

UNIVERSITY OF TECHNOLOGY, GRAZ

MASTER THESIS

---

# Differential cryptanalysis with SAT solvers

---

*Author:*

Lukas Prokop

*Supervisor:*

Maria Eichlseder  
Florian Mendel

*A thesis submitted in fulfillment of the requirements  
for the master's degree in Computer Science*

*at the*

Institute of Applied  
Information Processing and  
Communications

August 23, 2016







Lukas Prokop, BSc BSc

# **Differential cryptanalysis with SAT solvers**

## **MASTER'S THESIS**

to achieve the university degree of

Master of Science

Master's degree programme: Computer Science

submitted to

**Graz University of Technology**

Supervisor

Dipl.-Ing. Dr.techn., Florian Mendel

Institute of Applied Information Processing and Communications

Second advisor: Maria Eichlseder

Graz, June 2016

## **AFFIDAVIT**

I declare that I have authored this thesis independently, that I have not used other than the declared sources/resources, and that I have explicitly indicated all material which has been quoted either literally or by content from the sources used. The text document uploaded to TUGRAZonline is identical to the present master's thesis dissertation.

---

Date

---

Signature

# ABSTRACT

Hash functions are ubiquitous in the modern information age. They provide preimage, second preimage and collision resistance which are needed in a wide range of applications.

In August 2006, Wang et al. showed efficient attacks against several hash function designs including MD4, MD5, HAVAL-128 and RIPEMD. With these results differential cryptanalysis has been shown useful to break collision resistance in hash functions. Over the years advanced attacks based on those differential approaches have been developed.

To find collisions like Wang et al., a cryptanalyst needs to specify a differential characteristic. Looking at the differential behavior of the underlying operations of the hash algorithm shows how differential values propagate in the algorithm. The goal is to find a differential characteristic whose differences cancel out in the output. Once such a differential characteristic was discovered, in a second step the actual values for those differences are defined yielding an actual hash collision.

Finding a differential characteristic can be a cumbersome and tedious task. Whereas propagation can be automated using dedicated tools, finding an initial differential characteristic is a difficult task as it can be specified with arbitrary levels of granularity.

SAT solvers inherently implement both tasks. They consecutively propagate values which narrow the search space. The probability to find a satisfiable assignment increases if the narrowed search space has many satisfiable assignments. And finally the assignment reveals initial values. On the other hand, SAT solvers have no notion of differential values and therefore problem encoding becomes an important topic.

In this thesis we look at differential characteristics representing hash collisions and encode them as SAT problem. A SAT solver tells us whether this characteristic represents a valid hash state. We implemented a framework generating CNFs for these purposes and improved our CNF design to solve MD4 testcases as well as much more difficult SHA-256 testcases. Our greatest achievement was finding a MD4 full round hash collision and a SHA-256 hash collision over 27 rounds. Finally we also provide a small CNF analysis library to compare encoded problems with others.

**Keywords:** hash function, differential cryptanalysis, differential characteristic, MD4, SHA-256, collision resistance, satisfiability, SAT solver

## ACKNOWLEDGEMENTS

First of all I would like to thank my academic advisor for his continuous support during this project. Many hours of debugging were involved in writing this master thesis project, but thanks to Florian Mendel, this project came to a release with nice results. Also thanks for continuously reviewing this document.

I would also like to thank Maria Eichlseder for her great support. Her unique way to ask questions brought me back on track several times. Mate Soos supported me during my bachelor thesis with SAT related issues and his support continued with this master thesis in private conversations.

Also thanks to Roderick Bloem and Armin Biere who organized a meeting one year before submitting this work defining the main approaches involved in this thesis. Armin Biere released custom lingeling versions for us, which allowed us to influence the guessing strategy in lingeling. He also shared his thoughts about our testcases with us.

And finally I am grateful for the support by Martina, who also supported me during good and bad days with this thesis, and my parents which provided a prosperous environment to me to be able to stand where I am today.

Thank you.

どもありがとうございました。

All source codes are available at [lukas-prokop.at/proj/megosat](https://lukas-prokop.at/proj/megosat) and published under terms and conditions of Free/Libre Open Source Software. This document was printed with Lua<sup>A</sup>TeX in the Linux Libertine typeface.

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Overview . . . . .	1
1.2	Thesis Outline . . . . .	2
<b>2</b>	<b>Hash algorithms</b>	<b>3</b>
2.1	Preliminaries Redux . . . . .	3
2.1.1	Merkle-Damgård designs . . . . .	4
2.1.2	Padding and length extension attacks . . . . .	4
2.1.3	Example usage . . . . .	5
2.2	MD4 . . . . .	5
2.3	SHA-256 . . . . .	7
<b>3</b>	<b>Differential cryptanalysis</b>	<b>11</b>
3.1	Motivation . . . . .	11
3.2	Fundamentals . . . . .	12
3.3	Differential notation . . . . .	14
3.4	A simple addition example . . . . .	16
3.5	Differential characteristics in action . . . . .	16
<b>4</b>	<b>Satisfiability</b>	<b>21</b>
4.1	Basic notation and definitions . . . . .	21
4.1.1	Computational considerations . . . . .	23
4.1.2	SAT competitions . . . . .	23

4.2	The DIMACS de-facto standard . . . . .	24
4.3	Terminology . . . . .	25
4.4	Basic SAT solving techniques . . . . .	26
4.4.1	Boolean constraint propagation (BCP) . . . . .	26
4.4.2	Watched literals . . . . .	26
4.4.3	Remark . . . . .	27
4.5	SAT solvers in use . . . . .	27
<b>5</b>	<b>SAT features</b>	<b>31</b>
5.1	Definition . . . . .	32
5.2	Related work . . . . .	32
5.3	Statistical features . . . . .	33
5.4	Suggested SAT features . . . . .	34
5.5	Evaluation efficiency . . . . .	36
5.6	CNF dataset . . . . .	36
5.7	The average SAT problem . . . . .	37
5.8	Benford's law in CNF files . . . . .	38
<b>6</b>	<b>Problem encoding</b>	<b>41</b>
6.1	Basic approach . . . . .	41
6.2	algotocnf . . . . .	42
6.2.1	Two instances and its difference . . . . .	43
6.2.2	Adding the differential description . . . . .	44
6.2.3	Evaluating difference variables first . . . . .	46
6.2.4	A light-weight approach . . . . .	46
6.2.5	Influencing the evaluation order . . . . .	46
<b>7</b>	<b>Results</b>	<b>49</b>
7.1	Evaluating SAT features . . . . .	49
7.2	Finding hash collisions . . . . .	53



<i>CONTENTS</i>	ix
7.2.1 Attacking MD4 . . . . .	53
7.2.2 Improvements with differential description . . . . .	55
7.2.3 Modifying the guessing strategy . . . . .	55
7.3 Related work . . . . .	56
7.4 Conclusion . . . . .	56
7.5 Contributions . . . . .	56
<b>8 Summary and Future Work</b>	<b>61</b>
8.1 Summary of results . . . . .	61
8.2 Future work . . . . .	61
<b>Appendices</b>	<b>63</b>
<b>A Hardware setup</b>	<b>65</b>
<b>B Testcases</b>	<b>67</b>
B.1 MD4 testcase A . . . . .	67
B.2 MD4 testcase B . . . . .	67
B.3 MD4 testcase C . . . . .	67
B.4 SHA-256 testcase 18 rounds . . . . .	68
B.5 SHA-256 testcase 21 rounds . . . . .	68
B.6 SHA-256 testcase 23 rounds . . . . .	68
B.7 SHA-256 testcase 24 rounds . . . . .	68
<b>C Runtimes retrieved</b>	<b>75</b>





## Chapter 1

# Introduction

### 1.1 Overview

Hash functions are used as cryptographic primitives in many applications and protocols. They take an arbitrary input message and provide a hash value. Input message and hash value are considered as byte strings in a particular encoding. The hash value is of fixed length and satisfies several properties which make it useful in a variety of applications.

In this thesis we will consider the hash algorithms MD<sub>4</sub> and SHA-256. They use basic arithmetic functions like addition and bit-level functions such as XOR to transform an input to a hash value. We use a bit vector as input to this implementation and all operations applied to this bit vector will be represented as clauses of a SAT problem. Additionally we represent differential characteristics of hash collisions as SAT problem. If and only if satisfiability is given, the particular differential state is achievable using two different inputs leading to the same output. As far as SAT solvers return an actual model satisfying that state, we get an actual hash collision which can be verified and visualized. If the internal state of the hash algorithm is too large, the attack can be computationally simplified by modelling only a subset of steps of the hash algorithm or changing the modelled differential path.

Based on experience with these kind of problems with previous non-SAT-based tools we aim to apply best practices to a satisfiability setting. We will discuss which SAT techniques lead to best performance characteristics for our MD<sub>4</sub> and SHA-256 testcases.

## 1.2 Thesis Outline

This thesis is organized as follows:

**In Chapter 1** we briefly introduce basic subjects of this thesis. We explain our high-level goal involving hash functions and SAT solvers.

**In Chapter 2** we introduce the MD4 and SHA-256 hash functions. Certain design decisions imply certain properties which can be used in differential cryptanalysis. We discuss those decisions in this chapter after a formal definition of the function itself. Beginning with this chapter we develop a theoretical notion of our tools.

**In Chapter 3** we discuss approaches of differential cryptanalysis. We start off with work done by Wang, et al. and followingly introduce differential notation to simplify representation of differential states. This way we can easily dump hash collisions.

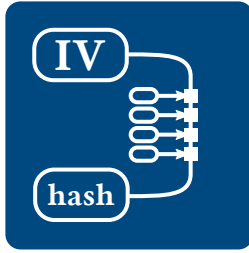
**In Chapter 4** we discuss SAT solving. We give a brief overview over used SAT solvers and discuss how we can speed up SAT solvers for cryptographic problems.

**In Chapter 5** we define SAT features which help us to classify SAT problems. This is a small subproject we did to look at properties of resulting DIMACS CNF files.

**In Chapter 6** we discuss how we represent a problem (i.e. the hash function and a differential characteristic) as SAT problem. This ultimately allows us to solve the problem using a SAT solver.

**In Chapter 7** we show data as result of our work. Runtimes are the main part of this chapter, but also results of the SAT features project are presented.

**In Chapter 8** we suggest future work based on our results.



## Chapter 2

# Hash algorithms

In this chapter we will define hash functions and their desired security properties. Followingly we look at SHA-256 and MD4 as established hash functions. MD4 unlike SHA-256 is practically broken but has a comparably small internal state. It therefore allows a good starting point to devise our attacks. In a next step we scaled up to SHA-256 which has an internal state size at least twice as large. In Chapter 6 we will represent them with Boolean algebra to make it possible to reason about states in those hash functions using SAT solvers.

### 2.1 Preliminaries Redux

#### Definition 2.1 (Hash function)

A *hash function* is a mapping  $h : X \rightarrow Y$  with  $X = \{0, 1\}^*$  and  $Y = \{0, 1\}^n$  for some fixed  $n \in \mathbb{N}_{\geq 1}$ .

- Let  $x \in X$ , then  $h(x)$  is called *hash value of  $x$* .
- Let  $h(x) = y \in Y$ , then  $x$  is called *preimage of  $y$* .

Hash functions are considered as cryptographic primitives used as building blocks in cryptographic protocols. A hash function has to satisfy the following security requirements:

#### Definition 2.2 (Preimage resistance)

Given  $y \in Y$ , a hash function  $h$  is *preimage resistant* iff it is computationally infeasible to find  $x \in X$  such that  $h(x) = y$ .

**Definition 2.3 (Second-preimage resistance)**

Given  $x \in X$ , a hash function  $h$  is *second-preimage resistant* iff it is computationally infeasible to find  $x_2 \in X$  with  $x \neq x_2$  such that  $h(x) = h(x_2)$ .  $x_2$  is called *second preimage*.

**Definition 2.4 (Collision resistance)**

A hash function  $h$  is *collision resistant* iff it is computationally infeasible to find any two  $x \in X$  and  $x_2 \in X$  with  $x \neq x_2$  such that  $h(x) = h(x_2)$ . Tuple  $(x, x_2)$  is called *collision*.

As far as hash functions accept input strings of arbitrary length, but return a fixed size output string, existence of collisions is unavoidable [30]. However, good hash functions make it very difficult to find collisions or preimages.

Any digital data can be hashed (i.e. used as input to a hash function) by considering it in binary representation. The format or encoding is not part of the hash function's specification.

**2.1.1 Merkle-Damgård designs**

The Merkle-Damgård design is a particular design of hash functions providing the following security guarantee:

**Definition 2.5 (Collision resistance inheritance)**

Let  $F_0$  be a collision resistant compression function. A hash function in Merkle-Damgård design is collision resistant if  $F_0$  is collision resistant.

This motivates thorough research of collisions in compression functions. The design was found independently by Ralph C. Merkle and Ivan B. Damgård. It was described by Merkle in his PhD thesis [17, p. 13–15] and followingly used in popular hash functions such as MD4, MD5 and the SHA2 hash function family. The single-pipe design works as follows:

1. Split the input into blocks of uniform block size. If necessary, apply padding to the last block to achieve full block size.
2. Compression function  $F_0$  is applied iteratively using the output  $y_{i-1}$  of the previous iteration and the next input block  $x_i$ , denoted  $y_i = F_0(y_{i-1}, x_i)$ .
3. An optional postprocessing function is applied.

**2.1.2 Padding and length extension attacks**

Hash functions of single-piped Merkle-Damgård design inherently suffer from length extension attacks. MD4 and SHA-256 apply padding to their input to

normalize their input size to a multiple of its block size. The compression function is applied afterwards. This design is vulnerable to length extensions.

Consider some collision  $(x_0, x_1)$  with  $F_0(x_0) = y = F_0(x_1)$  where  $x_0$  and  $x_1$  have a size of one block. Let  $p$  be a suffix with size of one block. Then also  $(x_0 \parallel p, x_1 \parallel p)$  (where  $\parallel$  denotes concatenation) represents a collision in single-piped Merkle-Damgård designs, because it holds that:

$$F_0(F_0(x_0), p) = F_0(F_0(x_1), p) \iff F_0(y, p) = F_0(y, p)$$

Hence  $(x_0 \parallel p, x_1 \parallel p)$  is a collision as well. As far as  $F_0$  is applied recursively to every block,  $p$  can be of arbitrary size and  $(x_0, x_1)$  can be of arbitrary uniform size.

Because of this vulnerability, cryptanalysts only need to find a collision in compression functions. In our tests will only consider input of one block and padding will be neglected due to this vulnerability.

### 2.1.3 Example usage

One example showing the use of hash functions as primitives are JSON Web Tokens (JWT) specified in RFC 7519 [15]. Its application allows web developers to represent claims to be transferred between two parties.

Section 8 defines implementation requirements and refers to RFC 7518 [10], which specifies cryptographic algorithms such as “HMAC SHA-256” to be implemented. It is (besides “none”) the only required signature and MAC algorithm.

## 2.2 MD4

MD4 is a cryptographic hash function originally described in RFC 1186 [26], updated in RFC 1320 [27] and declared obsolete by RFC 6150 [33]. It was invented by Ronald Rivest in 1990 with properties given in Table 2.1. In 1995 [5] successful full-round attacks have been found to break collision resistance. Followingly preimage and second-preimage resistance in MD4 have been broken as well. Some of those attacks are described in [28] and [20]. We derived a Python 3 implementation based on a Python 2 implementation and made it available on github [24].

block size	512 bits	namely variable block in RFC 1320 [27]
digest size	128 bits	as per Section 3.5 in RFC 1320 [27]
internal state size	128 bits	namely variables $A$ , $B$ , $C$ and $D$
word size	32 bits	as per Section 2 in RFC 1320 [27]

TABLE 2.1: MD4 hash algorithm properties

MD4 uses three auxiliary Boolean functions:

**Definition 2.6**

The Boolean IF function is defined as follows: If the first argument is true, the second argument is returned. Otherwise the third argument is returned.

The Boolean MAJ function returns true if the number of Boolean values true in arguments is at least 2. The Boolean XOR function returns true if the number of Boolean values true in arguments is odd.

Using the logical operators  $\wedge$  (AND),  $\vee$  (OR) and  $\neg$  (NEG) we can define them as (see Section 4.1 for a thorough discussion of these operators):

$$\text{IF}(X, Y, Z) := (X \wedge Y) \vee (\neg X \wedge Z) \quad (2.1)$$

$$\text{MAJ}(X, Y, Z) := (X \wedge Y) \vee (X \wedge Z) \vee (Y \wedge Z) \quad (2.2)$$

$$\begin{aligned} \text{XOR}(X, Y, Z) &:= (X \wedge \neg Y \wedge \neg Z) \vee (\neg X \wedge Y \wedge \neg Z) \\ &\quad \vee (\neg X \wedge \neg Y \wedge Z) \vee (X \wedge Y \wedge Z) \\ &:= (X \oplus Y \oplus Z) \end{aligned} \quad (2.3)$$

In the following, a brief overview over MD4's design is given.

**Padding and length extension.** First of all, padding is applied. A single bit 1 is appended to the input. As long as the input does not reach a length congruent 448 modulo 512, bit 0 is appended. Followingly, length appending takes place. Represent the length of the input (without the previous modifications) in binary and take its first 64 less significant bits. Append those 64 bits to the input.

**Initialization.** The message is split into 512-bit blocks (i.e. 16 32-bit words). Four state variables  $A_i$  with  $-4 \leq i < 0$  are initialized with these hexadecimal values:

$$[A_{-4}] \ 01234567 \quad [A_{-1}] \ 89abcdef \quad [A_{-2}] \ fedcba98 \quad [A_{-3}] \ 76543210$$

**Round function with state variable updates.** The round function is applied in three rounds with 16 iterations. In every iteration values  $A_{-1}$ ,  $A_{-2}$  and  $A_{-3}$  are taken as arguments to function  $F$ . Function  $F$  is IF in round 1, followed by MAJ for round 2 and XOR for the final round 3. The resulting value is added to  $A_{-1}$ , current message block  $M$  and constant  $X$ . Finally the 32-bit sum will be left-rotated by  $p$  positions. Left rotation is formally defined in Definition 2.7. The values of  $X$  and  $p$  are defined as follows:

Let  $i$  be the iteration counter between 1 and 16 and  $r$  the round between 1 and 3. Then  $X$  takes the value of the  $i$ -th column and  $r$ -th row of matrix  $C$ .  $p$  takes the value of row  $r$  and column  $i \bmod 4$  of matrix  $P$ .



$$C = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 \\ 0 & 4 & 8 & 12 & 1 & 5 & 9 & 13 & 2 & 6 & 10 & 14 & 3 & 7 & 11 & 15 \\ 0 & 8 & 4 & 12 & 2 & 10 & 6 & 14 & 1 & 9 & 5 & 13 & 3 & 11 & 7 & 15 \end{pmatrix}$$

$$P = \begin{pmatrix} 3 & 7 & 9 & 11 \\ 3 & 5 & 9 & 13 \\ 3 & 9 & 11 & 15 \end{pmatrix}$$

This round function design is visualized in Figure 2.1.

### 2.3 SHA-256

SHA-256 is a hash function from the SHA-2 family designed by the National Security Agency (NSA) and published in 2001 [9]. It uses a Merkle-Damgård construction with a Davies-Meyer compression function. The best known preimage attack was found in 2011 and breaks preimage resistance for 52 rounds [11]. The best known collision attack breaks collision resistance for 31 rounds of SHA-256 [16] and pseudo-collision resistance for 46 rounds [12].

block size	512 bits	as per Section 1 of the standard [9]
digest size	256 bits	mentioned as Message Digest size [9]
internal state size	256 bits	as per Section 1 of the standard [9]
word size	32 bits	as per Section 1 of the standard [9]

TABLE 2.2: SHA-256 hash algorithm properties

#### Definition 2.7 (Shifts, rotations and a notational remark)

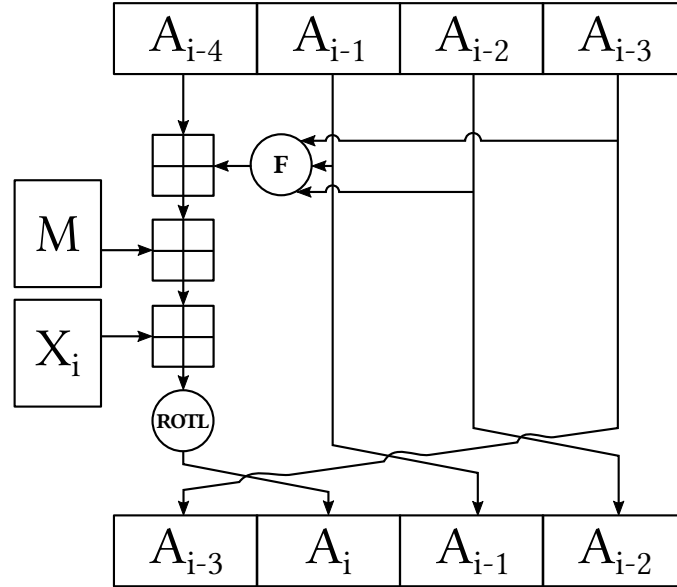
Consider a 32-bit word  $X$  with 32 binary values  $b_i$  with  $0 \leq i \leq 31$ .  $b_0$  refers to the least significant bit. Shifting ( $\ll$  and  $\gg$ ) and rotation ( $\lll$  and  $\ggg$ ) creates a new 32-bit word  $Y$  with 32 binary values  $a_i$ . We define the following notations:

$$Y := X \ll n \iff a_i := b_{i-n} \text{ if } 0 \leq i - n < 32 \text{ and } 0 \text{ otherwise}$$

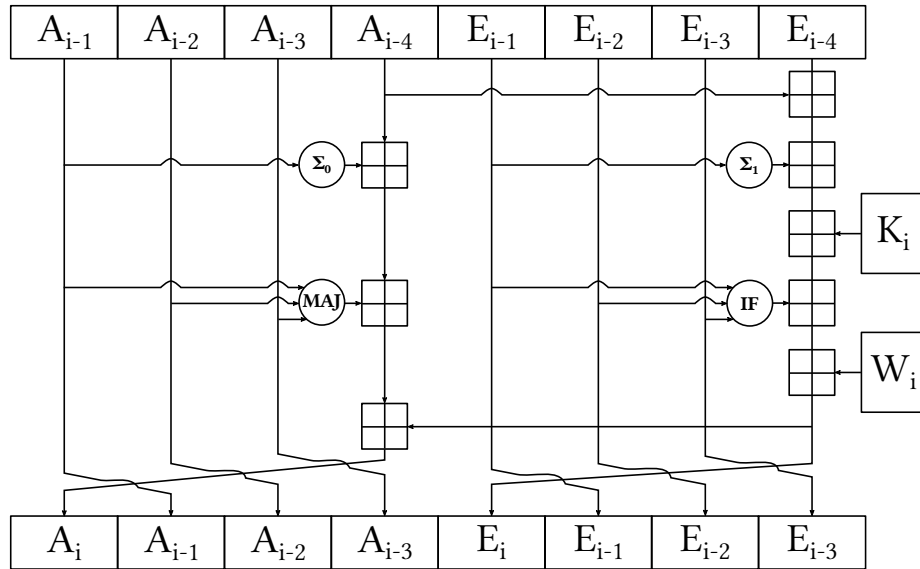
$$Y := X \gg n \iff a_i := b_{i+n} \text{ if } 0 \leq i + n < 32 \text{ and } 0 \text{ otherwise}$$

$$Y := X \lll n \iff a_i := b_{i-n \bmod 32} \text{ as used in MD}_4$$

$$Y := X \ggg n \iff a_i := b_{i+n \bmod 32}$$



**Figure 2.1:** MD4 round function updating state variables



**Figure 2.2:** SHA-256 round function as characterized in [6]

Besides MD4's MAJ and IF, another four auxiliary functions are defined. Recognize that  $\oplus$  denotes the XOR function whereas  $\boxplus$  denotes 32-bit addition.

$$\begin{aligned}\Sigma_0(X) &:= (X \ggg 2) \oplus (X \ggg 13) \oplus (X \ggg 22) \\ \Sigma_1(X) &:= (X \ggg 6) \oplus (X \ggg 11) \oplus (X \ggg 25) \\ \sigma_0(X) &:= (X \ggg 7) \oplus (X \ggg 18) \oplus (X \gg 3) \\ \sigma_1(X) &:= (X \ggg 17) \oplus (X \ggg 19) \oplus (X \gg 10)\end{aligned}$$

**Padding and length extension.** The padding and length extension scheme of MD4 is used also in SHA-256. Append bit 1 and followed by a sequence of bit 0 until the message reaches a length of 448 modulo 512 bits. Afterwards the first 64 bits of the binary representation of the original input are appended.

**Initialization.** In a similar manner to MD4, initialization of internal state variables (called “working variables” in [9, Section 6.2.2]) takes place before running the round function. The eight state variables are initialized with the following hexadecimal values:

$$\begin{aligned}A_{-1} &= 6a09e667 & A_{-2} &= bb67ae85 & A_{-3} &= 3c6ef372 & A_{-4} &= a54ff53a \\ E_{-1} &= 510e527f & E_{-2} &= 9b05688c & E_{-3} &= 1f83d9ab & E_{-4} &= 5be0cd19\end{aligned}$$

Furthermore SHA-256 uses 64 constant values in its round function. We initialize step constants  $K_i$  for  $0 \leq i < 64$  with the following hexadecimal values (which must be read left to right and top to bottom):

428a2f98	71374491	b5c0fbcf	e9b5dba5	3956c25b	59f111f1
923f82a4	ab1c5ed5	d807aa98	12835b01	243185be	550c7dc3
72be5d74	80deb1fe	9bdc06a7	c19bf174	e49b69c1	efbe4786
0fc19dc6	240ca1cc	2de92c6f	4a7484aa	5cb0a9dc	76f988da
983e5152	a831c66d	b00327c8	bf597fc7	c6e00bf3	d5a79147
06ca6351	14292967	27b70a85	2e1b2138	4d2c6dfc	53380d13
650a7354	766a0abb	81c2c92e	92722c85	a2bfe8a1	a81a664b
c24b8b70	c76c51a3	d192e819	d6990624	f40e3585	106aa070
19a4c116	1e376c08	2748774c	34b0bcb5	391c0cb3	4ed8aa4a
5b9cca4f	682e6ff3	748f82ee	78a5636f	84c87814	8cc70208
90bffffa	a4506ceb	bef9a3f7	c67178f2		

**Precomputation of W.** Let  $W_i$  for  $0 \leq i < 16$  be the sixteen 32-bit words of the padded input message. Then compute  $W_i$  for  $16 \leq i < 64$  the following way:

$$W_i := \sigma_1(W_{i-2}) + W_{i-7} + \sigma_0(W_{i-15}) + W_{i-16}$$

**Round function.** For every block of 512 bits, the round function is applied. The eight state variables are updated iteratively for  $i$  from 0 to 63.

$$\begin{aligned}E_i &:= A_{i-4} + E_{i-4} + \Sigma_1(E_{i-1}) + \text{IF}(E_{i-1}, E_{i-2}, E_{i-3}) + K_i + W_i \\ A_i &:= E_i - A_{i-4} + \Sigma_0(A_{i-1}) + \text{MAJ}(A_{i-1}, A_{i-2}, A_{i-3})\end{aligned}$$

$W_i$  and  $K_i$  refer to the previously initialized values.

**Computation of intermediate hash values.** Intermediate hash values for the Davies-Meyer construction are initialized with the following values:

$$\begin{array}{llll} H_0^{(0)} := A_{-1} & H_1^{(0)} := A_{-2} & H_2^{(0)} := A_{-3} & H_3^{(0)} := A_{-4} \\ H_4^{(i)} := E_{-1} & H_5^{(i)} := E_{-2} & H_6^{(i)} := E_{-3} & H_7^{(i)} := E_{-4} \end{array}$$

Every block creates its own  $E_i$  and  $A_i$  values for  $60 \leq i < 64$ . These are used to compute the next intermediate values:

$$\begin{array}{ll} H_0^{(j)} := A_{63} + H_0^{(i-1)} & H_4^{(j)} := E_{63} + H_4^{(i-1)} \\ H_1^{(j)} := A_{62} + H_1^{(i-1)} & H_5^{(j)} := E_{62} + H_5^{(i-1)} \\ H_2^{(j)} := A_{61} + H_2^{(i-1)} & H_6^{(j)} := E_{61} + H_6^{(i-1)} \\ H_3^{(j)} := A_{60} + H_3^{(i-1)} & H_7^{(j)} := E_{60} + H_7^{(i-1)} \end{array}$$

**Finalization.** The final hash digest of size 256 bits is provided as

$$H_0^{(N)} \parallel H_1^{(N)} \parallel H_2^{(N)} \parallel H_3^{(N)} \parallel H_4^{(N)} \parallel H_5^{(N)} \parallel H_6^{(N)} \parallel H_7^{(N)}$$

where  $N$  denotes the index of the last block and operator  $\parallel$  denotes concatenation. Hence  $H_0^{(N)}$  are the four least significant bytes of the digest.



“JUST BECAUSE IT’S AUTOMATIC DOESN’T  
MEAN IT WORKS.”  
—Daniel J. Bernstein

## Chapter 3

# Differential cryptanalysis

In Chapter 2 we defined two hash functions. In this chapter we consider such functions from a differential perspective. Differential considerations will turn out to yield successful collision attacks on hash functions. We introduce a notation to easily represent differential characteristics.

### 3.1 Motivation

In August 2004, Wang et al. published results at Crypto’04 [34] which revealed that MD4, MD5, HAVAL-128 and RIPEMD can be broken practically using differential cryptanalysis. Their work is based on preliminary work by Hans Dobbertin [5]. On an IBM P690 machine, an MD5 collision can be computed in about one hour using this approach. Collisions for HAVAL-128, MD4 and RIPEMD were found as well. Patrick Stach’s `md4coll.c` program [32] implements Wang’s approach and can find MD4 collisions in few seconds on my Thinkpad x220 setup specified in [Appendix A](#).

Let  $n$  denote the digest size, i.e. the size of the hash value  $h(x)$  in bits. Due to the birthday paradox, a collision attack has a generic complexity of  $2^{n/2}$  whereas preimage and second preimage attacks have generic complexities of  $2^n$ . In other words it is computationally easier to find any two colliding hash values than the preimage or second preimage for a given hash value.

Following results by Wang et al., differential cryptanalysis was shown as powerful tool for cryptanalysis of hash algorithms. This thesis applies those ideas to satisfiability approaches.

Message 1			
4d7a9c83	<b>d6cb927a</b>	<b>29d5a578</b>	57a7a5ee
de748a3c	dcc366b3	b683a020	3b2a5d9f
c69d71b3	f9e99198	d79f805e	a63bb2e8
<b>45dc8e31</b>	97e31fe5	2794bf08	b9e8c3e9
Message 2			
4d7a9c83	<b>56cb927a</b>	<b>b9d5a578</b>	57a7a5ee
de748a3c	dcc366b3	b683a020	3b2a5d9f
c69d71b3	f9e99198	d79f805e	a63bb2e8
<b>45dd8e31</b>	97e31fe5	2794bf08	b9e8c3e9
Hash value of Message 1 and Message 2			
5f5c1a0d	71b36046	1b5435da	9bod807a

TABLE 3.1: One of two MD4 hash collisions provided in [34]. A message represents one block of 512 bits. Values are given in hexadecimal, message words are enumerated from left to right, top to bottom. Differences are highlighted in bold for illustration purposes. For comparison the first bits of Message 1 are 11000001... and the last bits are ...10011101.

## 3.2 Fundamentals

### Definition 3.1 (*Hash collision*)

Given a hash function  $h$ , a hash collision is a pair  $(x_1, x_2)$  with  $x_1 \neq x_2$  such that  $h(x_1) = h(x_2)$ .

Pseudo-collisions are also often considered when attacking hash functions. A *pseudo collision* is given if a hash collision can be found for a given hash function, but the initial vectors (IV) can be chosen arbitrarily.

Hash algorithms consume input values as blocks of bits. As far as the length of the input must not conform to the block size, padding is applied. Now consider such a block of input values and another copy of it. We use those two blocks as inputs for two hash algorithm instances, but provide slight modifications in few bits. Differential cryptanalysis is based on the idea to consider those execution states and tracing those difference to learn about the propagation of message differences. Compare this setup with Figure 3.1.

At the very beginning only the few defined differences are given. But as the hash algorithm progresses in computation, differences are propagated to more and more bits. Most likely the final value will differ in many bits, because of a desirable hash algorithm property called *avalanche effect*. A small difference in the input should lead to a significant difference in the output (i.e. visually recognizable).

Visualizing those differences helps the cryptanalyst to find modifications yielding a small number of differences in the evaluation state. The propagation of



**Figure 3.1:** Common attack setting for a collision attack: Hash function  $f$  is applied to two inputs  $M$  and  $M^*$  which differ by some predefined bits.  $\Delta M$  describes the difference between these values. A hash collision is given if and only if output values  $C$  and  $C^*$  show the same value. In differential cryptanalysis we observe the differences between two instances applying function  $f$  to inputs  $M$  and  $M^*$ .

differences in a particular hash algorithm is called *differential path*. Empirical results in differential cryptanalysis indicate that sparse paths are desirable, because it is easier to cancel out few differences in the output compared to many differences. The cryptanalyst consecutively modifies the input values to eventually receive a collision in the output value.

### Definition 3.2

The propagation of differences in a particular function is called *differential path*. The complete differential state during a computation is called *differential characteristic*.

### Theorem 3.1

Assuming the number of differences in a differential path is small, this path is expected to result in a hash collision with higher probability.

bit	binary	hexadecimal representation / differential notation
$x_0$	d6cb927a	11010110110010111001001001111010
$x_1$	29d5a578	001010011101010101001010111000
$x_2$	45dc8e31	01000101110111001000111000110001
$x_0^*$	56cb927a	01010110110010111001001001111010
$x_1^*$	b9d5a578	101110011101010101001010111000
$x_2^*$	45dd8e31	01000101110111011000111000110001
$\Delta x$		u1010110110010111001001001111010 n01n100111010101010010101111000 010001011101110n1000111000110001

TABLE 3.2: The three words different between Message 1 and Message 2 of the original MD4 hash collision by Wang et al. The last three lines show how differences can be written down using bit conditions. As far as 4 symbols are not from the set  $\{0, 1\}$  it holds that the messages differ by 4 bits.

### 3.3 Differential notation

Differential notation helps us to visualize differential characteristics by defining so-called *generalized bit conditions*. It was introduced by Christian Rechberger and Christophe de Cannière in 2006 [2, Section 3.2], inspired by *signed differences* by Wang et al. and is shown in Table 3.3.

Consider two hash algorithm instances. Let  $x_i$  be some bit from the first instance and let  $x_i^*$  be the corresponding bit from the second instance. Differences are computed using a XOR and commonly denoted as  $\Delta x = x_i \oplus x_i^*$ . Bit conditions allow us to encode possible relations between bits  $x_i$  and  $x_i^*$ .

For example, let us take a look at the original Wang et al. hash collision in MD4 provided in Table 3.1. We extract all values with differences and represent them using differential notation. This gives us Table 3.2.

The following properties hold for bit conditions:

- If  $x_i = x_i^*$  holds and some value is known,  $\{0, 1\}$  contains its bit condition.
- If  $x_i \neq x_i^*$  holds and some value is known,  $\{u, n\}$  contains its bit condition.
- If  $x_i = x_i^*$  holds and the values are unknown, its bit condition is  $-$ .
- If  $x_i \neq x_i^*$  holds and the values are unknown, its bit condition is  $x$ .

Applying this notation to hash collisions means that arbitrary bit conditions (except for  $\#$ ) can be specified for the input values. In one of the intermediate iterations, we enforce a difference using one of the bit conditions  $\{u, n, x\}$ . This excludes trivial solutions with no differences from the set of possible solutions. And the final values need to lack differences thus are represented using a dash  $-$ .



$(x_i, x_i^*)$	(0, 0)	(1, 0)	(0, 1)	(1, 1)	$(x_i, x_i^*)$	(0, 0)	(1, 0)	(0, 1)	(1, 1)
?	✓	✓	✓	✓	3	✓	✓		
-	✓			✓	5	✓		✓	
x		✓	✓		7	✓	✓	✓	
0	✓				A		✓		✓
u		✓			B	✓	✓		✓
n			✓		C			✓	✓
1				✓	D	✓		✓	✓
#					E		✓	✓	✓

TABLE 3.3: Differential notation as introduced in [2]. The left-most column specifies a symbol called “bit condition” and right-side columns indicate which bit configurations are possible for two given bits  $x_i$  and  $x_i^*$ .

$\Delta x$	conjunctive normal form	$\Delta x$	conjunctive normal form
#	$(x) \wedge (\neg x)$	1	$(x) \wedge (x^*)$
0	$(\neg x) \wedge (\neg x^*)$	-	$\neg(x \oplus x^*)$
u	$(x) \wedge (\neg x^*)$	A	$(x)$
3	$(\neg x^*)$	B	$(x \vee \neg x^*)$
n	$(\neg x) \wedge (x^*)$	C	$(x^*)$
5	$(\neg x)$	D	$(\neg x \vee x^*)$
x	$(x \oplus x^*)$	E	$(x \vee x^*)$
7	$(\neg x \vee \neg x^*)$	?	

TABLE 3.4: All bit conditions represented as CNF using two Boolean variables  $x$  and  $x^*$  to represent two bits.

### 3.4 A simple addition example

Using this notation, we can now reason about the behavior of functions on differential values. We start with 1-bit addition as most basic exercise to the reader. Consider a matrix with two input rows and one output row. The values of the first two rows are added such that the bit difference at the third row is created.

Figure 3.5 illustrates this example. Remember that symbols such as  $-$  and  $\emptyset$  underlie semantics defined in Table 3.3. It is also interesting to see how propagation of values can work. In Figure 3.6 we see how an underspecified value  $?$  can be strengthened once we have checked which values can be taken. Recognize that the system is constrained by the function in use and the definition of the differential symbols.

Finally we can extend our testcases to 4 bits and retrieve testcases such as Table 3.7 and 3.8.

### 3.5 Differential characteristics in action

In the previous section we illustrated how propagation with differential values works and how differential characteristics are written down. It is always important to keep in mind which function the characteristic illustrates, because this is not documented with the characteristic.

Now consider MD4 as defined in Section 2.2. MD4 takes some input message (in our case limited to size of one block), the state variables are initialized and iteratively new  $A_i$  are computed.

Similarly, SHA-256 takes a message block  $M$  and initializes eight variables with an initial vector (IV). The remaining  $W_i$  are computed and iteratively, values  $A_i$  and  $E_i$  are computed.

Those values are structured in differential characteristics illustrated in Figure 3.2. Those layouts are used to specify our hash collisions we want to evaluate. Table 3.9 is also gives an application of the layout.

-	⇒	00	00	00	00	11	11	11	11
-		00	00	11	11	00	00	11	11
-		00	11	00	11	00	11	00	11

TABLE 3.5: A simple 1-bit addition example: On the left the differential characteristic is given. Two dashes, by definition, denote a missing difference in both arguments. The result of the addition most neither show a difference. This yields eight possible bit configurations where two values close to each other denote  $(M, M^*)$  of Figure 3.1. Due to the behavior of addition, we know that configurations 2, 3, 5 and 8 (from left to right) are invalid.

-	⇒	00	00	11	11
-		00	11	00	11
?		00	11	11	00

TABLE 3.6: Like Figure 3.5, but any difference value for the result bit is possible. As such we consider any possible bit configuration, but eventually recognize that only four bit configurations are consistent with the behavior of addition. Because all resulting configurations show no bit difference in the output bit, we can strengthen ? by replacing it with -. This illustrates how knowledge about differential states can be propagated.

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

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

TABLE 3.7: Testcases for 4-bit addition: The upper line shows valid differential characteristics for 4-bit addition whereas the lower line show invalid ones for 4-bit addition. The rows are conventionally named using capital letters.

A: ----	A: 7C-3	A: 0uCD
S: 0000	S: -3u?	S: ADC7

A: ---x	A: xxxx
S: 0000	S: 0000

TABLE 3.8: Differential characteristics for the SHA-2 Sigma function. The upper line shows valid states. The lower line shows invalid ones.

$i$	$VS_{i,0}$	$VS_{i,1}$	$VS_{i,2}$	$i$	$VS_{i,0}$	$VS_{i,1}$	$VS_{i,2}$
-4 A:	0110011101000101001000100000001			-4 A:	0110011101000101001000100000001		
-3 A:	00010000001100100101010001110110			-3 A:	00010000001100100101010001110110		
-2 A:	10011000101110101011100111111110			-2 A:	10011000101110101011100111111110		
-1 A:	11101111110011010101010110001001			-1 A:	11101111110011010101010110001001		
0 A:	01101011110101001110010000010010			0 A:	01101011110101001110010000010010		
1 A:	011010100100111111101100110001	W:	0100110101111010101110010000011	1 A:	011010100100111111101100110001	W:	0100110101111010101110010000011
2 A:	1010101010000000110101110010	W:	010101101100101110010010111010	2 A:	1010101010000000110101110010	W:	010101101100101110010010111010
3 A:	1010111000111010101001001010001	W:	010101110100111101001011101110	3 A:	1010111000111010101001001010001	W:	010101110100111101001011101110
4 A:	001011000100010101010111110010	W:	11011110011101001000101000111100	4 A:	00101100010001010101011110010	W:	11011110011101001000101000111100
5 A:	0001100110001010110100000001	W:	110111001100001101100101010011	5 A:	0001100110001010110100000001	W:	110111001100001101100101010011
6 A:	000110100100110001000001111010	W:	????????????????????????????????	6 A:	000110100100110001000001111010	W:	????????????????????????????????
7 A:	00101011100000010001001010000	W:	0011011001010101010111010011111	7 A:	00101011100000010001001010000	W:	0011011001010101010111010011111
8 A:	????????????????????????????????	W:	110001101001110101100011010011	8 A:	????????????????????????????????	W:	110001101001110101100011010011
9 A:	????????????????????????????????	W:	1111001111010011001000110011000	9 A:	????????????????????????????????	W:	1111001111010011001000110011000
10 A:	10-00100100000101????????????7110	W:	11010111001111100000001011110	10 A:	10-00100100000101????????????7110	W:	11010111001111100000001011110
11 A:	0100011010101010????????????7111	W:	1010011000110110100101101000	11 A:	0100011010101010????????????7111	W:	1010011000110110100101101000
12 A:	0010111001010111????????????7011	W:	010001011011100100011000110001	12 A:	0010111001010111????????????7011	W:	010001011011100100011000110001
13 A:	10-1-0100110001????????????7101	W:	100101111100011000111111100101	13 A:	10-1-0100110001????????????7101	W:	100101111100011000111111100101
14 A:	0000110101010011-----110	W:	001001111001010011111100001000	14 A:	0000110101010011-----110	W:	001001111001010011111100001000
15 A:	00011101010101-----100	W:	101100111101000110000111101001	15 A:	00011101010101-----100	W:	101100111101000110000111101001
16 A:	r00000010101010-----111			16 A:	r00000010101010-----111		
17 A:	0001111100011010-----110			17 A:	0001111100011010-----110		
18 A:	01010110000101-----100			18 A:	01010110000101-----100		
19 A:	u11000000010111-----100			19 A:	u11000000010111-----100		
20 A:	r1un10011111110110100000010100			20 A:	r1un10011111110110100000010100		
21 A:	111100110110000010111111010100			21 A:	111100110110000010111111010100		
22 A:	010110110011001001001001101010			22 A:	010110110011001001001001101010		
23 A:	010100001110111010001110001111			23 A:	010100001110111010001110001111		
24 A:	0000001000010010001101100011010			24 A:	0000001000010010001101100011010		
25 A:	101100001001011000101001101010			25 A:	101100001001011000101001101010		
26 A:	000010101000100101101101000001			26 A:	000010101000100101101101000001		
27 A:	00000110110111101010101010011			27 A:	00000110110111101010101010011		
28 A:	10110110010110101010100001001			28 A:	10110110010110101010100001001		
29 A:	1010001000001101010010000101001			29 A:	1010001000001101010010000101001		
30 A:	001010011101011110001101100011			30 A:	001010011101011110001101100011		
31 A:	111111001001001010101110101010			31 A:	111111001001001010101110101010		
32 A:	0100111110100100110100000101111			32 A:	0100111110100100110100000101111		
33 A:	0011100000111010101101100100			33 A:	0011100000111010101101100100		
34 A:	00100000011010111010000010101			34 A:	00100000011010111010000010101		
35 A:	r010000001100110000010001110010			35 A:	r010000001100110000010001110010		
36 A:	r0000111110101110111001010001			36 A:	r0000111110101110111001010001		
37 A:	1100100000010100100001100001100			37 A:	1100100000010100100001100001100		
38 A:	101100000110011111010011010100			38 A:	101100000110011111010011010100		
39 A:	000100100000101000110110001100			39 A:	000100100000101000110110001100		
40 A:	110000000100100001110001000101			40 A:	110000000100100001110001000101		
41 A:	000001101000010111101010010010			41 A:	000001101000010111101010010010		
42 A:	01001101011011111110100001010			42 A:	01001101011011111110100001010		
43 A:	010100000100011110100000110101			43 A:	010100000100011110100000110101		
44 A:	111110000001010111101100001100			44 A:	111110000001010111101100001100		
45 A:	100010101010101001011000000100			45 A:	100010101010101001011000000100		
46 A:	100000101001100101010001101100			46 A:	100000101001100101010001101100		
47 A:	10000001110010101010010111101			47 A:	10000001110010101010010111101		

TABLE 3.9: One of the original MD4 collisions by Wang et al, with a few bits underspecified (left) and propagated values (right). The question marks indicate that any bit configuration for the two bits are possible. Dashes indicate that the bits have the same configuration in both instances, but the value itself is unknown. However, it turns out the description with missing values in iteration 6 (message) and iterations 8–19 is complete enough such that missing values can be deduced by other values the description of the algorithm. Therefore the collision They propagates through the intermediate values until the differences cancel out after round 36.

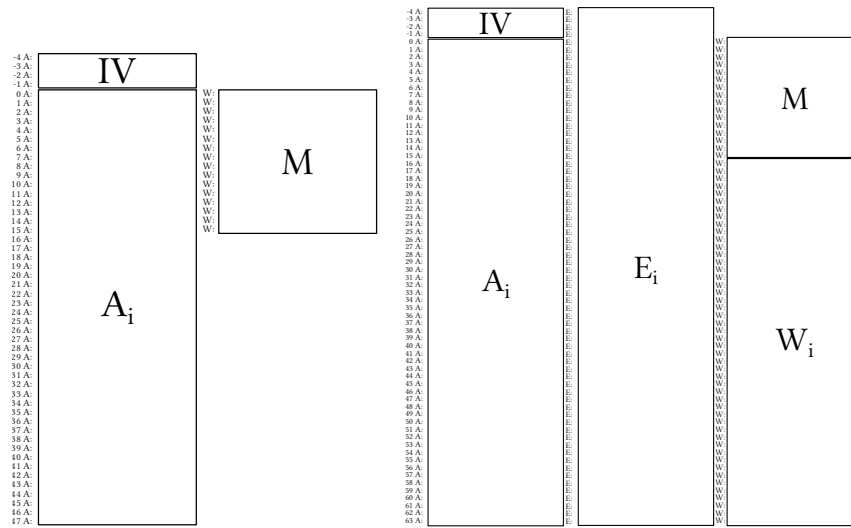


Figure 3.2: Layout of MD4 and SHA-256 differential characteristics





“WHAT IDIOT CALLED THEM LOGIC  
ERRORS RATHER THAN BOOL SHIT?”  
—Unknown

## Chapter 4

# Satisfiability

Boolean algebra allows us to describe functions over two-valued variables. Satisfiability is the question for an assignment such that a function evaluates to true. Satisfiability problems are solved by SAT solvers. We discuss the basic theory behind satisfiability. Because any computation can be represented as satisfiability problem, we are able to verify intermediate states of algorithms. In Chapter 6 we will represent a differential cryptanalysis problem such that it is solvable iff the corresponding SAT problem is satisfiable.

### 4.1 Basic notation and definitions

#### **Definition 4.1 (Boolean function)**

A *Boolean function* is a mapping  $h : X \rightarrow Y$  with  $X = \{0, 1\}^n$  for  $n \in \mathbb{N}_{\geq 1}$  and  $Y = \{0, 1\}$ .

#### **Definition 4.2 (Assignment)**

A  $k$ -*assignment* is an element of  $\{0, 1\}^k$ .

Let  $f$  be some  $k$ -ary Boolean function. An *assignment for function  $f$*  is any  $k$ -assignment.

#### **Definition 4.3 (Truth table)**

Let  $f$  be some  $k$ -ary Boolean function. The *truth table of Boolean function  $f$*  assigns truth value 0 or 1 to any assignment of  $f$ .

$x_1$	$x_2$	$f(x_1, x_2)$	$x_1$	$x_2$	$f(x_1, x_2)$	$v$	$f(v)$
1	1	1	1	1	1	1	0
1	0	0	1	0	1	0	1
0	1	0	0	1	1	(c) NOT	
0	0	0	0	0	0		

(A) AND

(B) OR

TABLE 4.1: Truth tables for AND, OR and NOT

Boolean functions are characterized by their corresponding truth table.

Table 4.1 shows example truth tables for the Boolean AND, OR and NOT functions. A different definition of the three functions is given the following way:

**Definition 4.4**

Let AND, OR and NOT be three Boolean functions.

- AND maps  $X = \{0, 1\}^2$  to 1 if all values of  $X$  are 1.
- OR maps  $X = \{0, 1\}^2$  to 1 if any value of  $X$  is 1.
- NOT maps  $X = \{0, 1\}^1$  to 1 if the single value of  $X$  is 0.

All functions return 0 in the other case.

Those functions are denoted  $a_0 \wedge a_1$ ,  $a_0 \vee a_1$  and  $\neg a_0$  respectively, for input parameters  $a_0$  and  $a_1$ .

It is interesting to observe, that any Boolean function can be represented using only these three operators. This can be proven by complete induction over the number of arguments  $k$  of the function.

Let  $k = 1$ . Then we consider any possible 2-assignment for one input variable  $x_1$  and one value of  $f(x_1)$ . Then four truth tables are possible listed in Table 4.2. The description shows the corresponding definition of  $f$  using AND, OR and NOT only.

Now let  $g$  be some  $k$ -ary function. Let  $(a_0, a_1, \dots, a_k)$  be the  $k$  input arguments to  $g$  and  $x_1 := g(a_0, a_1, \dots, a_k)$ . Then we can again look at Table 4.2 to discover that 4 cases are possible: 2 cases where the return value of our new  $(k + 1)$ -ary function depends on value  $x_1$  and 2 cases where the return value is constant.

This completes our proof.

Boolean functions have an important property which is described in the following definition:

**Definition 4.5**

A Boolean function  $f$  is *satisfiable* iff there exists at least one input  $x \in X$  such that  $f(x) = 1$ . Every input  $x \in X$  satisfying this property is called *model*.



$x_1$	$f(x_1)$	$x_1$	$f(x_1)$	$x_1$	$f(x_1)$	$x_1$	$f(x_1)$
1	1	1	1	1	0	1	0
0	1	0	0	0	1	0	0
(A) $f : x \mapsto 1$		(B) $f : x \mapsto x$		(C) $f : x \mapsto \neg x$		(D) $f : x \mapsto 0$	

TABLE 4.2: Unary  $f$  and its four possible cases

The corresponding tool to determine satisfiability is defined as follows:

**Definition 4.6**

A *SAT solver* is a tool to determine satisfiability (SAT or UNSAT) of a Boolean function. If satisfiability is given, it returns some model.

#### 4.1.1 Computational considerations

The generic complexity of SAT determination is given by  $2^n$  for  $n$  Boolean variables.

Let  $n$  be the number of variables of a Boolean function. No known algorithm exists to determine satisfiability in polynomial runtime. This means no algorithm solves the SAT problem with runtime behavior which depends polynomially on the growth of  $n$ .

This is known as the famous  $\mathcal{P} \stackrel{?}{=} \mathcal{NP}$  problem.

However, SAT solver can take advantage of the problem's description. For example consider function  $f$  in Display 4.1.

$$f(x_0, x_1, x_2) = x_0 \wedge (\neg x_1 \vee x_2) \quad (4.1)$$

Instead of trying all possible 8 cases for 3 Boolean variables, we can immediately see that  $x_0$  is required to be 1. So we don't need to test  $x_0 = 0$  and can skip 4 cases. This particular strategy is called *unit propagation*.

#### 4.1.2 SAT competitions

SAT research is heavily concerned with finding good heuristics to find some model for a given SAT problem as fast as possible. Biyearly [SAT competitions](#) take place to challenge SAT solvers in a set of benchmarks. The committee evaluates the most successful SAT solvers defined by solving the most problems within a given time frame.

SAT 2016 is currently ongoing, but in 2014 lingeling by Armin Biere has won first prize in the Application benchmarks track and second prize in the Hard

Combinatorial benchmarks track for SAT and UNSAT instances respectively. Its parallelized sibling plingeling and Cube & Conquer sibling treengeling have won prizes in parallel settings.

In Chapter 7 we will look at runtime results shown by (but not limited to) those SAT solvers.

## 4.2 The DIMACS de-facto standard

### Definition 4.7

A *conjunction* is a sequence of Boolean functions combined using a logical OR. A *disjunction* is a sequence of Boolean functions combined using a logical AND. A *literal* is a Boolean variable (*positive*) or its negation (*negative*).

A SAT problem is given in *Conjunctive Normal Form* (CNF) if the problem is defined as conjunction of disjunctions of literals.

A simple example for a SAT problem in CNF is the exclusive OR (XOR). It takes two Boolean values  $a$  and  $b$  as arguments and returns true if and only if the two arguments differ.

$$(a \vee b) \wedge (\neg a \vee \neg b) \quad (4.2)$$

Display 4.2 shows one conjunction (denoted  $\wedge$ ) of two disjunctions (denoted  $\vee$ ) of literals (denoted  $a$  and  $b$  where prefix  $\neg$  represents negation). This structure constitutes a CNF.

Analogously we define a *Disjunctive Normal Form* (DNF) as disjunction of conjunctions of literals. The negation of a CNF is in DNF, because literals are negated and conjunctions become disjunctions, vice versa.

### Theorem 4.1

Every Boolean function can be represented as CNF.

Theorem 4.1 is easy to prove. Consider the truth table of an arbitrary Boolean function  $f$  with  $k$  input arguments and  $j$  rows of output value false. We represent  $f$  as CNF.

Consider Boolean variables  $b_{i,l}$  with  $0 \leq i \leq j$  and  $0 \leq l \leq k$ . For every row  $i$  of the truth table with assignment  $(r_i)$ , add one disjunction to the CNF. This disjunction contains  $b_{i,l}$  if  $r_{i,l}$  is false. The disjunction contains  $\neg b_{i,l}$  if  $r_{i,l}$  is true.

As far as  $f$  is an arbitrary  $k$ -ary Boolean function, we have proven that any function can be represented as CNF.

SAT problems are usually represented in the DIMACS de-facto standard. Consider a SAT problem in CNF with  $nbclauses$  clauses and enumerate all variables

from 1 to  $nbvars$ . A DIMACS file is an ASCII text file. Lines starting with “c” are skipped (comment lines). The first remaining line has to begin with “p cnf” followed by  $nbclauses$  and  $nbvars$  separated by spaces (header line). All following non-comment lines are space-separated indices of Boolean variables optionally prefixed by a minus symbol. Then one line represents one clause and must be terminated with a zero symbol after a space. All lines are conjuncted to form a CNF.

Variations of the DIMACS de-facto standard also allow multiline clauses (the zero symbol constitutes the end of a clause) or arbitrary whitespace instead of spaces. Another variant terminates DIMACS files once it encounters a single percent sign on a line. The syntactical details are individually published on a per competition basis.

LISTING 4.1: Display 4.2 represented in DIMACS format

```
p cnf 2 2
a b
-a -b
```

### 4.3 Terminology

Given a conjunctive structure of disjunctions, we can define terms related to this structure. Those terms will be used in the SAT features we suggest in Section 5.4.

#### Definition 4.8

A *clause* is a disjunction of literals. A *k-clause* is a clause consisting of exactly  $k$  literals. A *unit clause* is a 1-clause. A *Horn clause* is a clause with at most one positive literal. A *definite clause* is a clause with exactly one positive literal. A *goal clause* is a clause with no positive literal.

#### Definition 4.9

Given a literal, its *negated literal* is the literal with its sign negated. A literal is *positive*, if its sign is positive. A literal is *negative* if its sign is negative. An *existential literal* is a literal which occurs exactly once and its negation does not occur. A *used variable* is a variable which occurs at least once in the CNF.

The *literal frequency* is the number of occurrences of a literal in the CNF divided by the number of clauses declared. Equivalently *variable frequency* defines the number of variable occurrences divided by the number of clauses declared.

#### Definition 4.10

The *clause length of a clause* is the number of literals contained. A clause is called *tautological* if a literal and its negated literal occurs in it.

A few basic properties hold in terms of satisfiability. For example existential literals are interesting, because they can be set to true and make one clause immediately satisfied without influencing other clauses.

## 4.4 Basic SAT solving techniques

### Definition 4.11

Given two CNFs  $A$  and  $B$ , they are called *equisatisfiable* if and only if  $A$  is satisfiable if and only if  $B$ .

#### 4.4.1 Boolean constraint propagation (BCP)

One of the most basic techniques to SAT solving is *Boolean Constraint Propagation*, also called *unit propagation*. It is so fundamental that SATzilla, introduced in Section 5.2, applies it immediately before looking at SAT features.

Let  $l$  be the literal of a unit clause in a CNF. Remove any clause containing  $l$  and replace any occurrences of  $\neg l$  from the CNF. It is easy to see, that the resulting CNF is equisatisfiable, because due to the unit clause  $l$  must be true. So any clause containing  $l$  is satisfied and  $\neg l$  yields false, where  $A \vee \perp$  is equivalent to  $A$  for any Boolean function  $A$ .

#### 4.4.2 Watched literals

Watched Literals are another fundamental concept in SAT solving. It is very expensive to check satisfiability of all clauses for every assigned value of a literal. Watched Literals is a neat technique to reduce the number of checks.

In each clause two unassigned literals are declared to be “watched”. Structurally it is implemented the other way around: A clauses watch list is maintained per literal. Now as long as at least two literals are unassigned, the clause cannot become false (recognize that a clause is false if all literals are false). Therefore the clause does not need to be visited as long as at least unassigned literals exist. This implies the following decision procedure:

- If all but one literal is false, propagate the remaining literal to be true.
- If all literals are false, report UNSAT.
- If any literal becomes true, watched literals do not change.
- Else replace the literal on the watch list with a remaining unassigned literal.

This empirical approach was established with the Chaff and zChaff SAT solvers [19] and has proven useful in various variants.

#### 4.4.3 Remark

The previous two techniques shall illustrate basic approaches, but actual SAT solving research requires decades of development to tune individual SAT solvers. Memory models and concurrency strategies lead to fundamentally different run-time behaviors of SAT solvers.

As such an initial idea to initiate an individual SAT solver specifically designed for solving problems in differential cryptanalysis was dropped, because development time is expected too long for a master thesis to be fruitful. As such we focused on popular and established SAT solvers of the SAT community.

### 4.5 SAT solvers in use

In this thesis we consider the several SAT solvers. They have been selected either by their popularity or their good results at previous SAT competitions:

- MiniSat 2.2.0
- CryptoMiniSat in versions 4.5.3 and 5
- treengeling, lingeling and plingeling, in versions:
  - lingeling ats1
  - lingeling ats101
  - lingeling ats102
  - lingeling ats104
  - lingeling baz
- glucose 4.0
- glucose syrup 4.0

Specifically this means the hash collision attacks we looked have run with these SAT solvers. The results are discussed in Section 7 and provided in Appendix C.

MiniSat is known as “Swiss army knife of SAT solving” meaning that it includes many well-established techniques that can be built upon. SAT competitions 2009, 2011, 2013 and 2014 included a special MiniSat hack track where participants are asked to modify MiniSat to prove the best performance with as little change to the

MiniSat codebase as possible. Even though is not one of the fastest SAT solvers today, it provides a nice codebase to experiment with.

CryptoMiniSat is a derivative of MiniSat, which was originally modified for cryptographic problems. It famously features XOR clauses meaning that binary clauses of structure  $a \oplus b$  could be added and will be resolved using Gaussian elimination. Temporarily development has been given up but most recently it was added again. Please recognize that our encoding introduced in Section 6.2 uses equivalence to model assignment and as such only clauses of structure  $r = a \oplus b$  emerge rendering this feature impractical to use.

glucose was the gold winner 2011 in the SAT+UNSAT application track. Modifications of glucose also ranked high throughout the years of SAT competition. glucose is a sequential SAT solver whereas glucose syrup is its parallelized version.

lingeling is SAT solver developed by Armin Biere. Lingeling has been the winner of several tracks in the SAT competitions 2011 to 2016. For example it has won gold in the SAT+UNSAT application track in 2014. lingeling has two siblings: plingeling and treengeling. plingeling is a parallelized version of lingeling. As such it executes in multiple threads and shares units and equivalences between those instances. treengeling is a Cube & Conquer solver meaning it partitions the problem into many subproblems and solves them individually.

lingeling releases ats101, ats102 and ats104 are non-public releases of lingeling. They have been developed in private communication with Armin Biere. Our main goal was to achieve a separation between two sets of variables. First all variables of the first need to be assigned in the best possible way. Afterwards the second set of variables is considered. Specifically variables modelling the differences between the two hash algorithm instances should constitute the first set.

ats101 implements that difference variables are guessed with false first and usual heuristics apply for all other variables. Our intermediate results with incomplete CNF files showed a high number of restarts. Therefore ats102 disables backjumping and therefore skips decisions for important variables. Finally ats104 is not expected to distinguish from ats102. It only provides further debugging information.

The SAT solvers have generally been run without any special options, except

- MiniSat was run with `pre=once` as it is generally recommended to run with the builtin preprocessor.
- Lingeling has been generally run with `phase=-1` to prefer false as initial assignment to literals. However, lingeling ats101 implements this with a more forceful strategy.

Testcases with lingeling have all been run 5 times with various seeds (for

reference, the default seed is 0). Only the mean runtime value is displayed in the results in Chapter 7.

Preprocessing is a difficult topic on its own. Sometimes preprocessing can provide a speedup, before actually solving the problem, but mostly SAT solvers implement preprocessing strategies themselves and run them repeatedly when solving the problem.







“TO BE USABLE EFFECTIVELY [...] THESE  
FEATURES MUST BE RELATED TO  
INSTANCE HARDNESS AND RELATIVELY  
CHEAP TO COMPUTE”  
—SATzilla

## Chapter 5

# SAT features

At the very beginning I was very intrigued by the question “What is an ‘average’ SAT problem?”. Answers to this question can help to optimize SAT solver memory layouts. Specifically for this thesis I wanted to find out whether our problems distinguish from “average” problems in any way such that we can use this distinction for runtime optimization.

I came up with 8 questions related to basic properties of SAT problems we will discuss in depth in this section. We will characterize an average SAT problem at Section 5.7:

1. Given an arbitrary literal. What is the percentage it is positive?
2. What is the clauses / variables ratio?
3. How many literals occur only once either positive or negative?
4. What is the average and longest clause length among CNF benchmarks?
5. How many Horn clauses exist in a CNF?
6. Are there any tautological clauses?
7. Are there any CNF files with more than one connected variable component?
8. How many variables of a CNF are covered by unit clauses?

We will now define the terms used in those questions.

## 5.1 Definition

### Definition 5.1 (*SAT feature*)

A *SAT feature* is a statistical value (named *feature value*) retrievable from some given SAT problem.

The most basic example of a SAT feature is the number of variables and clauses of a given SAT problem. This SAT feature is stored in the CNF header of a SAT problem encoded in the DIMACS format.

The general goal is to write a tool which evaluates several SAT features at the same time and retrieve them for comparison with other problems. Therefore it should be computationally easy to evaluate SAT features of a given SAT problem. A suggested computational limit is given with polynomial complexity in terms of number of variables and number of clauses for memory as well as runtime for evaluation algorithms. Sticking to this convention implies that evaluation of satisfiability must not be necessary to evaluate a SAT feature under the assumption that  $\mathcal{P} \neq \mathcal{NP}$ . Hence the number of valid models cannot be a SAT feature as far as satisfiability needs to be determined. But no actual hard computational limit is defined.

## 5.2 Related work

The most similar resource I found looking at SAT features was the SATzilla project [22, 35] in 2012. The authors systematically defined 138 SAT features categorized in 12 groups. Some features are only evaluated conditionally. The features themselves are not defined formally, but an implementation is provided bundled with example data. The following list provides an excerpt of the features:

**nvarsOrig** number of variables defined in the CNF header

**nvars** number of active variables

**reducedVars**  $\text{nvarsOrig} - \text{nvars}$ , divided by  $\text{nvars}$

**vars-clauses-ratio**  $\text{nvars}$  divided by number of active clauses

**POSNEG-RATIO-CLAUSE-mean** mean of  $2 \cdot \left\| 0.5 - \frac{\text{pos}}{\text{length}} \right\|$  where  $\text{pos}$  is the number of positive literals and  $\text{length}$  clause length of a specific clause

**POSNEG-RATIO-CLAUSE-entropy** like POSNEG-RATIO-CLAUSE-mean but entropy

**TRINARY+** number of clauses with clause length 1, 2 or 3 divided by number of active clauses

**HORNY-VAR-min** minimum number of times a variable occurs in a Horn clause

**cluster-coeff-mean** let neighbors of a clause be all clauses containing any literal negated and let clauses  $c_1$  and  $c_2$  be conflicting if  $c_1$  contains literal  $l$  and  $c_2$  contains  $\neg l$ , then return the mean of 2 times the number of conflicting neighbors of a clause  $c$  divided by the number of unordered pairs of neighbors, returned iff computable within 20 seconds for all clauses

Please recognize that active clauses are the unsatisfied clauses after BCP has been applied. Equivalently active variables are remaining variables after application of BCP.

Many SAT solvers collect feature values to improve algorithm selection, restart strategies and estimate problem sizes. Recent trends to apply Machine Learning to SAT solving imply feature evaluation. SAT features and the resulting satisfiability runtime are used as training data for Machine Learning. One example using SAT features for algorithm selection is ASlib [1].

The SAT solvers of Section 4.5 we use also compute features they use when computing a solution. For example CryptoMiniSat 4.5.3 prints the following lines

```
c [features] numVars 56118, numClauses 358991, var_cl_ratio 0.156,
binary 0.019, trinary 0.520, horn 0.387, horn_mean 0.000, horn_std
0.000, horn_min 0.000, horn_max 0.000, horn_spread 0.000,
vcg_var_mean 0.000, vcg_var_std 0.902, vcg_var_min 0.000,
vcg_var_max 0.000, vcg_var_spread -0.000, vcg_cls_mean 0.000,
...
```

Even though we will partially use equivalent features (like Horn clauses), many are actually related to the current state of evaluation like decisions per conflicts. We consider this as a property of the evaluation and not the SAT problem itself.

## 5.3 Statistical features

For our SAT features we need to define some basic statistical terminology. Let  $x_1, x_2, \dots, x_n$  be a finite sequence of numbers ( $n \in \mathbb{N}$ ).

**Arithmetic mean** (or short: mean) is defined as

$$\bar{x} = \frac{1}{n} \sum_{i=1}^n x_i$$

**Standard deviation** (or short: sd) with mean  $\bar{x}$  is defined as

$$\sigma(x) = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2}$$

**Median** with  $x_1 \leq x_2 \leq \dots \leq x_n$  (i.e. sorted ascendingly) is defined as

$$m = \begin{cases} x_{\text{mid}} & \text{if } n \text{ odd} \\ \frac{x_{\text{mid}} + x_{\text{mid}+1}}{2} & \text{if } n \text{ even} \end{cases} \quad \text{with } \text{mid} = \frac{n}{2}$$

and often considered more “robust” than the arithmetic mean.

**Entropy** is defined according to Claude Shannon’s information theory:

$$H(x) = - \sum_{i=1}^n x_i \cdot \log_2(x_i)$$

where  $0 \cdot \log_2(0) := 0$ .

Furthermore *count* refers to the number of elements  $n$ , *largest* refers to the maximum element  $\max_{1 \leq i \leq n}(x_i)$  and *smallest* refers to the minimum element  $\min_{1 \leq i \leq n}(x_i)$ .

## 5.4 Suggested SAT features

We wrote a tool called `cnf-analysis`. The evaluated features are partially inspired by SATzilla and `lingeling`. The latter prints basic statistics for every CNF it evaluates.

A summary of our suggested SAT features is given:

**clause\_variables\_sd\_mean**

mean of sd of variables in a clause

**clauses\_length\_largest, smallest, mean, median, sd)**

statistics related to the clause length

**connected\_literal\_variable\_components\_count**

two literals (variables) are connected if they occur in some clause together, count the number of connected components

**definite\_clauses\_count**

number of definite clauses in the CNF

**existential\_literals\_count**

number of existential literals in the CNF

**existential\_positive\_literals\_count**

number of positive, existential literals in the CNF

**(false, true)\_trivial**

is the CNF satisfied if all variables are claimed to be false (true)?

**goal\_clauses\_count**

number of goal clauses in the CNF

**literals\_count**

number of literals in the CNF (i.e. sum of clause lengths)

**literals\_frequency\_k\_to\_k + 5**

let  $n_l$  be the literal frequency of literal  $l$ , count the number of  $n_l$  satisfying

$\frac{k}{100} \leq n_l < \frac{k+5}{100}$  where  $k$  is a variable in  $\{0, 5, 10, \dots, 90, 95\}$  and  $k = 95$  counts  $\frac{k}{100} \leq n_l \leq \frac{k+5}{100}$ .

**literals\_frequency\_(largest, smallest, mean, median, sd)\_entropy**

statistics related to literal frequencies

**literals\_occurrence\_one\_count**

number of literals with occurrence 1

**nbclauses, nbvars** number of clauses (variables) as defined in the CNF header

**negative\_literals\_in\_clause\_(smallest, largest, mean)**

statistics related to number of negative literals in clauses

**(positive, negative)\_unit\_clause\_count**

number of unit clauses with a positive (negative) literal

**positive\_literals\_count**

number of positive literals in CNF

**positive\_literals\_in\_clause\_(largest, smallest, mean, median, sd)**

statistics related to number of positive literals in clauses

**positive\_negative\_literals\_in\_clause\_ratio\_(mean, entropy)**

let  $r_c$  be the number of positive literals divided by clause length of clause  $c$ , mean and related of all  $r_c$

**positive\_negative\_literals\_in\_clause\_ratio\_mean**

mean of all  $r_c$

**tautological\_literals\_count**

number of clauses which contain a tautological literal

**two\_literals\_clause\_count**

number of clauses with two literals

**variables\_frequency\_k\_to\_k + 5**

same as literals\_frequency\_k\_to\_k + 5 but for variables

**variables\_frequency\_(largest, smallest, mean, median, sd, entropy)**

same as literals\_frequency but for variables

**variables\_used\_count**

number of variables with occurrence greater o

## 5.5 Evaluation efficiency

The resource requirements of those features have been classified:

**Type 1** read the files as bytestring, a DIMACS CNF parser is not necessary, constant memory is used

**Type 2** features understand what a clause is, but still need constant memory

**Type 3** subquadratic runtime and linear memory

**Type 4** unrestricted

Memory and runtime is always considered in comparison with the filesize.

This classification should support future considerations regarding feature evaluation tools. The suggested SAT features above have been explicitly selected to avoid Type 4 implementations to limit the time to compute features. Furthermore tools evaluating only a subset of features (like Type 2 features) with better performance characteristics.

The Python implementation triggered MemoryErrors on a computer with 4 GB RAM for a 770 MB CNF file. Followingly a much more efficient Go implementation was implemented which requires much less memory and is much faster. `bench_573.smt2.cnf` took 1 second in Go instead of 2 minutes in Python. However, the data evaluated is less accurate compared to Python, because Python unlike Go provides a nice implementation of statistical tools in the standard library. Go algorithms were written on our own.

In the following section, we define the dataset we consider.

## 5.6 CNF dataset

To evaluate CNF features of a representative set of CNF files, it was necessary to identify equivalent CNF files in the best possible way. Therefore we defined

a hashing algorithm standardizing the CNF input provided to a SHA1 instance. Every CNF file is identifiable by its “cnfhash 2.0.0” hash value.

In the next step a complete set of CNF files of previous SAT competitions was collected. The following CNF file collections have been considered:

- SAT Race 2008
- SAT Competition 2013
- SAT09 Competition
- SAT Competition 2014
- SAT-Race 2010
- SAT-Race 2015
- SAT11 Competition
- SAT Competition 2016
- SAT Challenge 2012
- SATlib

The benchmarks are mostly contributed by the participants of the associated conferences. Others are reused from previous years. Individual projects allow to generate CNF files for specific problems in a selectable problem size; such as CNFgen [13] by Massimo Lauria.

Some files turned out to be problematic. In SATlib, 3 gzipped files couldn’t be decompressed and several files contain empty clauses. Empty clauses are assumed to immediately falsify the CNF and are therefore pointless. I removed trailing zeros in CNFs. Variants of the DIMACS standard also expect lines with a percent symbol to terminate the CNF. Besides those minor issues documented as part of the cnf-analysis project, 175 gigabytes of CNF files have been evaluated with a total of 68,069 CNF files (62,251 unique CNF files).

## 5.7 The average SAT problem

### Proposition 5.1

The set of public benchmarks in SAT competitions between 2008 and 2015 represent average SAT problems

It is important to point out that public benchmark files are specifically chosen to be evaluated before a conference is held. Hence they are expected to terminate within a given time frame and are therefore not oversized. On the one hand this ensures that the problems are feasible, but on the other hand they might be a biased selection. At this point no better data set is available and therefore we proceeded with this dataset.

According to my results, an average SAT problem consists of:

- 83,542 clauses in average ranging from 21 to 53,616,734 (median = 430,  $\sigma = 848388$ )

- The longest clause we found had 61,473 literals, but the longest clause of an average CNF covers 20 literals.
- The number of total literals in a CNF ranges from 60 up to 150,609,758.
- The clause-variables ratio lies between 1.22 and 27,720 with mean = 9.54 and  $\sigma = 139$ .
- The average length of a clause is expected to be 3. The largest clause length mean we found was 19.58 compared to 2.83 as the smallest clause length mean.
- Surprisingly, in average a CNF file has 205 connected literal components and 53 connected variable components. However both corresponding medians are 1 meaning that at least have of the problems still have only one component.
- In average 32,787 clauses are definite clauses and 35,094 clauses are goal clauses.
- In average a literal occurs in 1.4 % of the clauses of the CNF.
- 47 % of literals in a clause are positive.
- The arithmetic mean tells 124 unit clauses per CNF file can be expected, but the median tells it is mostly 0.
- The largest variable found was 13,842,706 and 13,829,558 variables were used at most.
- Exactly one CNF file was true-trivial (namely `dubois/dubois100.cnf` of SATlib) whereas 13 CNF files were false-trivial (of SAT competition 2014 and SAT-Race 2015).

## 5.8 Benford's law in CNF files

Given this huge set of CNF files and therefore integers, we evaluated whether Benford's law holds.

A paper by Theodore P. Hill [8] characterizes Benford's Law as the following conjecture:

### **Theorem 5.1**

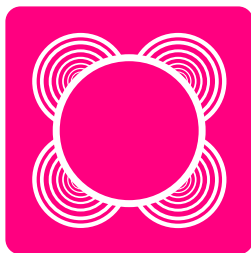
Consider arbitrary data from tables, listings or other sources in publications, newspaper and so on and so forth, the digit 1 occurs in about 30 % of the time. The first digit is 1 about 30 percent of the time and 9 only about 4.6 percent of the time.



We evaluated that the leading digits 1 to 9 occur with probabilities 28.76 %, 19.09 %, 13.56 %, 10.97 %, 7.48 %, 5.76 %, 5.12 %, 4.79 % and 4.46 % respectively. We concluded that:

Considering a deviation of 1.34 % for digit 1 (expected 30.1, actual 28.76) and 0.12 % for digit 9 (expected 4.58, actual 4.46), we claimed the CNF files considered satisfy Benford's law.





“THERE IS CONSENSUS THAT ENCODING  
TECHNIQUES USUALLY HAVE A DRAMATIC  
IMPACT ON THE EFFICIENCY OF THE SAT  
SOLVER”

—Magnus Björk

## Chapter 6

# Problem encoding

We already discussed how SAT solvers work and which input they take. We also sketched how hash algorithm properties got broken using differential cryptanalysis. In this section we combine those subjects and describe how we designed an attack setting.

We designed a basic prototype with the STP SMT solver. Followingly we wanted to tweak the CNF used by the SAT solver and wrote our own library *algotocnf* to generate CNFs for differential purposes; as illustrated in Section 3. There we distinguished 5 different tweaks. We evaluate the performance of those tweaks in Chapter 7.

Every section represents a major approach whereas subsections represent derivatives of this approach with minor tweaks.

### 6.1 Basic approach

Our first approach started with Simple Theorem Prover (STP) [7] initially written by Vijay Ganesh and David L. Dill. It is currently maintained by Mate Soos.

STP is an SMT solver which allows to declare bitvectors. A bitvector is an array of Boolean variables providing high-level constructs such as additions or right-shift through an interface. Writing all clauses individually to model a hash algorithm is too cumbersome to be done in practice and STP simplifies this process. STP is recommendable as a tool to model arithmetic and bitwise functions.

First we wrote an implementation using the CVC language to model the MD4 hash algorithm. We provide a bitvector to the hash algorithm instance. When applying the corresponding arithmetic operations we generate expressions such as `ASSERT(y = 0bin00000101);` to model the assignment of a constant. Here the desired constant is assigned variable `y`, because of equivalence. `y` is required to have the constant after this expression as value. Whereas we generate the `ASSERT` statement, it is STP's task to generate the CNF formula and solve it with a SAT solver.

We take two hash algorithm instances and an additional bitvector `diff` for every pair of bitvectors (`bv1`, `bv2`) where `bv2` represents the corresponding bitvector of the second hash algorithm instance to `bv1`. We claim `ASSERT(diff = BVXOR(bv1, bv2))` to ensure that `diff` represents the difference between `bv1` and `bv2`. Given the bitconditions for a bitvector from a differential characteristic, we require `diff` to enforce those particular differences. This corresponds to the idea of differential cryptanalysis introduced in Chapter 3.

It is now trivial to consider a differential characteristic such as Testcase B.1 and generate the corresponding CVC input for STP. STP solves this particular problem within a second. Testcase B.2 already provides a more complex example taking 40 minutes to solve. We used minisat as SAT solver in the backend, even though STP allows to exchange it for CryptoMiniSat which is a more modern and versatile SAT solver.

Even though STP allows to come to useful results pretty quickly, it seems cumbersome to model all hash algorithms in the CVC language. STP provides a python interface meaning that pure Python implementations of hash algorithms can be taken with little modifications to model the hash algorithm itself. We add code to declare the difference bitvectors `diff` and finally add the constraints resulting from the differential characteristic.

This interface switch introduces no significant performance difference.

As a next step, we wanted to improve the evaluation performance to tackle more difficult problems. We considered this design as a working prototype of a basic approach to be improved upon.

STP was not fruitful for our next goal, because we wanted to tweak the SAT design generated for the SAT solver and needed good control over the SAT encoding which we expected to have a major influence on the performance.

## 6.2 `algotocnf`

We implemented our own library *algotocnf* to achieve greater flexibility in SAT design.

### 6.2.1 Two instances and its difference

Similar to STP, *algotocnf* generates a CNF for a given hash algorithm implementation. Besides modelling bitvectors, it also implements differential bitvectors which inherently handle the difference bitvectors *diff* which contain difference variables. It can also directly operate with differential characteristics. Similarly to STP, it implements arithmetic and bitwise operations.

We think *algotocnf* mainly differs from other SMT tools like STP because of its implementation of differential logic.

To model our CNF *algotocnf* implements the following strategy:

1. Take a differential characteristic and the hash algorithm as input.
2. Every bit is therefore represented as a Boolean variable. If you apply addition, operator overloading in python will ensure that clauses are generated to describe the addition consisting of XORs and MAJs. Every operation is modelled as assignment. Hence an operation operating on a few Boolean variables is equivalent to a single variable which represents the result. Equivalently other operations related to integers are implemented as well.
3. Constants used in the implementation are automatically converted to bitvectors with unit clauses.
4. After running the hash algorithm with bitvectors per instance, all constraints related to the hash algorithm are added.
5. Followingly the differential characteristic is read. Values such as  $A_i$  represent intermediate states of bitvectors. Therefore the corresponding bitvectors are looked up and equivalences with temporary bitvectors are added. Those temporary bitvectors are initialized with all constraints resulting from the bit conditions of this bitvector. In conclusion all constraints resulting from the differential characteristic are added.
6. Finally the SAT solver is called. The CNF was mostly solved on a cluster specified in [Appendix A](#).
7. Afterwards the program is run again to create the exactly same problem instance and the solver's solution replaces symbolic values with actual Boolean values. The resulting differential characteristic is parsed backed and printed out as differential characteristic where expectedly many bit conditions have been strengthened.

When adding clauses resulting from the differential characteristic as constraints, the question arises how those bit conditions are encoded. Essentially, we

have only Boolean values available, but bit conditions tell constraints such as “a difference is given, but the actual value is unknown”.

It seemed trivial to add a *difference variable* for every pair of Boolean values representing a bit in the two instances. Furthermore the difference variable  $\Delta x$  is connected by a XOR with the variables of the pair  $(x, x')$ .

$$\Delta x = x \oplus x'$$

Therefore it should be trivial for a preprocessor to simplify the formula appropriately or actually we don’t expect runtime differences for the larger amount of variables.

And finally we expect the CNF to inherit a property of hash functions. Inputs are provided into the hash algorithm and strongly intermingled with other values. This should result in a high diffusion and almost every variable is expected to share a clause with another variable.

The difference variables design corresponds to `diff` bit vectors in the STP and therefore designs the difference described in Chapter 3. The design decisions of this encoding are fundamental to the resulting runtime discussed in Chapter 7.

### 6.2.2 Adding the differential description

Using the approach in the previous section, we were able to find actual MD4 collisions using a SAT solver (please refer to Section 7.2.1). A SHA256 implementation followed which obviously lead to worse runtime results, because the internal state of SHA-256 is much larger (by a factor of at least 2). Can we further improve the runtime of the SAT solver?

Because we work with bitvectors and apply high-level operations like MAJ or addition, we can additionally implement how differences in those operations propagate. Magnus Daum’s thesis on “Cryptanalysis of Hash Functions of the MD4-Family” [4, Table 4.4] discusses how differences propagate in Boolean functions. Trivially, XORs propagate differences the way they are <sup>1</sup>. Another example is MAJ: Let  $a, b$  and  $c$  be difference variables and MAJ is applied to both corresponding hash algorithm instances.  $r$  is the difference variable of the result. Then its differential behavior states that

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

where  $(IN) \implies OUT$  denotes an input-output relation. Because of this behavior we add clauses to explicit describe this behavior:

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

---

<sup>1</sup>A difference in the arguments of two XOR instances remains the same difference after applying XOR to each instance

We also model the second behavior:

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

This approach explicitly models differentiable behavior, which should be deducible by the SAT solver itself based on the clauses we added before. However, this lead to a major speedup which can be observed in the runtime results of Chapter 7.

### 6.2.3 Evaluating difference variables first

#### Proposition 6.1

Deriving difference values first, followed by actual bit values for the two instances, leads to a speedup.

This proposed principle is fundamental to differential cryptanalysis. A previous tool at our department implements propagation of hash algorithm values without a SAT solver and this strategy is essential to good performance. This strategy was introduced in the very early days of differential cryptanalysis and was also used by Wang et al. [34] to find their hash collisions.

So basically in terms of SAT solvers we want to guess values for difference variables first and once all have been assigned, we try to find actual values for the two hash algorithm instances.

It is important to point out that DIMACS does not specify a way to annotate Boolean variables. As such that SAT solver cannot distinguish between difference variables and variables of the instances. Therefore implementing this approach requires a custom SAT solver which is given with `lingeling ats101`.

Another proposition is important for this approach:

#### Proposition 6.2

Guessing difference values false first, followed by true, should solve hash collision problems faster.

This proposition is justified by the desire to find as little differences as possible in a hash collision to increase the probability of values cancelling each other out in the later rounds.

### 6.2.4 A light-weight approach

In this tweak we made a step back and considered the ideas of the previous section but neglected the differential description. This approach was interesting to recognize the effect introduced by adding the differential description.

### 6.2.5 Influencing the evaluation order

We took to idea to influence the evaluation order to the next level, by applying the following design:

Let  $\Delta x$  be the difference variable of pair  $(x, x')$ . We introduce a new Boolean variable  $x^*$ . We add clause

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



and explicitly tell the SAT solver to guess on  $x^*$  before guessing on  $\Delta x$ ,  $x$  or  $x'$ .

The SAT solver will assign  $x' = 0$  first, because of the evaluation order. So either  $\Delta x$  or  $x$  must be false.  $\Delta x$  is assigned false, because as difference variable it has a higher priority over  $x$ . Equivalently for  $x' = 1$  we have  $\Delta x$  needs to be true. So we actually achieve an early guess on the difference variable.

This another approach evaluates in the results chapter.





## Chapter 7

# Results

In Chapter 4 we discussed Boolean algebra; in particular we looked at satisfiability which is practically covered by SAT solvers. SAT solvers take Boolean functions in Conjunctive Normal Form and determine satisfiability. In Chapter 3 we looked at how we can analyze algorithms by looking at the progression of differences between algorithm instances. In particular we looked at hash algorithms introduced in Chapter 2.

With this background we designed a attack setting in Chapter 6 which enables us to verify and also find a hash collision given a differential characteristic given as starting point. Our goal is to find hash collisions in as little time as possible. Therefore we introduced several approaches in Section 6.2.

In this section we will evaluate those approaches. Furthermore we briefly discuss claims we made about average SAT problems. In Section 5 we looked at SAT features which to some extent characterize a SAT problem.

### 7.1 Evaluating SAT features

In the introduction of Chapter 5 we posed 8 questions. In the following, we want to answer them with the data provided by the cnf-analysis project.

**Given an arbitrary literal. What is the percentage it is positive?** We look at every clause and determine the ratio of positive to the total number of literals. We determine the mean per CNF file and the mean among all CNF files and retrieve a value of 0.48 meaning that 48 % of the literals are positive.

**What is the clauses / variables ratio?** In average a CNF file has 12,219 variables and 89,541 clauses. Its clauses-variables ratio is 7.328.

**How many literals occur only once either positive or negative?** In average there are 36 existential literals per CNF file, but its standard deviation of 967 is very high.

**What is the average and longest clause length among CNF benchmarks?** The average clause length is 3.04 with a standard deviation of 0.99 and the longest clause length found was 61,473. Long clauses are typically outliers excluding specific assignments.

**How many Horn clauses exist in a CNF?** In average 29,994 goal clauses and 31,315 definite clauses exist with an average number of 83649 clauses in a CNF file.

**Are there any tautological clauses?** In a file, 1679 tautological literals have been found. However, its mean is 0.07 with a standard deviation of 9.63 meaning that tautological clauses are very rare.

**Are there any CNF files with more than one connected variable component?** Indeed, an average CNF file contains 67.07 connected variable components. However, its median is 1 anyway implying that at least half of the CNF files have only 1 connected variable component.

**How many variables of a CNF are covered by unit clauses?** In average 124 variables are covered by unit clauses. This is an insignificant number compared to 12,219 variables in an average CNF.

The clauses/variables ratio was thoroughly studied by the SAT community [23]. A strong correlation between the instance's hardness and the ratio of number of clauses to number variables exists [31] though it is important to point out that this result holds for randomly generated SAT instances, which our benchmarks are not classified as.

Existential literals are interesting to discover, because they allow to remove a clause immediately. Consider a clause with literals  $(l_1, l_2, \dots, l_n)$ . If a guarantee exists such that the variable of any literal  $l_i$  does not occur in any other clause, we can claim  $l_i$  true rendering the clause satisfied.

Tautological clauses obviously also render clauses satisfied.

Connected variable components are interesting, because they split the SAT problem into several small subproblems which can be independently. Consider two sets of variables  $A$  and  $B$ . Now consider some clauses using only variables of  $A$  and some clauses using only variables of  $B$ . The overall CNF is satisfiable iff both clause sets are satisfiable. The overall CNF is falsifiable iff any clause set is

falsifiable. Hence if we know the connected variable components, we could easily create two parallel SAT solver instances and solve the problems independently. 4,607 out of 62,251 CNF files contained more than 1 connected variable component.

These properties represent very fundamental properties of the SAT problem. But for us the question arises whether we can distinguish our cryptoproblems from average problems?

- We looked at 36 files classified as cryptographic problems. They are considered cryptographic, because their file or folder name indicated they are related to hash functions or general cryptographic applications like AES. The specific selection can be identified by the crypto tag annotated to these CNF files as part of the cnf-analysis project.
- 62,533 clauses and 8,279 variables in average yield a variables-clauses ratio of 7.55.
- The 36 cryptographic SAT instances give a standard deviation of 0 for clause length meaning that all clauses had the same length.
- Whereas the number of connected variable components has a mean of 52.73 ( $\sigma = 1225$ , median = 1) for general problems, Our cryptographic problems considered had a mean of 1 ( $\sigma = 0$ , median = 1).
- The number of definite clauses is half its value for general problems (16,687 versus 32,787) and the number of goal clauses is 16 % of its value for general problems (5,767 versus 35,094).

No other value has been found to be significantly different from average problems (or its difference follows immediately by the non-uniform clause length). The number of connected variable components seems interesting because it might indicate diffusion in cryptographic problems. Diffusion means that variables strongly interact with many different variables due to the repetitive structure of cryptographic primitives. And finally the other differences can be explained by a certain SAT design which reoccurs in this benchmarks, because 36 is an exceptionally small number compared to 62,251 unique CNF problems.

Comparing our average problem with cryptographic problems did not draw any useful conclusions. Particularly a more thorough discussion of the SAT designs might be more valuable than our high-level features. We now specifically look at a SAT design we are familiar with: Do average SAT problems distinguish from *our* CNF benchmarks?

- For all MD4 testcases we have the same number of variables, because the internal state of the hash algorithm instances are always the same size. However, adding the differential description described in Section 6.2.2 increases

the number of clauses by about 47 % ( $\sigma = 0.0005$ ) for MD4 instances and by about 43 % ( $\sigma = 0.0008$ ) for SHA-256 instances. The additional variable introduced in Section 6.2.5 increases the number of variables by about 80 % and the number of clauses by factor 2.

MD4 C	253,984 / 48,704	MD4 C diff-desc	373,920 / 48,704
MD4 B	254,210 / 48,704	MD4 B diff-desc	374,146 / 48,704
MD4 A	254,656 / 48,704	MD4 A diff-desc	374,592 / 48,704
SHA-256 18	590,953 / 107,839	SHA-256 18 diff-desc	846,487 / 107,839
SHA-256 21	636,838 / 116,800	SHA-256 21 diff-desc	911,629 / 116,800
SHA-256 23	667,438 / 122,774	SHA-256 23 diff-desc	955,067 / 122,774
SHA-256 24	682,722 / 125,761	SHA-256 24 diff-desc	976,770 / 125,761

TABLE 7.1: Our testcases and their number of clauses / variables

Compared to 83,542 clauses and 12,219 variables for our average SAT problem, we consider our benchmark to be noticeably large. It is important to point out that the problem size does not necessarily correlate with the hardness of the SAT problem.

- The variables of clauses of average SAT problems have a standard deviation of 3,337 in average ( $\sigma = 1,261$ , median = 3,643). Our average SAT problem has a standard deviation of 1,004 in average ( $\sigma = 13,992$ , median = 22). Hence variables which got created at very points during the CNF generation are shared within one clause. The general statement, that variable enumeration is arbitrary and therefore this standard deviation has no meaning, holds but we need to consider that practically speaking variables created close to each other share close variable indices. Under these assumptions a large  $\sigma$  indicates variables are reused. We assume this is another indicator for high diffusion in cryptographic algorithms. Values are intermingled over and over throughout the repetitive structure of hash algorithms.
- Connected variables components are 129 for MD4 problems and 2 for SHA-256 problems. We couldn't explain where those components come from and the component size would help us to identify their source. We did not investigate further, because this number is constant with an increasing problem size.
- An average literal frequency of  $3.5 \cdot 10^{-5}$  for our benchmarks is much lower than 0.014 for average problems. We explain this with the larger problem size. Literal frequency is divided by the number of clauses of the CNF and is therefore smaller the larger the problem is.

In general we were not able to identify features which allows us to solve differential cryptanalysis problems more efficiently compared to general-purpose

SAT problems. We concluded writing your own SAT solver dedicated to solving differential cryptanalysis problems is not worth the effort.

## 7.2 Finding hash collisions

In this section we look at our benchmark results of Testcases provided in Appendix B. We make various propositions and substantiate them with runtime results. Runtimes are always provided in seconds.

### 7.2.1 Attacking MD4

#### Proposition 7.1

Testcase B.1 in the encoding described in Section 6.2.1 can be solved within one minute by all considered SAT solvers.

In our attack setting we started off with Testcase B.1. It serves rather as a toy example to verify correctness of our implementation than as an actual runtime benchmark. Be aware that invalid implementations either result in unsatisfiability for satisfiable testcases or runtime results are unexpected because the SAT solver could not take advantage of our SAT design implementations. This particular testcase can be solved easily with all major SAT solvers as can be seen in Table 7.2.

solver	version	propagations	decisions	restarts	runtime
MiniSat	2.2.0	3,813,726	250,759	—	3
CryptoMiniSat	4.5.3	140,000	2,441,566	539	26
	5	—	2,428,824	637	37
Lingeling	ats1	6,586,770	436,621	980	23
Glucose	4.0	14,727,839	990,491	272	8
Glucose Syrup	4.0	—	629,363	201	14

TABLE 7.2: Testcase B.1 can be solved within 1 minute by all SAT solvers

#### Proposition 7.2

Simplification reduces the problem size (number of variables and clauses).

Consider for example Testcase B.4 in the basic encoding introduced in Section 6.2.1. Then simplification will reduce the problem size down by 57–77 % of its original size (compare with Table 7.3).

#### Proposition 7.3

Using phase=-1 does not significantly improve the runtime of lingeling

simplification	variables	/	clauses	(variables left / clauses left)
none	590953	/	107839	(100 % / 100 %)
satelite	457972	/	69670	(77.50 % / 64.61 %)
cmsat	342139	/	61789	(57.90 % / 57.30 %)
lingeling	344544	/	107839	(58.30 % / 100.00 %)
minisat	391134	/	61845	(66.19 % / 57.35 %)

TABLE 7.3: Problem sizes of Testcase B.4 in the encoding of Section 6.2.1 after simplification

**Proposition 7.4**

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

TODO: is simplification worth it?

Appendix C provide a more exhaustive list of runtimes retrieved.

In Section 6.2 we introduced a basic encoding involving two hash algorithm instances and difference variables. Constraints resulting from the hash algorithm description and given differential characteristic are added.

We considered MD4 testcases A, B and C (compare with Appendices B.1, B.2 and B.3) and generated the corresponding CNF files. The SAT solvers mentioned in Section 4.5 were used to evaluate whether the problem is solvable in reasonably time. For every testcase we defined a time limit of at most 1 day (i.e. 86,400 seconds). A timeout is denoted by  $\top$ . Some testcases listed have been evaluated for a larger time limit.

In Table 7.4 it can be seen that the problem can be tackle by all SAT solvers. lingeling-ats104 being a outlier can be ignored, because this release is majorily concerned with providing debug information. As such it only shows that printing information to stdout can make a major performance difference.

In Table 7.5 we see that CryptoMiniSat 4.5.3, glucose 4.0 and glucose-syrup 4.0 couldn't solve the problem within the time limit of 1 day. However, other SAT solver were still able to find a hash collision. Please recognize that Table 7.4 provides runtime results for the testcase given in Table B.1; equivalently Table 7.5 for Table B.2 and Table 7.6 for Table B.3. Its caption gives an intuition how testcase B is more difficult than A and C is more difficult than B.

We end up with the result, that the hash collision given in Table B.3 can be solved by a limited set of modern SAT solvers. Of course the cryptanalyst needs to figure out good starting points for the hash collision and encode them in the differential characteristic, but this task is still considered practical, because this task can be easily automated.



TODO: is phase -1 worth it?

TODO: simplification runtime is not part of runtime

### 7.2.2 Improvements with differential description

Our next goal was to scale up to a more difficult problem. We considered SHA-256 which has a much larger internal state (at least by factor 2). So finding a hash collision is more difficult and we considered further strategies.

Consider testcases 18 B.4, 21 B.5, 23 B.6 and 24 B.7. The number indicates how many steps are covered by this testcase. We also tested a 27-round variant, but it is not listed here. Most SAT solvers could not solve this problem in feasible time. Therefore we excluded it from our list.

In Tables 7.7 to 7.10 we see several results which illustrate TODO

Followingly we added the clauses which directly encode how differences propagate in the hash algorithm; namely “differential description” of Section 6.2.2. If we compare the data, we can see TODO

We continued by trying the influence the guessing strategy.

### 7.2.3 Modifying the guessing strategy

As pointed out in Section 6.2.3, a best practice law of differential cryptanalysis states that difference variables should be assigned first. Afterwards propagation of actual values for the two instances can take place.

To enforce such a strategy, we tried several approaches:

1. Armin Biere provided us with a custom release of lingeling which enforces that a special set of variables is evaluated first. It is important that the CNF is still solved with usual SAT solver heuristics, because enforcing assignment of one variable after another leads to an increase in backtracking steps and restarts. Hence, we consider this release as a nice tradeoff. Difference variables are assigned “as early as possible, as late as necessary”.
2. Given this custom SAT solver we considered a SAT design which requires the SAT solver to prefer a certain. This particular design with a special Boolean variable is explained in Section 6.2.5.

### 7.3 Related work

In my bachelor thesis [25] we tried to integrate a SAT solver into our department's existing tool which encodes propagation explicitly. This approach was not very successful as restarts between hash algorithm rounds implied that intermediate results by the SAT solver get lost.

Research was already done by Ilya Mironov and Lintao Zhang [18] to apply SAT solvers to differential cryptanalysis specifically to find hash collision in MD4. However whereas their basic approach seems to correspond to our approach described in Section 6.2.1, our implementation uses additional SAT design tweaks to improve our results. Also because 10 years have gone since publication, SAT technology has progressed and modern SAT solvers on modern hardware provide better results.

TODO justify: differential description improves runtime

### 7.4 Conclusion

We successfully found hash collisions for round-reduced MD4 and SHA-256.

### 7.5 Contributions

To strengthen Reproducible Research, the source code and data resulting from this thesis is available online. It allows the reader to run the experiments again and verify our claims. We did our best to describe our hardware setup as accurately as possible. At the following website, any results part of this project are collected:

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

Several subprojects are part of this master thesis:

#### **algotocnf**

A python library implementing the encoding described in Chapter 6.

**Python3 library and program:** <https://github.com/prokls/algotocnf>

#### **cnf-hash**

A standardized way to produce a unique hash for CNF files

**Go implementation:** <https://github.com/prokls/cnf-hash-go>

**Python3 implementation:** <https://github.com/prokls/cnf-hash-py>

**Testsuite:** <https://github.com/prokls/cnf-hash-tests2>

**cnf-analysis**

Evaluate SAT features for a given CNF file.

**Go implementation:** <https://github.com/prokls/cnf-analysis-go>

**Python3 implementation:** <https://github.com/prokls/cnf-analysis-py>

**Testsuite:** <https://github.com/prokls/cnf-analysis-tests>

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	MD4, A	65
cryptominisat 4.5.3	MD4, A	24
cryptominisat 5.0.0	MD4, A	29
glucose 4.0	MD4, A	10
glucose-syrup 4.0	MD4, A	31
lingeling-ats1	MD4, A	TODO
lingeling-ats101	MD4, A	18
lingeling-ats102	MD4, A	TODO
lingeling-ats104	MD4, A	125,745
plingeling-ats101	MD4, A	88
treeneling-ats101	MD4, A	64

TABLE 7.4: Runtimes for MD4 testcase A with various SAT solvers

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	MD4, B	7,817
cryptominisat 4.5.3	MD4, B	T
cryptominisat 5.0.0	MD4, B	571
glucose 4.0	MD4, B	T
glucose-syrup 4.0	MD4, B	T
lingeling-ats1	MD4, B	TODO
lingeling-ats101	MD4, B	257
lingeling-ats102	MD4, B	TODO
lingeling-ats104	MD4, B	TODO
plingeling-ats101	MD4, B	1,860
treeneling-ats101	MD4, B	12,574

TABLE 7.5: Runtimes for MD4 testcase B with various SAT solvers

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	MD4, C	19,683
cryptominisat 4.5.3	MD4, C	T
cryptominisat 5.0.0	MD4, C	1064
glucose 4.0	MD4, C	T
glucose-syrup 4.0	MD4, C	T
lingeling-ats1	MD4, C	TODO
lingeling-ats101	MD4, C	TODO
lingeling-ats102	MD4, C	TODO
lingeling-ats104	MD4, C	TODO
plingeling-ats101	MD4, C	TODO
treeneling-ats101	MD4, C	TODO

TABLE 7.6: Runtimes for MD4 testcase C with various SAT solvers

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	SHA-256, 18	TODO
cryptominisat 4.5.3	SHA-256, 18	TODO
cryptominisat 5.0.0	SHA-256, 18	TODO
glucose 4.0	SHA-256, 18	TODO
glucose-syrup 4.0	SHA-256, 18	TODO
lingeling-ats1	SHA-256, 18	TODO
lingeling-ats101	SHA-256, 18	25
lingeling-ats102	SHA-256, 18	TODO
lingeling-ats104	SHA-256, 18	TODO
plingeling-ats101	SHA-256, 18	TODO
treeneling-ats101	SHA-256, 18	TODO

TABLE 7.7: Runtimes for SHA-256 testcase 18 with various SAT solvers

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	SHA-256, 21	TODO
cryptominisat 4.5.3	SHA-256, 21	TODO
cryptominisat 5.0.0	SHA-256, 21	TODO
glucose 4.0	SHA-256, 21	TODO
glucose-syrup 4.0	SHA-256, 21	TODO
lingeling-ats1	SHA-256, 21	TODO
lingeling-ats101	SHA-256, 21	27,511
lingeling-ats102	SHA-256, 21	TODO
lingeling-ats104	SHA-256, 21	TODO
plingeling-ats101	SHA-256, 21	TODO
treeneling-ats101	SHA-256, 21	TODO

TABLE 7.8: Runtimes for SHA-256 testcase 21 with various SAT solvers

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	SHA-256, 23	TODO
cryptominisat 4.5.3	SHA-256, 23	TODO
cryptominisat 5.0.0	SHA-256, 23	TODO
glucose 4.0	SHA-256, 23	TODO
glucose-syrup 4.0	SHA-256, 23	TODO
lingeling-ats1	SHA-256, 23	TODO
lingeling-ats101	SHA-256, 23	59,227
lingeling-ats102	SHA-256, 23	TODO
lingeling-ats104	SHA-256, 23	TODO
plingeling-ats101	SHA-256, 23	TODO
treeneling-ats101	SHA-256, 23	TODO

TABLE 7.9: Runtimes for SHA-256 testcase 23 with various SAT solvers

SAT solver	testcase	runtime (in seconds)
minisat 2.2.0	SHA-256, 24	TODO
cryptominisat 4.5.3	SHA-256, 24	TODO
cryptominisat 5.0.0	SHA-256, 24	TODO
glucose 4.0	SHA-256, 24	TODO
glucose-syrup 4.0	SHA-256, 24	TODO
lingeling-ats1	SHA-256, 24	TODO
lingeling-ats101	SHA-256, 24	65,956
lingeling-ats102	SHA-256, 24	TODO



## **Chapter 8**

# **Summary and Future Work**

### **8.1 Summary of results**

In this thesis we looked at

### **8.2 Future work**





# **Appendices**



## Appendix A

### Hardware setup

In the following we introduce two hardware setups which were used to run our testcases. The first setup is referred to as “Thinkpad x220” throughout the document whereas the second setup is referred to as “Cluster”.

<i>Type model</i>	Thinkpad Lenovo x220 tablet, 4299-2P6
<i>Processor</i>	Intel i5-2520M, 2.50 GHz, dual-core, Hyperthreaded
<i>RAM</i>	16 GB (extension to common retail setup)
<i>Memory</i>	160 GB SSD
<i>L3 cache size</i>	3072 KB

TABLE A.1: Thinkpad x220 Tablet specification [14]

<i>Processor</i>	Intel Xeon X5690, 3.47 GHz, 6 cores, Hyperthreaded
<i>RAM</i>	192 GB
<i>L3 cache size</i>	12288 KB

TABLE A.2: Cluster node nehalem192go specification [3]

TODO: other cluster cores



# Appendix B

## Testcases

### B.1 MD<sub>4</sub> testcase A

*Please compare with Figure B.1.*

We can clearly see that all difference variables are defined. Either they are true (bit condition **x**) or false (bit condition **-**), but no variable has an undeciable state like **?**. At the top we can see bit conditions 0 and 1 encoding the MD<sub>4</sub> initial vector defined by the hash algorithm. The differences **x** introduce the hash collision and with round 47 being set of **-** only, the output is forced to be equal between both hash algorithm instances. This testcase is a trivial version of the differential characteristic described in [29].

### B.2 MD<sub>4</sub> testcase B

*Please compare with Figure B.2.*

In this testcase we have less knowledge about the state than in testcase A because many values are encoded with **?** meaning that neither their difference nor their actual values are known. However, of course some **x** exists to introduce a hash collision and the last round only consists of dashes to assert no difference in the output. So unlike testcase A, the SAT solver needs to figure out the difference variables in rounds 0–11 increasing its overall runtime in all SAT solver implementations.

### B.3 MD<sub>4</sub> testcase C

*Please compare with Figure B.3.*

This testcases introduces a hash collision which is expected to cancel out at round

32. At the same time no information is provided about the intermediate state of the hash algorithm in rounds 0–20.

## B.4 SHA-256 testcase 18 rounds

*Please compare with Figure B.4.*

All SHA-256 testcases got derived from a paper by Ivica Nikolić and Alex Biryukov [21]. Recall that message input of one block only fills  $W_0$  to  $W_{15}$ .  $W_{16}$  or later are generated based on the previous message words. This differential characteristic depicts a hash collision introduced in round 3. When solving this differential characteristic differences will especially occur in the most-significant bit of words with unspecified difference. Differences cancel out after round 7.

## B.5 SHA-256 testcase 21 rounds

*Please compare with Figure B.5.*

Unlike Testcase B.4 word  $A_5$  is underspecified with question marks. This certainly makes the problem harder for a SAT solver. At the same time differences of the message words  $W_9$  and  $W_{10}$  are specified. This makes the problem easier. At the same time the whole collision covers 21 rounds, unlike Testcase B.4 with 18 rounds.

## B.6 SHA-256 testcase 23 rounds

*Please compare with Figure B.6.*

Message word  $W_9$  specifies no difference, but the collision is extended to 23 rounds.

## B.7 SHA-256 testcase 24 rounds

*Please compare with Figure B.7.*

No measures were taken to simplify the problem for the SAT solver, but the hash collision needs to be found for 24 rounds, which makes the problem hard for the SAT solver because of its increased state size.



$i$	A	W
-4	A: 01100111010001010010001100000001	
-3	A: 00010000001100100101010001110110	
-2	A: 10011000101110101101110001111110	
-1	A: 111011111100110110101110001001	
0	A: x-----	W: --x-----
1	A: -----	W: -----
2	A: -----x-----	W: x-----
3	A: xxx-----	W: -----
4	A: -----xx	W: x-----
5	A: -----xxxxxxxxxxxxx-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-----	W: -----
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: -----	

Figure B.1: Differential characteristic of MD<sub>4</sub> testcase A



$i$	A	W
-4	A: 01100111010001010010001100000001	
-3	A: 00010000001100100101010001110110	
-2	A: 1001100010111010110111001111110	
-1	A: 1110111111001101010101110001001	
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: -----	

Figure B.2: Differential characteristic of MD<sub>4</sub> testcase B

$i$	A	W
-4	A: 01100111010001010010001100000001	
-3	A: 00010000001100100101010001110110	
-2	A: 10011000101110101101110001111110	
-1	A: 111011111100110110101110001001	
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: -----	

Figure B.3: Differential characteristic of MD<sub>4</sub> testcase C

$i$		A		E		W
-4	A:	-----	E:	-----		
-3	A:	-----	E:	-----		
-2	A:	-----	E:	-----		
-1	A:	-----	E:	-----		
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:	-----

Figure B.4: SHA256 hash collision over 18 rounds

$i$		A		E		W
-4	A:	-----	E:	-----		
-3	A:	-----	E:	-----		
-2	A:	-----	E:	-----		
-1	A:	-----	E:	-----		
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:	-----

Figure B.5: SHA-256 hash collision over 21 rounds

$i$		A		E		W
-4	A:	-----	E:	-----		
-3	A:	-----	E:	-----		
-2	A:	-----	E:	-----		
-1	A:	-----	E:	-----		
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:	-----

Figure B.6: SHA-256 hash collision over 23 rounds

$i$		A		E		W
-4	A:	-----	E:	-----		
-3	A:	-----	E:	-----		
-2	A:	-----	E:	-----		
-1	A:	-----	E:	-----		
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:	-----

Figure B.7: SHA-256 hash collision over 24 rounds

## Appendix C

# Runtimes retrieved

TODO

FAILED means unexpected exit code or missing results.

TIMEOUT mean did not terminate within 1 day.

SUCCESS means SAT within 1 day.

Results cover 50 CNFs

cmsat5	83	occurences
minisat	169	occurences
lingeling-ats1o4	267	occurences
minisat-core	85	occurences
glucose-syrup	84	occurences
lingeling-ats1o1	1145	occurences
treengeling-ats1o1	84	occurences
lingeling-ats1o2	250	occurences
plingeling-ats1o1	85	occurences
cmsat4	84	occurences
glucose	84	occurences

FAILED=303    TIMEOUT=722    SUCCESS=1395

SAT solver	CNF file	simplified	phase	vars/clauses	propagation
cmsat4	algotocnf_1.cnf	none	no	48704 / 253984	
cmsat4	algotocnf_1.cnf	cmsat	no	24503 / 111931	
cmsat4	algotocnf_1.cnf	minisat	no	20895 / 118236	
cmsat4	algotocnf_1.cnf	satelite	no	27495 / 153262	
cmsat4	algotocnf_18-t9.cnf	none	no	107839 / 590953	140000
cmsat4	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139	0
cmsat4	algotocnf_18-t9.cnf	lingeling	no	107839 / 344544	90000
cmsat4	algotocnf_18-t9.cnf	minisat	no	61845 / 391134	120000
cmsat4	algotocnf_18-t9.cnf	satelite	no	69670 / 457972	0
cmsat4	algotocnf_18-t9_diff-desc.cnf	none	no	107839 / 846487	140000
cmsat4	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489	120000
cmsat4	algotocnf_18-t9_diff-desc.cnf	lingeling	no	107839 / 404666	0
cmsat4	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431	0
cmsat4	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408	140000
cmsat4	algotocnf_1_diff-desc.cnf	none	no	48704 / 373920	860000
cmsat4	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142	520000
cmsat4	algotocnf_1_diff-desc.cnf	lingeling	no	48704 / 101182	530000
cmsat4	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393	800000
cmsat4	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602	780000
cmsat4	algotocnf_2.cnf	none	no	48704 / 254210	
cmsat4	algotocnf_2.cnf	cmsat	no	24323 / 111661	
cmsat4	algotocnf_2.cnf	minisat	no	20895 / 118688	
cmsat4	algotocnf_2.cnf	satelite	no	27775 / 154276	
cmsat4	algotocnf_21-t9.cnf	none	no	116800 / 636838	
cmsat4	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308	
cmsat4	algotocnf_21-t9.cnf	minisat	no	65572 / 414470	
cmsat4	algotocnf_21-t9.cnf	satelite	no	74562 / 486714	
cmsat4	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 911629	1540000
cmsat4	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	1510000
cmsat4	algotocnf_21-t9_diff-desc.cnf	lingeling	no	116800 / 404126	1290000
cmsat4	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965	1560000
cmsat4	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	1540000
cmsat4	algotocnf_23-t9.cnf	none	no	122774 / 667438	
cmsat4	algotocnf_23-t9.cnf	cmsat	no	64880 / 369775	
cmsat4	algotocnf_23-t9.cnf	minisat	no	67979 / 429734	
cmsat4	algotocnf_23-t9.cnf	satelite	no	77835 / 506217	

SAT solver	CNF file	simplified	phase	vars/clauses	propagati
cmsat4	algotocnf_23-t9_diff-desc.cnf	none	no	122774 / 955067	
cmsat4	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118	
cmsat4	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080 / 550727	
cmsat4	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545	
cmsat4	algotocnf_24-t9.cnf	none	no	125761 / 682722	
cmsat4	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228	
cmsat4	algotocnf_24-t9.cnf	minisat	no	69023 / 436292	
cmsat4	algotocnf_24-t9.cnf	satelite	no	79486 / 515977	
cmsat4	algotocnf_24-t9_diff-desc.cnf	none	no	125761 / 976770	
cmsat4	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014	
cmsat4	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312 / 558731	
cmsat4	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154 / 750557	
cmsat4	algotocnf_27-t10-diff.cnf	none	no	134722 / 728349	o
cmsat4	algotocnf_27-t10-diff.cnf	cmsat	no	o / o	o
cmsat4	algotocnf_27-t10-diff.cnf	lingeling	no	134722 / o	o
cmsat4	algotocnf_27-t10-diff.cnf	minisat	no	o / o	o
cmsat4	algotocnf_27-t10-diff.cnf	satelite	no	o / o	o
cmsat4	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	o / o	o
cmsat4	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	134722 / o	o
cmsat4	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	o / o	o
cmsat4	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	o / o	o
cmsat4	algotocnf_27-t10-simplified.cnf	none	no	134722 / 728542	
cmsat4	algotocnf_27-t10-simplified.cnf	cmsat	no	67175 / 392680	
cmsat4	algotocnf_27-t10-simplified.cnf	minisat	no	72909 / 460404	
cmsat4	algotocnf_27-t10-simplified.cnf	satelite	no	84442 / 544998	
cmsat4	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722 / 1041847	
cmsat4	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no	56223 / 302443	
cmsat4	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no	89667 / 586309	
cmsat4	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735 / 789589	
cmsat4	algotocnf_27-t10.cnf	none	no	134722 / 728030	
cmsat4	algotocnf_27-t10.cnf	cmsat	no	72044 / 411276	
cmsat4	algotocnf_27-t10.cnf	minisat	no	73897 / 465248	
cmsat4	algotocnf_27-t10.cnf	satelite	no	85274 / 549734	
cmsat4	algotocnf_27-t10_diff-desc.cnf	none	no	134722 / 1041335	
cmsat4	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956 / 311219	

SAT solver	CNF file	simplified	phase	vars/clauses	propagation
cmsat4	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850 / 619480	
cmsat4	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733 / 857675	
cmsat4	algotocnf_2_diff-desc.cnf	none	no	48704 / 374146	950000
cmsat4	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870	550000
cmsat4	algotocnf_2_diff-desc.cnf	lingeling	no	48704 / 106546	490000
cmsat4	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436	720000
cmsat4	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577	700000
cmsat4	algotocnf_3.cnf	none	no	48704 / 254656	70000
cmsat4	algotocnf_3.cnf	cmsat	no	23893 / 111403	70000
cmsat4	algotocnf_3.cnf	lingeling	no	48704 / 100941	0
cmsat4	algotocnf_3.cnf	minisat	no	20895 / 119580	60000
cmsat4	algotocnf_3.cnf	satelite	no	28647 / 156910	60000
cmsat4	algotocnf_3_diff-desc.cnf	none	no	48704 / 374592	0
cmsat5	algotocnf_1.cnf	none	no	48704 / 253984	
cmsat5	algotocnf_1.cnf	cmsat	no	24503 / 111931	
cmsat5	algotocnf_1.cnf	minisat	no	20895 / 118236	
cmsat5	algotocnf_1.cnf	satelite	no	27495 / 153262	
cmsat5	algotocnf_18-t9.cnf	none	no	107839 / 590953	
cmsat5	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139	
cmsat5	algotocnf_18-t9.cnf	lingeling	no	107839 / 344544	
cmsat5	algotocnf_18-t9.cnf	minisat	no	61845 / 391134	
cmsat5	algotocnf_18-t9.cnf	satelite	no	69670 / 457972	
cmsat5	algotocnf_18-t9_diff-desc.cnf	none	no	107839 / 846487	
cmsat5	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489	
cmsat5	algotocnf_18-t9_diff-desc.cnf	lingeling	no	107839 / 404666	
cmsat5	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408	
cmsat5	algotocnf_1_diff-desc.cnf	none	no	48704 / 373920	
cmsat5	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142	
cmsat5	algotocnf_1_diff-desc.cnf	lingeling	no	48704 / 101182	
cmsat5	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393	
cmsat5	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602	
cmsat5	algotocnf_2.cnf	none	no	48704 / 254210	
cmsat5	algotocnf_2.cnf	cmsat	no	24323 / 111661	
cmsat5	algotocnf_2.cnf	minisat	no	20895 / 118688	
cmsat5	algotocnf_2.cnf	satelite	no	27775 / 154276	



SAT solver	CNF file	simplified	phase	vars/clauses	propagations	d
cmsat5	algotocnf_21-t9.cnf	none	no	116800 / 636838		
cmsat5	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308		
cmsat5	algotocnf_21-t9.cnf	minisat	no	65572 / 414470		
cmsat5	algotocnf_21-t9.cnf	satelite	no	74562 / 486714		
cmsat5	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 911629		2
cmsat5	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049		2
cmsat5	algotocnf_21-t9_diff-desc.cnf	lingeling	no	116800 / 404126		2
cmsat5	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965		1
cmsat5	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755		
cmsat5	algotocnf_23-t9.cnf	none	no	122774 / 667438		
cmsat5	algotocnf_23-t9.cnf	cmsat	no	64880 / 369775		
cmsat5	algotocnf_23-t9.cnf	minisat	no	67979 / 429734		
cmsat5	algotocnf_23-t9.cnf	satelite	no	77835 / 506217		
cmsat5	algotocnf_23-t9_diff-desc.cnf	none	no	122774 / 955067		3
cmsat5	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118		5
cmsat5	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080 / 550727		4
cmsat5	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545		2
cmsat5	algotocnf_24-t9.cnf	none	no	125761 / 682722		
cmsat5	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228		
cmsat5	algotocnf_24-t9.cnf	minisat	no	69023 / 436292		
cmsat5	algotocnf_24-t9.cnf	satelite	no	79486 / 515977		
cmsat5	algotocnf_24-t9_diff-desc.cnf	none	no	125761 / 976770		5
cmsat5	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014		7
cmsat5	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312 / 558731		4
cmsat5	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154 / 750557		3
cmsat5	algotocnf_27-t10-diff.cnf	none	no	134722 / 728349		
cmsat5	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0		
cmsat5	algotocnf_27-t10-diff.cnf	lingeling	no	134722 / 0		
cmsat5	algotocnf_27-t10-diff.cnf	minisat	no	0 / 0		
cmsat5	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0		
cmsat5	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0		
cmsat5	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	134722 / 0		
cmsat5	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0		
cmsat5	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0		
cmsat5	algotocnf_27-t10-simplified.cnf	none	no	134722 / 728542		

SAT solver	CNF file	simplified	phase	vars/clauses
cmsat5	algotocnf_27-t10-simplified.cnf	cmsat	no	67175 / 392680
cmsat5	algotocnf_27-t10-simplified.cnf	minisat	no	72909 / 460404
cmsat5	algotocnf_27-t10-simplified.cnf	satelite	no	84442 / 544998
cmsat5	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722 / 1041847
cmsat5	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no	56223 / 302443
cmsat5	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no	89667 / 586309
cmsat5	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735 / 789589
cmsat5	algotocnf_27-t10.cnf	none	no	134722 / 728030
cmsat5	algotocnf_27-t10.cnf	cmsat	no	72044 / 411276
cmsat5	algotocnf_27-t10.cnf	minisat	no	73897 / 465248
cmsat5	algotocnf_27-t10.cnf	satelite	no	85274 / 549734
cmsat5	algotocnf_27-t10_diff-desc.cnf	none	no	134722 / 1041335
cmsat5	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956 / 311219
cmsat5	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850 / 619480
cmsat5	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733 / 857675
cmsat5	algotocnf_2_diff-desc.cnf	none	no	48704 / 374146
cmsat5	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870
cmsat5	algotocnf_2_diff-desc.cnf	lingeling	no	48704 / 106546
cmsat5	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436
cmsat5	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577
cmsat5	algotocnf_3.cnf	none	no	48704 / 254656
cmsat5	algotocnf_3.cnf	cmsat	no	23893 / 111403
cmsat5	algotocnf_3.cnf	lingeling	no	48704 / 100941
cmsat5	algotocnf_3.cnf	minisat	no	20895 / 119580
cmsat5	algotocnf_3.cnf	satelite	no	28647 / 156910
cmsat5	algotocnf_3_diff-desc.cnf	none	no	48704 / 374592
glucose	algotocnf_1.cnf	none	no	48704 / 225124
glucose	algotocnf_1.cnf	cmsat	no	24503 / 111931
glucose	algotocnf_1.cnf	minisat	no	20895 / 118236
glucose	algotocnf_1.cnf	satelite	no	27495 / 153262
glucose	algotocnf_18-t9.cnf	none	no	107839 / 582936
glucose	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139
glucose	algotocnf_18-t9.cnf	lingeling	no	102616 / 344544
glucose	algotocnf_18-t9.cnf	minisat	no	61845 / 391134
glucose	algotocnf_18-t9.cnf	satelite	no	69670 / 457972

SAT solver	CNF file	simplified	phase	vars/clauses	propagations	decisions
glucose	algotocnf_18-t9_diff-desc.cnf	none	no	107839 / 831263	10471476	6444
glucose	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489	20143829	12469
glucose	algotocnf_18-t9_diff-desc.cnf	lingeling	no	99452 / 404666	7239871	7647
glucose	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431	15403560	9340
glucose	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408	30131933	15390
glucose	algotocnf_1_diff-desc.cnf	none	no	48704 / 330692	1231386505	47264
glucose	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142	1038552689	32670
glucose	algotocnf_1_diff-desc.cnf	lingeling	no	40554 / 101182	1251948097	59378
glucose	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393	785694216	29540
glucose	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602	751454677	28310
glucose	algotocnf_2.cnf	none	no	48704 / 224220		
glucose	algotocnf_2.cnf	cmsat	no	24323 / 111661		
glucose	algotocnf_2.cnf	minisat	no	20895 / 118688		
glucose	algotocnf_2.cnf	satelite	no	27775 / 154276		
glucose	algotocnf_21-t9.cnf	none	no	116800 / 627112		
glucose	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308		
glucose	algotocnf_21-t9.cnf	minisat	no	65572 / 414470		
glucose	algotocnf_21-t9.cnf	satelite	no	74562 / 486714		
glucose	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 894072		
glucose	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	2790904343	82667
glucose	algotocnf_21-t9_diff-desc.cnf	lingeling	no	104860 / 404126	1838242760	74906
glucose	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965	3062139546	87991
glucose	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	3468599865	98765
glucose	algotocnf_23-t9.cnf	none	no	122774 / 656628		
glucose	algotocnf_23-t9.cnf	cmsat	no	64880 / 369775		
glucose	algotocnf_23-t9.cnf	minisat	no	67979 / 429734		
glucose	algotocnf_23-t9.cnf	satelite	no	77835 / 506217		
glucose	algotocnf_23-t9_diff-desc.cnf	none	no	122774 / 936270		
glucose	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118		
glucose	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080 / 550727		
glucose	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545		
glucose	algotocnf_24-t9.cnf	none	no	125761 / 671432		
glucose	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228		
glucose	algotocnf_24-t9.cnf	minisat	no	69023 / 436292		
glucose	algotocnf_24-t9.cnf	satelite	no	79486 / 515977		

SAT solver	CNF file	simplified	phase	vars/clauses
glucose	algotocnf_24-t9_diff-desc.cnf	none	no	125761 / 957493
glucose	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014
glucose	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312 / 558731
glucose	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154 / 750557
glucose	algotocnf_27-t10-diff.cnf	none	no	134722 / 8320
glucose	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0
glucose	algotocnf_27-t10-diff.cnf	lingeling	no	0 / 0
glucose	algotocnf_27-t10-diff.cnf	minisat	no	0 / 0
glucose	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0
glucose	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0
glucose	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	0 / 0
glucose	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0
glucose	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0
glucose	algotocnf_27-t10-simplified.cnf	none	no	134722 / 715830
glucose	algotocnf_27-t10-simplified.cnf	cmsat	no	67175 / 392680
glucose	algotocnf_27-t10-simplified.cnf	minisat	no	72909 / 460404
glucose	algotocnf_27-t10-simplified.cnf	satelite	no	84442 / 544998
glucose	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722 / 1020826
glucose	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no	56223 / 302443
glucose	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no	89667 / 586309
glucose	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735 / 789589
glucose	algotocnf_27-t10.cnf	none	no	134722 / 717878
glucose	algotocnf_27-t10.cnf	cmsat	no	72044 / 411276
glucose	algotocnf_27-t10.cnf	minisat	no	73897 / 465248
glucose	algotocnf_27-t10.cnf	satelite	no	85274 / 549734
glucose	algotocnf_27-t10_diff-desc.cnf	none	no	134722 / 1022874
glucose	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956 / 311219
glucose	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850 / 619480
glucose	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733 / 857675
glucose	algotocnf_2_diff-desc.cnf	none	no	48704 / 329788
glucose	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870
glucose	algotocnf_2_diff-desc.cnf	lingeling	no	40767 / 106546
glucose	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436
glucose	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577
glucose	algotocnf_3.cnf	none	no	48704 / 222436

SAT solver	CNF file	simplified	phase	vars/clauses	propagations	decision
glucose	algotocnf_3.cnf	cmsat	no	23893 / 111403	23157475	127
glucose	algotocnf_3.cnf	lingeling	no	44000 / 100941	9187396	73
glucose	algotocnf_3.cnf	minisat	no	20895 / 119580	16616478	104
glucose	algotocnf_3.cnf	satelite	no	28647 / 156910	15878157	100
glucose	algotocnf_3_diff-desc.cnf	none	no	48704 / 328004	9899755	53
glucose-syrup	algotocnf_1.cnf	none	no	48704 / 225124		1739
glucose-syrup	algotocnf_1.cnf	cmsat	no	24503 / 111931		1289
glucose-syrup	algotocnf_1.cnf	minisat	no	20895 / 118236		1306
glucose-syrup	algotocnf_1.cnf	satelite	no	27495 / 153262		1303
glucose-syrup	algotocnf_18-t9.cnf	none	no	107839 / 582936		62
glucose-syrup	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139		64
glucose-syrup	algotocnf_18-t9.cnf	lingeling	no	102616 / 344544		49
glucose-syrup	algotocnf_18-t9.cnf	minisat	no	61845 / 391134		72
glucose-syrup	algotocnf_18-t9.cnf	satelite	no	69670 / 457972		68
glucose-syrup	algotocnf_18-t9_diff-desc.cnf	none	no	107839 / 831263		74
glucose-syrup	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489		201
glucose-syrup	algotocnf_18-t9_diff-desc.cnf	lingeling	no	99452 / 404666		48
glucose-syrup	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431		53
glucose-syrup	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408		59
glucose-syrup	algotocnf_1_diff-desc.cnf	none	no	48704 / 330692		281
glucose-syrup	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142		856
glucose-syrup	algotocnf_1_diff-desc.cnf	lingeling	no	40554 / 101182		120
glucose-syrup	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393		764
glucose-syrup	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602		133
glucose-syrup	algotocnf_2.cnf	none	no	48704 / 224220		1743
glucose-syrup	algotocnf_2.cnf	cmsat	no	24323 / 111661		1497
glucose-syrup	algotocnf_2.cnf	minisat	no	20895 / 118688		1414
glucose-syrup	algotocnf_2.cnf	satelite	no	27775 / 154276		1717
glucose-syrup	algotocnf_21-t9.cnf	none	no	116800 / 627112		822
glucose-syrup	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308		872
glucose-syrup	algotocnf_21-t9.cnf	minisat	no	65572 / 414470		788
glucose-syrup	algotocnf_21-t9.cnf	satelite	no	74562 / 486714		806
glucose-syrup	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 894072		485
glucose-syrup	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049		246
glucose-syrup	algotocnf_21-t9_diff-desc.cnf	lingeling	no	104860 / 404126		305

SAT solver	CNF file	simplified	phase	vars/clauses
glucose-syrup	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965
glucose-syrup	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755
glucose-syrup	algotocnf_23-t9.cnf	none	no	122774 / 656628
glucose-syrup	algotocnf_23-t9.cnf	cmsat	no	64880 / 369775
glucose-syrup	algotocnf_23-t9.cnf	minisat	no	67979 / 429734
glucose-syrup	algotocnf_23-t9.cnf	satelite	no	77835 / 506217
glucose-syrup	algotocnf_23-t9_diff-desc.cnf	none	no	122774 / 936270
glucose-syrup	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118
glucose-syrup	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080 / 550727
glucose-syrup	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545
glucose-syrup	algotocnf_24-t9.cnf	none	no	125761 / 671432
glucose-syrup	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228
glucose-syrup	algotocnf_24-t9.cnf	minisat	no	69023 / 436292
glucose-syrup	algotocnf_24-t9.cnf	satelite	no	79486 / 515977
glucose-syrup	algotocnf_24-t9_diff-desc.cnf	none	no	125761 / 957493
glucose-syrup	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014
glucose-syrup	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312 / 558731
glucose-syrup	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154 / 750557
glucose-syrup	algotocnf_27-t10-diff.cnf	none	no	134722 / 8320
glucose-syrup	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff.cnf	lingeling	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff.cnf	minisat	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0
glucose-syrup	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0
glucose-syrup	algotocnf_27-t10-simplified.cnf	none	no	134722 / 715830
glucose-syrup	algotocnf_27-t10-simplified.cnf	cmsat	no	67175 / 392680
glucose-syrup	algotocnf_27-t10-simplified.cnf	minisat	no	72909 / 460404
glucose-syrup	algotocnf_27-t10-simplified.cnf	satelite	no	84442 / 544998
glucose-syrup	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722 / 1020826
glucose-syrup	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no	56223 / 302443
glucose-syrup	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no	89667 / 586309
glucose-syrup	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735 / 789589

SAT solver	CNF file	simplified	phase	vars/clauses	propagations
glucose-syrup	algotocnf_27-t10.cnf	none	no	134722 / 717878	
glucose-syrup	algotocnf_27-t10.cnf	cmsat	no	72044 / 411276	
glucose-syrup	algotocnf_27-t10.cnf	minisat	no	73897 / 465248	
glucose-syrup	algotocnf_27-t10.cnf	satelite	no	85274 / 549734	
glucose-syrup	algotocnf_27-t10_diff-desc.cnf	none	no	134722 / 1022874	
glucose-syrup	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956 / 311219	
glucose-syrup	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850 / 619480	
glucose-syrup	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733 / 857675	
glucose-syrup	algotocnf_2_diff-desc.cnf	none	no	48704 / 329788	
glucose-syrup	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870	
glucose-syrup	algotocnf_2_diff-desc.cnf	lingeling	no	40767 / 106546	
glucose-syrup	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436	
glucose-syrup	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577	
glucose-syrup	algotocnf_3.cnf	none	no	48704 / 222436	
glucose-syrup	algotocnf_3.cnf	cmsat	no	23893 / 111403	
glucose-syrup	algotocnf_3.cnf	lingeling	no	44000 / 100941	
glucose-syrup	algotocnf_3.cnf	minisat	no	20895 / 119580	
glucose-syrup	algotocnf_3.cnf	satelite	no	28647 / 156910	
glucose-syrup	algotocnf_3_diff-desc.cnf	none	no	48704 / 328004	
lingeling-ats101	algotocnf_1.cnf	cmsat	no	24503 / 111931	830112341
lingeling-ats101	algotocnf_1.cnf	cmsat	yes	24503 / 111931	820517590
lingeling-ats101	algotocnf_1.cnf	minisat	no	20895 / 118236	575783290
lingeling-ats101	algotocnf_1.cnf	minisat	yes	20895 / 118236	333100908
lingeling-ats101	algotocnf_1.cnf	satelite	no	27495 / 153262	855959855
lingeling-ats101	algotocnf_1.cnf	satelite	yes	27495 / 153262	455268862
lingeling-ats101	algotocnf_18-t9.cnf	none	no	107839 / 590953	6579999
lingeling-ats101	algotocnf_18-t9.cnf	none	yes	107839 / 590953	6637382
lingeling-ats101	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139	19838315
lingeling-ats101	algotocnf_18-t9.cnf	cmsat	yes	61789 / 342139	20128556
lingeling-ats101	algotocnf_18-t9.cnf	lingeling	no	102616 / 344544	4891154
lingeling-ats101	algotocnf_18-t9.cnf	lingeling	yes	102616 / 344544	3026807
lingeling-ats101	algotocnf_18-t9.cnf	minisat	no	61845 / 391134	6037622
lingeling-ats101	algotocnf_18-t9.cnf	minisat	yes	61845 / 391134	8386925
lingeling-ats101	algotocnf_18-t9.cnf	satelite	no	69670 / 457972	4521332
lingeling-ats101	algotocnf_18-t9.cnf	satelite	yes	69670 / 457972	6584687

SAT solver	CNF file	simplified	phase	vars/clauses
lingeling-ats101	algotocnf_18-t9_diff-desc-sc_ocnf.cnf	none	no	196473 / 1197423
lingeling-ats101	algotocnf_18-t9_diff-desc-sc_ocnf.cnf	none	yes	196473 / 1197423
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	none	yes	107839 / 846487
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	cmsat	yes	57114 / 303489
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	lingeling	no	99452 / 404666
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	lingeling	yes	99452 / 404666
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	minisat	yes	78055 / 511431
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408
lingeling-ats101	algotocnf_18-t9_diff-desc.cnf	satelite	yes	85386 / 692408
lingeling-ats101	algotocnf_18-t9_diff-desc_ocnf.cnf	none	no	107839 / 846487
lingeling-ats101	algotocnf_18-t9_diff-desc_ocnf.cnf	none	yes	107839 / 846487
lingeling-ats101	algotocnf_18-t9_ocnf.cnf	none	no	107839 / 590953
lingeling-ats101	algotocnf_18-t9_ocnf.cnf	none	yes	107839 / 590953
lingeling-ats101	algotocnf_1_diff-desc-sc_ocnf.cnf	none	no	85760 / 522144
lingeling-ats101	algotocnf_1_diff-desc-sc_ocnf.cnf	none	yes	85760 / 522144
lingeling-ats101	algotocnf_1_diff-desc.cnf	none	no	48704 / 373920
lingeling-ats101	algotocnf_1_diff-desc.cnf	none	yes	48704 / 373920
lingeling-ats101	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142
lingeling-ats101	algotocnf_1_diff-desc.cnf	cmsat	yes	15402 / 73142
lingeling-ats101	algotocnf_1_diff-desc.cnf	lingeling	no	40554 / 101182
lingeling-ats101	algotocnf_1_diff-desc.cnf	lingeling	yes	40554 / 101182
lingeling-ats101	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393
lingeling-ats101	algotocnf_1_diff-desc.cnf	minisat	yes	25107 / 158393
lingeling-ats101	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602
lingeling-ats101	algotocnf_1_diff-desc.cnf	satelite	yes	30950 / 226602
lingeling-ats101	algotocnf_1_diff-desc_ocnf.cnf	none	no	48704 / 373920
lingeling-ats101	algotocnf_1_diff-desc_ocnf.cnf	none	yes	48704 / 373920
lingeling-ats101	algotocnf_1_ocnf.cnf	none	no	48704 / 253984
lingeling-ats101	algotocnf_1_ocnf.cnf	none	yes	48704 / 253984
lingeling-ats101	algotocnf_2.cnf	none	no	48704 / 254210
lingeling-ats101	algotocnf_2.cnf	none	yes	48704 / 254210
lingeling-ats101	algotocnf_2.cnf	cmsat	no	24323 / 111661
lingeling-ats101	algotocnf_2.cnf	cmsat	yes	24323 / 111661



SAT solver	CNF file	simplified	phase	vars/clauses	propagat
lingeling-ats101	algotocnf_2.cnf	minisat	no	20895 / 118688	2541176
lingeling-ats101	algotocnf_2.cnf	minisat	yes	20895 / 118688	1376618
lingeling-ats101	algotocnf_2.cnf	satelite	no	27775 / 154276	3691672
lingeling-ats101	algotocnf_2.cnf	satelite	yes	27775 / 154276	5825908
lingeling-ats101	algotocnf_21-t9.cnf	none	no	116800 / 636838	6567493
lingeling-ats101	algotocnf_21-t9.cnf	none	yes	116800 / 636838	1224816
lingeling-ats101	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308	8081065
lingeling-ats101	algotocnf_21-t9.cnf	cmsat	yes	63555 / 358308	5169630
lingeling-ats101	algotocnf_21-t9.cnf	minisat	no	65572 / 414470	7555279
lingeling-ats101	algotocnf_21-t9.cnf	minisat	yes	65572 / 414470	3766091
lingeling-ats101	algotocnf_21-t9.cnf	satelite	no	74562 / 486714	9417657
lingeling-ats101	algotocnf_21-t9.cnf	satelite	yes	74562 / 486714	5033023
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 911629	3799761
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	none	yes	116800 / 911629	8977998
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	1939016
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	cmsat	yes	59528 / 318049	7115202
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965	1719807
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	minisat	yes	81650 / 534965	1086561
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	8199245
lingeling-ats101	algotocnf_21-t9_diff-desc.cnf	satelite	yes	90236 / 720755	4633920
lingeling-ats101	algotocnf_21-t9_diff-desc_ocnf.cnf	none	no	116800 / 911629	4787172
lingeling-ats101	algotocnf_21-t9_diff-desc_ocnf.cnf	none	yes	116800 / 911629	5057198
lingeling-ats101	algotocnf_23-t9.cnf	none	no	122774 / 667438	1140674
lingeling-ats101	algotocnf_23-t9.cnf	none	yes	122774 / 667438	9255197
lingeling-ats101	algotocnf_23-t9.cnf	cmsat	no	64880 / 369775	9492444
lingeling-ats101	algotocnf_23-t9.cnf	cmsat	yes	64880 / 369775	14551473
lingeling-ats101	algotocnf_23-t9.cnf	minisat	no	67979 / 429734	7755711
lingeling-ats101	algotocnf_23-t9.cnf	satelite	no	77835 / 506217	9669970
lingeling-ats101	algotocnf_23-t9.cnf	satelite	yes	77835 / 506217	10029572
lingeling-ats101	algotocnf_23-t9_diff-desc-sc_ocnf.cnf	none	no	222613 / 1350343	35575573
lingeling-ats101	algotocnf_23-t9_diff-desc-sc_ocnf.cnf	none	yes	222613 / 1350343	41256543
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	none	no	122774 / 955067	9459499
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	none	yes	122774 / 955067	6955287
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118	7067769
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	cmsat	yes	57510 / 307118	1221950

SAT solver	CNF file	simplified	phase	vars/clauses
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080 / 550727
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	minisat	yes	84080 / 550727
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545
lingeling-ats101	algotocnf_23-t9_diff-desc.cnf	satelite	yes	93504 / 740545
lingeling-ats101	algotocnf_23-t9_diff-desc_ocnf.cnf	none	no	122774 / 955067
lingeling-ats101	algotocnf_23-t9_diff-desc_ocnf.cnf	none	yes	122774 / 955067
lingeling-ats101	algotocnf_23-t9_ocnf.cnf	none	no	122774 / 667438
lingeling-ats101	algotocnf_23-t9_ocnf.cnf	none	yes	122774 / 667438
lingeling-ats101	algotocnf_24-t9.cnf	none	no	125761 / 682722
lingeling-ats101	algotocnf_24-t9.cnf	none	yes	125761 / 682722
lingeling-ats101	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228
lingeling-ats101	algotocnf_24-t9.cnf	cmsat	yes	65579 / 377228
lingeling-ats101	algotocnf_24-t9.cnf	minisat	no	69023 / 436292
lingeling-ats101	algotocnf_24-t9.cnf	minisat	yes	69023 / 436292
lingeling-ats101	algotocnf_24-t9.cnf	satelite	no	79486 / 515977
lingeling-ats101	algotocnf_24-t9.cnf	satelite	yes	79486 / 515977
lingeling-ats101	algotocnf_24-t9_diff-desc-sc_ocnf.cnf	none	no	227841 / 1380914
lingeling-ats101	algotocnf_24-t9_diff-desc-sc_ocnf.cnf	none	yes	227841 / 1380914
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	none	no	125761 / 976770
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	none	yes	125761 / 976770
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	cmsat	yes	56447 / 302014
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312 / 558731
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	minisat	yes	85312 / 558731
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154 / 750557
lingeling-ats101	algotocnf_24-t9_diff-desc.cnf	satelite	yes	95154 / 750557
lingeling-ats101	algotocnf_24-t9_diff-desc_ocnf.cnf	none	no	125761 / 976770
lingeling-ats101	algotocnf_24-t9_diff-desc_ocnf.cnf	none	yes	125761 / 976770
lingeling-ats101	algotocnf_27-t10-diff.cnf	none	no	134722 / 728349
lingeling-ats101	algotocnf_27-t10-diff.cnf	none	yes	134722 / 728349
lingeling-ats101	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff.cnf	cmsat	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff.cnf	lingeling	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff.cnf	lingeling	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff.cnf	minisat	no	0 / 0

SAT solver	CNF file	simplified	phase	vars/clauses
lingeling-ats101	algotocnf_27-t10-diff.cnf	minisat	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff.cnf	satelite	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	none	no	134722 / 1041654
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	none	yes	134722 / 1041654
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	minisat	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	satelite	yes	0 / 0
lingeling-ats101	algotocnf_27-t10-diff_diff-desc_ocnf.cnf	none	no	134722 / 1041654
lingeling-ats101	algotocnf_27-t10-diff_diff-desc_ocnf.cnf	none	yes	134722 / 1041654
lingeling-ats101	algotocnf_27-t10-diff_ocnf.cnf	none	no	134722 / 728349
lingeling-ats101	algotocnf_27-t10-diff_ocnf.cnf	none	yes	134722 / 728349
lingeling-ats101	algotocnf_27-t10-simplified.cnf	none	no	134722 / 728542
lingeling-ats101	algotocnf_27-t10-simplified.cnf	none	yes	134722 / 728542
lingeling-ats101	algotocnf_27-t10-simplified.cnf	cmsat	no	67175 / 392680
lingeling-ats101	algotocnf_27-t10-simplified.cnf	cmsat	yes	67175 / 392680
lingeling-ats101	algotocnf_27-t10-simplified.cnf	minisat	no	72909 / 460404
lingeling-ats101	algotocnf_27-t10-simplified.cnf	minisat	yes	72909 / 460404
lingeling-ats101	algotocnf_27-t10-simplified.cnf	satelite	no	84442 / 544998
lingeling-ats101	algotocnf_27-t10-simplified.cnf	satelite	yes	84442 / 544998
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc-sc_ocnf.cnf	none	no	243525 / 1472595
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc-sc_ocnf.cnf	none	yes	243525 / 1472595
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722 / 1041847
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	none	yes	134722 / 1041847
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735 / 789589
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	yes	100735 / 789589
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc_ocnf.cnf	none	no	134722 / 1041847
lingeling-ats101	algotocnf_27-t10-simplified_diff-desc_ocnf.cnf	none	yes	134722 / 1041847
lingeling-ats101	algotocnf_27-t10-simplified_ocnf.cnf	none	no	134722 / 728542
lingeling-ats101	algotocnf_27-t10-simplified_ocnf.cnf	none	yes	134722 / 728542

SAT solver	CNF file	simplified	phase	vars/clauses
lingeling-ats101	algotocnf_27-t10.cnf	none	no	134722 / 728030
lingeling-ats101	algotocnf_27-t10.cnf	none	yes	134722 / 728030
lingeling-ats101	algotocnf_27-t10.cnf	cmsat	no	72044 / 411276
lingeling-ats101	algotocnf_27-t10.cnf	cmsat	yes	72044 / 411276
lingeling-ats101	algotocnf_27-t10.cnf	minisat	no	73897 / 465248
lingeling-ats101	algotocnf_27-t10.cnf	minisat	yes	73897 / 465248
lingeling-ats101	algotocnf_27-t10_diff-desc-sc_ocnf.cnf	none	no	243525 / 1472083
lingeling-ats101	algotocnf_27-t10_diff-desc-sc_ocnf.cnf	none	yes	243525 / 1472083
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	none	no	134722 / 1041335
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	none	yes	134722 / 1041335
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956 / 311219
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	cmsat	yes	57956 / 311219
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850 / 619480
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733 / 857675
lingeling-ats101	algotocnf_27-t10_diff-desc.cnf	satelite	yes	105733 / 857675
lingeling-ats101	algotocnf_27-t10_diff-desc_ocnf.cnf	none	no	134722 / 1041335
lingeling-ats101	algotocnf_27-t10_diff-desc_ocnf.cnf	none	yes	134722 / 1041335
lingeling-ats101	algotocnf_27-t10_ocnf.cnf	none	no	134722 / 728030
lingeling-ats101	algotocnf_27-t10_ocnf.cnf	none	yes	134722 / 728030
lingeling-ats101	algotocnf_2_diff-desc-sc_ocnf.cnf	none	no	85760 / 522370
lingeling-ats101	algotocnf_2_diff-desc-sc_ocnf.cnf	none	yes	85760 / 522370
lingeling-ats101	algotocnf_2_diff-desc.cnf	none	no	48704 / 374146
lingeling-ats101	algotocnf_2_diff-desc.cnf	none	yes	48704 / 374146
lingeling-ats101	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870
lingeling-ats101	algotocnf_2_diff-desc.cnf	cmsat	yes	15342 / 72870
lingeling-ats101	algotocnf_2_diff-desc.cnf	lingeling	no	40767 / 106546
lingeling-ats101	algotocnf_2_diff-desc.cnf	lingeling	yes	40767 / 106546
lingeling-ats101	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436
lingeling-ats101	algotocnf_2_diff-desc.cnf	minisat	yes	23531 / 149436
lingeling-ats101	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577
lingeling-ats101	algotocnf_2_diff-desc.cnf	satelite	yes	29428 / 204577
lingeling-ats101	algotocnf_2_diff-desc_ocnf.cnf	none	no	48704 / 374146
lingeling-ats101	algotocnf_2_diff-desc_ocnf.cnf	none	yes	48704 / 374146
lingeling-ats101	algotocnf_2_ocnf.cnf	none	no	48704 / 254210
lingeling-ats101	algotocnf_2_ocnf.cnf	none	yes	48704 / 254210

SAT solver	CNF file	simplified	phase	vars/clauses	propagat
lingeling-ats101	algotocnf_3.cnf	none	no	48704 / 254656	1384778
lingeling-ats101	algotocnf_3.cnf	none	yes	48704 / 254656	1300597
lingeling-ats101	algotocnf_3.cnf	cmsat	no	23893 / 111403	2581772
lingeling-ats101	algotocnf_3.cnf	cmsat	yes	23893 / 111403	2729811
lingeling-ats101	algotocnf_3.cnf	lingeling	no	44000 / 100941	1075071
lingeling-ats101	algotocnf_3.cnf	lingeling	yes	44000 / 100941	998189
lingeling-ats101	algotocnf_3.cnf	minisat	no	20895 / 119580	1174573
lingeling-ats101	algotocnf_3.cnf	minisat	yes	20895 / 119580	1024653
lingeling-ats101	algotocnf_3.cnf	satelite	no	28647 / 156910	1791273
lingeling-ats101	algotocnf_3.cnf	satelite	yes	28647 / 156910	1577492
lingeling-ats101	algotocnf_3_diff-desc-sc_ocnf.cnf	none	no	85760 / 522816	3147777
lingeling-ats101	algotocnf_3_diff-desc-sc_ocnf.cnf	none	yes	85760 / 522816	3776333
lingeling-ats101	algotocnf_3_diff-desc.cnf	none	no	48704 / 374592	521025
lingeling-ats101	algotocnf_3_diff-desc.cnf	none	yes	48704 / 374592	344378
lingeling-ats101	algotocnf_3_diff-desc_ocnf.cnf	none	no	48704 / 374592	629567
lingeling-ats101	algotocnf_3_diff-desc_ocnf.cnf	none	yes	48704 / 374592	556136
lingeling-ats101	algotocnf_3_ocnf.cnf	none	no	48704 / 254656	1378843
lingeling-ats101	algotocnf_3_ocnf.cnf	none	yes	48704 / 254656	122475
lingeling-ats102	algotocnf_18-t9_diff-desc_ocnf.cnf	none	no	107839 / 846487	2919960
lingeling-ats102	algotocnf_1_diff-desc_ocnf.cnf	none	no	48704 / 373920	1385390
lingeling-ats102	algotocnf_1_ocnf.cnf	none	no	48704 / 253984	2233118
lingeling-ats102	algotocnf_21-t9.cnf	none	no	116800 / 636838	6567493
lingeling-ats102	algotocnf_21-t9.cnf	satelite	no	74562 / 486714	9417657
lingeling-ats102	algotocnf_21-t9_diff-desc-sc_ocnf.cnf	none	no	212157 / 1289169	13886232
lingeling-ats102	algotocnf_21-t9_diff-desc.cnf	lingeling	no	104860 / 404126	2064556
lingeling-ats102	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	2367713
lingeling-ats102	algotocnf_21-t9_diff-desc_ocnf.cnf	none	no	116800 / 911629	3524212
lingeling-ats102	algotocnf_21-t9_ocnf.cnf	none	no	116800 / 636838	1268850
lingeling-ats102	algotocnf_23-t9.cnf	satelite	no	77835 / 506217	11185442
lingeling-ats102	algotocnf_23-t9_diff-desc-sc_ocnf.cnf	none	no	222613 / 1350343	13598362
lingeling-ats102	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545	2975485
lingeling-ats102	algotocnf_24-t9.cnf	none	no	125761 / 682722	8197106
lingeling-ats102	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228	13872340
lingeling-ats102	algotocnf_24-t9.cnf	minisat	no	69023 / 436292	10756062
lingeling-ats102	algotocnf_24-t9_diff-desc-sc_ocnf.cnf	none	no	227841 / 1380914	15199857

SAT solver	CNF file	simplified	phase	vars/
lingeling-ats102	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447
lingeling-ats102	algotocnf_24-t9_diff-desc_ocnf.cnf	none	no	125761
lingeling-ats102	algotocnf_24-t9_ocnf.cnf	none	no	125761
lingeling-ats102	algotocnf_27-t10_diff.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10_diff.cnf	cmsat	no	0
lingeling-ats102	algotocnf_27-t10_diff.cnf	lingeling	no	0
lingeling-ats102	algotocnf_27-t10_diff.cnf	satelite	no	0
lingeling-ats102	algotocnf_27-t10_diff_diff-desc.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10_diff_diff-desc.cnf	cmsat	no	0
lingeling-ats102	algotocnf_27-t10_diff_diff-desc.cnf	lingeling	no	0
lingeling-ats102	algotocnf_27-t10_diff_diff-desc.cnf	minisat	no	0
lingeling-ats102	algotocnf_27-t10_diff_diff-desc.cnf	satelite	no	0
lingeling-ats102	algotocnf_27-t10_diff_diff-desc_ocnf.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10_diff_ocnf.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10-simplified.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10-simplified.cnf	cmsat	no	67175
lingeling-ats102	algotocnf_27-t10-simplified.cnf	minisat	no	72909
lingeling-ats102	algotocnf_27-t10-simplified.cnf	satelite	no	84442
lingeling-ats102	algotocnf_27-t10-simplified_diff-desc-sc_ocnf.cnf	none	no	243525
lingeling-ats102	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no	56223
lingeling-ats102	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735
lingeling-ats102	algotocnf_27-t10-simplified_diff-desc_ocnf.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10-simplified_ocnf.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10.cnf	cmsat	no	72044
lingeling-ats102	algotocnf_27-t10_diff-desc-sc_ocnf.cnf	none	no	243525
lingeling-ats102	algotocnf_27-t10_diff-desc.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956
lingeling-ats102	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733
lingeling-ats102	algotocnf_27-t10_diff-desc_ocnf.cnf	none	no	134722
lingeling-ats102	algotocnf_27-t10_ocnf.cnf	none	no	134722
lingeling-ats102	algotocnf_2_diff-desc_ocnf.cnf	none	no	48704
lingeling-ats102	algotocnf_2_ocnf.cnf	none	no	48704
lingeling-ats102	algotocnf_3_ocnf.cnf	none	no	48704
lingeling-ats104	algotocnf_18-t9_diff-desc-sc_ocnf.cnf	none	no	196473

SAT solver	CNF file	simplified	phase	vars/clauses	prop
lingeling-ats104	algotocnf_18-t9_ocnf.cnf	none	no	107839 / 590953	49
lingeling-ats104	algotocnf_1_diff-desc_ocnf.cnf	none	no	48704 / 373920	119
lingeling-ats104	algotocnf_1_ocnf.cnf	none	no	48704 / 253984	20
lingeling-ats104	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308	808
lingeling-ats104	algotocnf_21-t9.cnf	satelite	no	74562 / 486714	941
lingeling-ats104	algotocnf_21-t9_diff-desc-sc_ocnf.cnf	none	no	212157 / 1289169	159
lingeling-ats104	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 911629	379
lingeling-ats104	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	76
lingeling-ats104	algotocnf_21-t9_diff-desc.cnf	lingeling	no	104860 / 404126	206
lingeling-ats104	algotocnf_21-t9_diff-desc_ocnf.cnf	none	no	116800 / 911629	249
lingeling-ats104	algotocnf_21-t9_ocnf.cnf	none	no	116800 / 636838	14
lingeling-ats104	algotocnf_23-t9.cnf	satelite	no	77835 / 506217	104
lingeling-ats104	algotocnf_23-t9_diff-desc-sc_ocnf.cnf	none	no	222613 / 1350343	963
lingeling-ats104	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545	254
lingeling-ats104	algotocnf_23-t9_diff-desc_ocnf.cnf	none	no	122774 / 955067	251
lingeling-ats104	algotocnf_23-t9_ocnf.cnf	none	no	122774 / 667438	89
lingeling-ats104	algotocnf_24-t9.cnf	none	no	125761 / 682722	819
lingeling-ats104	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228	150
lingeling-ats104	algotocnf_24-t9.cnf	minisat	no	69023 / 436292	107
lingeling-ats104	algotocnf_24-t9_diff-desc-sc_ocnf.cnf	none	no	227841 / 1380914	116
lingeling-ats104	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014	135
lingeling-ats104	algotocnf_24-t9_diff-desc_ocnf.cnf	none	no	125761 / 976770	344
lingeling-ats104	algotocnf_24-t9_ocnf.cnf	none	no	125761 / 682722	36
lingeling-ats104	algotocnf_27-t10-diff.cnf	none	no	134722 / 728349	1
lingeling-ats104	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff.cnf	lingeling	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff_diff-desc-sc_ocnf.cnf	none	no	243525 / 1472402	2
lingeling-ats104	algotocnf_27-t10-diff_diff-desc.cnf	none	no	134722 / 1041654	1
lingeling-ats104	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0	
lingeling-ats104	algotocnf_27-t10-diff_diff-desc_ocnf.cnf	none	no	134722 / 1041654	1
lingeling-ats104	algotocnf_27-t10-diff_ocnf.cnf	none	no	134722 / 728349	1

SAT solver	CNF file	simplified	phase	vars/
lingeling-ats104	algotocnf_27-t10-simplified.cnf	none	no	134722
lingeling-ats104	algotocnf_27-t10-simplified.cnf	minisat	no	72909
lingeling-ats104	algotocnf_27-t10-simplified.cnf	satelite	no	84442
lingeling-ats104	algotocnf_27-t10-simplified_diff-desc-sc_ocnf.cnf	none	no	243525
lingeling-ats104	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722
lingeling-ats104	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735
lingeling-ats104	algotocnf_27-t10-simplified_diff-desc_ocnf.cnf	none	no	134722
lingeling-ats104	algotocnf_27-t10-simplified_ocnf.cnf	none	no	134722
lingeling-ats104	algotocnf_27-t10.cnf	none	no	134722
lingeling-ats104	algotocnf_27-t10.cnf	cmsat	no	72044
lingeling-ats104	algotocnf_27-t10.cnf	minisat	no	73897
lingeling-ats104	algotocnf_27-t10.cnf	satelite	no	85274
lingeling-ats104	algotocnf_27-t10_diff-desc-sc_ocnf.cnf	none	no	243525
lingeling-ats104	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956
lingeling-ats104	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850
lingeling-ats104	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733
lingeling-ats104	algotocnf_27-t10_diff-desc_ocnf.cnf	none	no	134722
lingeling-ats104	algotocnf_27-t10_ocnf.cnf	none	no	134722
lingeling-ats104	algotocnf_3_ocnf.cnf	none	no	48704
minisat	algotocnf_1.cnf	none	no	48704
minisat	algotocnf_1.cnf	none	no	
minisat	algotocnf_1.cnf	cmsat	no	
minisat	algotocnf_1.cnf	cmsat	no	24503
minisat	algotocnf_1.cnf	minisat	no	20895
minisat	algotocnf_1.cnf	minisat	no	
minisat	algotocnf_1.cnf	satelite	no	
minisat	algotocnf_1.cnf	satelite	no	27495
minisat	algotocnf_18-t9.cnf	none	no	107839
minisat	algotocnf_18-t9.cnf	none	no	
minisat	algotocnf_18-t9.cnf	cmsat	no	61789
minisat	algotocnf_18-t9.cnf	cmsat	no	
minisat	algotocnf_18-t9.cnf	lingeling	no	
minisat	algotocnf_18-t9.cnf	lingeling	no	102616
minisat	algotocnf_18-t9.cnf	minisat	no	61845
minisat	algotocnf_18-t9.cnf	minisat	no	



SAT solver	CNF file	simplified	phase	vars/clauses	propagations	decision
minisat	algotocnf_18-t9.cnf	satelite	no	69670 / 457972	17335955	8932
minisat	algotocnf_18-t9.cnf	satelite	no			
minisat	algotocnf_18-t9_diff-desc.cnf	none	no			
minisat	algotocnf_18-t9_diff-desc.cnf	none	no	107839 / 831263	18671534	8573
minisat	algotocnf_18-t9_diff-desc.cnf	cmsat	no			
minisat	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489	21547194	10018
minisat	algotocnf_18-t9_diff-desc.cnf	lingeling	no	99452 / 404666	7408845	6092
minisat	algotocnf_18-t9_diff-desc.cnf	lingeling	no			
minisat	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431	6527792	3836
minisat	algotocnf_18-t9_diff-desc.cnf	minisat	no			
minisat	algotocnf_18-t9_diff-desc.cnf	satelite	no			
minisat	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408	7396646	4010
minisat	algotocnf_1_diff-desc.cnf	none	no			
minisat	algotocnf_1_diff-desc.cnf	none	no	48704 / 330692	145509993	47117
minisat	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142	221480273	68306
minisat	algotocnf_1_diff-desc.cnf	cmsat	no			
minisat	algotocnf_1_diff-desc.cnf	lingeling	no	40554 / 101182	407709713	18029
minisat	algotocnf_1_diff-desc.cnf	lingeling	no			
minisat	algotocnf_1_diff-desc.cnf	minisat	no			
minisat	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393	166787763	53998
minisat	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602	267008243	80165
minisat	algotocnf_1_diff-desc.cnf	satelite	no			
minisat	algotocnf_2.cnf	none	no			
minisat	algotocnf_2.cnf	none	no	48704 / 224220	201587749	94597
minisat	algotocnf_2.cnf	cmsat	no	24323 / 111661	2750894175	90426
minisat	algotocnf_2.cnf	cmsat	no			
minisat	algotocnf_2.cnf	minisat	no			
minisat	algotocnf_2.cnf	minisat	no	20895 / 118688	491695491	21320
minisat	algotocnf_2.cnf	satelite	no	27775 / 154276	1522804488	65886
minisat	algotocnf_2.cnf	satelite	no			
minisat	algotocnf_21-t9.cnf	none	no			
minisat	algotocnf_21-t9.cnf	none	no			
minisat	algotocnf_21-t9.cnf	cmsat	no			
minisat	algotocnf_21-t9.cnf	cmsat	no			
minisat	algotocnf_21-t9.cnf	minisat	no			

SAT solver	CNF file	simplified	phase	vars/clauses	propagation
minisat	algotocnf_21-t9.cnf	minisat	no		
minisat	algotocnf_21-t9.cnf	satelite	no		
minisat	algotocnf_21-t9.cnf	satelite	no		
minisat	algotocnf_21-t9_diff-desc.cnf	none	no		
minisat	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 894072	9147981007
minisat	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	577921212
minisat	algotocnf_21-t9_diff-desc.cnf	cmsat	no		
minisat	algotocnf_21-t9_diff-desc.cnf	lingeling	no	104860 / 404126	1058635766
minisat	algotocnf_21-t9_diff-desc.cnf	lingeling	no		
minisat	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965	3082155154
minisat	algotocnf_21-t9_diff-desc.cnf	minisat	no		
minisat	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	4261434766
minisat	algotocnf_21-t9_diff-desc.cnf	satelite	no		
minisat	algotocnf_23-t9.cnf	none	no		
minisat	algotocnf_23-t9.cnf	none	no		
minisat	algotocnf_23-t9.cnf	cmsat	no		
minisat	algotocnf_23-t9.cnf	cmsat	no		
minisat	algotocnf_23-t9.cnf	minisat	no		
minisat	algotocnf_23-t9.cnf	minisat	no		
minisat	algotocnf_23-t9.cnf	satelite	no		
minisat	algotocnf_23-t9.cnf	satelite	no		
minisat	algotocnf_23-t9_diff-desc.cnf	none	no		
minisat	algotocnf_23-t9_diff-desc.cnf	none	no		
minisat	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118	3433286956
minisat	algotocnf_23-t9_diff-desc.cnf	cmsat	no		
minisat	algotocnf_23-t9_diff-desc.cnf	minisat	no		
minisat	algotocnf_23-t9_diff-desc.cnf	minisat	no		
minisat	algotocnf_23-t9_diff-desc.cnf	satelite	no		
minisat	algotocnf_23-t9_diff-desc.cnf	satelite	no		
minisat	algotocnf_24-t9.cnf	none	no		
minisat	algotocnf_24-t9.cnf	none	no		
minisat	algotocnf_24-t9.cnf	cmsat	no		
minisat	algotocnf_24-t9.cnf	cmsat	no		
minisat	algotocnf_24-t9.cnf	minisat	no		
minisat	algotocnf_24-t9.cnf	minisat	no		

SAT solver	CNF file	simplified	phase	vars/clauses	propagations	de
minisat	algotocnf_24-t9.cnf	satelite	no			
minisat	algotocnf_24-t9.cnf	satelite	no			
minisat	algotocnf_24-t9_diff-desc.cnf	none	no			
minisat	algotocnf_24-t9_diff-desc.cnf	none	no			
minisat	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014	3471709121	54
minisat	algotocnf_24-t9_diff-desc.cnf	cmsat	no			
minisat	algotocnf_24-t9_diff-desc.cnf	minisat	no			
minisat	algotocnf_24-t9_diff-desc.cnf	minisat	no			
minisat	algotocnf_24-t9_diff-desc.cnf	satelite	no			
minisat	algotocnf_24-t9_diff-desc.cnf	satelite	no			
minisat	algotocnf_27-t10-diff.cnf	none	no	134722 / 8320	134722	
minisat	algotocnf_27-t10-diff.cnf	none	no			
minisat	algotocnf_27-t10-diff.cnf	cmsat	no			
minisat	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0	0	
minisat	algotocnf_27-t10-diff.cnf	lingeling	no	0 / 0	0	
minisat	algotocnf_27-t10-diff.cnf	lingeling	no			
minisat	algotocnf_27-t10-diff.cnf	minisat	no			
minisat	algotocnf_27-t10-diff.cnf	minisat	no	0 / 0	0	
minisat	algotocnf_27-t10-diff.cnf	satelite	no			
minisat	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0	0	
minisat	algotocnf_27-t10-diff_diff-desc.cnf	none	no	134722 / 8320	134722	
minisat	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no			
minisat	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0	0	
minisat	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no			
minisat	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	0 / 0	0	
minisat	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0	0	
minisat	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no			
minisat	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no			
minisat	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0	0	
minisat	algotocnf_27-t10-simplified.cnf	none	no			
minisat	algotocnf_27-t10-simplified.cnf	none	no			
minisat	algotocnf_27-t10-simplified.cnf	cmsat	no			
minisat	algotocnf_27-t10-simplified.cnf	cmsat	no			
minisat	algotocnf_27-t10-simplified.cnf	minisat	no			
minisat	algotocnf_27-t10-simplified.cnf	minisat	no			

SAT solver	CNF file	simplified	phase	vars/clauses	pr
minisat	algotocnf_27-t10-simplified.cnf	satelite	no		
minisat	algotocnf_27-t10-simplified.cnf	satelite	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	none	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	none	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no		
minisat	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no		
minisat	algotocnf_27-t10.cnf	none	no		
minisat	algotocnf_27-t10.cnf	none	no		
minisat	algotocnf_27-t10.cnf	cmsat	no		
minisat	algotocnf_27-t10.cnf	cmsat	no		
minisat	algotocnf_27-t10.cnf	minisat	no		
minisat	algotocnf_27-t10.cnf	minisat	no		
minisat	algotocnf_27-t10.cnf	satelite	no		
minisat	algotocnf_27-t10.cnf	satelite	no		
minisat	algotocnf_27-t10_diff-desc.cnf	none	no		
minisat	algotocnf_27-t10_diff-desc.cnf	none	no		
minisat	algotocnf_27-t10_diff-desc.cnf	cmsat	no		
minisat	algotocnf_27-t10_diff-desc.cnf	cmsat	no		
minisat	algotocnf_27-t10_diff-desc.cnf	minisat	no		
minisat	algotocnf_27-t10_diff-desc.cnf	minisat	no		
minisat	algotocnf_27-t10_diff-desc.cnf	satelite	no		
minisat	algotocnf_27-t10_diff-desc.cnf	satelite	no		
minisat	algotocnf_2_diff-desc.cnf	none	no	48704 / 329788	
minisat	algotocnf_2_diff-desc.cnf	none	no		
minisat	algotocnf_2_diff-desc.cnf	cmsat	no		
minisat	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870	
minisat	algotocnf_2_diff-desc.cnf	lingeling	no		
minisat	algotocnf_2_diff-desc.cnf	lingeling	no	40767 / 106546	
minisat	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436	
minisat	algotocnf_2_diff-desc.cnf	minisat	no		
minisat	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577	

SAT solver	CNF file	simplified	phase	vars/clauses	propagations	decisions
minisat	algotocnf_2_diff-desc.cnf	satelite	no			
minisat	algotocnf_3.cnf	none	no	48704 / 222436	13991247	8535
minisat	algotocnf_3.cnf	none	no			
minisat	algotocnf_3.cnf	cmsat	no	23893 / 111403	15330537	8946
minisat	algotocnf_3.cnf	cmsat	no			
minisat	algotocnf_3.cnf	lingeling	no			
minisat	algotocnf_3.cnf	lingeling	no	44000 / 100941	3922854	3284
minisat	algotocnf_3.cnf	minisat	no	20895 / 119580	11055439	7059
minisat	algotocnf_3.cnf	minisat	no			
minisat	algotocnf_3.cnf	satelite	no			
minisat	algotocnf_3.cnf	satelite	no	28647 / 156910	15840699	1019
minisat	algotocnf_3_diff-desc.cnf	none	no			
minisat	algotocnf_3_diff-desc.cnf	none	no	48704 / 328004	8355604	4517
minisat-core	algotocnf_1.cnf	none	no	48704 / 225124	12249636981	19487
minisat-core	algotocnf_1.cnf	cmsat	no	24503 / 111931	1345904991	45407
minisat-core	algotocnf_1.cnf	minisat	no	20895 / 118236	1001195109	41539
minisat-core	algotocnf_1.cnf	satelite	no	27495 / 153262	2852530112	91754
minisat-core	algotocnf_18-t9.cnf	none	no	107839 / 582936	197561807	5771
minisat-core	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139	3714952	3362
minisat-core	algotocnf_18-t9.cnf	lingeling	no	102616 / 344544	27126157	3729
minisat-core	algotocnf_18-t9.cnf	minisat	no	61845 / 391134	11474979	6664
minisat-core	algotocnf_18-t9.cnf	satelite	no	69670 / 457972	48139459	2806
minisat-core	algotocnf_18-t9_diff-desc.cnf	none	no	107839 / 831263	134492463	5454
minisat-core	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489	22660129	1033
minisat-core	algotocnf_18-t9_diff-desc.cnf	lingeling	no	99452 / 404666	4783352	1249
minisat-core	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431	6527792	3836
minisat-core	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408	68801966	3555
minisat-core	algotocnf_1_diff-desc.cnf	none	no	48704 / 330692	556973568	10855
minisat-core	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142	565587287	15477
minisat-core	algotocnf_1_diff-desc.cnf	lingeling	no	40554 / 101182	130669677	6453
minisat-core	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393	166787763	5399
minisat-core	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602	218192599	7694
minisat-core	algotocnf_2.cnf	none	no	48704 / 224220	4474027487	81273
minisat-core	algotocnf_2.cnf	cmsat	no	24323 / 111661	3271551070	10951
minisat-core	algotocnf_2.cnf	minisat	no	20895 / 118688	491695491	21320

SAT solver	CNF file	simplified	phase	vars/clauses	propag
minisat-core	algotocnf_2.cnf	satelite	no	27775 / 154276	13561
minisat-core	algotocnf_21-t9.cnf	none	no		
minisat-core	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308	97208
minisat-core	algotocnf_21-t9.cnf	minisat	no		
minisat-core	algotocnf_21-t9.cnf	satelite	no		
minisat-core	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 894072	61849
minisat-core	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	30333
minisat-core	algotocnf_21-t9_diff-desc.cnf	lingeling	no	104860 / 404126	23091
minisat-core	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965	30821
minisat-core	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	20288
minisat-core	algotocnf_23-t9.cnf	none	no		
minisat-core	algotocnf_23-t9.cnf	cmsat	no		
minisat-core	algotocnf_23-t9.cnf	minisat	no		
minisat-core	algotocnf_23-t9.cnf	satelite	no		
minisat-core	algotocnf_23-t9_diff-desc.cnf	none	no		
minisat-core	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118	66867
minisat-core	algotocnf_23-t9_diff-desc.cnf	minisat	no		
minisat-core	algotocnf_23-t9_diff-desc.cnf	satelite	no		
minisat-core	algotocnf_24-t9.cnf	none	no		
minisat-core	algotocnf_24-t9.cnf	cmsat	no		
minisat-core	algotocnf_24-t9.cnf	minisat	no		
minisat-core	algotocnf_24-t9.cnf	satelite	no		
minisat-core	algotocnf_24-t9_diff-desc.cnf	none	no		
minisat-core	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014	33082
minisat-core	algotocnf_24-t9_diff-desc.cnf	minisat	no		
minisat-core	algotocnf_24-t9_diff-desc.cnf	satelite	no		
minisat-core	algotocnf_27-t10-diff.cnf	none	no	134722 / 8320	134
minisat-core	algotocnf_27-t10-diff.cnf	cmsat	no	0 / 0	0
minisat-core	algotocnf_27-t10-diff.cnf	lingeling	no	0 / 0	0
minisat-core	algotocnf_27-t10-diff.cnf	minisat	no	0 / 0	0
minisat-core	algotocnf_27-t10-diff.cnf	satelite	no	0 / 0	0
minisat-core	algotocnf_27-t10-diff_diff-desc.cnf	none	no	134722 / 8320	134
minisat-core	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0 / 0	0
minisat-core	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	0 / 0	0
minisat-core	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0 / 0	0

SAT solver	CNF file	simplified	phase	vars/clauses	propa
minisat-core	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0 / 0	
minisat-core	algotocnf_27-t10-simplified.cnf	none	no		
minisat-core	algotocnf_27-t10-simplified.cnf	cmsat	no		
minisat-core	algotocnf_27-t10-simplified.cnf	minisat	no		
minisat-core	algotocnf_27-t10-simplified.cnf	satelite	no		
minisat-core	algotocnf_27-t10-simplified_diff-desc.cnf	none	no		
minisat-core	algotocnf_27-t10-simplified_diff-desc.cnf	cmsat	no		
minisat-core	algotocnf_27-t10-simplified_diff-desc.cnf	minisat	no		
minisat-core	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no		
minisat-core	algotocnf_27-t10.cnf	none	no		
minisat-core	algotocnf_27-t10.cnf	cmsat	no		
minisat-core	algotocnf_27-t10.cnf	minisat	no		
minisat-core	algotocnf_27-t10.cnf	satelite	no		
minisat-core	algotocnf_27-t10_diff-desc.cnf	none	no		
minisat-core	algotocnf_27-t10_diff-desc.cnf	cmsat	no		
minisat-core	algotocnf_27-t10_diff-desc.cnf	minisat	no		
minisat-core	algotocnf_27-t10_diff-desc.cnf	satelite	no		
minisat-core	algotocnf_2_diff-desc.cnf	none	no	48704 / 329788	6426
minisat-core	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870	1001
minisat-core	algotocnf_2_diff-desc.cnf	lingeling	no	40767 / 106546	1283
minisat-core	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436	1695
minisat-core	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577	2143
minisat-core	algotocnf_3.cnf	none	no	48704 / 222436	1346
minisat-core	algotocnf_3.cnf	cmsat	no	23893 / 111403	162
minisat-core	algotocnf_3.cnf	lingeling	no	44000 / 100941	497
minisat-core	algotocnf_3.cnf	minisat	no	20895 / 119580	1109
minisat-core	algotocnf_3.cnf	satelite	no	28647 / 156910	814
minisat-core	algotocnf_3_diff-desc.cnf	none	no	48704 / 328004	820
plingeling-ats101	algotocnf_1.cnf	cmsat	no	24503 / 111931	8548
plingeling-ats101	algotocnf_1.cnf	minisat	no	20895 / 118236	8304
plingeling-ats101	algotocnf_1.cnf	satelite	no	27495 / 153262	12438
plingeling-ats101	algotocnf_18-t9.cnf	none	no	107839 / 590953	5891
plingeling-ats101	algotocnf_18-t9.cnf	cmsat	no	61789 / 342139	3575
plingeling-ats101	algotocnf_18-t9.cnf	lingeling	no	107839 / 344544	1992
plingeling-ats101	algotocnf_18-t9.cnf	minisat	no	61845 / 391134	303

SAT solver	CNF file	simplified	phase	vars/clauses	propag
plingeling-ats101	algotocnf_18-t9.cnf	satelite	no	69670 / 457972	39631
plingeling-ats101	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114 / 303489	94961
plingeling-ats101	algotocnf_18-t9_diff-desc.cnf	lingeling	no	107839 / 404666	74562
plingeling-ats101	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055 / 511431	5270
plingeling-ats101	algotocnf_18-t9_diff-desc.cnf	satelite	no	85386 / 692408	37528
plingeling-ats101	algotocnf_1_diff-desc.cnf	none	no	48704 / 373920	42891
plingeling-ats101	algotocnf_1_diff-desc.cnf	cmsat	no	15402 / 73142	35481
plingeling-ats101	algotocnf_1_diff-desc.cnf	lingeling	no	48704 / 101182	31808
plingeling-ats101	algotocnf_1_diff-desc.cnf	minisat	no	25107 / 158393	19652
plingeling-ats101	algotocnf_1_diff-desc.cnf	satelite	no	30950 / 226602	24912
plingeling-ats101	algotocnf_2.cnf	none	no	48704 / 254210	112788
plingeling-ats101	algotocnf_2.cnf	cmsat	no	24323 / 111661	81450
plingeling-ats101	algotocnf_2.cnf	minisat	no	20895 / 118688	31248
plingeling-ats101	algotocnf_2.cnf	satelite	no	27775 / 154276	68889
plingeling-ats101	algotocnf_21-t9.cnf	none	no	116800 / 636838	130188
plingeling-ats101	algotocnf_21-t9.cnf	cmsat	no	63555 / 358308	172558
plingeling-ats101	algotocnf_21-t9.cnf	minisat	no	65572 / 414470	191274
plingeling-ats101	algotocnf_21-t9.cnf	satelite	no	74562 / 486714	132702
plingeling-ats101	algotocnf_21-t9_diff-desc.cnf	none	no	116800 / 911629	185148
plingeling-ats101	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528 / 318049	144502
plingeling-ats101	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650 / 534965	217187
plingeling-ats101	algotocnf_21-t9_diff-desc.cnf	satelite	no	90236 / 720755	238047
plingeling-ats101	algotocnf_23-t9.cnf	none	no	122774 / 667438	231925
plingeling-ats101	algotocnf_23-t9.cnf	cmsat	no	64880 / 369775	251983
plingeling-ats101	algotocnf_23-t9.cnf	minisat	no	67979 / 429734	261991
plingeling-ats101	algotocnf_23-t9.cnf	satelite	no	77835 / 506217	228831
plingeling-ats101	algotocnf_23-t9_diff-desc.cnf	none	no	122774 / 955067	558888
plingeling-ats101	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510 / 307118	254882
plingeling-ats101	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080 / 550727	397121
plingeling-ats101	algotocnf_23-t9_diff-desc.cnf	satelite	no	93504 / 740545	531778
plingeling-ats101	algotocnf_24-t9.cnf	none	no	125761 / 682722	768191
plingeling-ats101	algotocnf_24-t9.cnf	cmsat	no	65579 / 377228	274278
plingeling-ats101	algotocnf_24-t9.cnf	minisat	no	69023 / 436292	251062
plingeling-ats101	algotocnf_24-t9.cnf	satelite	no	79486 / 515977	295147
plingeling-ats101	algotocnf_24-t9_diff-desc.cnf	none	no	125761 / 976770	438780



SAT solver	CNF file	simplified	phase	vars/clauses	prop
plingeling-ats101	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447 / 302014	3183
plingeling-ats101	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312 / 558731	3305
plingeling-ats101	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154 / 750557	2932
plingeling-ats101	algotocnf_27-t10_diff.cnf	none	no	134722 / 728349	107
plingeling-ats101	algotocnf_27-t10_diff.cnf	cmsat	no	0 / 0	
plingeling-ats101	algotocnf_27-t10_diff.cnf	lingeling	no	134722 / 0	
plingeling-ats101	algotocnf_27-t10_diff.cnf	minisat	no	0 / 0	
plingeling-ats101	algotocnf_27-t10_diff.cnf	satelite	no	0 / 0	
plingeling-ats101	algotocnf_27-t10_diff_diff-desc.cnf	none	no	134722 / 1041654	16
plingeling-ats101	algotocnf_27-t10_diff_diff-desc.cnf	cmsat	no	0 / 0	
plingeling-ats101	algotocnf_27-t10_diff_diff-desc.cnf	lingeling	no	134722 / 0	
plingeling-ats101	algotocnf_27-t10_diff_diff-desc.cnf	minisat	no	0 / 0	
plingeling-ats101	algotocnf_27-t10_diff_diff-desc.cnf	satelite	no	0 / 0	
plingeling-ats101	algotocnf_27-t10-simplified.cnf	none	no	134722 / 728542	2742
plingeling-ats101	algotocnf_27-t10-simplified.cnf	cmsat	no	67175 / 392680	3254
plingeling-ats101	algotocnf_27-t10-simplified.cnf	minisat	no	72909 / 460404	2559
plingeling-ats101	algotocnf_27-t10-simplified.cnf	satelite	no	84442 / 544998	3270
plingeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	none	no	134722 / 1041847	2920
plingeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735 / 789589	2987
plingeling-ats101	algotocnf_27-t10.cnf	none	no	134722 / 728030	2933
plingeling-ats101	algotocnf_27-t10.cnf	cmsat	no	72044 / 411276	2922
plingeling-ats101	algotocnf_27-t10.cnf	minisat	no	73897 / 465248	2383
plingeling-ats101	algotocnf_27-t10_diff-desc.cnf	none	no	134722 / 1041335	2859
plingeling-ats101	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956 / 311219	3117
plingeling-ats101	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850 / 619480	3257
plingeling-ats101	algotocnf_27-t10_diff-desc.cnf	satelite	no	105733 / 857675	2846
plingeling-ats101	algotocnf_2_diff-desc.cnf	none	no	48704 / 374146	474
plingeling-ats101	algotocnf_2_diff-desc.cnf	cmsat	no	15342 / 72870	203
plingeling-ats101	algotocnf_2_diff-desc.cnf	lingeling	no	48704 / 106546	214
plingeling-ats101	algotocnf_2_diff-desc.cnf	minisat	no	23531 / 149436	107
plingeling-ats101	algotocnf_2_diff-desc.cnf	satelite	no	29428 / 204577	166
plingeling-ats101	algotocnf_3.cnf	none	no	48704 / 254656	452
plingeling-ats101	algotocnf_3.cnf	cmsat	no	23893 / 111403	126
plingeling-ats101	algotocnf_3.cnf	lingeling	no	48704 / 100941	531
plingeling-ats101	algotocnf_3.cnf	minisat	no	20895 / 119580	472

SAT solver	CNF file	simplified	phase	vars/clauses	pro
plingeling-ats101	algotocnf_3.cnf	satelite	no	28647 / 156910	6
plingeling-ats101	algotocnf_3_diff-desc.cnf	none	no	48704 / 374592	2
treengeling-ats101	algotocnf_1.cnf	cmsat	no	24503.0 / 111931.0	1
treengeling-ats101	algotocnf_1.cnf	minisat	no	20895.0 / 118236.0	1
treengeling-ats101	algotocnf_1.cnf	satelite	no	27495.0 / 153262.0	1
treengeling-ats101	algotocnf_18-t9.cnf	none	no	107839.0 / 590953.0	
treengeling-ats101	algotocnf_18-t9.cnf	cmsat	no	61789.0 / 342139.0	
treengeling-ats101	algotocnf_18-t9.cnf	lingeling	no	107839.0 / 344544.0	
treengeling-ats101	algotocnf_18-t9.cnf	minisat	no	61845.0 / 391134.0	
treengeling-ats101	algotocnf_18-t9.cnf	satelite	no	69670.0 / 457972.0	
treengeling-ats101	algotocnf_18-t9_diff-desc.cnf	cmsat	no	57114.0 / 303489.0	1
treengeling-ats101	algotocnf_18-t9_diff-desc.cnf	lingeling	no	107839.0 / 404666.0	
treengeling-ats101	algotocnf_18-t9_diff-desc.cnf	minisat	no	78055.0 / 511431.0	2
treengeling-ats101	algotocnf_1_diff-desc.cnf	none	no	48704.0 / 373920.0	3
treengeling-ats101	algotocnf_1_diff-desc.cnf	cmsat	no	15402.0 / 73142.0	5
treengeling-ats101	algotocnf_1_diff-desc.cnf	minisat	no	25107.0 / 158393.0	1
treengeling-ats101	algotocnf_1_diff-desc.cnf	satelite	no	30950.0 / 226602.0	5
treengeling-ats101	algotocnf_2.cnf	none	no	48704.0 / 254210.0	1
treengeling-ats101	algotocnf_2.cnf	cmsat	no	24323.0 / 111661.0	2
treengeling-ats101	algotocnf_2.cnf	minisat	no	20895.0 / 118688.0	
treengeling-ats101	algotocnf_2.cnf	satelite	no	27775.0 / 154276.0	1
treengeling-ats101	algotocnf_21-t9.cnf	satelite	no	74562.0 / 486714.0	48
treengeling-ats101	algotocnf_21-t9_diff-desc.cnf	none	no	116800.0 / 911629.0	7
treengeling-ats101	algotocnf_21-t9_diff-desc.cnf	cmsat	no	59528.0 / 318049.0	4
treengeling-ats101	algotocnf_21-t9_diff-desc.cnf	minisat	no	81650.0 / 534965.0	21
treengeling-ats101	algotocnf_23-t9.cnf	none	no	122774.0 / 667438.0	43
treengeling-ats101	algotocnf_23-t9.cnf	cmsat	no	64880.0 / 369775.0	42
treengeling-ats101	algotocnf_23-t9.cnf	minisat	no	67979.0 / 429734.0	43
treengeling-ats101	algotocnf_23-t9.cnf	satelite	no	77835.0 / 506217.0	34
treengeling-ats101	algotocnf_23-t9_diff-desc.cnf	none	no	122774.0 / 955067.0	20
treengeling-ats101	algotocnf_23-t9_diff-desc.cnf	cmsat	no	57510.0 / 307118.0	6
treengeling-ats101	algotocnf_23-t9_diff-desc.cnf	minisat	no	84080.0 / 550727.0	11
treengeling-ats101	algotocnf_24-t9.cnf	cmsat	no	65579.0 / 377228.0	39
treengeling-ats101	algotocnf_24-t9.cnf	minisat	no	69023.0 / 436292.0	42
treengeling-ats101	algotocnf_24-t9.cnf	satelite	no	79486.0 / 515977.0	50

SAT solver	CNF file	simplified	phase	vars/clauses	1
treengeling-ats101	algotocnf_24-t9_diff-desc.cnf	none	no	125761.0 / 976770.0	
treengeling-ats101	algotocnf_24-t9_diff-desc.cnf	cmsat	no	56447.0 / 302014.0	
treengeling-ats101	algotocnf_24-t9_diff-desc.cnf	minisat	no	85312.0 / 558731.0	
treengeling-ats101	algotocnf_24-t9_diff-desc.cnf	satelite	no	95154.0 / 750557.0	
treengeling-ats101	algotocnf_27-t10-diff.cnf	none	no	134722.0 / 728349.0	
treengeling-ats101	algotocnf_27-t10-diff.cnf	cmsat	no	0.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff.cnf	lingeling	no	134722.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff.cnf	minisat	no	0.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff.cnf	satelite	no	0.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	cmsat	no	0.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	lingeling	no	134722.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	minisat	no	0.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-diff_diff-desc.cnf	satelite	no	0.0 / 0.0	
treengeling-ats101	algotocnf_27-t10-simplified.cnf	cmsat	no	67175.0 / 392680.0	
treengeling-ats101	algotocnf_27-t10-simplified.cnf	minisat	no	72909.0 / 460404.0	
treengeling-ats101	algotocnf_27-t10-simplified.cnf	satelite	no	84442.0 / 544998.0	
treengeling-ats101	algotocnf_27-t10-simplified_diff-desc.cnf	satelite	no	100735.0 / 789589.0	
treengeling-ats101	algotocnf_27-t10.cnf	none	no	134722.0 / 728030.0	
treengeling-ats101	algotocnf_27-t10.cnf	cmsat	no	72044.0 / 411276.0	
treengeling-ats101	algotocnf_27-t10.cnf	minisat	no	73897.0 / 465248.0	
treengeling-ats101	algotocnf_27-t10_diff-desc.cnf	none	no	134722.0 / 1041335.0	
treengeling-ats101	algotocnf_27-t10_diff-desc.cnf	cmsat	no	57956.0 / 311219.0	
treengeling-ats101	algotocnf_27-t10_diff-desc.cnf	minisat	no	94850.0 / 619480.0	
treengeling-ats101	algotocnf_2_diff-desc.cnf	cmsat	no	15342.0 / 72870.0	
treengeling-ats101	algotocnf_2_diff-desc.cnf	lingeling	no	48704.0 / 106546.0	
treengeling-ats101	algotocnf_2_diff-desc.cnf	minisat	no	23531.0 / 149436.0	
treengeling-ats101	algotocnf_2_diff-desc.cnf	satelite	no	29428.0 / 204577.0	
treengeling-ats101	algotocnf_3.cnf	none	no	48704.0 / 254656.0	
treengeling-ats101	algotocnf_3.cnf	cmsat	no	23893.0 / 111403.0	
treengeling-ats101	algotocnf_3.cnf	lingeling	no	48704.0 / 100941.0	
treengeling-ats101	algotocnf_3.cnf	minisat	no	20895.0 / 119580.0	
treengeling-ats101	algotocnf_3.cnf	satelite	no	28647.0 / 156910.0	



# List of Figures

2.1	MD4 round function updating state variables . . . . .	8
2.2	SHA-256 round function as characterized in [6] . . . . .	8
3.1	Common attack setting for a collision attack . . . . .	13
3.2	Layout of MD4 and SHA-256 differential characteristics . . . . .	19
B.1	MD4 testcase A . . . . .	70
B.2	MD4 B testcase . . . . .	71
B.3	MD4 testcase C . . . . .	72
B.4	SHA256 hash collision over 18 rounds . . . . .	73
B.5	SHA-256 hash collision over 21 rounds . . . . .	73
B.6	SHA-256 hash collision over 23 rounds . . . . .	74
B.7	SHA-256 hash collision over 24 rounds . . . . .	74



# List of Tables

2.1	MD4 hash algorithm properties . . . . .	5
2.2	SHA-256 hash algorithm properties . . . . .	7
3.1	Hexadecimal values of one MD4 collisions given in paper [34] . .	12
3.2	Bit differences in the original Wang et al. hash collision . . . . .	14
3.3	Differential notation as introduced in [2] . . . . .	15
3.4	Representation of bit conditions as CNF . . . . .	15
3.5	A simple 1-bit addition example . . . . .	17
3.6	Propagation of bit conditions in a differential characteristic . . . .	17
3.7	Testcases for 4-bit addition . . . . .	17
3.8	Differential characteristics for the SHA-2 Sigma function . . . . .	17
3.9	One of the original MD4 collisions by Wang et al, with a few bits underspecified and followingly propagated . . . . .	18
4.1	Truth tables for AND, OR and NOT . . . . .	22
4.2	Unary $f$ and its four possible cases . . . . .	23
7.1	Our testcases and their number of clauses / variables . . . . .	52
7.2	Testcase B.1 can be solved within 1 minute by all SAT solvers . .	53
7.3	Problem sizes after simplification . . . . .	54
7.4	Runtimes for MD4 testcase A with various SAT solvers . . . . .	58
7.5	Runtimes for MD4 testcase B with various SAT solvers . . . . .	58
7.6	Runtimes for MD4 testcase C with various SAT solvers . . . . .	58

7.7	Runtimes for SHA-256 testcase 18 with various SAT solvers . . . .	59
7.8	Runtimes for SHA-256 testcase 21 with various SAT solvers . . . .	59
7.9	Runtimes for SHA-256 testcase 23 with various SAT solvers . . . .	59
7.10	Runtimes for SHA-256 testcase 24 with various SAT solvers . . . .	59
A.1	Thinkpad x220 Tablet specification [14] . . . . .	65
A.2	Cluster node nehalem192go specification [3] . . . . .	65



# Bibliography

- [1] Bernd Bischl et al. “ASlib: A benchmark library for algorithm selection”. In: *Artificial Intelligence* 237 (2016), pp. 41–58. ISSN: 0004-3702. DOI: <http://dx.doi.org/10.1016/j.artint.2016.04.003>. URL: <http://www.sciencedirect.com/science/article/pii/S0004370216300388> (visited on 07/23/2016).
- [2] Christophe De Cannière and Christian Rechberger. “Finding SHA-1 Characteristics: General Results and Applications”. In: *ASIACRYPT*. Ed. by Xuejia Lai and Kefei Chen. Vol. 4284. LNCS. Springer, 2006, pp. 1–20. ISBN: 3-540-49475-8. URL: [http://dx.doi.org/10.1007/11935230\\_1](http://dx.doi.org/10.1007/11935230_1) (visited on 08/23/2016).
- [3] Intel Corporation. *Intel Xeon Processor X5690 (12M Cache, 3.46 GHz, 6.40 GT/s Intel QPI) Specifications*. URL: [http://ark.intel.com/products/52576/Intel-Xeon-Processor-X5690-12M-Cache-3\\_46-GHz-6\\_40-GTs-Intel-QPI](http://ark.intel.com/products/52576/Intel-Xeon-Processor-X5690-12M-Cache-3_46-GHz-6_40-GTs-Intel-QPI) (visited on 04/05/2016).
- [4] Magnus Daum. “Cryptanalysis of Hash functions of the MD4-family”. PhD thesis. Ruhr-Universität Bochum, Universitätsbibliothek, 2005.
- [5] Hans Dobbertin. “Cryptanalysis of MD4”. In: *Journal of Cryptology* 11.4 (1998), pp. 253–271. ISSN: 1432-1378. DOI: [10.1007/s001459900047](http://dx.doi.org/10.1007/s001459900047). URL: <http://dx.doi.org/10.1007/s001459900047> (visited on 03/15/2016).
- [6] Christoph Dobraunig, Maria Eichlseder, and Florian Mendel. “Analysis of SHA-512/224 and SHA-512/256”. In: *Advances in Cryptology–ASIACRYPT 2015*. Springer, 2014, pp. 612–630.
- [7] Vijay Ganesh and David L Dill. “A decision procedure for bit-vectors and arrays”. In: *International Conference on Computer Aided Verification*. Springer, 2007, pp. 519–531.
- [8] Theodore P Hill. “The First Digit Phenomenon A century-old observation about an unexpected pattern in many numerical tables applies to the stock market, census statistics and accounting data”. In: *American Scientist* 86.4 (1998), pp. 358–363.

- [9] National Institute of Standards Information Technology Laboratory and Technology. “Federal Information Processing Standards Publication 180-4”. In: *National Bureau of Standards, US Department of Commerce* (2015). URL: <http://dx.doi.org/10.6028/NIST.FIPS.180-4> (visited on 05/10/2016).
- [10] M. Jones. *JSON Web Algorithms (JWA)*. RFC 7518. The Internet Engineering Task Force, 2015, pp. 1–69. URL: <https://tools.ietf.org/html/rfc7518> (visited on 05/09/2016).
- [11] Dmitry Khovratovich, Christian Rechberger, and Alexandra Savelieva. “Bi-cliques for preimages: attacks on Skein-512 and the SHA-2 family”. In: *Fast Software Encryption*. Springer. 2012, pp. 244–263.
- [12] Mario Lamberger and Florian Mendel. “Higher-Order Differential Attack on Reduced SHA-256”. In: *IACR Cryptology ePrint Archive 2011* (2011), p. 37.
- [13] Massimo Lauria. *CNFgen – Cool benchmarks for your SAT solver!* URL: <https://massimolauria.github.io/cnfgem/> (visited on 08/03/2016).
- [14] Lenovo Group Ltd. *ThinkPad X220 Tablet (4299) - Onsite (2011)*. URL: [http://www.lenovo.com/shop/america/content/pdf/system\\_data/x220t\\_tech\\_specs.pdf](http://www.lenovo.com/shop/america/content/pdf/system_data/x220t_tech_specs.pdf) (visited on 04/05/2016).
- [15] N. Sakimura M. Jones J. Bradley. *JSON Web Token (JWT)*. RFC 7519. The Internet Engineering Task Force, 2015, pp. 16–16. URL: <https://tools.ietf.org/html/rfc7519#section-8> (visited on 05/09/2016).
- [16] Florian Mendel, Tomislav Nad, and Martin Schl  ffer. “Improving local collisions: new attacks on reduced SHA-256”. In: *Advances in Cryptology–EUROCRYPT 2013*. Springer, 2013, pp. 262–278.
- [17] RC Merkle. “Secrecy, Authentication, and Public Key Systems”. PhD thesis. PhD thesis, Stanford University, Dpt of Electrical Engineering, 1979.
- [18] Ilya Mironov and Lintao Zhang. “Applications of SAT solvers to cryptanalysis of hash functions”. In: *International Conference on Theory and Applications of Satisfiability Testing*. Springer. 2006, pp. 102–115.
- [19] Matthew W Moskewicz et al. “Chaff: Engineering an efficient SAT solver”. In: *Proceedings of the 38th annual Design Automation Conference*. ACM. 2001, pp. 530–535.
- [20] Yusuke Naito et al. “Improved Collision Attack on MD4”. In: (2005), pp. 1–5. URL: <http://eprint.iacr.org/> (visited on 03/15/2016).
- [21] Ivica Nikoli   and Alex Biryukov. “Collisions for step-reduced SHA-256”. In: *International Workshop on Fast Software Encryption*. Springer. 2008, pp. 1–15.
- [22] Eugene Nudelman et al. “Satzilla: An algorithm portfolio for SAT”. In: *Solver description, SAT competition 2004* (2004).
- [23] Eugene Nudelman et al. “Understanding random SAT: Beyond the clauses-to-variables ratio”. In: *International Conference on Principles and Practice of Constraint Programming*. Springer. 2004, pp. 438–452.

- [24] prokls. *MD4 in pure Python 3.4*. URL: <https://gist.github.com/prokls/86b3c037df19a8c957fe> (visited on 04/10/2015).
- [25] Lukas Prokop. *Using SAT Solvers to Detect Contradictions in Differential Characteristics*. URL: [http://lukas-prokop.at/proj/bakk\\_iaik/thesis.pdf](http://lukas-prokop.at/proj/bakk_iaik/thesis.pdf) (visited on 08/23/2016).
- [26] Ronald Rivest. *The MD4 Message Digest Algorithm*. RFC 1186. The Internet Engineering Task Force, 1990, pp. 1–18. URL: <https://tools.ietf.org/html/rfc1186> (visited on 03/15/2016).
- [27] Ronald Rivest. *The MD4 Message-Digest Algorithm*. RFC 1320. The Internet Engineering Task Force, 1992, pp. 1–20. URL: <https://tools.ietf.org/html/rfc1320> (visited on 03/15/2016).
- [28] Yu Sasaki et al. “New Message Difference for MD4”. In: (2007), pp. 1–20. URL: <http://www.iacr.org/archive/fse2007/45930331/45930331.pdf> (visited on 03/15/2016).
- [29] Yu Sasaki et al. “New message difference for MD4”. In: *International Workshop on Fast Software Encryption*. Springer. 2007, pp. 329–348.
- [30] Martin Schl  ffer and Elisabeth Oswald. “Searching for differential paths in MD4”. In: *Fast Software Encryption*. Springer. 2006, pp. 242–261.
- [31] Bart Selman, David G Mitchell, and Hector J Levesque. “Generating hard satisfiability problems”. In: *Artificial intelligence* 81.1 (1996), pp. 17–29.
- [32] Patrick Stach. *MD4 collision generator*. URL: [http://crppit.epfl.ch/documentation/Hash\\_Function/Fastcoll\\_MD4/md4coll.c](http://crppit.epfl.ch/documentation/Hash_Function/Fastcoll_MD4/md4coll.c) (visited on 04/05/2016).
- [33] S. Turner and L. Chen. *The MD4 Message Digest Algorithm*. RFC 6150. The Internet Engineering Task Force, 2011, pp. 1–10. URL: <https://tools.ietf.org/html/rfc6150> (visited on 03/15/2016).
- [34] Xiaoyun Wang et al. “Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD.” In: *IACR Cryptology ePrint Archive* 2004 (2004), p. 199.
- [35] Lin Xu et al. “SATzilla: portfolio-based algorithm selection for SAT”. In: *Journal of Artificial Intelligence Research* (2008), pp. 565–606.