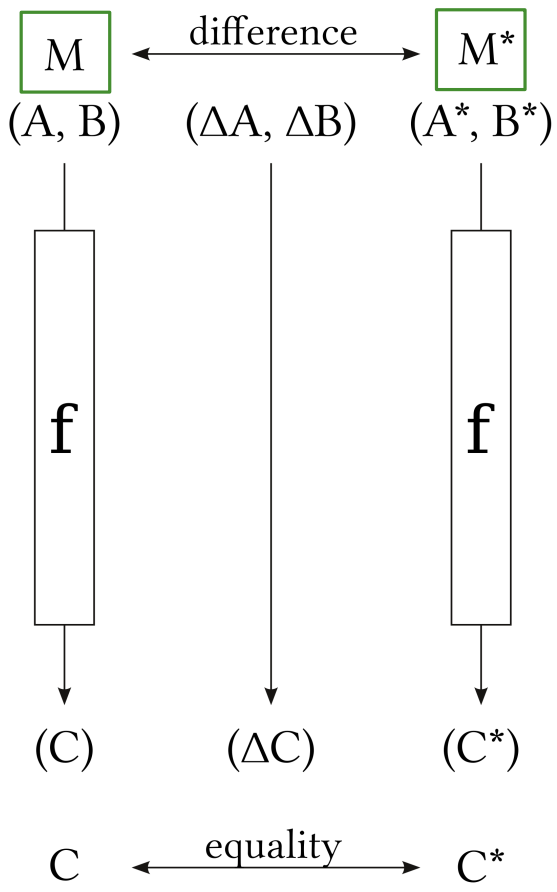
- Differential cryptanalysis
- SHA-256 and MD4
- Satisfiability
- SAT features
- Example hash collision (Wang et al.)
- MD4 testcases & results
- SHA-256 testcases & results

Differential cryptanalysis



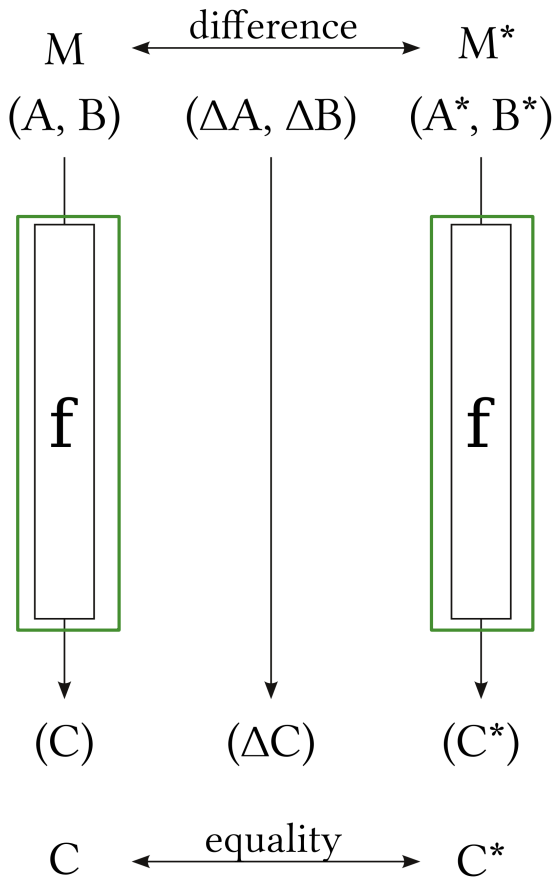
Differential cryptanalysis

We use two slightly different input messages

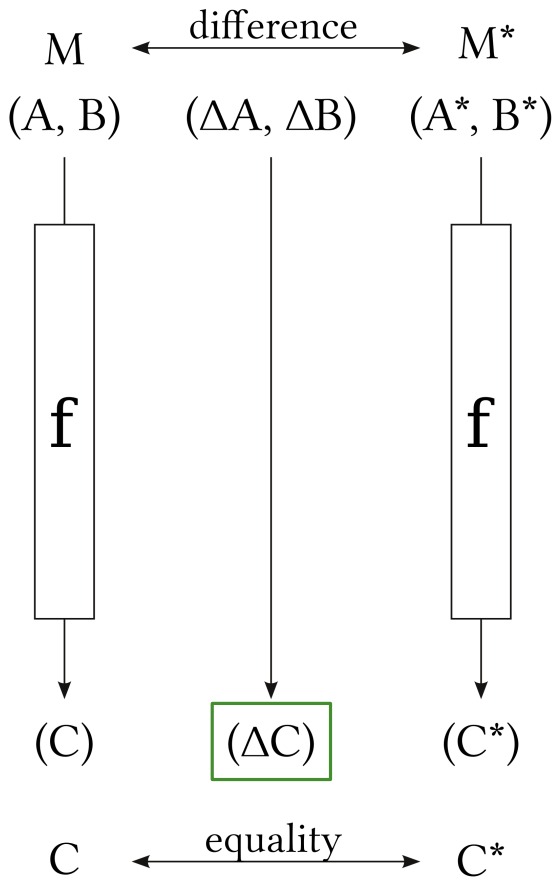


Differential cryptanalysis

We apply the cryptographic algorithm to both instances

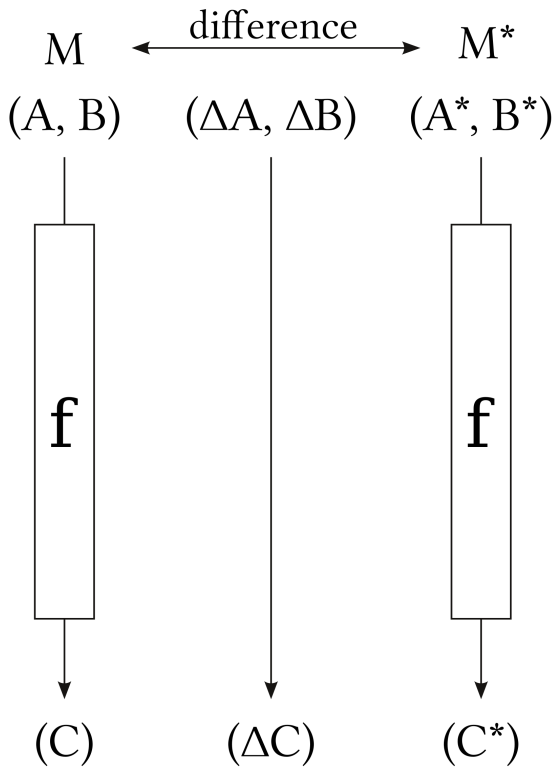


Differential cryptanalysis



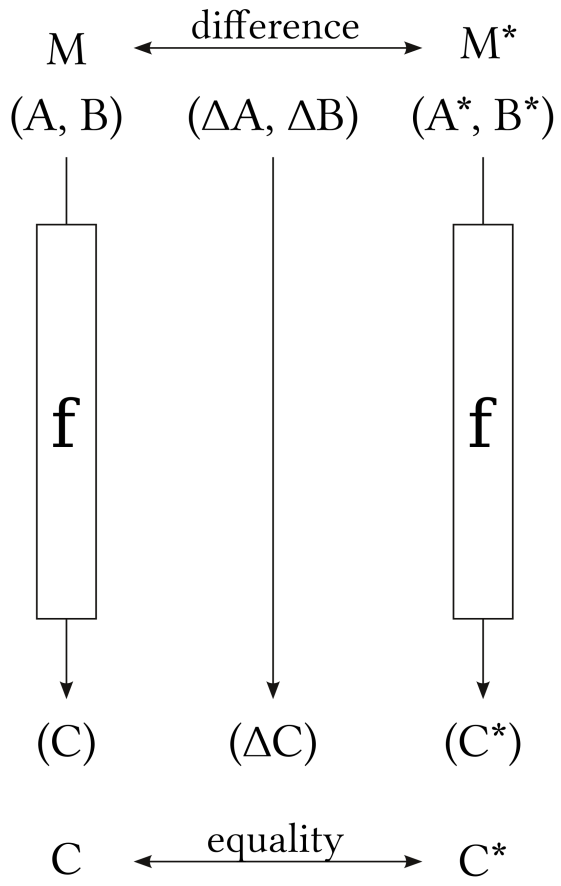
Differences cancel out

Differential cryptanalysis



Equality is given

Differential cryptanalysis



A *hash collision* is a pair (x_1, x_2) such that $x_1 \neq x_2$ with $f(x_1) = f(x_2)$.

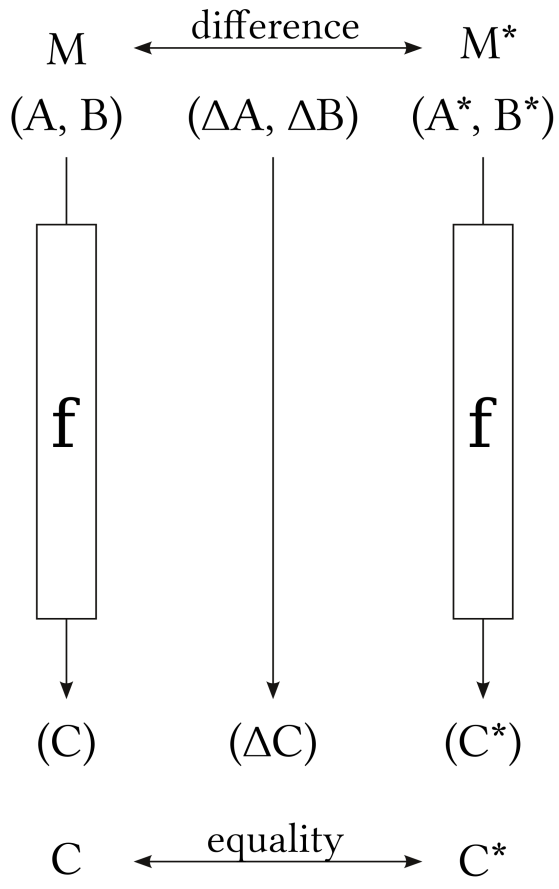
Differential cryptanalysis

We use two slightly different input messages

We apply the cryptographic algorithm to both instances

Differences cancel out

Equality is given



A *hash collision* is a pair (x_1, x_2) such that $x_1 \neq x_2$ with $f(x_1) = f(x_2)$.

Differential cryptanalysis focuses on the behavior of differences when f is progressing.

Differential cryptanalysis

Wang et al. defined signed differences.
De Cannière and Rechberger [**01**] defined *generalized bit conditions*.

(x_i, x_i^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
?	✓	✓	✓	✓
-	✓			✓
x		✓	✓	
0	✓			
u		✓		
n			✓	
1				✓
#				

(x_i, x_i^*)	$(0,0)$	$(1,0)$	$(0,1)$	$(1,1)$
3	✓	✓		
5	✓		✓	
7	✓	✓	✓	
A		✓		✓
B	✓	✓		✓
C			✓	✓
D	✓		✓	✓
E		✓	✓	✓

Differential cryptanalysis

addition $A + B = S$

A: `0100`

B: `1x-1`

S: `??-1`

Differential cryptanalysis

addition $A + B = S$

A: 0100
B: 1x-1
S: ??-1

$\Rightarrow$

A:	0100	0100	0100	0100	
B:	1001	1011	1101	1001	...
S:	1101	1111	0001	1111	
A:	0100	0100	0100	0100	
B:	1101	1111	1001	1101	...
S:	0001	0011	1101	1011	

Differential cryptanalysis

addition $A + B = S$

A: 0100
B: 1x-1
S: ??-1

$\Rightarrow$

A:	0100	0100	0100	0100	
B:	1001	1011	1101	1001	...
S:	1101	1111	0001	1111	
A:	0100	0100	0100	0100	
B:	1101	1111	1001	1101	...
S:	0001	0011	1101	1011	

Differential cryptanalysis

addition $A + B = S$

A: 0100
B: 1x-1
S: ?x-1

$\Leftarrow$

A:	0100	0100	0100	0100	
B:	1001	1011	1101	1001	...
S:	1101	1111	0001	1111	
A:	0100	0100	0100	0100	
B:	1101	1111	1001	1101	...
S:	0001	0011	1101	1011	

Differential cryptanalysis

addition $A + B = S$

A: 0100
B: 1x-1
S: ?x-1

$\Leftarrow$

A:	0100	0100	0100	0100	
B:	1001	1011	1101	1001	...
S:	1101	1111	0001	1111	
A:	0100	0100	0100	0100	
B:	1101	1111	1001	1101	...
S:	0001	0011	1101	1011	

Valid 4-bit addition differential characteristics:

A:	0011	A:	---x	A:	---x	A:	---x
B:	0101	B:	---x	B:	---x	B:	---x
S:	1000	S:	????	S:	???-	S:	x???

Invalid 4-bit addition differential characteristics:

A:	0011	A:	---x	A:	----
B:	0101	B:	---x	B:	---x
S:	0000	S:	???x	S:	x-??

Differential cryptanalysis

We have constraints due to

- bit conditions (differential characteristic).
- the operation applied.

Our f is MD4 or SHA-256

MD4:

- Ronald Rivest, 1990
- RFC 1320
- broken since 1995
- 128 bits internal state size

Our f is MD4 or SHA-256

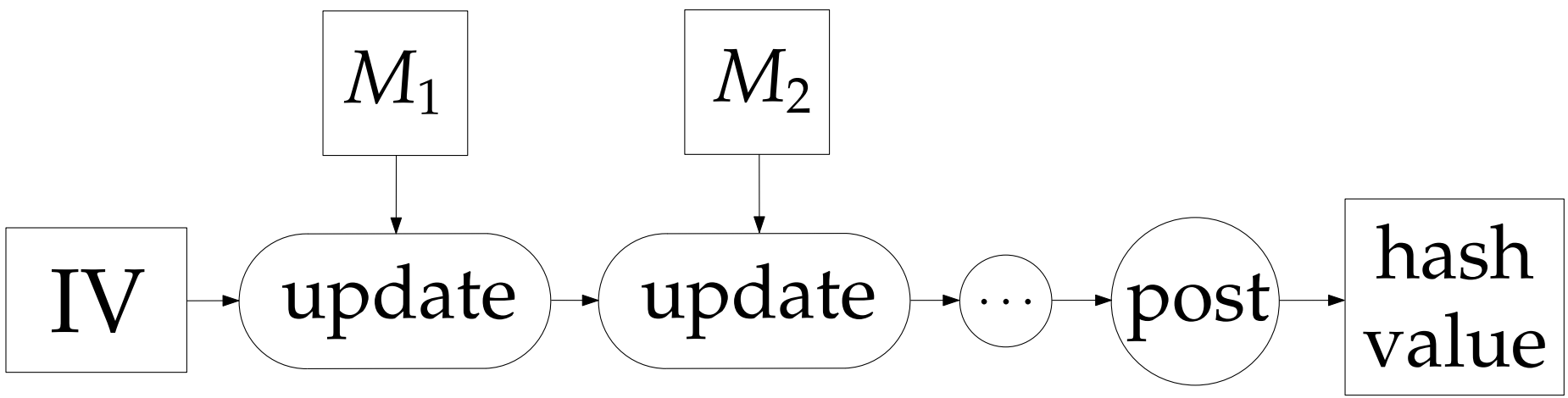
SHA-256:

- NSA, 2001
- NIST publication 180-4
- best practical pseudo-collision attack breaks 38 rounds [**02**]
- 256 bits internal state size

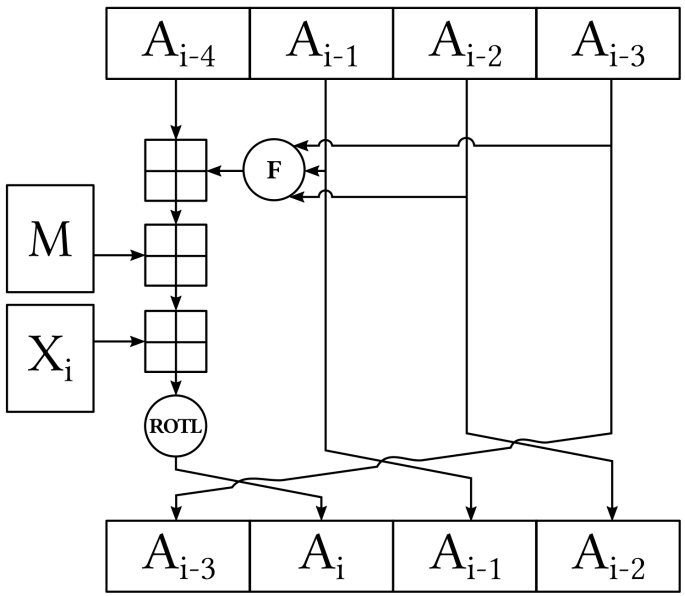
Our f is MD4 or SHA-256

Merkle-Damgård constructions:

MD4: 48 steps
SHA-256: 64 steps

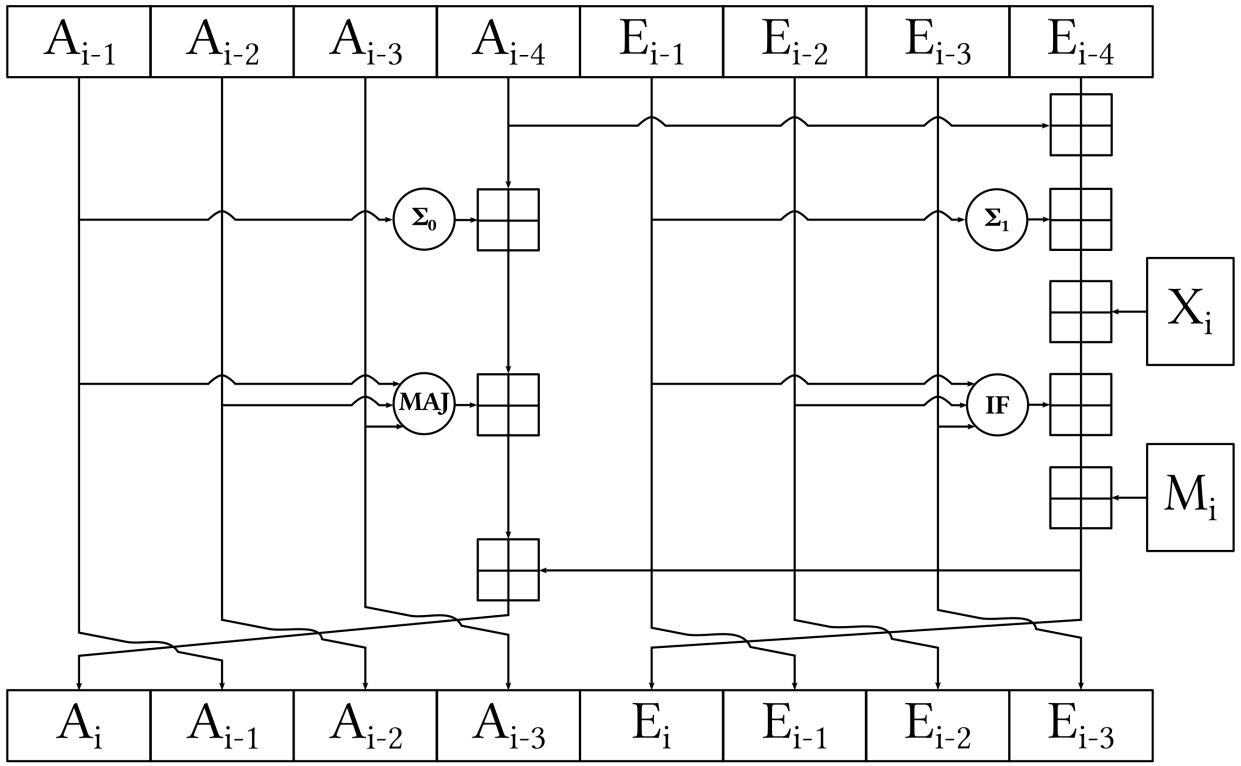


Our f is MD4 or SHA-256



MD4 update function

Our f is MD4 or SHA-256



SHA-256 update function

And now

for something completely different

Satisfiability

- A Boolean function is a mapping $h : X \rightarrow Y$ with $X = \{0,1\}^n$ for $n \in \mathbb{N}_{\geq 1}$ and $Y = \{0,1\}$.
- *AND* maps $X = \{0,1\}^2$ to 1 iff $X = (1,1)$.

x_1	x_2	$f(x_1, x_2)$
1	1	1
1	0	0
0	1	0
0	0	0

Satisfiability

A Boolean function f is *satisfiable* iff there exists some assignment m such that $f(m) = 1$.

$$f(x_1, x_2) = (x_1 \vee \neg x_2) \wedge (\neg x_1)$$

f is satisfiable because $m = (0, 0)$ evaluates to 1.

A *SAT solver* is a tool to evaluate whether a certain Boolean function is satisfiable or not.

Satisfiability

$f(x_1, x_2) =$
$(x_1 \vee \neg x_2) \wedge$
$(\neg x_1)$

```
p cnf 2 2
1 -2 0
-1 0
```

```
c Lingeling SAT Solver
c
s SATISFIABLE
v -1 -2 0
c
c 0 decisions, 0.0 decisions/sec
c 0 conflicts, 0.0 conflicts/sec
c 2 propagations, 0.0 megaprops/sec
c 0.0 seconds, 0.0 MB
```

$m = (0, 0)$

Satisfiability

Our strategy: We write a boolean equation system such that the formula is satisfiable iff all constraints of bit conditions and the operation can be satisfied.

Satisfiability

What is an average problem solved by a SAT solver?

Satisfiability

What is an average problem solved by a SAT solver?

Approach: Get a large data set and compute the mean.

www.satcompetition.org

The international SAT Competitions web page

SAT 2016 competition

Organizers	Marijn Heule, Matti Järvisalo Tomáš Balyo
Proceedings	Descriptions of the solvers and benchmarks
Benchmarks	Available here
Solvers	Available here

	Gold	Silver	Bronze	Gold	Silver	Bronze	Gold	Silver	Bronze
	Agile Track			Main Track			Random Track		
SAT+UNSAT	Riss	TB_Glucose	CHBR_Glucose	MapleCOMSPS	Riss	Lingeling	Dimetheus	CSCCSat	DCCAlm
	Parallel Track			No-Limit Track			Incremental Library Track		

Satisfiability

SATlib 53,225 CNF files, 26 GB

Satisfiability

SATlib	53,225 CNF files, 26 GB
SAT competition 2016	5,849 CNF files, 38 GB

Satisfiability

SATlib 53,225 CNF files, 26 GB

SAT competition 2016 5,849 CNF files, 38 GB

SAT competition 2008–2016 + SATlib

Satisfiability

SATlib 53,225 CNF files, 26 GB

SAT competition 2016 5,849 CNF files, 38 GB

SAT competition 2008–2016 + SATlib

68,069 CNF files, 188 GB

⇒ https://github.com/prokls/cnf-files-download

⇒ https://github.com/prokls/cnf-analysis-py
https://github.com/prokls/cnf-analysis-go
https://github.com/prokls/cnf-analysis-tests

Satisfiability

Normalization problem:

```
p cnf 2 2
1 -2 0
-1 0
```

```
c this file was submitted by ...
c for SAT race ...
p cnf 2 2
1 -2 0
-1 0
%
0
```

Satisfiability

Normalization problem:

```
p cnf 2 2
1 -2 0
-1 0
```

=

```
c this file was submitted by ...
c for SAT race ...
p cnf 2 2
1 -2 0
-1 0
%
0
```

⇒ hash algorithm on normalized input

⇒ https://github.com/prokls/cnf-hash-py
https://github.com/prokls/cnf-hash-go
https://github.com/prokls/cnf-hash-tests2

Satisfiability

Normalization problem:

```
p cnf 2 2
1 -2 0
-1 0
```

=

```
c this file was submitted by ...
c for SAT race ...
p cnf 2 2
1 -2 0
-1 0
%
0
```

⇒ hash algorithm on normalized input

⇒ https://github.com/prokls/cnf-hash-py
https://github.com/prokls/cnf-hash-go
https://github.com/prokls/cnf-hash-tests2

⇒ 62251 unique CNF files, 160 GB

SAT features

nbvars No. of variables acc. to CNF header

true_trivial
is the CNF satisfied if all variables are set to true?

connected_variable_components_count
number of components where variables are in the same component if they occur in a clause together

SAT features

MD5 sum:

cnfhash: cnf2$c9151ac8b29bdd9f2873edccd9a2aa2c0120e2fe

e.g. cnf2$c9151ac8b29bdd9f2873edccd9a2aa2c0120e2fe

Lookup

Yay! SAT features file found and loaded.


```
▼ object {8}
    @version : 1.0.0
    @timestamp : 2016-08-14T20:34:40.174717242
    @cnfhash : cnf2$c9151ac8b29bdd9f2873edccd9a2aa2c0120e2fe
  ▼ featuring {90}
      literals_frequency_20_to_25 : 0
      variables_frequency_75_to_80 : 0
      existential_literals_count : 0
      positive_literals_in_clause_largest : 8
```

SAT features

Results:

- There is no distinctive property of our testcases.
- But data indicates that values are strongly intermingled (high diffusion)
- Problem size (number of clauses & variables) is rather large; no indicator of hardness of problem

Example hash collision

Recall . . .

- how bit conditions propagated
- how MD4 and SHA-256 worked

Example hash collision

Wang, Lai, Feng, Chen, Yu

"Cryptanalysis of the Hash Functions MD4 and RIPEMD"

EUROCRYPT 2005

i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000001		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001001		
0	A:	0 11010 1111 01010 01110 01000 00100 10	W:	01001101011110101001110010000011
1	A:	0 11101 1001 00111 11110 11100 u110001	W:	u10 1011 0110 0101 1100 1001 0011 11010
2	A:	1 01010 1101 00000 00111 0u01n 1110010	W:	n01 n10 0111 0101 1010 0101 0101 11000
3	A:	1 01011 u100 11110 10101 00100 1010001	W:	010 1011 1101 0011 1101 0010 1111 01110
4	A:	0 01011 0001 10001 10101 01011 1110010	W:	110 1111 0011 1101 0010 0010 1000 11100
5	A:	0 00110 1001 10001 010u1 1010 0000001	W:	110 1110 0110 0011 0110 0101 0100 11
6	A:	0 00110 1100 unuu1 1000 1000 0001 1110 10	W:	101 1011 0100 0011 1010 0000 0100 00000
7	A:	0 01010 1110 0000 010nnn 0110 0101 0000	W:	001 1101 1001 0100 1011 0110 0111 11111
8	A:	0 11100 1100 1000 1u111 1111 0110 000	W:	110 0011 0100 1110 1011 0011 0110 10011
9	A:	1 01011 n01u nnnn 0001 1111 1001 1001 11	W:	111 1100 1111 0100 1100 1001 1001 11000
10	A:	1 0n001 0010 0001 0 1010 0000 1 0101 10	W:	110 1011 1100 1111 1000 0000 1001 11110
11	A:	u 1000 1 1010 1101 1 0010 0101 1111 11	W:	101 0011 0001 1011 1011 0110 0101 1 01000
12	A:	0 01011 u00u 1010 1 1111 1100 0111 011	W:	010 0010 1110 1 110n 1 0001 1 0001 1 0001
13	A:	1 0nn1n 0100 1100 0 1010 0001 1 1001 01	W:	100 1011 1111 0011 0011 1111 1111 00101
14	A:	0 00010 1001 0100 0 1100 0 1000 1 0101 10	W:	001 0011 1100 1010 0101 1111 1100 0 1000
15	A:	0 00111 1010 101u 0 1011 0011 0101 0100	W:	101 1100 1111 0 1000 1 0000 1 1111 0 1001
16	A:	n 00n0u n011 0100 1 0100 1 0110 1011 11		
17	A:	0 00111 1100 1110 1 0001 0 0100 0011 10		
18	A:	0 10101 1100 0011 0 1000 0 0001 0 0101 00		
19	A:	u 1n100 0000 0101 1 1001 1 0101 1 0001 00		
20	A:	n 1un1 0011 1111 0 1101 0 0000 0 1101 00		
21	A:	1 11100 1110 1100 0 0101 1 1111 1 0101 00		
22	A:	0 10111 0111 0011 0 1001 1 0011 0 1110 10		
23	A:	0 10100 0011 1011 1 0110 0 1111 0 0011 11		
24	A:	0 00000 1000 1001 0 0011 1 0111 0 0110 10		
25	A:	1 01100 0010 1011 0 0001 0 1001 1 1010 10		
26	A:	0 00010 1010 0100 1 0111 1 0110 1 0000 01		
27	A:	0 00001 1011 1011 1 0101 1 0101 0 1100 11		
28	A:	1 01101 1001 0111 0 1011 0 1100 0 1001 01		
29	A:	1 01000 1000 0011 0 1010 0 1000 1 1010 01		
30	A:	0 01010 0111 1011 1 1100 1 1110 1 1000 11		
31	A:	1 11111 0010 0100 1 0110 1 0111 1 0110 10		
32	A:	0 10011 1111 0100 1 0011 0 1000 0 1011 11		
33	A:	0 01110 0000 1111 0 1011 0 1110 1 1001 00		
34	A:	0 01000 0001 1101 0 1111 0 1000 0 0101 01		
35	A:	n 01000 0000 1100 1 0000 1 0001 1 1100 10		
36	A:	n 00001 1111 1010 1 1101 1 1100 1 0110 01		
37	A:	1 10010 0000 0110 1 0010 0 0110 0 0011 00		
38	A:	1 01100 0001 1001 1 1110 1 0011 1 0101 00		
39	A:	0 00100 1000 0010 1 0001 1 0110 0 0111 00		
40	A:	1 10000 0001 0010 0 0111 0 0011 0 0001 01		
41	A:	0 00001 1010 0001 1 0111 1 0101 0 1001 10		
42	A:	0 10011 1011 0111 0 1111 1 1101 0 0001 10		
43	A:	0 10100 0001 1000 1 1101 0 0000 1 1011 01		
44	A:	1 11110 0000 0101 1 0111 1 0111 0 0011 00		
45	A:	1 00010 1011 0110 1 0010 1 1000 0 0001 00		
46	A:	1 00000 1010 0110 0 1010 1 0001 1 0111 00		
47	A:	1 00000 0111 1001 0 1101 1 0100 1 0111 01		

Example hash collision

i		A		W
−4	A:	0 11001 1101 00010 10010 0011 0000000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001001		
0	A:	0 11010 1111 01010 01110 01000 00100 10	W:	010 0110 10111 10101 00111 00100 00011
1	A:	0 11101 1001 00111 11110 11100 u110001	W:	u10 1011 01100 10111 00100 10011 11010
2	A:	1 01010 1101 00000 00111 0n01n 11100 10	W:	n01 n100 11101 01011 01001 01011 11000
3	A:	1 01011 u100 11110 10101 00100 1010001	W:	010 1011 11010 01111 01001 01111 01110
4	A:	0 01011 0001 10001 10101 01011 11100 10	W:	110 1111 00111 01001 00010 10001 11100
5	A:	0 00110 1001 10001 010u1 10100 000000 01	W:	110 1110 01100 00110 11001 10101 10011
6	A:	0 00110 1100 uuuu1 10001 00000 11110 10	W:	101 1011 01000 00111 01000 00001 00000
7	A:	0 01010 1110 00000 10nnn 01100 1010000	W:	001 1101 10010 10100 10111 01100 11111
8	A:	0 11100 1100 10001 u1111 11111 0110000	W:	110 0011 01001 11010 11100 01101 10011
9	A:	1 01011 n01u nnnu0001111 10011 00111 11	W:	111 1100 11110 10011 00100 01100 11000
10	A:	1 0n001 0010 00010 10100 00001 01011 10	W:	110 1011 11001 11111 00000 00010 11110
11	A:	u 10001 1010 11011 00100 10101 11111 11	W:	101 0011 00011 10111 01100 10111 01000
12	A:	0 01011 u00u 10101 11111 11000 11110 11	W:	010 0010 11101 110n1 00011 10001 10001
13	A:	1 0nn1n 0100 11000 10100 00011 1100101	W:	100 1011 11110 00110 00111 11111 00101
14	A:	0 00010 1001 01000 11000 10001 10101 10	W:	001 0011 11001 01001 01111 11000 01000
15	A:	0 00111 1010 101u0 10110 01101 10101 00	W:	101 1100 11110 10001 10000 11111 01001
16	A:	n 00n0u n011 01001 01001 10110 10111 11		
17	A:	0 00111 1100 11101 00001 00100 00111 10		
18	A:	0 10101 1100 00110 10000 00001 00101 00		
19	A:	u 1n100 0000 01011 11001 10101 10001 00		
20	A:	n 1un10 0111 11110 11101 00000 01101 00		
21	A:	1 11100 1110 11000 00101 11111 10101 00		
22	A:	0 10111 0111 00110 10011 00110 01110 10		
23	A:	0 10100 0011 10111 01100 01111 00011 11		
24	A:	0 00000 1000 01001 00011 01110 00110 10		
25	A:	1 01100 0010 01011 00001 01001 11010 10		
26	A:	0 00010 1010 00100 10111 01110 1000001		
27	A:	0 00001 1011 10111 10101 10101 01100 11		
28	A:	1 01101 1001 01110 10110 11000 0100101		
29	A:	1 01000 1000 00110 10100 10000 1101001		
30	A:	0 01010 0111 01011 11100 01110 11000 11		
31	A:	1 11111 0010 01001 01101 01111 01101 10		
32	A:	0 10011 1111 01001 00110 10000 01011 11		
33	A:	0 01110 0000 11110 10110 11101 11001 00		
34	A:	0 01000 0001 11010 11110 10000 0010101		
35	A:	n 01000 0000 11001 10000 01000 11100 10		
36	A:	n 00001 1111 10101 11101 11100 1011001		
37	A:	1 10010 0000 01101 00100 00110 00011 00		
38	A:	1 01100 0001 10011 11110 10011 01011 00		
39	A:	0 00100 1000 00101 00001 10110 00111 00		
40	A:	1 10000 0001 00100 00111 00011 0000101		
41	A:	0 00001 1010 00011 01111 01010 01001 10		
42	A:	0 10011 1011 01110 11111 11101 00001 10		
43	A:	0 10100 0001 10001 11101 00000 1101101		
44	A:	1 11110 0000 01011 01111 01110 00011 00		
45	A:	1 00010 1011 01101 10010 11000 00001 00		
46	A:	1 00000 1010 01100 10101 10001 10111 00		
47	A:	1 00000 0111 10010 11011 01001 0111101		

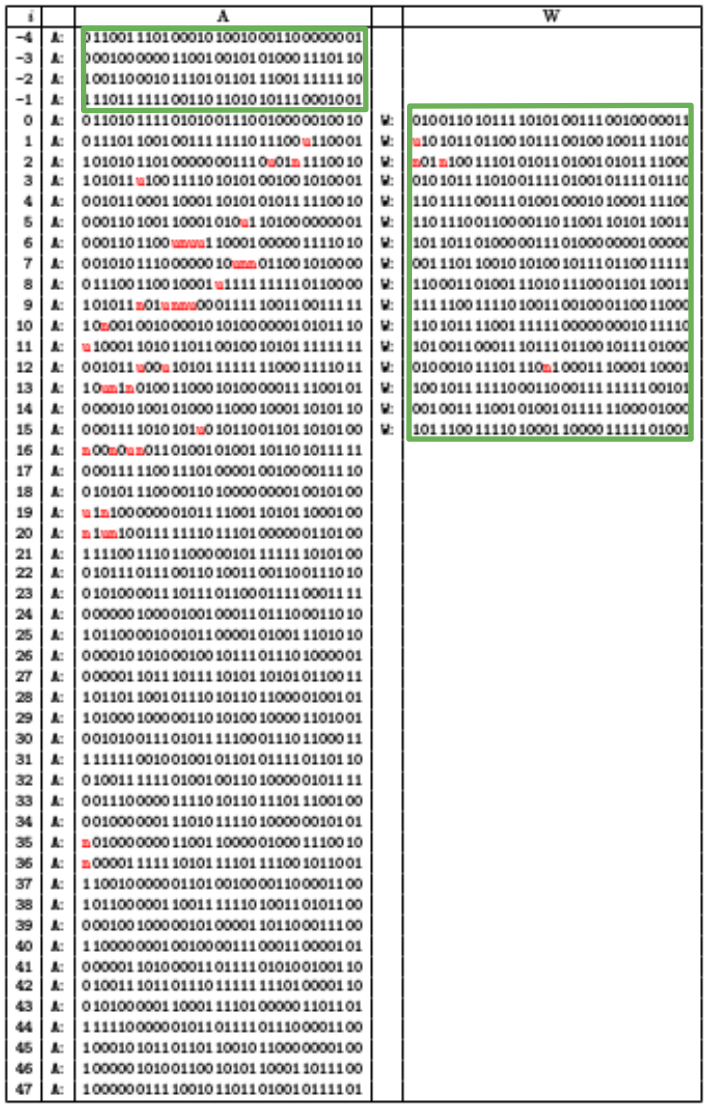
Example hash collision

i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 001		
0	A:	0 11010 1111 01010 01110 01000 00100 10	W:	0100110 10111 10101 00111 00100 00011
1	A:	0 11101 1001 00111 11110 11100 ?110 001	W:	?10 1011 01100 10111 00100 10011 11010
2	A:	1 01010 1101 00000 00111 0?01? 1110 10	W:	?01 ?100 11101 01011 01001 01011 11000
3	A:	1 01011 ?100 11110 10101 00100 1010 001	W:	010 1011 11010 01111 01001 01111 01110
4	A:	0 01011 0001 10001 10101 01011 11100 10	W:	110 1111 00111 01001 00010 10001 11100
5	A:	0 00110 1001 10001 010?1 10100 0000 001	W:	110 1110 01100 00110 11001 10101 10011
6	A:	0 00110 1100 ???? 1 10001 00000 11110 10	W:	101 1011 01000 00111 01000 00001 00000
7	A:	0 01010 1110 00000 10??? 01100 10100 00	W:	001 1101 10010 10100 10111 01100 11111
8	A:	0 11100 1100 10001 ?1111 11111 0110 000	W:	110 0011 01001 11010 11100 01101 10011
9	A:	1 01011 ?01? ???? 0001 111 10011 00111 11	W:	111 1100 11110 10011 00100 01100 11000
10	A:	1 0?001 00100 00010 10100 00001 01011 10	W:	110 1011 11001 11111 00000 00010 11110
11	A:	?10001 1010 11011 00100 10101 1111 11	W:	101 0011 00011 10111 01100 10111 01000
12	A:	0 01011 ?00? 10101 1111 11000 1110 11	W:	010 0010 11101 110?1 00011 10001 10001
13	A:	1 0??1? 0100 11000 10100 0011 1100 101	W:	100 1011 11110 00110 00111 11111 00101
14	A:	0 00010 1001 01000 11000 10001 10101 10	W:	001 0011 11001 01001 01111 11000 01000
15	A:	0 00111 1010 101?0 10110 01101 1010 100	W:	101 1100 11110 10001 10000 11111 01001
16	A:	?00?0?? 011 01001 01001 10110 10111 11		
17	A:	0 00111 1100 11101 00001 00100 00111 10		
18	A:	0 10101 1100 00110 10000 00001 00101 00		
19	A:	?1? 10000 00101 11001 10101 10001 00		
20	A:	?1?? 10011 11110 11101 00000 01101 00		
21	A:	1 11100 1110 11000 00101 11111 10101 00		
22	A:	0 10111 0111 00110 10011 00110 01110 10		
23	A:	0 10100 0011 10111 01100 01111 0001 11		
24	A:	0 00000 1000 01001 00011 01110 00110 10		
25	A:	1 01100 00101 01011 00001 01001 11010 10		
26	A:	0 00010 1010 00100 10111 01110 1000 001		
27	A:	0 00001 1011 10111 10101 10101 01100 11		
28	A:	1 01101 1001 01110 10110 11000 01001 01		
29	A:	1 01000 1000 00110 10100 10000 1101 001		
30	A:	0 01010 0111 01011 11100 01110 11000 11		
31	A:	1 11111 0010 01001 01101 01111 01101 10		
32	A:	0 10011 1111 01001 00110 10000 01011 11		
33	A:	0 01110 0000 11110 10110 11101 11001 00		
34	A:	0 01000 0001 11010 11110 10000 00101 01		
35	A:	?01000 0000 11001 10000 01000 11100 10		
36	A:	?0000 1111 10101 11101 11100 10110 01		
37	A:	1 10010 0000 01101 00100 00110 0001 100		
38	A:	1 01100 0001 10011 11110 10011 01011 00		
39	A:	0 00100 1000 00101 00001 10110 00111 00		
40	A:	1 10000 0001 00100 00111 00011 0000 101		
41	A:	0 00001 1010 00011 01111 01010 01001 10		
42	A:	0 10011 1011 01110 11111 11101 00001 10		
43	A:	0 10100 0001 10001 11101 00000 11011 01		
44	A:	1 11110 0000 01011 01111 01110 0001 100		
45	A:	1 00010 1011 01101 10010 11000 0000 100		
46	A:	1 00000 1010 01100 10101 10001 1011 00		
47	A:	1 00000 0111 10010 11011 01001 0111 101		

input message

Example hash collision

initial vectors

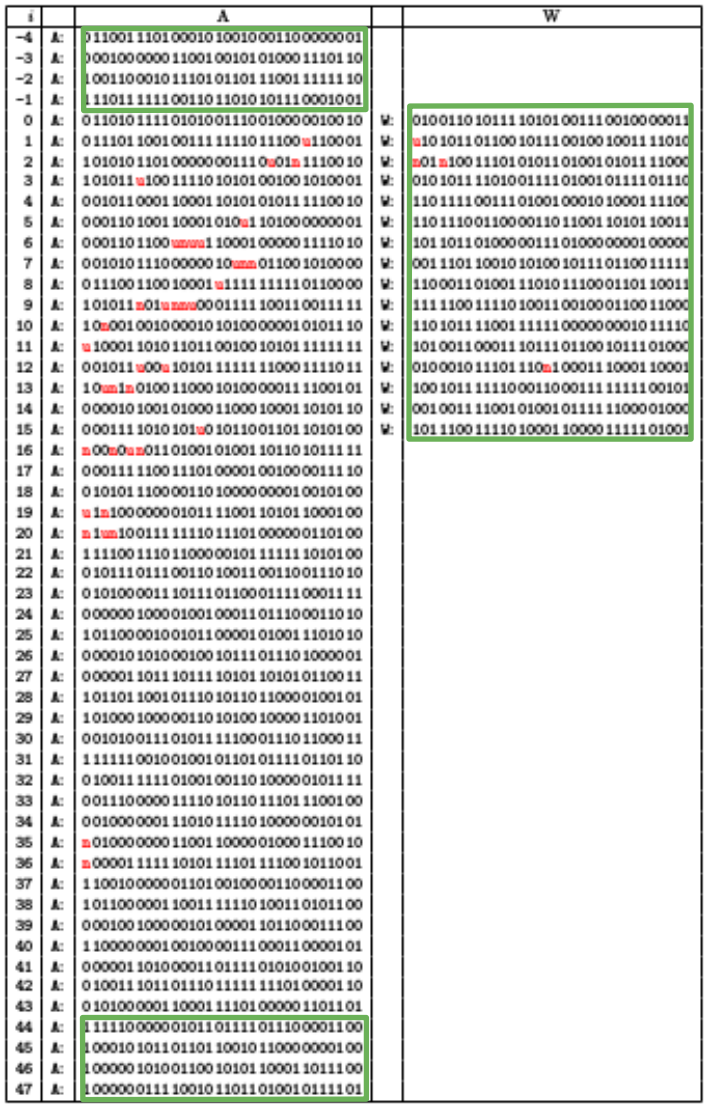


i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 001		
0	A:	0 11010 1111 01010 01110 01000 00100 10	W:	0100110 10111 10101 00111 00100 00011
1	A:	0 11101 1001 00111 11110 11100 u1100 01	W:	u10 1011 01100 10111 00100 10011 11010
2	A:	1 01010 1101 00000 00111 0u01n 11100 10	W:	u01 n100 11101 01011 01001 01011 11000
3	A:	1 01011 u100 11110 10101 00100 10100 01	W:	010 1011 11010 01111 01001 01111 01110
4	A:	0 01011 0001 10001 10101 01011 11100 10	W:	110 1111 00111 01001 00010 10001 11100
5	A:	0 00110 1001 10001 010u1 10100 00000 01	W:	110 1110 01100 00110 11001 10101 10011
6	A:	0 00110 1100 uuuu1 10001 00000 11110 10	W:	101 1011 01000 00111 01000 00001 00000
7	A:	0 01010 1110 00000 10uun 01100 10100 00	W:	001 1101 10010 10100 10111 01100 11111
8	A:	0 11100 1100 10001 u1111 11111 01100 00	W:	110 0011 01001 11010 11100 01101 10011
9	A:	1 01011 n01u uuuu0 0011 11 10011 00111 11	W:	111 1100 11110 10011 00100 01100 11000
10	A:	1 0un0 0100 0010 10100 0001 01011 10	W:	110 1011 11001 11111 00000 00010 11110
11	A:	u 1000 1010 11011 00100 10101 11111 11	W:	101 0011 00011 10111 01100 10111 01000
12	A:	0 01011 u00u 10101 11111 11000 11110 11	W:	010 0010 11101 110n1 00011 10001 10001
13	A:	1 0un1n 0100 11000 10100 0011 11001 01	W:	100 1011 11110 00110 00111 11111 00101
14	A:	0 00010 1001 01000 11000 10001 10101 10	W:	001 0011 11001 01001 01111 11000 01000
15	A:	0 00111 1010 101u0 10110 01101 10101 00	W:	101 1100 11110 10001 10000 11111 01001
16	A:	n 00u0u un011 01001 01001 10110 10111 11		
17	A:	0 00111 1100 11101 00001 00100 00111 10		
18	A:	0 10101 1100 00110 10000 00001 00101 00		
19	A:	u 1n100 0000 01011 11001 10101 10001 00		
20	A:	n 1un1 0011 11110 11101 00000 01101 00		
21	A:	1 11100 1110 11000 00101 11111 10101 00		
22	A:	0 10111 0111 00110 10011 00110 01110 10		
23	A:	0 10100 0011 10111 01100 01111 00011 11		
24	A:	0 00000 1000 01001 00011 01110 00110 10		
25	A:	1 01100 0010 01011 00001 01001 11010 10		
26	A:	0 00010 1010 00100 10111 01110 10000 01		
27	A:	0 00001 1011 10111 10101 10101 01100 11		
28	A:	1 01101 1001 01110 10110 11000 01001 01		
29	A:	1 01000 1000 00110 10100 10000 11010 01		
30	A:	0 01010 0111 01011 11100 01110 11000 11		
31	A:	1 11111 0010 01001 01101 01111 01101 10		
32	A:	0 10011 1111 01001 00110 10000 01011 11		
33	A:	0 01110 0000 11110 10110 11101 11001 00		
34	A:	0 01000 0001 11010 11110 10000 00101 01		
35	A:	n 01000 0000 11001 10000 01000 11100 10		
36	A:	n 00001 1111 10101 11101 11100 10110 01		
37	A:	1 10010 0000 01101 00100 00110 00011 00		
38	A:	1 01100 0001 10011 11110 10011 01011 00		
39	A:	0 00100 1000 00101 00001 10110 00111 00		
40	A:	1 10000 0001 00100 00111 00011 00001 01		
41	A:	0 00001 1010 00011 01111 01010 01001 10		
42	A:	0 10011 1011 01110 11111 11101 00001 10		
43	A:	0 10100 0001 10001 11101 00000 11011 01		
44	A:	1 11110 0000 01011 01111 01110 00011 00		
45	A:	1 00010 1011 01101 10010 11000 00001 00		
46	A:	1 00000 1010 01100 10101 10001 10111 00		
47	A:	1 00000 0111 10010 11011 01001 01111 01		

input message

Example hash collision

initial vectors



i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 001		
0	A:	0 11010 1111 01010 01110 01000 00100 10	W:	0100110 10111 10101 00111 00100 00011
1	A:	0 11101 1001 00111 11110 11100 u1100 01	W:	u10 1011 01100 10111 00100 10011 11010
2	A:	1 01010 1101 00000 00111 0u01n 11100 10	W:	u01 n100 11101 01011 01001 01011 11000
3	A:	1 01011 u100 11110 10101 00100 10100 01	W:	010 1011 11010 01111 01001 01111 01110
4	A:	0 01011 0001 10001 10101 01011 11100 10	W:	110 1111 00111 01001 00010 10001 11100
5	A:	0 00110 1001 10001 010u1 10100 00000 01	W:	110 1110 01100 00110 11001 10101 10011
6	A:	0 00110 1100 uuuu1 10001 00000 11110 10	W:	101 1011 01000 00111 01000 00001 00000
7	A:	0 01010 1110 00000 10uun 01100 10100 00	W:	001 1101 10010 10100 10111 01100 11111
8	A:	0 11100 1100 10001 u1111 11111 01100 00	W:	110 0011 01001 11010 11100 01101 10011
9	A:	1 01011 n01u uuuu0 0011 11 10011 00111 11	W:	111 1100 11110 10011 00100 01100 11000
10	A:	1 0un0 0100 0010 10100 0001 01011 10	W:	110 1011 11001 11111 00000 00010 11110
11	A:	u 1000 1010 11011 00100 10101 11111 11	W:	101 0011 00011 10111 01100 10111 01000
12	A:	0 01011 u00u 10101 11111 11000 11110 11	W:	010 0010 11101 110n1 00011 10001 10001
13	A:	1 0un1n 0100 11000 10100 00011 11001 01	W:	100 1011 11110 00110 00111 11111 00101
14	A:	0 00010 1001 01000 11000 10001 10101 10	W:	001 0011 11001 01001 01111 11000 01000
15	A:	0 00111 1010 101u0 10110 01101 10101 00	W:	101 1100 11110 10001 10000 11111 01001
16	A:	n 00u0 u u011 01001 01001 10110 10111 11		
17	A:	0 00111 1100 11101 00001 00100 00111 10		
18	A:	0 10101 1100 00110 10000 00001 00101 00		
19	A:	u 1n100 0000 01011 11001 10101 10001 00		
20	A:	n 1un100 111 11110 11101 00000 01101 00		
21	A:	1 11100 1110 11000 00101 11111 10101 00		
22	A:	0 10111 0111 00110 10011 00110 01110 10		
23	A:	0 10100 0011 10111 01100 01111 00011 11		
24	A:	0 00000 1000 01001 00011 01110 00110 10		
25	A:	1 01100 00101 01011 00001 01001 11010 10		
26	A:	0 00010 1010 00100 10111 01110 10000 01		
27	A:	0 00001 1011 10111 10101 10101 01100 11		
28	A:	1 01101 1001 01110 10110 11000 01001 01		
29	A:	1 01000 1000 00110 10100 10000 11010 01		
30	A:	0 01010 0111 01011 11100 01110 11000 11		
31	A:	1 11111 0010 01001 01101 01111 01101 10		
32	A:	0 10011 1111 01001 00110 10000 01011 11		
33	A:	0 01110 0000 11110 10110 11101 11001 00		
34	A:	0 01000 0001 11010 11110 10000 00101 01		
35	A:	n 01000 0000 11001 10000 01000 11100 10		
36	A:	n 00001 1111 10101 11101 11100 10110 01		
37	A:	1 10010 0000 01101 00100 00110 00011 00		
38	A:	1 01100 0001 10011 11110 10011 01011 00		
39	A:	0 00100 1000 00101 00001 10110 00111 00		
40	A:	1 10000 0001 00100 00111 00011 00001 01		
41	A:	0 00001 1010 00011 01111 01010 01001 10		
42	A:	0 10011 1011 01110 11111 11101 00001 10		
43	A:	0 10100 0001 10001 11101 00000 11011 01		
44	A:	1 11110 0000 01011 01111 01110 00011 00		
45	A:	1 00010 1011 01101 10010 11000 00001 00		
46	A:	1 00000 1010 01100 10101 10001 10111 00		
47	A:	1 00000 0111 10010 11011 01001 01111 01		

input message

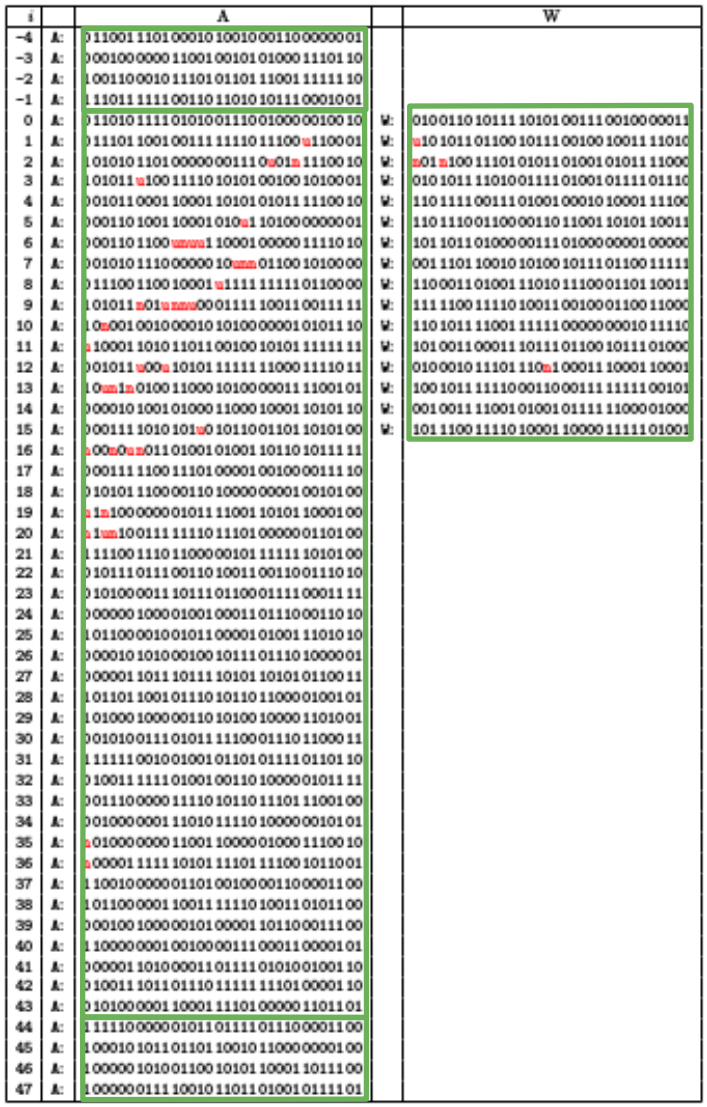
output words

Example hash collision

initial vectors

intermediate values

output words

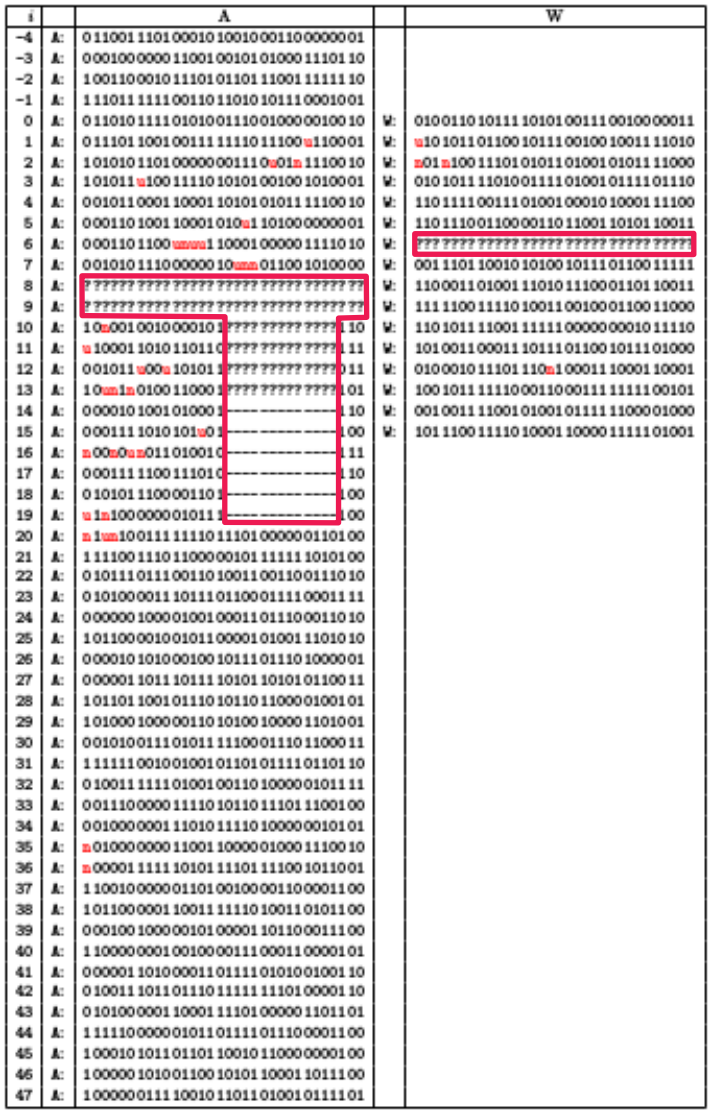


i		A		W
−4	A:	11001 1101 00010 10010 00110 00000 01		
−3	A:	00100 0000 11001 00101 01000 11101 10		
−2	A:	00110 0010 11101 01101 11001 11111 10		
−1	A:	11011 1111 00110 11010 10111 0001 001		
0	A:	11010 1111 01010 01110 01000 00100 10	W:	01001 10 10111 10101 00111 00100 00011
1	A:	11101 1001 00111 11110 11100 u1100 01	W:	u10 1011 01100 10111 00100 10011 11010
2	A:	01010 1101 00000 00111 0u01n 11100 10	W:	u01 n100 11101 01011 01001 01011 11000
3	A:	01011 u100 11110 10101 00100 10100 01	W:	010 1011 11010 01111 01001 01111 01110
4	A:	01011 0001 10001 10101 01011 11100 10	W:	110 1111 00111 01001 00010 10001 11100
5	A:	00110 1001 10001 010u1 10100 00000 01	W:	110 1110 01100 00110 11001 10101 10011
6	A:	00110 1100 uuuu1 10001 00000 11110 10	W:	101 1011 01000 00111 01000 00001 00000
7	A:	01010 1110 00000 10uun 01100 10100 00	W:	001 1101 10010 10100 10111 01100 11111
8	A:	11100 1100 10001 u1111 11111 01100 00	W:	110 0011 01001 11010 11100 01101 10011
9	A:	01011 n01u uuuu0 0011 11 10011 00111 11	W:	111 1100 11110 10011 00100 01100 11000
10	A:	0un001 00100 00101 01000 00010 10111 10	W:	110 1011 11001 11111 00000 00010 11110
11	A:	u10001 10101 10110 01001 01011 11111 11	W:	101 0011 00011 10111 01100 10111 01000
12	A:	01011 u00u 10101 11111 11000 11110 11	W:	010 0010 11101 110n1 00011 10001 10001
13	A:	0un1n 0100 11000 10100 00011 11001 01	W:	100 1011 11110 00110 00111 11111 00101
14	A:	00010 1001 01000 11000 10001 10101 10	W:	001 0011 11001 01001 01111 11000 01000
15	A:	00111 1010 101u0 10110 01101 10101 00	W:	101 1100 11110 10001 10000 11111 01001
16	A:	u00u0unu011 01001 01001 10110 10111 11		
17	A:	00111 1100 11101 00001 00100 00111 10		
18	A:	10101 1100 00110 10000 00010 01010 00		
19	A:	u1n1000 0000 01011 11001 10101 10001 00		
20	A:	u1un100 111 11110 11101 00000 01101 00		
21	A:	11100 1110 11000 00101 11111 10101 00		
22	A:	10111 0111 00110 10011 00110 01110 10		
23	A:	10100 0011 10111 01100 01111 00011 11		
24	A:	00000 1000 01001 00011 01110 00110 10		
25	A:	01100 00101 01011 00001 01001 11010 10		
26	A:	00010 1010 00100 10111 01110 10000 01		
27	A:	00001 1011 10111 10101 10101 01100 11		
28	A:	01101 1001 01110 10110 11000 01001 01		
29	A:	01000 1000 00110 10100 10000 11010 01		
30	A:	01010 0111 01011 11100 01110 11000 11		
31	A:	11111 0010 01001 01101 01111 01101 10		
32	A:	10011 1111 01001 00110 10000 01011 11		
33	A:	01110 0000 11110 10110 11101 11001 00		
34	A:	01000 0001 11010 11110 10000 00101 01		
35	A:	u0100 0000 11001 10000 01000 11100 10		
36	A:	u0000 1111 10101 11101 11100 10110 01		
37	A:	10010 0000 01101 00100 00110 00011 00		
38	A:	01100 0001 10011 11110 10011 01011 00		
39	A:	00100 1000 00101 00001 10110 00111 00		
40	A:	10000 0001 00100 00111 00011 00001 01		
41	A:	00001 1010 00011 01111 01010 01001 10		
42	A:	10011 1011 01110 11111 11101 00001 10		
43	A:	10100 0001 10001 11101 00000 11011 01		
44	A:	11110 0000 01011 01111 01110 00011 00		
45	A:	00010 1011 01101 10010 11000 00001 00		
46	A:	00000 1010 01100 10101 10001 10111 00		
47	A:	00000 0111 10010 11011 01001 01111 01		

input message

Example hash collision

underspecified

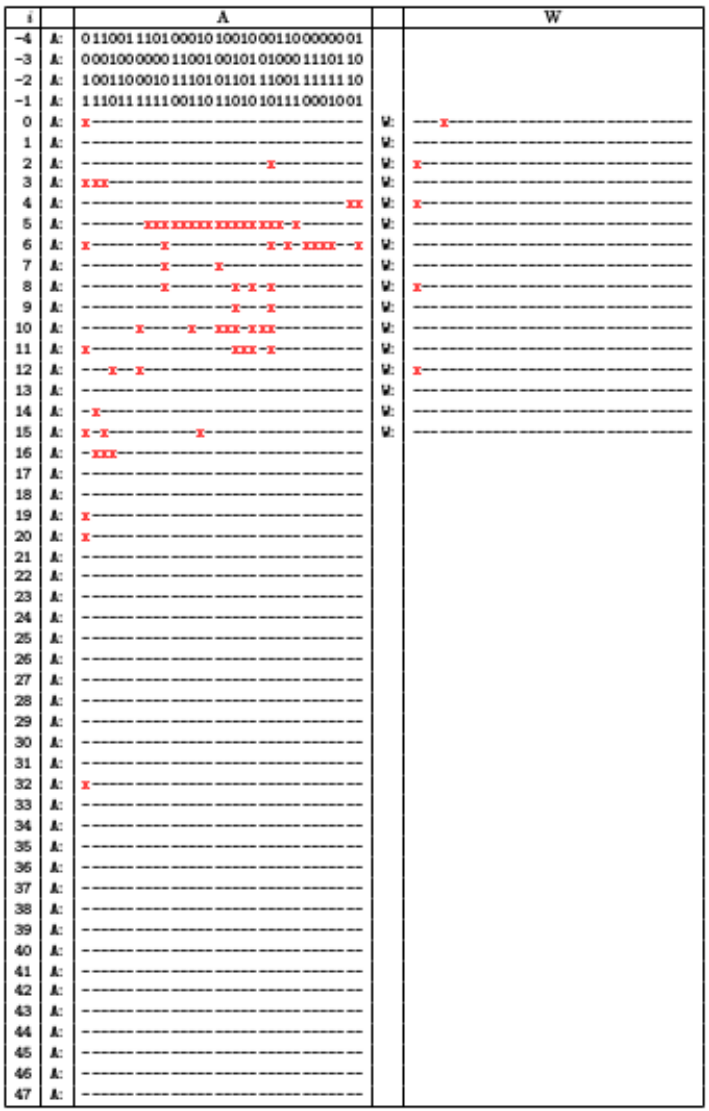


i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 0 01		
0	A:	0 11010 1111 01010 01110 01000 00100 10	W:	0100110 10111 10101 00111 00100 00011
1	A:	0 11101 1001 00111 11110 11100 ?110 001	W:	?10 1011 01100 10111 00100 10011 11010
2	A:	1 01010 1101 00000 00111 0?01? 1110 10	W:	?01 ?100 11101 01011 01001 01011 11000
3	A:	1 01011 ?100 11110 10101 00100 1010 001	W:	010 1011 11010 01111 01001 01111 01110
4	A:	0 01011 0001 10001 10101 01011 11100 10	W:	110 1111 00111 01001 00010 10001 11100
5	A:	0 00110 1001 10001 010?1 10100 0000 001	W:	110 1110 01100 00110 11001 10101 10011
6	A:	0 00110 1100 ???? 1 10001 00000 11110 10	W:	??? ???? ????? ????? ????? ????? ?????
7	A:	0 01010 1110 00000 10??? 01100 1010 000	W:	001 1101 10010 10100 10111 01100 11111
8	A:	? ????? ???? ????? ????? ????? ????? ??	W:	1100011 01001 11010 11100 01101 10011
9	A:	? ????? ???? ????? ????? ????? ????? ??	W:	111 1100 11110 10011 00100 01100 11000
10	A:	1 0?001 0010 00010 1???? ????? ???? 1 10	W:	110 1011 11001 11111 00000 00010 11110
11	A:	?10001 1010 11011 0???? ????? ???? 1 11	W:	101 0011 00011 10111 01100 10111 01000
12	A:	0 01011 ?00?1 01011 1???? ????? ???? 0 11	W:	0100010 11101 110?1 00011 10001 10001
13	A:	1 0??1? 0100 11000 1???? ????? ???? 1 01	W:	100 1011 11110 00110 00111 11111 00101
14	A:	0 00010 1001 01000 1 ---------- 1 10	W:	001 0011 11001 01001 01111 11000 01000
15	A:	0 00111 1010 101?0 1 ---------- 1 00	W:	101 1100 11110 10001 10000 11111 01001
16	A:	?00?0??011 01001 0 ---------- 1 11		
17	A:	0 00111 1100 11101 0 ---------- 1 10		
18	A:	0 10101 1100 00110 1 ---------- 1 00		
19	A:	?1?1 0000 0001 1011 1 ---------- 1 00		
20	A:	?1?? 1001 11110 11101 00000 01101 00		
21	A:	1 11100 1110 11000 00101 11111 10101 00		
22	A:	0 10111 0111 00110 10011 00110 01110 10		
23	A:	0 10100 0011 10111 01100 11110 0011 11		
24	A:	0 00000 1000 01001 00011 01110 00110 10		
25	A:	1 01100 0010 01011 00001 01001 11010 10		
26	A:	0 00010 1010 00100 10111 01110 1000 001		
27	A:	0 00001 1011 10111 10101 10101 01100 11		
28	A:	1 01101 1001 01110 10110 11000 01001 01		
29	A:	1 01000 1000 00110 10100 10000 11010 01		
30	A:	0 01010 0111 01011 11100 01110 11000 11		
31	A:	1 11111 0010 01001 01101 01111 01101 10		
32	A:	0 10011 1111 01001 00110 10000 01011 11		
33	A:	0 01110 0000 11110 10110 11101 11001 00		
34	A:	0 01000 0001 11010 11110 10000 00101 01		
35	A:	?01000 0000 11001 10000 01000 11100 10		
36	A:	?0000 1111 10101 11101 11100 10110 01		
37	A:	1 10010 0000 01101 00100 01100 00110 00		
38	A:	1 01100 0001 10011 11110 10011 01011 00		
39	A:	0 00100 1000 00101 00001 10110 00111 00		
40	A:	1 10000 0001 00100 00111 00011 0000 101		
41	A:	0 00001 1010 00011 01111 01010 01001 10		
42	A:	0 10011 1011 01110 11111 11101 00001 10		
43	A:	0 10100 0001 10001 11101 00000 11011 01		
44	A:	1 11110 0000 01011 01111 01110 00011 00		
45	A:	1 00010 1011 01101 10010 11000 00001 00		
46	A:	1 00000 1010 01100 10101 10001 10111 00		
47	A:	1 00000 0111 10010 11011 01001 01111 01		

Attack!

Attacking MD4 & SHA-256

MD4 testcases & results

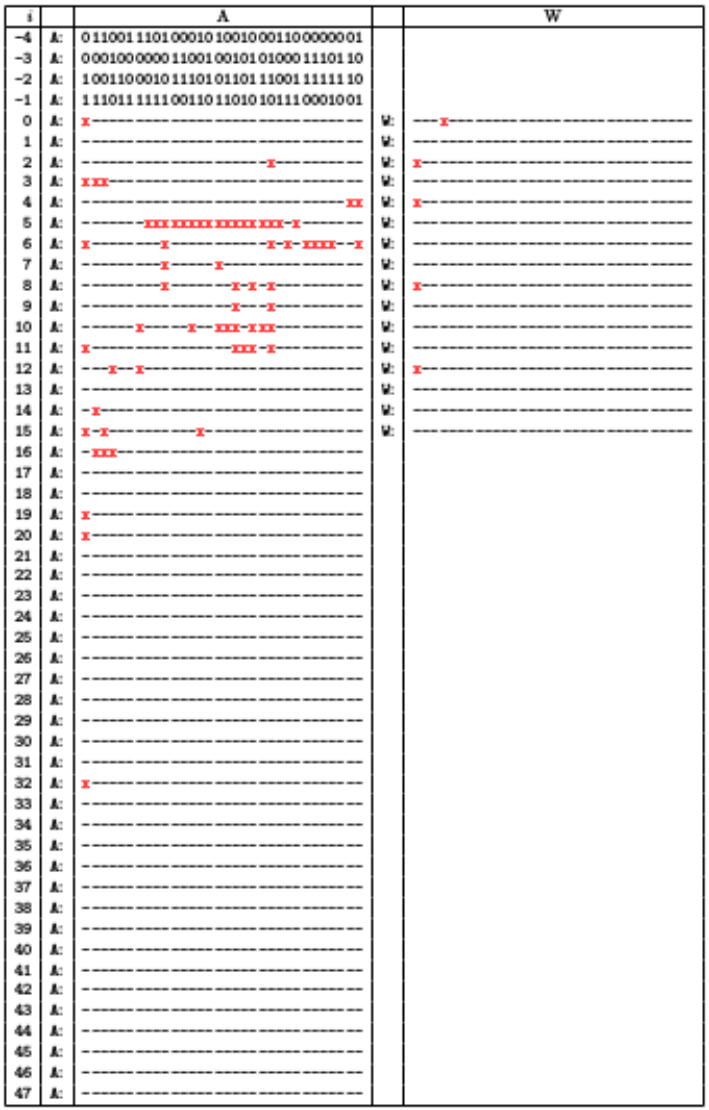


i		A		W
−4	A:	0 11001 1101 00010 10010 00110 0000 01		
−3	A:	0 00100 0000 11001 00101 01000 1110 1 10		
−2	A:	1 00110 0010 11101 01101 11001 1111 1 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 0 01		
0	A:	x	W:	-x
1	A:	-	W:	-
2	A:	-x	W:	x
3	A:	xx	W:	-
4	A:	-x	W:	x
5	A:	-xxxxxxxxxxxx-x	W:	-
6	A:	x-x-x-x-xxxx--x	W:	-
7	A:	-x-x	W:	-
8	A:	-x-x-x	W:	x
9	A:	-x-x	W:	-
10	A:	-x-x-xxx-xx	W:	-
11	A:	x-xxx-x	W:	-
12	A:	-x-x	W:	x
13	A:	-	W:	-
14	A:	-x	W:	-
15	A:	x-x-x	W:	-
16	A:	-xxx		
17	A:	-		
18	A:	-		
19	A:	x		
20	A:	x		
21	A:	-		
22	A:	-		
23	A:	-		
24	A:	-		
25	A:	-		
26	A:	-		
27	A:	-		
28	A:	-		
29	A:	-		
30	A:	-		
31	A:	-		
32	A:	x		
33	A:	-		
34	A:	-		
35	A:	-		
36	A:	-		
37	A:	-		
38	A:	-		
39	A:	-		
40	A:	-		
41	A:	-		
42	A:	-		
43	A:	-		
44	A:	-		
45	A:	-		
46	A:	-		
47	A:	-		

Testcase A [03]

All differences set. Just determine actual bits in both instances.

MD4 testcases & results



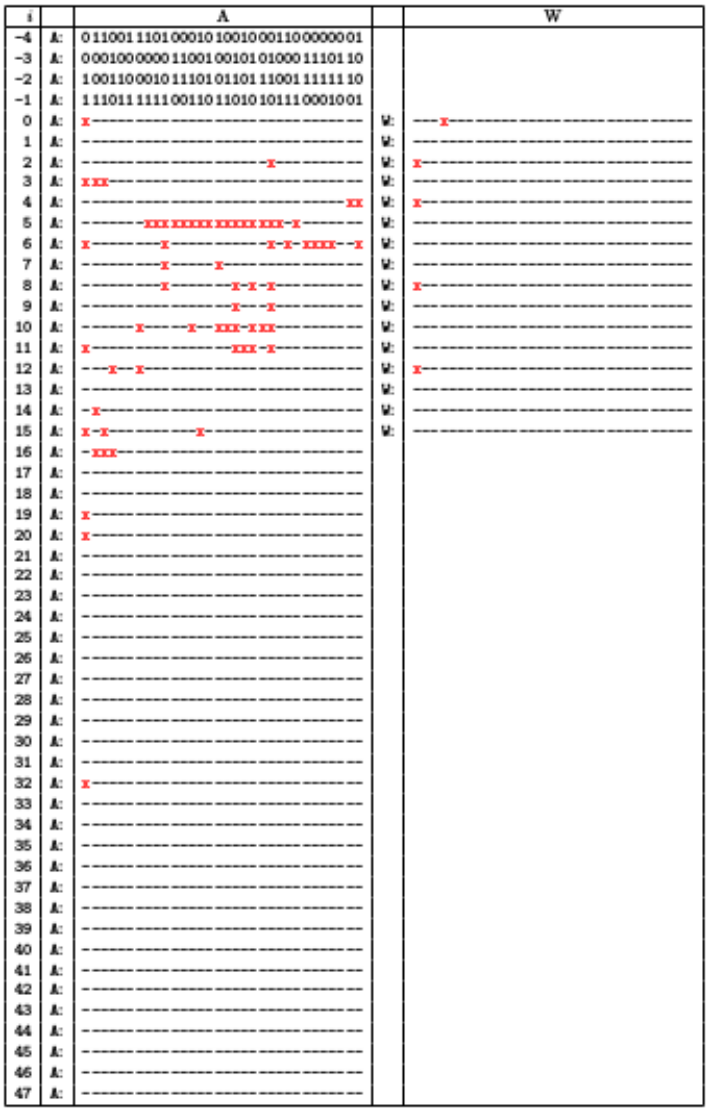
Testcase A [03]

All differences set. Just determine actual bits in both instances.

always seconds

solver	version	runtime
MiniSat	2.2.0	3
CryptoMiniSat	4.5.3	26
	5	29
Lingeling	ats1	23
Plingeling	ats1	88
Treengeling	ats1	64
Glucose	4.0	8
Glucose Syrup	4.0	14

MD4 testcases & results



i		A		W
−4	A:	0 11001 1101 00010 10010 00110 0000 01		
−3	A:	0 00100 0000 11001 00101 01000 1110 10		
−2	A:	1 00110 0010 11101 01101 11001 1111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 01		
0	A:	x	W:	--x
1	A:	-	W:	
2	A:	-------------x	W:	x
3	A:	xxx	W:	
4	A:	----------------------------xx	W:	x
5	A:	-------xxx xxxxx xxxxx xxx-x	W:	
6	A:	x-------x----------x-x-xxxx--x	W:	
7	A:	--------x-----x	W:	
8	A:	--------x-------x-x-x	W:	x
9	A:	----------------x---x	W:	
10	A:	-------x-----x--xxx-xxx	W:	
11	A:	x-----------------xxx-x	W:	
12	A:	---x--x	W:	x
13	A:	-	W:	
14	A:	-x	W:	
15	A:	x-x---------x	W:	
16	A:	-xxx		
17	A:	-		
18	A:	-		
19	A:	x		
20	A:	x		
21	A:	-		
22	A:	-		
23	A:	-		
24	A:	-		
25	A:	-		
26	A:	-		
27	A:	-		
28	A:	-		
29	A:	-		
30	A:	-		
31	A:	-		
32	A:	x		
33	A:	-		
34	A:	-		
35	A:	-		
36	A:	-		
37	A:	-		
38	A:	-		
39	A:	-		
40	A:	-		
41	A:	-		
42	A:	-		
43	A:	-		
44	A:	-		
45	A:	-		
46	A:	-		
47	A:	-		

Interesting fact:
In 2006, Mironov and Zhang [**04**] evaluated such testcases *within 10 minutes*.

MD4 testcases & results

i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 0 01		
0	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---x----------
1	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
2	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
3	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
4	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
5	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
6	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
7	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
8	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
9	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
10	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
11	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
12	A:	? ????? ???? ????- ---------- ----------	W:	x----------
13	A:	? ????? ???? ????- ---------- ----------	W:	----------
14	A:	? ????? ???? ????- ---------- ----------	W:	----------
15	A:	? ????? ???? ????- ---------- ----------	W:	----------
16	A:	? ??x---------- ---------- ----------		
17	A:	?---------- ---------- ---------- ----------		
18	A:	?---------- ---------- ---------- ----------		
19	A:	?---------- ---------- ---------- ----------		
20	A:	x---------- ---------- ---------- ----------		
21	A:	---------- ---------- ---------- ----------		
22	A:	---------- ---------- ---------- ----------		
23	A:	---------- ---------- ---------- ----------		
24	A:	---------- ---------- ---------- ----------		
25	A:	---------- ---------- ---------- ----------		
26	A:	---------- ---------- ---------- ----------		
27	A:	---------- ---------- ---------- ----------		
28	A:	---------- ---------- ---------- ----------		
29	A:	---------- ---------- ---------- ----------		
30	A:	---------- ---------- ---------- ----------		
31	A:	---------- ---------- ---------- ----------		
32	A:	x---------- ---------- ---------- ----------		
33	A:	---------- ---------- ---------- ----------		
34	A:	---------- ---------- ---------- ----------		
35	A:	---------- ---------- ---------- ----------		
36	A:	---------- ---------- ---------- ----------		
37	A:	---------- ---------- ---------- ----------		
38	A:	---------- ---------- ---------- ----------		
39	A:	---------- ---------- ---------- ----------		
40	A:	---------- ---------- ---------- ----------		
41	A:	---------- ---------- ---------- ----------		
42	A:	---------- ---------- ---------- ----------		
43	A:	---------- ---------- ---------- ----------		
44	A:	---------- ---------- ---------- ----------		
45	A:	---------- ---------- ---------- ----------		
46	A:	---------- ---------- ---------- ----------		
47	A:	---------- ---------- ---------- ----------		

Testcase B [03]

Words in rounds 0–11 completely undetermined.

MD4 testcases & results

i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 0 01		
0	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---x---------- ---------- ---------- ----------
1	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
2	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x--------- ---------- ---------- ---------- ----------
3	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
4	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x--------- ---------- ---------- ---------- ----------
5	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
6	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
7	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
8	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x--------- ---------- ---------- ---------- ----------
9	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
10	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
11	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
12	A:	? ????? ???? ????- ---------- ---------- --	W:	x--------- ---------- ---------- ---------- ----------
13	A:	? ????? ???? ????- ---------- ---------- --	W:	---------- ---------- ---------- ---------- ----------
14	A:	? ????? ???? ????- ---------- ---------- --	W:	---------- ---------- ---------- ---------- ----------
15	A:	? ????? ???? ????- ---------- ---------- --	W:	---------- ---------- ---------- ---------- ----------
16	A:	? ??x---------- ---------- ---------- --		
17	A:	?---------- ---------- ---------- ---------- --		
18	A:	?---------- ---------- ---------- ---------- --		
19	A:	?---------- ---------- ---------- ---------- --		
20	A:	x---------- ---------- ---------- ---------- --		
21	A:	---------- ---------- ---------- ---------- --		
22	A:	---------- ---------- ---------- ---------- --		
23	A:	---------- ---------- ---------- ---------- --		
24	A:	---------- ---------- ---------- ---------- --		
25	A:	---------- ---------- ---------- ---------- --		
26	A:	---------- ---------- ---------- ---------- --		
27	A:	---------- ---------- ---------- ---------- --		
28	A:	---------- ---------- ---------- ---------- --		
29	A:	---------- ---------- ---------- ---------- --		
30	A:	---------- ---------- ---------- ---------- --		
31	A:	---------- ---------- ---------- ---------- --		
32	A:	x---------- ---------- ---------- ---------- --		
33	A:	---------- ---------- ---------- ---------- --		
34	A:	---------- ---------- ---------- ---------- --		
35	A:	---------- ---------- ---------- ---------- --		
36	A:	---------- ---------- ---------- ---------- --		
37	A:	---------- ---------- ---------- ---------- --		
38	A:	---------- ---------- ---------- ---------- --		
39	A:	---------- ---------- ---------- ---------- --		
40	A:	---------- ---------- ---------- ---------- --		
41	A:	---------- ---------- ---------- ---------- --		
42	A:	---------- ---------- ---------- ---------- --		
43	A:	---------- ---------- ---------- ---------- --		
44	A:	---------- ---------- ---------- ---------- --		
45	A:	---------- ---------- ---------- ---------- --		
46	A:	---------- ---------- ---------- ---------- --		
47	A:	---------- ---------- ---------- ---------- --		

Testcase B [03]

Words in rounds 0–11 completely undetermined.

~ 20 minutes

MD4 testcases & results

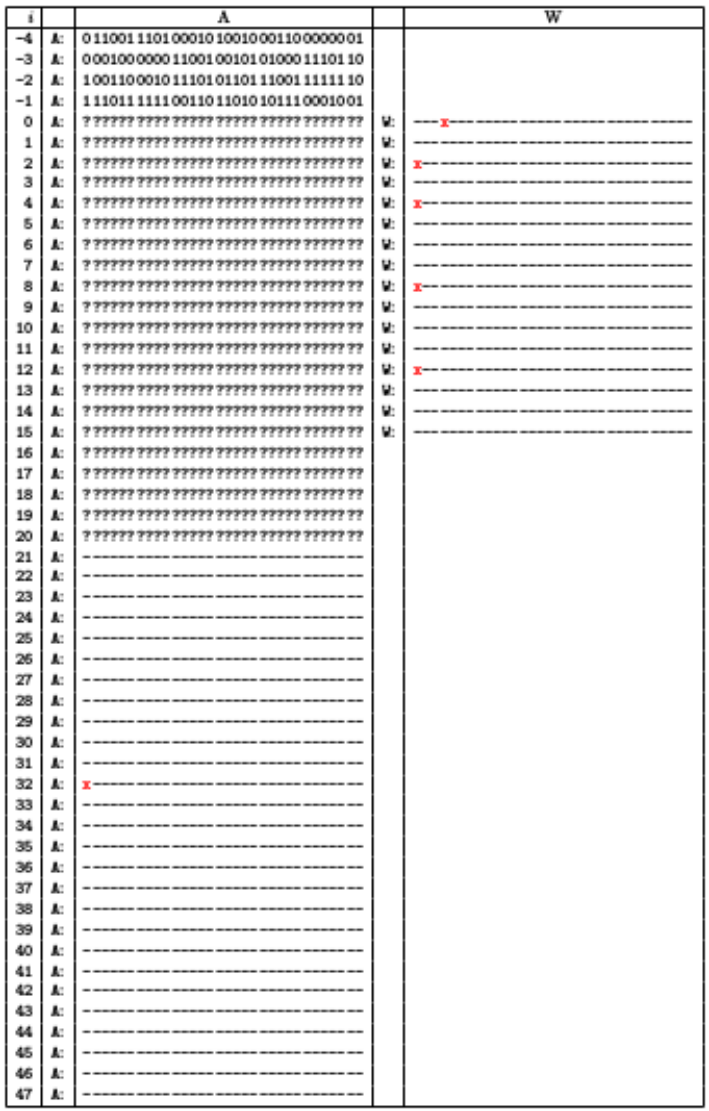
i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 0 01		
0	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---x---------- ---------- ---------- ----------
1	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
2	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
3	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
4	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
5	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
6	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
7	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
8	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
9	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
10	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
11	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
12	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
13	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
14	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
15	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
16	A:	? ????? ???? ????? ????? ????? ????? ??		
17	A:	? ????? ???? ????? ????? ????? ????? ??		
18	A:	? ????? ???? ????? ????? ????? ????? ??		
19	A:	? ????? ???? ????? ????? ????? ????? ??		
20	A:	? ????? ???? ????? ????? ????? ????? ??		
21	A:	---------- ---------- ---------- ---------- --		
22	A:	---------- ---------- ---------- ---------- --		
23	A:	---------- ---------- ---------- ---------- --		
24	A:	---------- ---------- ---------- ---------- --		
25	A:	---------- ---------- ---------- ---------- --		
26	A:	---------- ---------- ---------- ---------- --		
27	A:	---------- ---------- ---------- ---------- --		
28	A:	---------- ---------- ---------- ---------- --		
29	A:	---------- ---------- ---------- ---------- --		
30	A:	---------- ---------- ---------- ---------- --		
31	A:	---------- ---------- ---------- ---------- --		
32	A:	x---------- ---------- ---------- ---------- --		
33	A:	---------- ---------- ---------- ---------- --		
34	A:	---------- ---------- ---------- ---------- --		
35	A:	---------- ---------- ---------- ---------- --		
36	A:	---------- ---------- ---------- ---------- --		
37	A:	---------- ---------- ---------- ---------- --		
38	A:	---------- ---------- ---------- ---------- --		
39	A:	---------- ---------- ---------- ---------- --		
40	A:	---------- ---------- ---------- ---------- --		
41	A:	---------- ---------- ---------- ---------- --		
42	A:	---------- ---------- ---------- ---------- --		
43	A:	---------- ---------- ---------- ---------- --		
44	A:	---------- ---------- ---------- ---------- --		
45	A:	---------- ---------- ---------- ---------- --		
46	A:	---------- ---------- ---------- ---------- --		
47	A:	---------- ---------- ---------- ---------- --		

Testcase C [03]

Words in rounds 0–20 completely undetermined.

Collision still given in round 32.

MD4 testcases & results



i		A		W
−4	A:	0 11001 1101 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 0 01		
0	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---x---------- ---------- ---------- ----------
1	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
2	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
3	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
4	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
5	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
6	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
7	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
8	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
9	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
10	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
11	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
12	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x---------- ---------- ---------- ---------- ----------
13	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
14	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
15	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ----------
16	A:	? ????? ???? ????? ????? ????? ????? ??		
17	A:	? ????? ???? ????? ????? ????? ????? ??		
18	A:	? ????? ???? ????? ????? ????? ????? ??		
19	A:	? ????? ???? ????? ????? ????? ????? ??		
20	A:	? ????? ???? ????? ????? ????? ????? ??		
21	A:	---------- ---------- ---------- ---------- ---------- --		
22	A:	---------- ---------- ---------- ---------- ---------- --		
23	A:	---------- ---------- ---------- ---------- ---------- --		
24	A:	---------- ---------- ---------- ---------- ---------- --		
25	A:	---------- ---------- ---------- ---------- ---------- --		
26	A:	---------- ---------- ---------- ---------- ---------- --		
27	A:	---------- ---------- ---------- ---------- ---------- --		
28	A:	---------- ---------- ---------- ---------- ---------- --		
29	A:	---------- ---------- ---------- ---------- ---------- --		
30	A:	---------- ---------- ---------- ---------- ---------- --		
31	A:	---------- ---------- ---------- ---------- ---------- --		
32	A:	x---------- ---------- ---------- ---------- ---------- --		
33	A:	---------- ---------- ---------- ---------- ---------- --		
34	A:	---------- ---------- ---------- ---------- ---------- --		
35	A:	---------- ---------- ---------- ---------- ---------- --		
36	A:	---------- ---------- ---------- ---------- ---------- --		
37	A:	---------- ---------- ---------- ---------- ---------- --		
38	A:	---------- ---------- ---------- ---------- ---------- --		
39	A:	---------- ---------- ---------- ---------- ---------- --		
40	A:	---------- ---------- ---------- ---------- ---------- --		
41	A:	---------- ---------- ---------- ---------- ---------- --		
42	A:	---------- ---------- ---------- ---------- ---------- --		
43	A:	---------- ---------- ---------- ---------- ---------- --		
44	A:	---------- ---------- ---------- ---------- ---------- --		
45	A:	---------- ---------- ---------- ---------- ---------- --		
46	A:	---------- ---------- ---------- ---------- ---------- --		
47	A:	---------- ---------- ---------- ---------- ---------- --		

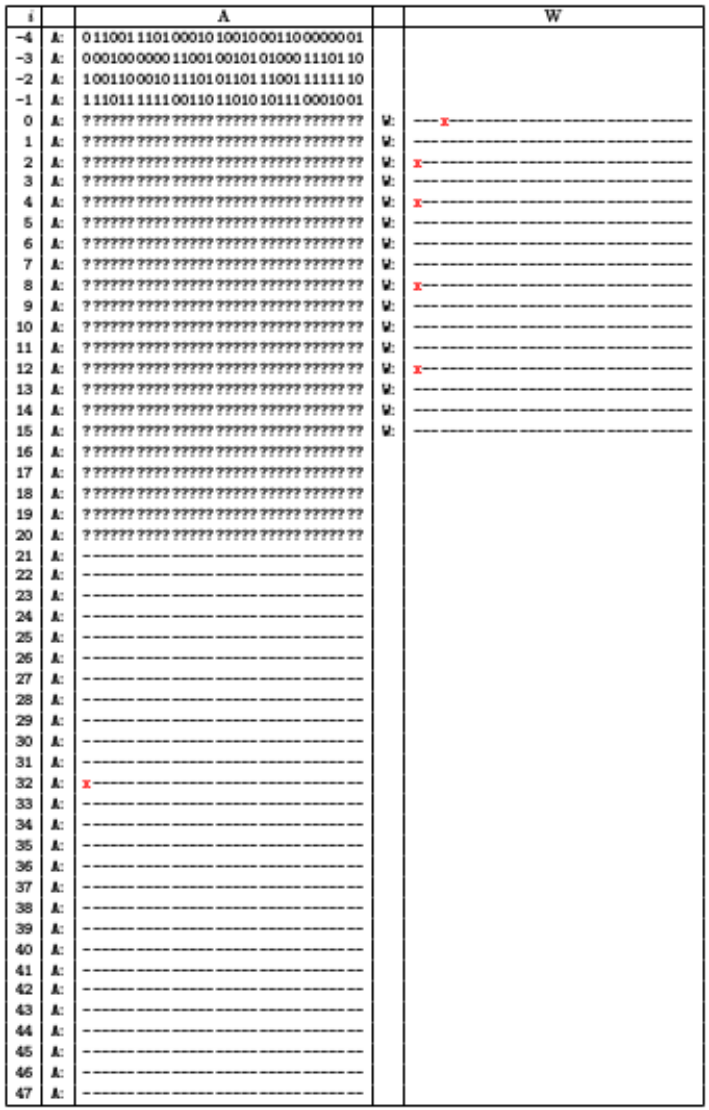
Testcase C [03]

Words in rounds 0–20 completely undetermined.

Collision still given in round 32.

~ 18 minutes

MD4 testcases & results



i		A		W
−4	A:	0 11001 11010 00010 10010 00110 00000 01		
−3	A:	0 00100 0000 11001 00101 01000 11101 10		
−2	A:	1 00110 0010 11101 01101 11001 11111 10		
−1	A:	1 11011 1111 00110 11010 10111 0001 001		
0	A:	? ????? ???? ????? ????? ????? ????? ??	W:	---x----------
1	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
2	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
3	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
4	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
5	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
6	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
7	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
8	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
9	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
10	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
11	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
12	A:	? ????? ???? ????? ????? ????? ????? ??	W:	x----------
13	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
14	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
15	A:	? ????? ???? ????? ????? ????? ????? ??	W:	----------
16	A:	? ????? ???? ????? ????? ????? ????? ??		
17	A:	? ????? ???? ????? ????? ????? ????? ??		
18	A:	? ????? ???? ????? ????? ????? ????? ??		
19	A:	? ????? ???? ????? ????? ????? ????? ??		
20	A:	? ????? ???? ????? ????? ????? ????? ??		
21	A:	----------		
22	A:	----------		
23	A:	----------		
24	A:	----------		
25	A:	----------		
26	A:	----------		
27	A:	----------		
28	A:	----------		
29	A:	----------		
30	A:	----------		
31	A:	----------		
32	A:	x----------		
33	A:	----------		
34	A:	----------		
35	A:	----------		
36	A:	----------		
37	A:	----------		
38	A:	----------		
39	A:	----------		
40	A:	----------		
41	A:	----------		
42	A:	----------		
43	A:	----------		
44	A:	----------		
45	A:	----------		
46	A:	----------		
47	A:	----------		

Testcase C [03]
Words in rounds 0–20 completely undetermined.
Collision still given in round 32.

~ 18 minutes

Nice, but we want to attack SHA-256, which is much more difficult.

Tweaking SAT encoding

Definition. Given two CNFs A and B, they are called *equisatisfiable* iff A is satisfiable iff B.

CNF simplification is done to transform the CNF into a representation which improves the performance of the SAT solver.

satelite

cmsat

lingeling

minisat

Tweaking SAT encoding

Simplification reduces the problem size.

simplification	variables	percent of none	clauses	percent of none
none	48,704	100 %	253,984	100 %
cmsat	24,503	50 %	111,931	44 %
lingeling	48,704	100 %	106,626	42 %
minisat	20,895	43 %	118,236	47 %
satelite	27,495	56 %	153,262	60 %

for Testcase C

Tweaking SAT encoding

Simplification as preprocessing step does not significantly improve the runtime of SAT solvers.

solver	version	none	cmsat	lingeling	minisat	satelite
MiniSat	2.2.0	4,519	7,649	1,337	1,476	1,293
CryptoMiniSat	5	1,064	973	1,201	4,470	3,920
Lingeling	ats1	1,492	906	356	860	1,297
Treengeling	ats1	1,281	13,401	20,903	13,790	10,840
Plingeling	ats1	2,310	1,232	955	1,384	2,030

for Testcase C

Tweaking SAT encoding

Definition. *Differential description*

Boolean function `IF` returns the second argument, if the first is true, otherwise the third argument.

Differential behavior:

$(0,1,1) \implies 1 \qquad (0,0,0) \implies 0$

$$(\neg a \wedge b \wedge c) \implies r \iff a \vee \neg b \vee \neg c \vee r$$

$$(\neg a \wedge \neg b \wedge \neg c) \implies \neg r \iff a \vee b \vee c \vee \neg r$$

Tweaking SAT encoding

Idea. *Assigning false first*

Few differences are more likely to cancel out.
$\Longrightarrow$ Guess all difference variables *false* first.

Basic idea of differential cryptanalysis:
Assign all difference variables first.

Tweaking SAT encoding

Definition. *Preference variables*

Let Δx be the difference variable of pair (x, x'). We introduce a new Boolean variable x^* called *preference variable*. We add clause

$$x^* = (\Delta x \wedge x)$$

Assume x^* is assigned (Boolean false) first. Assume Δx is assigned first. Worked well in a previous, non-SAT tool.

SHA-256 testcases

i		A		E		W
-4	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-3	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-2	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-1	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
0	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
1	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
2	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
3	A:	x---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
4	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
5	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
6	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
7	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
8	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
9	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
10	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
11	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	?????????? ?????????? ?????????? ?????????? ?????????? ?????????? ??????????
12	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
13	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
14	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
15	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
16	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
17	A:	---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------

Testcase 18 [**05**]

SHA-256 testcases

i		A		E		W
-4	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-3	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-2	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-1	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
0	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
1	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
2	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
3	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
4	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
5	A:	x??? ????? ????? ????? ????? ????? ????? ?????	E:	? ????? ????? ????? ????? ????? ????? ??	W:	??? ????? ????? ????? ????? ????? ????? ?????
6	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ????? ????? ????? ????? ????? ??	W:	??? ????? ????? ????? ????? ????? ????? ?????
7	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ????? ????? ????? ????? ????? ??	W:	??? ????? ????? ????? ????? ????? ????? ?????
8	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ????? ????? ????? ????? ????? ??	W:	??? ????? ????? ????? ????? ????? ????? ?????
9	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ????? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
10	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
11	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
12	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
13	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	??? ????? ????? ????? ????? ????? ????? ?????
14	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
15	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
16	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
17	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
18	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
19	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------
20	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ----------

Testcase 21 **[05]**

SHA-256 testcases

i		A		E		W
-4	A:	----------	E:	----------	W:	
-3	A:	----------	E:	----------	W:	
-2	A:	----------	E:	----------	W:	
-1	A:	----------	E:	----------	W:	
0	A:	----------	E:	----------	W:	----------
1	A:	----------	E:	----------	W:	----------
2	A:	----------	E:	----------	W:	----------
3	A:	----------	E:	----------	W:	----------
4	A:	----------	E:	----------	W:	----------
5	A:	----------	E:	----------	W:	----------
6	A:	----------	E:	----------	W:	----------
7	A:	x?????????	E:	??????????	W:	??????????
8	A:	----------	E:	??????????	W:	??????????
9	A:	----------	E:	??????????	W:	----------
10	A:	----------	E:	??????????	W:	??????????
11	A:	----------	E:	??????????	W:	----------
12	A:	----------	E:	----------	W:	----------
13	A:	----------	E:	----------	W:	----------
14	A:	----------	E:	----------	W:	----------
15	A:	----------	E:	----------	W:	??????????
16	A:	----------	E:	----------	W:	----------
17	A:	----------	E:	----------	W:	----------
18	A:	----------	E:	----------	W:	----------
19	A:	----------	E:	----------	W:	----------
20	A:	----------	E:	----------	W:	----------
21	A:	----------	E:	----------	W:	----------
22	A:	----------	E:	----------	W:	----------

Testcase 23 [**05**]

SHA-256 testcases

i		A		E		W
-4	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-3	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-2	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
-1	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	
0	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
1	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
2	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
3	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
4	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
5	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
6	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
7	A:	x??? ????? ???? ????? ????? ????? ????? ????	E:	? ????? ???? ????? ????? ????? ????? ??	W:	??? ???? ????? ????? ????? ????? ?????
8	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ???? ????? ????? ????? ????? ??	W:	??? ???? ????? ????? ????? ????? ?????
9	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
10	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ???? ????? ????? ????? ????? ??	W:	??? ???? ????? ????? ????? ????? ?????
11	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	? ????? ???? ????? ????? ????? ????? ??	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
12	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
13	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
14	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
15	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	??? ???? ????? ????? ????? ????? ?????
16	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
17	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
18	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
19	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
20	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
21	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
22	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------
23	A:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	E:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------	W:	---------- ---------- ---------- ---------- ---------- ---------- ---------- ----------

Testcase 24 [**05**]

SHA-256 results

A differential description encoding improves the runtime compared to a missing differential description.

	CryptoMiniSat 5		lingeling-ats1	
testcase	**w/o dd**	**w/ dd**	**w/o dd**	**w/ dd**
MD4, C	1,064	231	798	53
SHA-256, 18	37	37	31	160
SHA-256, 21	⊤	7,855	28,621	5,513
SHA-256, 23	⊤	26,212	76,196	1,450
SHA-256, 24	⊤	37,194	78,017	1,235

SHA-256 results

Lingeling option `--phase=-1` improves its runtime for our testcases.

Option `--phase=-1` of lingeling is described as “default phase” set to –1 (negative), 0 (default, Jeroslow-Wang strategy [**06**]) or 1 (positive).

testcase	18		21		23		24	
phase	0	-1	0	-1	0	-1	0	-1
runtime	31	22	28,621	19,717	76,196	71,677	85,774	70,259

SHA-256 results

Evaluating difference variables false first improves the runtime.

testcase	C	18	21	23	24
basic approach (ats1)	798	31	28,621	76,196	85,774
diff-first-false (ats1o1)	652	29	27,599	59,312	66,052

SHA-256 results

Adding preference variables dramatically worsens performance.

testcase	A	B	C
CNF with diff-desc	11	133	155
pref variables added	8	50	62

SHA-256 results

Adding preference variables dramatically worsens performance.

testcase	A	B	C	18	21	23	24
CNF with diff-desc	11	133	155	49	2,282	1,314	2,632
pref variables added	8	50	62	⊤	⊤	⊤	⊤

Conclusion

- 1 very successful tweak (diff-desc)
- 2 promising tweaks
- 1 insignificant tweak (CNF simplification)
- 1 worsening tweak (preference variables)

We found full-round hash collisions in MD4.

We found a hash collision
in 24 rounds-reduced SHA-256.

References

01 Christophe De Cannière and Christian Rechberger.
"Finding SHA-1 Characteristics: General Results and Applications"

02 Florian Mendel, Tomislav Nad, Martin Schläffer.
"Improving Local Collisions: New Attacks on Reduced SHA-256"

03 Noboru Kunihiro, Kazuo Ohta, Yu Sasaki and Lei Wang.
"New message difference for MD4" (MD4 testcases)

04 Ilya Mironov and Lintao Zhang.
"Applications of SAT solvers to cryptanalysis of hash functions"

05 Alex Biryukov and Ivica Nikolić.
"Collisions for step-reduced SHA-256" (SHA-256 testcases)

06 Robert G. Jeroslow and Jinchang Wang.
"Solving Propositional Satisfiability Problems"

Silly walk image Leo Antunes **Knight image** Springfield Punx

どうもありがとうございました

Acknowledgements: Florian Mendel, Maria Eichlseder, Armin Biere, Roderick Bloem, Mate Soos, Martina, my parents and many others . . .

All resources available online at:

http://lukas-prokop.at/proj/megosat