Review of the Hranicky dissertation

Overall: The dissertation is not especially innovative, but it represents useful detailed analysis of ways to speed password cracking using distributed processing.

Overall: I have included output of my English-improvement program, suggesting a variety of wording improvements. Most are correct, but a few are not, so check them before implementing them.

Abstract: This and section 1 should identify the main contributions of the work. A Ph.D. dissertation is supposed to be novel work that no one in the world has done before, so describe what is novel in your work.

Abstract: An abstract should also identify results of the dissertation research, not just describe the techniques used. How much of a performance improvement over existing methods did you obtain for your major methods? How many different methods did you evalaute compared to previous attempts to compare methods? Is the number of password storage methods you can handle significantly larger than with other distributed password-cracking tools?

Abstract: The first-person word "I" is not generally appropriate in academic writing; "we" is conventionally used since the work is usually part of a team.

Chapter 1: You should mention that some of your methods also apply to key guessing, not just password guessing.

Chapter 1, third paragraph: You should mention that malicious attackers and intelligence agencies will not cooperate in releasing their passwords, and their activities are important data for digital forensics.

Sixth paragraph: You need to explain why parallel processing is possible with password guessing, since login attempts need to be done sequentially. You need to explain the traditional approach of testing the password hash file here, not later. Also you need to explain here why software limits on the number of password-guessing attempts are not relevant to your approach.

1.1.3: Quotation marks are strange in the PDF around “pwc” and “Solar Designer”. Doublecheck all quotation marks to see if they look right in PDF.

1.3: This section is inadequate in describing the contributions because this is an engineering-oriented dissertation and the contributions are best measured quantitatively. How much better than existing methods were your methods? A new idea is not a contribution unless it is shown to have significant advantages over existing ideas.

1.3, fourth paragraph: "Probabilistic" should not be capitalized. Just because a phrase has a capitalized acronym does not mean any of its words should be capitalized.

1.4: “Novelty” should be “novel”.

Figure 2.1: This needs more explanation. What does "verify" mean? What does it mean that a password is correct?

2.2.1, first word: Eliminate the “the”, and eliminate articles in front of mass nouns like “search”.

2.3.1, second paragraph: "The calculation may require to compute": This is not grammatical since an infinitive in English is not grammatically a noun phrase. A gerund is better, i.e. "may require computing".

2.3.1: You should mention that cryptographic hashes are not unique, so cracking a password with a cryptographic hash just requires finding one of the possible passwords that map to that hash. If hashes are fewer bits than passwords, there can be many such passwords. Discuss here, not later.

Second paragraph: Clearly operating systems should strongly protect the password files from access so attackers cannot crack it. Explain why their strong protections are inadequate.

Fourth paragraph: "easier" should be "more easily" since an adverb is needed in modifying "cracking"

2.4: For completeness, you should mention password extraction by keyloggers and sensing of electronic emissions. These would be much less time-consuming than your methods.

3, first sentence: “Boundary” should be “limit”. “Getting over” should be “getting over it”.

3.1, first paragraph: Variable "l" should be defined here. Also, you seem to be saying p = p/s.

3.1.1, first sentence: This seems to say each password candidate must be verified to be the correct one.

Equation 3.2: Is this an upper bound, a lower bound, or an independence-assumption estimate?

Fourth paragraph: This seems to be assuming that each candidate attempt takes the same amount of time. Explain here why this is a reasonable assumption, since there are plenty of algorithms which have widely varying computation times.

3.1.2, second paragraph, last sentence: "Flew" doesn't make sense here; do you mean "ran"? Table 3.1: This needs more explanation. Is "passwords per second" the time to crack the passwords or count of password candidates that can be processed? Doesn't this speed depend on the difficulty level (like length) of the passwords to be cracked, which you don't report?

Section 3.5, fourth paragraph from the end: "criterium" is usually "criterion" in English.

3.6, first paragraph: You need to first explain why workload distribution is nontrivial for your task. If you have similar hardware and operating systems, password verification should take the same amount of time for each candidate. So if you just divide candidates into equal-sized batches, you should get optimal workload distribution. Discuss why that doesn't work.

3.7: You need to describe at the start of this section the assumptions about the task that Fitcrack makes. What is the input, what is its format, and what sizes of input can you handle? I assume that the main part of the input is a set of stored hashes, but also you need input of the type of hash method being used, and the software to do it. You should also list the specific password-storage algorithms you can handle with Fitcrack, since section 3.7 should be your primary summary of what it is. You should also state if the code is publicly available, and why or why not.

3.9.1, Table 3.12: Are these actual measurements, unlike the numbers in Tables 3.10 and 3.11? On what machine were they measured?

Paragraph after Table 3.12: The figure numbers suddenly jump to 3.25, so they should be changed to start with 3.13. Cracking time measured on what hardware? “Good” should be “improvement”. Labels on the vertical axes in Figure 3.25 should indicate these are worst-case times since this is a key point that needs to be emphasized. How did you know they were the worst case, did you just run for a while and find the worst time? If you didn’t run, the vertical axes should be labeled “number of atomic operations” or something similar, not “time”, and the assumed architecture and processor times described.

Next paragraph: Again, you refer to worst-case times, but how are you sure they are the worst? Did you do measurements or are you guessing? If guessing, you should explain your method. If the CPU or GPU garbage-collects the cache during these measurements, that could cause the worst-case time to be unfairly large, so how did you compensate for that?

4.2.5, first paragraph: This is puzzling and needs more explanation. Improvement of probabilistic grammar guessing in general, or just the last method you discussed? The advantage of a probabilistic grammar is that it produces more realistic password guesses, so it should take less time to crack a password from a real hash list on the average, contradicting what the first sentence says. Also, the second sentence doesn't seem plausible since guessing each password is independent of guessing the others if they are considered sequentially.

4.6, last paragraph: Why is there much text output? Shouldn't the output be very small, since it only needs to report password matches?

4.9.4: This section fails to answer the main question the reader has, namely how much faster cracking can be done using a probabilistic model than by assuming all possible passwords are equally likely. Please answer this in this section. The second sentence of the first paragraph appears to contradict what you said at the start of 4.2.5.

Chapter 5: This needs some quantitative conclusions as well mentioning methods you developed. How much better than existing methods can you do?

Suggested changes to ascii_hranicky_dissertation_890.txt:
*** Sentence 24: Replace "frequently" by "often" in:
Therefore, they frequently protect devices, systems, documents, and disks
*** Sentence 27: Replace "enormous" by "very large" in:
While its basic principle is relatively simple, the complex-ity of a single cracking session may be enormous
*** Sentence 45: Replace "amount of time" by "time" in:
Solving tasks is thus more efficient and takes less amount of time
*** Sentence 195: Replace "contained in" by "in" in:
The research contained in the thesis was supported by the following projects:
*** Sentence 196: Replace "mitigation" by "fix" or "improvement" or "relief" in:
Modern Tools for Detection and Mitigation of Cyber Criminality on the New Gener-ation Internet, no. VG20102015022 granted by Ministry of the Interior of the Czech Republic,
*** Sentence 1079: Replace "utilization" by "use" in:
3.1.2 Utilization of GPGPU
*** Sentence 1254: Replace "may need to" by "may" in:
However, instead of 10 thousand, we may need to check billions of possibilities
*** Sentence 1256: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
For-tunately, there are ways how to make the checking faster, and the aim of this thesis to accelerate the password cracking
*** Sentence 1257: Replace "not possible" by "impossible" in:
An approach that is not possible with a mechanical lock is to verify multiple passwords at the same time
*** Sentence 1258: Replace "substantial" by "large" in:
Parallel processing brings substantial benefits, especially with the use of General-purpose computing on graphics processing units (GPGPU) [17, 221, 83]
*** Sentence 1258: Delete "the use of" if followed by a gerund or noun describing an action in:
Parallel processing brings substantial benefits, especially with the use of General-purpose computing on graphics processing units (GPGPU) [17, 221, 83]

*** Sentence 1260: Replace "different options" by "options" in:
Therefore, I de-scribe and compare different options on how to distribute password cracking tasks between multiple nodes
*** Sentence 1264: Replace "he or she" by "they" in:
If the child knows any clue like #"there is number one in the first position#" or #"the combination contains number 7#", he or she may finish much faster
*** Sentence 1265: Replace "a particular person" by "someone" in:
If the lock is configurable and a particular person chose the combination, the child may take this as a benefit
*** Sentence 1268: Replace "utilize" by "use" in:
The child may also utilize knowledge about the password#'s creator
*** Sentence 1272: Replace "employing" by "using" in:
Employing statistical analysis and mathematical probability allows guessing passwords more precisely [136, 213, 114]
*** Sentence 1273: Replace "existing techniques" by "current techniques" in:
In the thesis, I show various improvements to existing techniques and propose how to use them in a parallel and distributed password cracking trial
*** Sentence 1275: Replace "deal with" by "concern" or "handle" or "encounter" in:
The need to deal with cryptographic protection is undisputable
*** Sentence 1276: Replace "undertaken" by "done" in:
To identify the most sig-nificant challenges in digital forensics, Al Fahdi et al. performed a survey undertaken by 42 forensic experts from law enforcement, industry, and academia
*** Sentence 1278: Replace "one of the" by "one" if followed by a plural noun, and make it singular in:
In a survey from Harichandran et al. with 99 participants, mostly from North America and Europe, encryption was identified as one of the three most crucial challenges
*** Sentence 1278: Replace "crucial" by "key" in:
In a survey from Harichandran et al. with 99 participants, mostly from North America and Europe, encryption was identified as one of the three most crucial challenges
*** Sentence 1279: Replace "performed by" by "done by" in:
The growing importance of encryption is noticeable from the surveys performed by Forensic Focus that asked about the biggest challenge forensic investigators face today
*** Sentence 1284: Replace "one of the" by "one" if followed by a plural noun, and make it singular in:
Roussev discusses pervasive encryption as one of the six major issues in today#'s forensics [176]
*** Sentence 1289: Delete "use of" in:
The first documented use of password protection on computers dates back to the 1960s
*** Sentence 1291: Replace "encountered" by "met" or "saw" or "seen" in:
The same system also encountered the first security breach
*** Sentence 1293: Replace "gained access to" by "accessed" in:
Since the passwords were stored in a plaintext form, Scherr gained access to all user accounts [122]
*** Sentence 1295: Replace "pre-defined" by "predefined" in:
The square root of a password was modified by the #"AND#" operation with a pre-defined mask to discard some bits
*** Sentence 1300: Replace "states that" by "says" if "states" is a verb in:
McIlroy states that the explicit intention was to stimulate code-breaking ex-periments, and Morris himself was able to break crypt by hand [121]
*** Sentence 1300: Replace "was able to" by "could" in:
McIlroy states that the explicit intention was to stimulate code-breaking ex-periments, and Morris himself was able to break crypt by hand [121]
*** Sentence 1311: Replace "employ" by "use" in:
Despite its original purpose being encryption, it is possible to employ DES for one-way hashing [123]
*** Sentence 1316: Replace "is performed" by "is done" in:
The encryption is performed 25 times, and the resulting 64 bits are repacked to become a string of 11 printable characters
*** Sentence 1324: Delete "the method of" in:

In 1982, Ron Rivest improved the concept with the method of distinguished points that reduced the number of necessary lookup operations [174]
*** Sentence 1326: Replace "lan" by "local-area network" in:
Microsoft also used DES for calculating Lan Manager (LM) hashes
*** Sentence 1330: Replace "two separate" by "two" in:
Moreover, passwords longer than eight characters can be cracked in two separate chunks [125]
*** Sentence 1332: Replace "in contrast to" by "compared to" in:
The new version uses Unicode encoding, but in contrast to UNIX, does not employ salt or multiple iterations [179, 125]
*** Sentence 1332: Replace "employ" by "use" in:
The new version uses Unicode encoding, but in contrast to UNIX, does not employ salt or multiple iterations [179, 125]
*** Sentence 1339: Replace "publicly available" by "public" in:
The first publicly available password cracking tools were released in the early 1990s
*** Sentence 1345: Replace "were able to" by "could" in:
Both Crack and Cracker Jack were able to use values from the GECOS field in the password file [93]
*** Sentence 1358: Replace "a lot of" by "much" or "many" in:
The tool offered high performance but required a lot of space for precomputed tables since each candidate password was hashed with 212 possible salts
*** Sentence 1359: Replace "it was necessary to" by "one must" in:
For each password, it was necessary to store an additional 4 kB of data
*** Sentence 1359: Replace "an additional" by "another" in:
For each password, it was necessary to store an additional 4 kB of data
*** Sentence 1365: Replace "in addition to" by "besides" in:
In addition to Cracker Jack#'s features, John the Ripper had an incremental brute-force attack mode [159]
*** Sentence 1367: Replace "capable of" by "that can" or "that could" if preceded by a noun, and change following word to a verb in:
It was the first tool capable of cracking NTLM hashes
*** Sentence 1370: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
In 1998, The Electronic Frontier Foundation (EFF) presented a machine called EFF DES Cracker, nicknamed #"Deep Crack,#" based on ASIC chips
*** Sentence 1388: Replace "is used for" by "is for" in:
AES is used for encrypting both RAR v3 [6] and v5 archives [175]
*** Sentence 1390: Replace "one of the" by "one" if followed by a plural noun, and make it singular in:
TrueCrypt and VeraCrypt also support AES as one of the multiple encryption options [218]
*** Sentence 1391: Replace "via" by "by" in:
While AES serves for encryption of data, storing and verifying passwords is usually per-formed via one-way hash functions
*** Sentence 1396: Replace "allows to" by "allows one to" or "allows them", etc. in:
Moreover, it provides a variable number of iterations, which allows to strengthen it over time to remain resistant against attacks [167]
*** Sentence 1399: Replace "bits in length" by "bits" in:
The SHA-2 functions are much more secure than the original SHA-1 and produce digests from 224 to 512 bits in length [138]
*** Sentence 1401: Replace "in the process of" by "while" in:
We can also observe advances in the process of key derivation, i.e., the process of making a fixed-size encryption key from a password
*** Sentence 1412: Replace "was able to" by "could" in:
The version from 2002 was able to crack multiple encrypted media formats, categorized into three levels by difficulty
*** Sentence 1418: Replace "was capable of" by "could" change following word to a verb in:
Their Password Recovery Kit (see Section 2.4.7) from 1998 was capable of cracking Office 95 and 97 documents

*** Sentence 1419: Replace "capable of" by "that can" or "that could" if preceded by a noun, and change following word to a verb in:
An improved version available in 2002 was also capable of decrypt-ing PDF documents, WinZip archives, and Windows NT/NTLM passwords [67]
*** Sentence 1422: Replace "game-changer" by "major improvement" in:
A game-changer in hash cracking arrived in 2003 when Philippe Oeschlinn presented rainbow tables, inspired by the cryptanalytic time-memory tradeoff from Hellman and Rivest
*** Sentence 1422: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
A game-changer in hash cracking arrived in 2003 when Philippe Oeschlinn presented rainbow tables, inspired by the cryptanalytic time-memory tradeoff from Hellman and Rivest
*** Sentence 1423: Replace "storage space" by "storage" in:
Unlike classic lookup tables used in Qcrack, rainbow tables use the concept of chains and hash reduction that decreased the necessary storage space dramatically [142]
*** Sentence 1425: Replace "publicly available" by "public" in:
The goal is the devel-opment of a general-purpose implementation of Oechslin#'s technique, precomputing hashes and maintaining a publicly available rainbow table repository
*** Sentence 1427: Replace "known as" by "called" in:
In 2009, Jens Steube, known as #"atom#", decided to fix the missing multi-threading support in John the Ripper#'s dictionary attack mode
*** Sentence 1430: Replace "gpu" by "graphical processing unit" in:
The release of NVIDIA CUDA [141] in 2007 and OpenCL [134] from the Khronos Group in 2009 allowed using GPU units for general-purpose computing
*** Sentence 1432: Replace "gpu" by "graphical processing unit" in:
In 2008, Elcomsoft company, a commer-cial creator of password cracking solutions (see Section 2.4.5), introduced GPU accelerated computing of some of the supported algorithms
*** Sentence 1432: Replace "some of the" by "some" if followed by a plural noun in:
In 2008, Elcomsoft company, a commer-cial creator of password cracking solutions (see Section 2.4.5), introduced GPU accelerated computing of some of the supported algorithms
*** Sentence 1433: Replace "gpu" by "graphical processing unit" in:
The same year, Graves proposed a solution for cracking NTLM and MD4 hashes with rainbow tables on GPU
*** Sentence 1435: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
In 2009, Kipper et al. presented an implementation of AES for GPU [106]
*** Sentence 1435: Replace "gpu" by "graphical processing unit" in:
In 2009, Kipper et al. presented an implementation of AES for GPU [106]
*** Sentence 1437: Replace "gpu" by "graphical processing unit" in:
The first wave of GPU crackers included other, mostly free but later aban-doned, projects: GPU md5 Crack, Multihash CUDA bruteforcer, Extreme GPU Brute-forcer, ISHASHGPU, and Bars WF Bruteforce
*** Sentence 1437: Replace "extreme" by "high" in:
The first wave of GPU crackers included other, mostly free but later aban-doned, projects: GPU md5 Crack, Multihash CUDA bruteforcer, Extreme GPU Brute-forcer, ISHASHGPU, and Bars WF Bruteforce
*** Sentence 1439: Replace "gpu" by "graphical processing unit" in:
Bakker et al. compared the performance of Ex-treme GPU Bruteforcer, ISHASHGPU, Bars WF Bruteforce, and the commercial solution from Elcomsoft
*** Sentence 1440: Replace "massive" by "large" in:
All four tools showed a massive speedup on GPU in comparison to CPU cracking
*** Sentence 1440: Replace "gpu" by "graphical processing unit" in:
All four tools showed a massive speedup on GPU in comparison to CPU cracking
*** Sentence 1440: Replace "cpu" by "processor" in:
All four tools showed a massive speedup on GPU in comparison to CPU cracking
*** Sentence 1444: Replace "gpus" by "graphical processing units" in:
The main advantage of OpenCL is that it was supported by GPUs from both NVIDIA and ATI/AMD
*** Sentence 1447: Replace "gpu" by "graphical processing unit" in:

Unlike Cracker Jack and John the Ripper, the new tool applied word-mangling rules on GPU kernel, which dramatically reduced the number of necessary PCI-E transfers [193]
*** Sentence 1449: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
In 2011, Sprengers presented a CUDA-based MD5 cracker
*** Sentence 1455: Replace "gpu" by "graphical processing unit" in:
In the same year, AccessData added support for GPU acceleration to their PRTK 7.0 and DNA 7.0 tools [34]
*** Sentence 1458: Replace "in the past" by "previously" if not followed by a noun in:
In the past years, Team hashcat won several years of DEFCON and DerbyCon Crack Me If You Can (CMYIC) contests [220]
*** Sentence 1462: Replace "gpu" by "graphical processing unit" in:
Despite the revolutionary GPU acceleration and massive improvements in password crack-ing performance, attacking state-of-the-art cryptographic protection is still very difficult
*** Sentence 1462: Replace "massive" by "large" in:
Despite the revolutionary GPU acceleration and massive improvements in password crack-ing performance, attacking state-of-the-art cryptographic protection is still very difficult
*** Sentence 1462: Replace "state-of-the-art" by "recent" in:
Despite the revolutionary GPU acceleration and massive improvements in password crack-ing performance, attacking state-of-the-art cryptographic protection is still very difficult
*** Sentence 1466: Replace "extremely" by "very" in:
Cracking bcrypt hashes with a higher number of iterations is extremely challenging
*** Sentence 1470: Replace "employs" by "uses" in:
However, its successor, the VeraCrypt, employs 655,331 iterations of RIPEMD-160 and 500,000 itera-tions of SHA-2 [218, 196]
*** Sentence 1472: Delete "the use of" if followed by a gerund or noun describing an action in:
The use of salt eliminates possible rainbow table attacks, and every iteration is costly
*** Sentence 1478: Replace "intentionally designed" by "designed" in:
The algorithm was intentionally designed to have high memory requirements to prevent massively parallel attacks
*** Sentence 1484: Replace "state-of-the-art" by "recent" in:
Even a multi-GPU machine with state-of-the-art tools and optimized algorithms may not be enough
*** Sentence 1486: Replace "put together" by "assemble" or "assembled" in:
One solution is to put together a grid or cluster of machines to achieve the desired performance
*** Sentence 1489: Replace "likely to be" by "likely" unless followed by a participle in:
We may only verify the candidate passwords that are likely to be correct
*** Sentence 1492: Replace "present" by "show" or "give" or "offer" if a transitive verb in:
Thereby, I present the work related to this subject in Section 4.2
*** Sentence 1495: Replace "a smaller amount of" by "less" in:
In other words, proposing techniques that allow finding passwords in a smaller amount of time
*** Sentence 1495: Replace "amount of time" by "time" in:
In other words, proposing techniques that allow finding passwords in a smaller amount of time
*** Sentence 1499: Delete "the use of" if followed by a gerund or noun describing an action in:
Focus on the use of GPGPU-based solutions
*** Sentence 1500: Replace "amongst" by "among" in:
Explore the possible techniques to distribute the workload amongst multiple nodes
*** Sentence 1501: Replace "existing frameworks" by "current frameworks" in:
Analyze existing frameworks for distributed computing in terms of their suitability for password cracking
*** Sentence 1501: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
Analyze existing frameworks for distributed computing in terms of their suitability for password cracking
*** Sentence 1507: Replace "by performing a" by "by a" in:
Experimentally evaluate the solution by performing a series of experiments under various settings
*** Sentence 1510: Replace "utilizing" by "using" in:
Study the methods for the time-space tradeoff attacks and utilizing the knowledge about existing passwords

*** Sentence 1511: Delete "the use of" if followed by a gerund or noun describing an action in:
Explore the use of statistical analysis and mathematical probability to model users#' password creation habits
*** Sentence 1523: Replace "while there are" by "despite" in:
While there are multiple commonly-used attack modes, it is necessary to take their properties and requirements into account
*** Sentence 1523: Replace "it is necessary to" by "one must" in:
While there are multiple commonly-used attack modes, it is necessary to take their properties and requirements into account
*** Sentence 1525: Replace "present" by "show" or "give" or "offer" if a transitive verb in:
Moreover, I present distribution techniques for two additional modes with external password generators: the PRINCE and the PCFG attacks
*** Sentence 1527: Replace "utilize" by "use" in:
problem efficiently between the computation nodes to minimize the overhead and utilize the maximum of available hardware resources
*** Sentence 1528: Replace "utilize" by "use" in:
I utilize the above-shown methods to create a general-purpose high-efficiency GPGPU password cracking system called Fitcrack [87]
*** Sentence 1528: Replace "above-shown" by "previously shown" in:
I utilize the above-shown methods to create a general-purpose high-efficiency GPGPU password cracking system called Fitcrack [87]
*** Sentence 1530: Replace "denoted" by "meant" or "indicated" or "represented" in:
The design reflects the re-quirements denoted in Section 3.3
*** Sentence 1531: Replace "is capable of" by "can" and change following word to a verb in:
I experimentally verify that the new solution is capable of performing distributed attacks reliably and efficiently
*** Sentence 1535: Replace "utilize" by "use" in:
The principle is to utilize the knowledge of users#' password creation habits
*** Sentence 1538: Replace "leads to" by "causes" or "enables" or "finds" in:
Firstly, the thesis shows that removing specific rewrite rules leads to a massive speedup of password guessing without having a considerable impact on the success rate
*** Sentence 1538: Replace "massive" by "large" in:
Firstly, the thesis shows that removing specific rewrite rules leads to a massive speedup of password guessing without having a considerable impact on the success rate
*** Sentence 1538: Replace "without having a" by "without a" in:
Firstly, the thesis shows that removing specific rewrite rules leads to a massive speedup of password guessing without having a considerable impact on the success rate
*** Sentence 1549: Replace "utilizing" by "using" in:
It analyzes possible ways of utilizing multiple nodes concerning different tasks and attack modes
*** Sentence 1549: Replace "concerning" by "about" in:
It analyzes possible ways of utilizing multiple nodes concerning different tasks and attack modes
*** Sentence 1552: Replace "the state-of-the-art" by "the latest" in:
It describes multiple enhancements to the state-of-the-art cracking with probabilistic context-free grammars, including a parallel and distributed so-lution
*** Sentence 1554: Replace "provides an overview of" by "surveys" or "summarizes" in:
Appendix A provides an overview of the most common password-protected formats and describes concrete procedures for password verification
*** Sentence 1558: Delete "a process of" in:
Password recovery is a process of obtaining passwords for accessing protected content
*** Sentence 1558: Replace "obtaining" by "getting" in:
Password recovery is a process of obtaining passwords for accessing protected content
*** Sentence 1559: Replace "performed by" by "done by" in:
When performed by force, the procedure is commonly referred to as password cracking [117]

*** Sentence 1559: Replace "referred to as" by "called" in:
When performed by force, the procedure is commonly referred to as password cracking [117]
*** Sentence 1562: Replace "consists of two" by "has two" in:
In a nutshell, password cracking consists of two phases: a) password generation and b) pass-word verification
*** Sentence 1565: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Figure 2.1: An illustration of the password cracking process There are two types of password cracking attacks:
*** Sentence 1569: Replace "e.g.," by "for example," in:
The main drawback of such an attack is that the defender#'s security features can be active, e.g., the verification is temporarily disabled after reaching several attempts, etc.
*** Sentence 1569: Replace "etc." by "and so on" in:
The main drawback of such an attack is that the defender#'s security features can be active, e.g., the verification is temporarily disabled after reaching several attempts, etc.
*** Sentence 1570: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
Offline attack - when the attacker has direct access to password hash or encrypted content, there is no need to communicate with the live system
*** Sentence 1571: Replace "e.g.," by "for example," in:
Attackers can generate and verify the passwords on their own machines, e.g., using a GPU-equipped HPC cluster
*** Sentence 1575: Replace "referred to as" by "called" in:
Password cracking examines a series of candidate passwords, also referred to as password guesses
*** Sentence 1577: Replace "utilize" by "use" in:
The password generation may utilize both existing string fragments or build entirely new ones from a pre-defined set of characters
*** Sentence 1577: Replace "pre-defined" by "predefined" in:
The password generation may utilize both existing string fragments or build entirely new ones from a pre-defined set of characters
*** Sentence 1579: Delete "the use of" if followed by a gerund or noun describing an action in:
Smarter methods also introduce the use of mathematical probability and statistics to guess passwords more precisely
*** Sentence 1584: Replace "at least one" by "a" or "an" in:
Was the password created to respect some policies: minimal length, at least one number, and special symbol, etc.
*** Sentence 1584: Replace "etc." by "and so on" in:
Was the password created to respect some policies: minimal length, at least one number, and special symbol, etc.
*** Sentence 1586: Replace "launching the attack" by "attacking" in:
The attacker shall answer these questions before launching the attack
*** Sentence 1589: Delete "one or more" in:
The configuration contains one or more alphabets and a series of rules that define how to build strings from them
*** Sentence 1592: Replace "utilize" by "use" in:
More advanced alternatives may utilize additional rules for specifying what characters are allowed in which position, etc. The main advantage of the exhaustive search is that, if appropriately configured, it eventually finds the correct password
*** Sentence 1592: Replace "etc." by "and so on" in:
More advanced alternatives may utilize additional rules for specifying what characters are allowed in which position, etc. The main advantage of the exhaustive search is that, if appropriately configured, it eventually finds the correct password
*** Sentence 1593: Replace "enormous" by "very large" in:
The main drawback is usually the enormous number of candidate passwords

*** Sentence 1596: Replace "utilize" by "use" in:
Dictionary-based attacks utilize existing wordlists of strings
*** Sentence 1597: Replace "employs" by "uses" in:
The classic dictionary attack employs a single wordlist where each line represents a candidate password
*** Sentence 1599: Replace "e.g.," by "for example," in:
Some tools also support additional password-mangling rules that modify the strings before use, e.g., capitalize the first letter, swap or substitute some characters, etc. Concrete techniques are discussed in Section 3.8.1
*** Sentence 1599: Replace "etc." by "and so on" in:
Some tools also support additional password-mangling rules that modify the strings before use, e.g., capitalize the first letter, swap or substitute some characters, etc. Concrete techniques are discussed in Section 3.8.1
*** Sentence 1601: Replace "employ" by "use" in:
The combination may use fixed-position placements (see Section 3.8.2) or employ letter chains like the PRINCE
*** Sentence 1607: Replace "state-of-the-art" by "recent" in:
Advanced state-of-the-art password guessing techniques often employ mathematical proba-bility and use results of statistical analysis
*** Sentence 1607: Replace "employ" by "use" in:
Advanced state-of-the-art password guessing techniques often employ mathematical proba-bility and use results of statistical analysis
*** Sentence 1609: Replace "extremely" by "very" in:
Such methods are extremely effi-cient against human-created passwords since they can reflect the users#' password-creating habits
*** Sentence 1610: Replace "utilize" by "use" in:
They may utilize the knowledge obtained from previously-known passwords, the creator#'s country of origin, language, personal information, and other useful details
*** Sentence 1613: Replace "it is necessary to" by "one must" in:
Once we get a candidate password, it is necessary to verify it for correctness
*** Sentence 1616: Replace "publicly available" by "public" in:
While proprietary applications often hide the internal implementation of password handling, open formats are usually well-documented, and the specification of necessary password verification steps are mostly publicly available
*** Sentence 1621: Replace "impact of" by "effect of" in:
The motivation is to minimize the impact of a possible security breach so that the attacker does not instantly pick up passwords of all users
*** Sentence 1625: Replace "illustrates" by "shows" in:
Figure 2.2 illustrates the principle
*** Sentence 1627: Delete "one or more" in:
The calculation may require to compute one or more iterations of a single hash function or a combination of hash functions
*** Sentence 1628: Replace "referred to as" by "called" in:
Once we get an output, we compare it with the known hash, also referred to as the verification value
*** Sentence 1632: Replace "do not need to" by "need not" in:
Therefore, for password verification, we do not need to decrypt the contents
*** Sentence 1634: Replace "in the case of" by "for" in:
In the case of shorter passwords, the lookup table [174] or rainbow
*** Sentence 1637: Replace "employ" by "use" in:
Therefore, many formats employ cryptographic salt - a pseudorandom high-entropy value added to the password before calculating the hash
*** Sentence 1637: Replace "value added" by "added value" if referring to a product feature in:
Therefore, many formats employ cryptographic salt - a pseudorandom high-entropy value added to the password before calculating the hash

*** Sentence 1638: Delete "there is" and insert "occurs" or "is" or a similar word later in:
The salt makes the password longer so that there is a very low probability that it matches any pre-computed table
*** Sentence 1639: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
The salt needs to be stored together with the hash since it is necessary for the verification
*** Sentence 1639: Replace "together with" by "with" in:
The salt needs to be stored together with the hash since it is necessary for the verification
*** Sentence 1641: Replace "value added" by "added value" if referring to a product feature in:
A cryptographic pepper is another extra high-entropy value added to the password before hashing by some applications
*** Sentence 1643: Delete "the use of" if followed by a gerund or noun describing an action in:
The use of pepper follows the NIST recommendations to use a secret value known only to the verifier
*** Sentence 1661: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
In many cases, there is no verification value with the stored password hash
*** Sentence 1663: Replace "need to" by "must" if "need" is a verb in:
First, we need to get an encryption key
*** Sentence 1667: Replace "together with" by "with" in:
As the pseudorandom function, HMAC is typically used together with a hash function like SHA-2 or other [132]
*** Sentence 1669: Replace "need to" by "must" if "need" is a verb in:
To perform the decryption-based verification automatically, we need to know a part of the plaintext
*** Sentence 1670: Delete "there is" and insert "occurs" or "is" or a similar word later in:
After the decryption, we check if there is the string we are looking for
*** Sentence 1675: Replace "is illustrated" by "is shown" in:
The principle of the decryption-based password verification is illustrated in Figure 2.3
*** Sentence 1675: Replace "illustrated in" by "shown in" in:
The principle of the decryption-based password verification is illustrated in Figure 2.3
*** Sentence 1700: Replace "illustrated in" by "shown in" in:
In such a case, we use a checksum-based password verification, as illustrated in Figure 2.4
*** Sentence 1707: Delete "there is" and insert "occurs" or "is" or a similar word later in:
For each file inside the archive, there is a header with a CRC checksum of the file
*** Sentence 1708: Replace "it is necessary to" by "one must" in:
For recovery, it is necessary to decrypt and decompress the data of at least one of the files inside the archive
*** Sentence 1708: Replace "at least one of the" by "some" if followed by a plural noun, else "some of the" in:
For recovery, it is necessary to decrypt and decompress the data of at least one of the files inside the archive
*** Sentence 1709: Replace "need to" by "must" if "need" is a verb in:
Then, we need to compute a CRC checksum from it
*** Sentence 1713: Replace "two different" by "two" in:
passwords (see Section A.2.1) since the checksum is relatively short and thus two different inputs may produce the same CRC code
*** Sentence 1743: Delete "the use of" if followed by a gerund or noun describing an action in:
For this attack mode, John the Ripper provides the use of password-mangling rules that extend the repertoire of password guesses by modifications like letter capitalization, character swapping, and others
*** Sentence 1743: Replace "modifications" by "changes" in:
For this attack mode, John the Ripper provides the use of password-mangling rules that extend the repertoire of password guesses by modifications like letter capitalization, character swapping, and others
*** Sentence 1745: Replace "all of the" by "all" or "all the" if followed by a plural noun in:
The Fitcrack system, proposed in this thesis, also supports all of the JtR#'s mangling rules
*** Sentence 1747: Replace "a large set of" by "many" if followed by a plural noun, and change a following verb to plural in:
It also applies a large set of mangling rules
*** Sentence 1752: Replace "employ" by "use" in:

Therefore, the user may employ an external password generator, connect it via a pipe, and use JtR as a backend cracker to verify password guesses
*** Sentence 1752: Replace "via" by "by" in:
Therefore, the user may employ an external password generator, connect it via a pipe, and use JtR as a backend cracker to verify password guesses
*** Sentence 1753: Replace "frequently" by "often" in:
The tool is also frequently referenced in many scientific studies from the password cracking area [66, 109, 213, 211]
*** Sentence 1754: Replace "gpu" by "graphical processing unit" in:
Starting from 2011, JtR provides GPU acceleration for a still increasing number of supported algorithms [158]
*** Sentence 1757: Replace "utilize" by "use" in:
From all supported formats, 88 utilize GPU-accelerated cracking
*** Sentence 1760: Replace "in addition to" by "besides" in:
In addition to the freely-available distribution, there is a commercial Pro version with extended upgrades and enterprise support
*** Sentence 1760: Delete "there is" and insert "occurs" or "is" or a similar word later in:
In addition to the freely-available distribution, there is a commercial Pro version with extended upgrades and enterprise support
*** Sentence 1760: Replace "enterprise" by "organization" in:
In addition to the freely-available distribution, there is a commercial Pro version with extended upgrades and enterprise support
*** Sentence 1767: Replace "incorporates" by "includes" in:
Moreover, Cain & Abel incorporates many other ex-isting tools into it
*** Sentence 1774: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
First, there is no GPU acceleration
*** Sentence 1774: Replace "gpu" by "graphical processing unit" in:
First, there is no GPU acceleration
*** Sentence 1775: Replace "modifications" by "changes" in:
Next, while the tool supports password-mangling rules, the only available modifications are case mangling, swapping characters, and appending characters to the end of each candidate password
*** Sentence 1776: Replace "e.g.," by "for example," in:
The attacks based on frequency analysis, e.g., based on Markovian models, are not supported
*** Sentence 1778: Replace "etc." by "and so on" in:
creating rainbow tables [142], submitting password hashes to online lookup databases, etc.
*** Sentence 1781: Replace "nowadays" by "today" in:
Sadly, the project nowadays seems to be abandoned
*** Sentence 1793: Replace "lacks the ability to" by "cannot" in:
The included HashGen utility could calculate new hashes to extend the default set [165, 111] While the built-in cracking rules are more sophisticated than in Cain & Abel, L0phtcrack lacks the ability to define custom word mangling rules [211]
*** Sentence 1794: Replace "enterprise" by "organization" in:
In 2020, Terrahash the L0pthrack was purchased11 by Terrahash LLC, a company cre-ated by inventors of the popular hashcat tool and the creators of Hashstack, an enterprise distributed password cracking solution
*** Sentence 1796: Replace "gpu" by "graphical processing unit" in:
Thanks to this change, the tool now supports GPU acceleration and the User info attack that corresponds to JtR#'s Single crack mode [110]
*** Sentence 1799: Replace "publicly available" by "public" in:
In 2015, the code was made publicly available under the MIT license, and it is nowadays an open-source project with a large fan base and a community of contributors
*** Sentence 1799: Replace "nowadays" by "today" in:
In 2015, the code was made publicly available under the MIT license, and it is nowadays an open-source project with a large fan base and a community of contributors

*** Sentence 1800: Delete "there were" and insert "occurred" or "were possible" or similar word later in:
Originally, there were three tools: the legacy hashcat for CPU-based cracking, the oclHashcat with the OpenCL cracking kernels for NVIDIA/AMD cards, and the cudaHashcat dedicated for NVIDIA only
*** Sentence 1811: Replace "does not have" by "lacks" in:
Unlike many other tools, hashcat does not have a graphical user interface and is therefore designed for advanced users
*** Sentence 1811: Replace "not have a" by "lack a" in:
Unlike many other tools, hashcat does not have a graphical user interface and is therefore designed for advanced users
*** Sentence 1815: Replace "employ" by "use" in:
While hashcat can crack Office documents, ZIP, 7z, and RAR archives, encrypted disk volumes, or even cryptocurrency wallets, the user needs first to employ external utilities or #"scraper#" scripts to extract all necessary metadata from the password-protected medium
*** Sentence 1816: Replace "in addition to" by "besides" in:
The extracted so-called #"hash#" has a common format and, in addition to the raw hash, may also contain other values like iteration count, cryptographic salt, version, key length, or even part of the encrypted and/or compressed content [95]
*** Sentence 1816: Replace "and/or" by "or" in:
The extracted so-called #"hash#" has a common format and, in addition to the raw hash, may also contain other values like iteration count, cryptographic salt, version, key length, or even part of the encrypted and/or compressed content [95]
*** Sentence 1818: Replace "need to" by "must" if "need" is a verb in:
With hashcat, you first need to extract the hash
*** Sentence 1822: Replace "in the past" by "previously" if not followed by a noun in:
(CMIYC) contests15 in the past 10 years [220]
*** Sentence 1824: Replace "each of these" by "each" in:
In Section 3.8, I discuss each of these attack modes in detail
*** Sentence 1829: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Nevertheless, there is a difference in their application
*** Sentence 1830: Replace "gpu" by "graphical processing unit" in:
While JtR modified the dictionary words on the host machine#'s CPU, hashcat#'s rule engine is implemented inside the GPU kernels
*** Sentence 1835: Replace "similar to" by "like" in:
In 2020, hashcat developers announced a new mode called #"association attack,#" which should be similar to JtR#'s single crack mode
*** Sentence 1837: Replace "in addition to" by "besides" in:
In addition to the source code, hashcat developers provide pre-compiled binaries for both Linux and Windows systems
*** Sentence 1843: Replace "in addition to" by "besides" in:
In addition to the set of single-purpose tools, Elcomsoft Distributed Password Recovery (EDPR), released in 2006, is an all-in-one solution for distributed cracking [59]
*** Sentence 1843: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
In addition to the set of single-purpose tools, Elcomsoft Distributed Password Recovery (EDPR), released in 2006, is an all-in-one solution for distributed cracking [59]
*** Sentence 1848: Replace "not possible" by "impossible" in:
Yet, it is not possible to define custom rules
*** Sentence 1852: Replace "most of the" by "most" if followed by a plural noun in:
Most of the crackers provide GPU acceleration, but not all of them
*** Sentence 1852: Replace "gpu" by "graphical processing unit" in:
Most of the crackers provide GPU acceleration, but not all of them
*** Sentence 1855: Replace "i tested" by "we tested" in:
In my early research, I tested three Elcomsoft tools

*** Sentence 1865: Replace "gpu" by "graphical processing unit" in:
Since version 7, released in 2014, the software offers GPU acceleration using NVIDIA CUDA [34]
*** Sentence 1867: Replace "gpu" by "graphical processing unit" in:
The GPU acceleration is, however, currently available only for MS Office and WinZIP [5]
*** Sentence 1867: Replace "currently available" by "available" in:
The GPU acceleration is, however, currently available only for MS Office and WinZIP [5]
*** Sentence 1870: Replace "etc." by "and so on" in:
For creating word fragments, it offers multiple language profiles: European, Arabic, Russian, etc. Unfortunately, the PRTK can not use an external password generator [5]
*** Sentence 1870: Replace "can not" by "cannot" in:
For creating word fragments, it offers multiple language profiles: European, Arabic, Russian, etc. Unfortunately, the PRTK can not use an external password generator [5]
*** Sentence 1874: Replace "was capable of" by "could" change following word to a verb in:
An early version from 1998 was capable of cracking MS Office 95 and 97 passwords [150]
*** Sentence 1878: Replace "attempt to" by "try to" in:
It can perform a deep scan of the system to locate password-protected items and attempt to crack their passwords
*** Sentence 1881: Replace "modifications" by "changes" in:
First, it has a dictionary attack with advanced features like patterns and case modifications
*** Sentence 1884: Replace "similar to" by "like" in:
The mask attack is similar to hashcat#'s brute-force and allows specifying what characters to use at each position
*** Sentence 1885: Replace "used in combination with" by "combined with" in:
#"Known Password/Part attack#" can be used in combination with other modes if the user knows part of the guessed password
*** Sentence 1887: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
There are multiple editions from Passware Kit Basic to Passware Kit Forensic with different pricing, capabilities, and supported formats
*** Sentence 1889: Replace "gpu" by "graphical processing unit" in:
Approxi-mately half of them are crackable with GPU acceleration, while the rest is CPU-only
*** Sentence 1896: Replace "lan" by "local-area network" in:
The tool can perform a rainbow table attack on Windows Lan Manager (LM) and NTLM hashes
*** Sentence 1910: Replace "in contrast to" by "compared to" in:
In contrast to RainbowCrack, Ophcrack does not support GPU acceleration
*** Sentence 1910: Replace "gpu" by "graphical processing unit" in:
In contrast to RainbowCrack, Ophcrack does not support GPU acceleration
*** Sentence 1914: Replace "lan" by "local-area network" in:
The initial version supported only Microsoft Lan Manager (LM) hashes and contained three tools for 32-bit Windows: rtgen, rtsort, and rcrack
*** Sentence 1922: Replace "gpu" by "graphical processing unit" in:
For both Windows and Linux, Rainbow Crack now supports GPU acceleration with NVIDIA CUDA and AMD OpenCL
*** Sentence 1923: Replace "gpu" by "graphical processing unit" in:
Nevertheless, calculating on GPU only works with purchased tables
*** Sentence 1932: Replace "utilizing" by "using" in:
Once we reach that boundary, the only way of getting over is by utilizing more nodes
*** Sentence 1933: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
As there are many options for distributed processing, it is necessary to choose methods that meet the requirements of a given task
*** Sentence 1933: Replace "it is necessary to" by "one must" in:
As there are many options for distributed processing, it is necessary to choose methods that meet the requirements of a given task
*** Sentence 1944: Replace "present" by "show" or "give" or "offer" if a transitive verb in:

I present the system#'s architecture, necessary server daemons to work with BOINC, client modules, communication between nodes, and others
*** Sentence 1946: Replace "utilizing" by "using" in:
For each attack mode, I propose a unique distribution strategy that allows controlling and utilizing available resources efficiently
*** Sentence 1947: Replace "by performing a" by "by a" in:
Finally, I verify the usability of the proposed methods by performing a series of practical experiments with a proof-of-concept implementation of Fitcrack
*** Sentence 1967: Replace "cpu" by "processor" in:
The cracking performance I measured using Elcomsoft Advanced Archive Password Recovery 4.54 (see Section 2.4.5) and a single Intel(R) Core i7 CPU 920 was ###=8, 102 p/s [83]
*** Sentence 1971: Replace "obtain" by "get" in:
Therefore, I show how parallel and distributed computing can increase the overall performance and help obtain results in an acceptable time
*** Sentence 1975: Replace "etc." by "and so on" in:
For different formats, the procedure consists of different steps and requires different inputs like the number of hash function iterations, cryptographic salt or pepper, padding, etc. However, for a single cracking session, the only parameter that changes is the password itself
*** Sentence 1977: Replace "since there is" by "with" in:
Since there is no mutual dependence between different password candidates, we can verify them separately
*** Sentence 1977: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
Since there is no mutual dependence between different password candidates, we can verify them separately
*** Sentence 1980: Replace "be performed" by "be done" in:
Figure 3.1 shows how the password cracking can be performed in parallel using #" i processor cores
*** Sentence 2015: Replace "does not have" by "lacks" in:
While cracking raw hashes usually does not have high memory requirements, for formats where we need to decrypt part of the protected content (e.g., VeraCrypt, PKZIP, or RAR 3.0), the amount of available memory may become a bottleneck in the password cracking process
*** Sentence 2015: Replace "need to" by "must" if "need" is a verb in:
While cracking raw hashes usually does not have high memory requirements, for formats where we need to decrypt part of the protected content (e.g., VeraCrypt, PKZIP, or RAR 3.0), the amount of available memory may become a bottleneck in the password cracking process
*** Sentence 2020: Replace "in use" by "used" in:
This approach is most beneficial if cryptographic salt is not in use
*** Sentence 2021: Replace "is illustrated" by "is shown" in:
An example of parallel hashlist cracking is illustrated by Figure 3.2
*** Sentence 2022: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
For each password, the hash only needs to be calculated once
*** Sentence 2027: Replace "need to" by "must" if "need" is a verb in:
Before the final comparison, we need to apply each salt to the password and recompute the hash function again
*** Sentence 2050: Replace "utilization" by "use" in:
Utilization of GPGPU-
*** Sentence 2052: Replace "impact of" by "effect of" in:
Neglecting the impact of memory and caching, from Equation 3.2, we can state that the two main factors influencing the theoretical performance are the number of cores and processor clock frequency
*** Sentence 2052: Replace "state that" by "say" if "state" is a verb in:
Neglecting the impact of memory and caching, from Equation 3.2, we can state that the two main factors influencing the theoretical performance are the number of cores and processor clock frequency
*** Sentence 2054: Replace "carry out" by "complete" or "execute" or "do" unless referring to physical motion in:
Central processing units (CPU), designed to carry out instructions of an operating sys-tem and applications, usually contain few very fast cores

*** Sentence 2055: Replace "cpus" by "processors" in:
Today#'s desktop CPUs usually have 2 to 18 cores, while for server and high-end workstations, the number may be higher
*** Sentence 2057: Replace "cpus" by "processors" in:
To boost up paral-lelization, some CPUs employ a multithreading technology like Intel Hyper-Threading
*** Sentence 2057: Replace "employ" by "use" in:
To boost up paral-lelization, some CPUs employ a multithreading technology like Intel Hyper-Threading
*** Sentence 2059: Replace "cpus" by "processors" in:
In the past few years, the operating frequency of CPUs flew between 2 to 5 GHz and did not increase dramatically due to energy and thermal constraints [107]
*** Sentence 2060: Delete "were designed to" and change following verb to past tense in:
Graphics processing units (GPU), on the other hand, were designed to render graphics, which requires to perform operations on large vectors and matrixes of values
*** Sentence 2060: Replace "render" by "make" in:
Graphics processing units (GPU), on the other hand, were designed to render graphics, which requires to perform operations on large vectors and matrixes of values
*** Sentence 2061: Replace "gpus" by "graphical processing units" in:
Thus, GPUs have a lower operating frequency but contain thousands of cores
*** Sentence 2073: Replace "cpu" by "processor" in:
CPU (b) GPU
*** Sentence 2073: Replace "gpu" by "graphical processing unit" in:
CPU (b) GPU
*** Sentence 2074: Replace "cpu" by "processor" in:
Figure 3.3: The difference between CPU and GPU
*** Sentence 2074: Replace "gpu" by "graphical processing unit" in:
Figure 3.3: The difference between CPU and GPU
*** Sentence 2075: Replace "is equipped with" by "has" in:
clock of popular NVIDIA GTX 1080 Ti2 is 1,481 Mhz. However, the card is equipped with 3,584 CUDA cores
*** Sentence 2076: Replace "gpu" by "graphical processing unit" in:
The architecture of a GPU allows performing parallel operations on large sets of data
*** Sentence 2077: Replace "gpus" by "graphical processing units" in:
Thus, despite their generally lower clock rates, GPUs may provide incomparably higher performance for specific tasks
*** Sentence 2078: Replace "gpu" by "graphical processing unit" in:
Since a GPU is programmable, its use is not limited to graphics only
*** Sentence 2080: Replace "employing" by "using" in:
Employing GPGPU helps accelerate the computation of complex problems in various areas from linear algebra [115], through machine learning [190], to cryptographic algorithms [135, 14, 17]
*** Sentence 2081: Replace "cpu" by "processor" in:
Figure 3.3 shows the difference in the architecture of a CPU and a GPU
*** Sentence 2081: Replace "gpu" by "graphical processing unit" in:
Figure 3.3 shows the difference in the architecture of a CPU and a GPU
*** Sentence 2082: Replace "cpu" by "processor" in:
A typical CPU core, shown in Figure 3.3(a), communicates with DRAM through one or more cache layers, contains a controller, and a set of arithmetic logic units
*** Sentence 2082: Replace "shown in figure" by "in figure" in:
A typical CPU core, shown in Figure 3.3(a), communicates with DRAM through one or more cache layers, contains a controller, and a set of arithmetic logic units
*** Sentence 2082: Delete "one or more" in:
A typical CPU core, shown in Figure 3.3(a), communicates with DRAM through one or more cache layers, contains a controller, and a set of arithmetic logic units
*** Sentence 2082: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:

A typical CPU core, shown in Figure 3.3(a), communicates with DRAM through one or more cache layers, contains a controller, and a set of arithmetic logic units
*** Sentence 2083: Replace "in the case of" by "for" in:
In the case of a multicore CPU, each core has its own controller and can work independently
*** Sentence 2084: Replace "share the same" by "share the" or "share a" or "share an" in:
A GPU, depicted in Figure 3.3(b), is a programmable parallel multiprocessor, where groups of cores share the same controller
*** Sentence 2086: Replace "terminology" by "terms" and make a following verb plural in:
The group is called a CUDA Core on NVIDIA GPUs, or SIMD unit in AMD/OpenCL terminology [141, 134]
*** Sentence 2087: Replace "gpu" by "graphical processing unit" in:
For password cracking, the number of cores richly compensates the slightly lower oper-ating frequency of a GPU
*** Sentence 2088: Replace "gpu" by "graphical processing unit" in:
Using the principles described in Section 3.1.1, we can benefit from the architecture of a GPU to verify masses of passwords in parallel
*** Sentence 2089: Replace "cpu" by "processor" in:
In my preliminary research between 2014 and 2016, I evaluated CPU and GPU password cracking performance using different software [83]
*** Sentence 2089: Replace "gpu" by "graphical processing unit" in:
In my preliminary research between 2014 and 2016, I evaluated CPU and GPU password cracking performance using different software [83]
*** Sentence 2090: Replace "cpu" by "processor" in:
The experimental machine contained Intel(R) Core i7 CPU 920 @ 2.67Ghz processor, 16 GB of DDR3 RAM, and two AMD Tri-X R9 290x GPU cards
*** Sentence 2090: Replace "gpu" by "graphical processing unit" in:
The experimental machine contained Intel(R) Core i7 CPU 920 @ 2.67Ghz processor, 16 GB of DDR3 RAM, and two AMD Tri-X R9 290x GPU cards
*** Sentence 2093: Replace "does not have" by "lacks" in:
As oclHashcat does not have a non-OpenCL implementation of the cracking algorithms, I did not test the CPU
*** Sentence 2093: Replace "not have a" by "lack a" in:
As oclHashcat does not have a non-OpenCL implementation of the cracking algorithms, I did not test the CPU
*** Sentence 2093: Replace "i did" by "we did" in:
As oclHashcat does not have a non-OpenCL implementation of the cracking algorithms, I did not test the CPU
*** Sentence 2093: Replace "cpu" by "processor" in:
As oclHashcat does not have a non-OpenCL implementation of the cracking algorithms, I did not test the CPU
*** Sentence 2099: Replace "gpu" by "graphical processing unit" in:
As we can see, in every case, the GPU provided higher performance than the CPU
*** Sentence 2099: Replace "cpu" by "processor" in:
As we can see, in every case, the GPU provided higher performance than the CPU
*** Sentence 2101: Replace "cpu" by "processor" in:
For Wrathion, a single-GPU cracking was 30.28 times faster than using the CPU method
*** Sentence 2102: Replace "cpu" by "processor" in:
With the dual-GPU deployment, the cracking was 60.56 times faster than with the CPU
*** Sentence 2103: Replace "gpu" by "graphical processing unit" in:
For John the Ripper, the GPU cracking was 39.38 times faster in comparison with the CPU
*** Sentence 2103: Replace "cpu" by "processor" in:
For John the Ripper, the GPU cracking was 39.38 times faster in comparison with the CPU
*** Sentence 2113: Replace "cpu" by "processor" in:

CPU
*** Sentence 2119: Replace "gpu" by "graphical processing unit" in:
1x GPU
*** Sentence 2125: Replace "gpu" by "graphical processing unit" in:
2x GPU
*** Sentence 2131: Replace "gpu" by "graphical processing unit" in:
GPU
*** Sentence 2137: Replace "gpu" by "graphical processing unit" in:
2x GPU
*** Sentence 2143: Replace "cpu" by "processor" in:
CPU
*** Sentence 2149: Replace "gpu" by "graphical processing unit" in:
1x GPU
*** Sentence 2155: Replace "cpu" by "processor" in:
CPU
*** Sentence 2161: Replace "gpu" by "graphical processing unit" in:
1x GPU
*** Sentence 2166: Replace "gpu" by "graphical processing unit" in:
Table 3.1: Cracking performance in passwords per second and GPU acceleration using different tools on ZIP, DOC, and PDF [83]
*** Sentence 2167: Delete "there was" and insert "occurred" or "was" or similar word later in:
In Section 3.1, there was an example of a WinZIP archive with a 7-character alphanu-meric password that required 14 years to be cracked using brute-force
*** Sentence 2168: Replace "gpus" by "graphical processing units" in:
Using two GPUs and Wrathion tool, the same password can be cracked within 185 days, assuming the values in Table 3.1
*** Sentence 2178: Replace "need to" by "must" if "need" is a verb in:
For a multi-GPU password cracking machine, we need to consider multiple factors, including:
*** Sentence 2181: Replace "e.g." by "for example," in:
The phenomenon of cryptocurrency mining lead manufacturers like ASUS to create many-slot motherboards, e.g. H370 MINING MASTER6 containing
*** Sentence 2183: Replace "gpus" by "graphical processing units" in:
Through riser cards, we can connect GPUs to PCI-e x1 slots in
*** Sentence 2187: Replace "enterprise" by "organization" in:
For HPC computing and professional GPGPU applications, manufacturers provide enterprise GPU servers
*** Sentence 2187: Replace "gpu" by "graphical processing unit" in:
For HPC computing and professional GPGPU applications, manufacturers provide enterprise GPU servers
*** Sentence 2188: Replace "gpu" by "graphical processing unit" in:
For example, Supermicro offers7 GPU Systems with up to 20 GPUs per machine
*** Sentence 2188: Replace "gpus" by "graphical processing units" in:
For example, Supermicro offers7 GPU Systems with up to 20 GPUs per machine
*** Sentence 2190: Delete "there is" and insert "occurs" or "is" or a similar word later in:
There is a maximum number of PCI-e lanes supported by the CPU
*** Sentence 2190: Replace "cpu" by "processor" in:
There is a maximum number of PCI-e lanes supported by the CPU
*** Sentence 2193: Replace "gpus" by "graphical processing units" in:
Size - High-end GPUs are relatively big in dimensions, mainly due to the coolers
*** Sentence 2195: Replace "enterprise" by "organization" in:
Enterprise GPU servers from SuperMicro or Dell have cases and backplanes designed precisely for the cards to fit
*** Sentence 2195: Replace "gpu" by "graphical processing unit" in:
Enterprise GPU servers from SuperMicro or Dell have cases and backplanes designed precisely for the cards to fit

*** Sentence 2198: Replace "gpus" by "graphical processing units" in:
Heat - With a higher workload, the GPUs produce a high amount of heat
*** Sentence 2198: Replace "a high amount of" by "much" in:
Heat - With a higher workload, the GPUs produce a high amount of heat
*** Sentence 2200: Replace "enterprise" by "organization" in:
Enterprise server solutions have unified systems that allow using even GPUs with passive coolers
*** Sentence 2200: Replace "gpus" by "graphical processing units" in:
Enterprise server solutions have unified systems that allow using even GPUs with passive coolers
*** Sentence 2201: Replace "be used as" by "be" in:
Water cooling can also be used as a quiet alternative
*** Sentence 2203: Replace "employ" by "use" in:
Servers from SuperMicro, HP, ASUS, or Dell employ modular architectures with up to 3,000 W per unit
*** Sentence 2207: Replace "is not enough" by "is insufficient" in:
Desktop motherboards support only a single PSU, which is not enough for machines with six or more high-end GPUs
*** Sentence 2207: Replace "gpus" by "graphical processing units" in:
Desktop motherboards support only a single PSU, which is not enough for machines with six or more high-end GPUs
*** Sentence 2209: Replace "advantageous" by "desirable" or "helpful" in:
Price - It is always to consider if investing in a multi-GPU single-machine solution is more advantageous than using multiple nodes
*** Sentence 2210: Replace "utilize" by "use" in:
Moreover, a distributed solution may utilize existing computers
*** Sentence 2211: Replace "it is necessary to" by "one must" in:
For the sake of completeness, it is necessary to mention that some manufacturers specialize in designing hardware solutions dedicated to GPGPU password cracking
*** Sentence 2215: Replace "gpu" by "graphical processing unit" in:
In constrast to Terahash, Decryptum machines are based on desktop motherboards, currently the H370 MINING MASTER, and thus the GPU connection is limited to PCI-e x1
*** Sentence 2216: Delete "it is clear that" in:
Based on the observations mentioned above, it is clear that there is always a limit to the performance that a single machine can provide
*** Sentence 2216: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Based on the observations mentioned above, it is clear that there is always a limit to the performance that a single machine can provide
*** Sentence 2221: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Sadly, there are only a few #"bigger#" currently-developed projects
*** Sentence 2224: Replace "enterprise" by "organization" in:
The enterprise applications, on the other hand, are #"black box#" solutions
*** Sentence 2226: Replace "employed" by "used" in:
The detailed specification, their architecture, and employed algorithms are proprietary company know-how that is purposedly hidden from the public
*** Sentence 2230: Replace "employing" by "using" in:
With the -network parameter, the tool allowed employing a network of heterogeneous worksta-tions in a single cracking task
*** Sentence 2231: Replace "via" by "by" in:
A distributed cracking session had a single master machine and multiple hosts, communicating via Remote Shell (RSH), Remote Copy (RCP), and optionally Network File System (NFS) [140]
*** Sentence 2232: Replace "utilize" by "use" in:
In the network.conf configuration file, the administrator configured what host machines to utilize
*** Sentence 2234: Replace "accordingly" by "so" in:
The workload was divided accordingly to the performance of nodes
*** Sentence 2239: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:

The master process called, cpw (crack passwords), spawned a set of worker processes cow (check one word)
*** Sentence 2244: Replace "much of the" by "much" in:
Much of the related work is based on the famous John the Ripper (JtR) tool, described in Section 2.4.1
*** Sentence 2247: Replace "performed by" by "done by" in:
The first published academic work on the case was performed by Lim, who modified the sources by adding MPI support for the Incremental brute-force attack (see Section 3.8.3) mode [112]
*** Sentence 2249: Replace "pre-defined" by "predefined" in:
The master processor divided the keyspace (the number of possible candidate passwords [180]) into a pre-defined number of chunks, while each slave processor received an equal chunk to solve
*** Sentence 2259: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
There is no need to recompute the hash of a single password twice, especially with complex algorithms like bcrypt [167] or SHA-3 [139]
*** Sentence 2260: Delete "use of" in:
Bengtsson showed the practical use of MPI-based brute-force and dictionary attacks using the Beowulf high-performance computing (HPC) cluster for cracking MD5-based Unix shadow files
*** Sentence 2261: Replace "similar to" by "like" in:
Similar to Steiggner and Wilke#'s approach [189], both attacks were based on simple password-by-password keyspace division and demonstrated using a proof-of-concept application called brutest
*** Sentence 2262: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
The cracking network consisted of a root node responsible for creating and distributing work, and a set of slave nodes used for the actual cracking
*** Sentence 2269: Replace "gpus" by "graphical processing units" in:
The Divided dictionary algorithm evenly split dictionary words between MPI nodes equipped with GPUs
*** Sentence 2270: Replace "gpus" by "graphical processing units" in:
Using CUDA, GPUs on each node locally calculated the hashes and compared them with the ones that should be cracked [17]
*** Sentence 2274: Replace "three different" by "three" in:
For interconnection, Marks used three different lines: 10 Gb/s Ethernet for data transfer, 1 Gb/s Ethernet, and InfiniBand for controlling the computation process
*** Sentence 2275: Replace "utilizing" by "using" in:
Marks also proposed a software framework called Hybrid GPU/CPU Cluster (HGPC) utilizing a master-slave communication model using an XML-based protocol over a TCP/IP net-work
*** Sentence 2276: Replace "was able to" by "could" in:
A proof-of-concept implementation was able to crack MD5, SHA-1, and four versions of SHA-2 hashes
*** Sentence 2279: Replace "gpu" by "graphical processing unit" in:
While cracking MD5 hashes on NVIDIA Tesla M2050, Marks achieved the speed of around 800 Mh/s, while hashcat users report11 cracking over 1200 Mh/s using the same GPU
*** Sentence 2282: Replace "employing" by "using" in:
Since my use-case also covers grid computing with existing computers and employing heterogeneous networks of a possibly changing set of nodes, I would like to present existing related non-HPC solutions
*** Sentence 2282: Replace "to present" by "to show" in:
Since my use-case also covers grid computing with existing computers and employing heterogeneous networks of a possibly changing set of nodes, I would like to present existing related non-HPC solutions
*** Sentence 2284: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
The architecture consisted of a master server and a set of compute nodes, which were either CPU-based or used GPU acceleration based on CUDA
*** Sentence 2284: Replace "gpu" by "graphical processing unit" in:
The architecture consisted of a master server and a set of compute nodes, which were either CPU-based or used GPU acceleration based on CUDA
*** Sentence 2287: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Since Crumpacker uses BOINC, there are similarities to my solution, the Fitcrack
*** Sentence 2289: Replace "amount of time" by "time" in:

Similarly to my proposal, he decided to standardize the size of the workunit (a BOINC term for a chunk) by counting out the number of passwords that one computer could check in the desired amount of time
*** Sentence 2291: Delete "one or more" in:
While Fitcrack uses the idea of independent jobs, each having one or more input hashes, Crumpacker#'s server backend employs the JtR database as unified hash storage
*** Sentence 2291: Replace "employs" by "uses" in:
While Fitcrack uses the idea of independent jobs, each having one or more input hashes, Crumpacker#'s server backend employs the JtR database as unified hash storage
*** Sentence 2295: Replace "eight different" by "eight" in:
Fitcrack serves as the general-purpose cracking system and allows for cracking over 300 hashcat-supported hash formats using eight different attack modes
*** Sentence 2299: Replace "there are no" by "no" and insert "occur" or "are" or similar word later in:
There are no additional features like integrated hash scrapers, user account management, or even a graphical user interface
*** Sentence 2307: Replace "e.g.," by "for example," in:
For in-stance, it supports some formats which hashcat does not, e.g., encrypted RAR3 archives with an unprotected header
*** Sentence 2309: Replace "performed on" by "on" or "done on" in:
They require a large piece of work performed on the CPU of the host machine
*** Sentence 2309: Replace "cpu" by "processor" in:
They require a large piece of work performed on the CPU of the host machine
*** Sentence 2311: Replace "encountered" by "met" or "saw" or "seen" in:
As described in Section 3.5, I studied the possibilities of JtR integration to Fitcrack and encountered similar problems with distributing incremental mode as Crumpacker reported [47]
*** Sentence 2314: Replace "existing frameworks" by "current frameworks" in:
The resulting technical report compares existing frameworks and describes differ-ent architectures and technologies for workload distribution [103]
*** Sentence 2315: Replace "gpu" by "graphical processing unit" in:
Kasabov considers MPI combined with OpenCL as the best practical approach for setting up a password cracking GPU cluster, underlying the possibility to use a combination of MPI and OpenMP12 to gain fine-grained parallelism [215]
*** Sentence 2315: Replace "use a combination of" by "combine" in:
Kasabov considers MPI combined with OpenCL as the best practical approach for setting up a password cracking GPU cluster, underlying the possibility to use a combination of MPI and OpenMP12 to gain fine-grained parallelism [215]
*** Sentence 2316: Replace "to support" by "for" in:
However, the research is merely theoretical and provides no proof-of-concept tool or experimental results to support the conclusions
*** Sentence 2320: Replace "take advantage of" by "exploit" in:
Still, the report includes a brief study of BOINC, emphasizing its advan-tages in automation, including integrity checks, workunit replication, checkpointing, and other features that my Fitcrack system [87, 84, 81] and Crumpacker#'s JtR-based solution take advantage of [47]
*** Sentence 2323: Replace "at the time of" by "at" or "during" in:
Moreover, the statement #"BOINC API lacks functions for managing projects#" [103] is, at the time of writing this thesis, not entirely true
*** Sentence 2325: Replace "e.g.," by "for example," in:
The rest can be added by writing a custom interface, e.g., the Fitcrack WebAdmin described in Section 3.7.6
*** Sentence 2329: Delete "the use of" if followed by a gerund or noun describing an action in:
As Veerman states [154], the use of MPI requires the cracking tool to either support MPI or be modifiable for adding the MPI support
*** Sentence 2330: Replace "to support" by "for" in:
Since Veerman wants the solution to support both closed-source cracking software, such modification may not always be possible

*** Sentence 2332: Replace "similar to" by "like" in:
Generally, the design is similar to the Fitcrack system#'s architecture, described in Section 3.7
*** Sentence 2343: Replace "above-shown" by "previously shown" in:
While the above-shown work is mostly from academic research and hacker enthusiasts, I would like to cover existing enterprise distributed cracking solutions from the commercial sphere as well
*** Sentence 2343: Replace "enterprise" by "organization" in:
While the above-shown work is mostly from academic research and hacker enthusiasts, I would like to cover existing enterprise distributed cracking solutions from the commercial sphere as well
*** Sentence 2347: Replace "different types of" by "different" in:
The 2020#'s version 8.2.1 supports over 70 different types of password-protected media
*** Sentence 2350: Replace "gpu" by "graphical processing unit" in:
The GPU acceleration, however, is only for Microsoft Office and WinZIP formats
*** Sentence 2364: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
And there is no native support for complex algorithms like bcrypt [167], scrypt [157], or SHA-3 [139]
*** Sentence 2366: Replace "enterprise" by "organization" in:
The new feature, available for the Enterprise and Forensic editions of the Passware Kit, allowed to increase the cracking performance by utilizing multiple ma-chines
*** Sentence 2366: Replace "utilizing" by "using" in:
The new feature, available for the Enterprise and Forensic editions of the Passware Kit, allowed to increase the cracking performance by utilizing multiple ma-chines
*** Sentence 2372: Replace "gpu" by "graphical processing unit" in:
The measured values are comparable to hashcat on the same GPU [145]
*** Sentence 2373: Replace "gpu" by "graphical processing unit" in:
From all supported formats, only 80 provide GPU acceleration
*** Sentence 2374: Replace "gpu" by "graphical processing unit" in:
For instance, PDF does not support GPU at all
*** Sentence 2377: Replace "it is necessary to" by "one must" in:
Since I decided to use hashcat as a cracking engine because of its performance and variety of supported algorithms (see Section 3.5), it is necessary to mention existing work, despite being out of the academic sphere
*** Sentence 2378: Replace "enterprise" by "organization" in:
Hashstack14 is an enterprise solution from Sagitta HPC, a subsidiary of Terahash LLC
*** Sentence 2380: Replace "extreme" by "high" in:
The authors refer to the solution as the #"hashcat on catnip#" and claim it provides extreme scalability
*** Sentence 2381: Replace "api" by "applications programming interface" or "interface" in:
It should support 375+ highly-optimized hash formats, six attack modes, multi-user support with granular access control lists, and API to automate workflows
*** Sentence 2382: Replace "gpu" by "graphical processing unit" in:
Nevertheless, the solution is closed-source except for a few plugins available15 on GitHub and distributed exclusively with Sagitta#'s GPU cracking appliances
*** Sentence 2383: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
McAtee et al. presented the Cracklord16, a system for hardware resource management, which supports creating job queues and contains a simple hashcat plugin
*** Sentence 2384: Replace "allows to" by "allows one to" or "allows them", etc. in:
The plugin allows to remotely run a dictionary or a brute-force attack with a limited set of options
*** Sentence 2391: Replace "gpu" by "graphical processing unit" in:
In 2015, Jakub Samek, a student from Czech Technical University in Prague, used Hashtopolis system with cudaHashcat to create a virtual GPU cluster for his bachelor#'s thesis [178]
*** Sentence 2393: Replace "most of the" by "most" if followed by a plural noun in:
Since most of the code was still usable, Sein Coray created a fork called Hashtopussy, later rebranded to Hashtopolis in 2018
*** Sentence 2394: Delete "one or more" in:
Hashtopolis18 uses a network with a server, and one or more agents #--machines used as cracking nodes

*** Sentence 2397: Replace "allows to" by "allows one to" or "allows them", etc. in:
The user interface allows to create and manage cracking tasks, hashlist, and others
*** Sentence 2401: Replace "many of the" by "many" if followed by a plural noun in:
Many of the features of Fitcrack and Hashtopolis are similar
*** Sentence 2404: Replace "employ" by "use" in:
Hashtopolis runs solely on an HTTP server and does not employ any other actively running server daemons
*** Sentence 2405: Replace "via" by "by" in:
While Fitcrack#'s WebAdmin has a separate frontend and backend connected via a REST API, Hashtopolis is a monolithic application
*** Sentence 2406: Replace "via" by "by" in:
Without modification, the only control of Hashtopolis is via the graphical user interface
*** Sentence 2407: Replace "api" by "applications programming interface" or "interface" in:
In contrast, Fitcrack#'s backend API allows controlling the system even from an external application
*** Sentence 2409: Replace "needs to" by "must" or "should" if "needs" is a verb in:
Hashtopolis treats all attacks the same, and the configuration is up to the user who needs to specify hashcat#'s command-line arguments manually
*** Sentence 2411: Delete "one or more" in:
For each task, the user selects a hashlist, one or more files (e.g., password dictionaries) to be transferred to the client, and an attack command in the form of hashcat program options
*** Sentence 2412: Replace "in contrast to" by "compared to" in:
In contrast to Fitcrack, the user needs to define most attack-based hashcat options by hand
*** Sentence 2412: Replace "needs to" by "must" or "should" if "needs" is a verb in:
In contrast to Fitcrack, the user needs to define most attack-based hashcat options by hand
*** Sentence 2414: Replace "a state-of-the-art" by "the latest" in:
Being the only well-known maintained open-source solution for distributed computing with the current version of hashcat, I consider Hashtopolis a state-of-the-art tool in my research area
*** Sentence 2419: Replace "crucial" by "key" in:
Performance - The overall performance of the system is the most crucial factor
*** Sentence 2420: Replace "utilize" by "use" in:
The tool should utilize GPGPU technologies like OpenCL [134] or CUDA [141] to accel-erate cryptographic algorithms and acquire as high cracking performance as possible
*** Sentence 2421: Replace "utilized" by "used" in:
Efficiency - In an ideal state, all available processors are utilized all the time during the entire task
*** Sentence 2421: Replace "entire task" by "task" in:
Efficiency - In an ideal state, all available processors are utilized all the time during the entire task
*** Sentence 2423: Delete "there is" and insert "occurs" or "is" or a similar word later in:
In distributed computing, there is always an overhead that computing nodes require for communication, i.e., the interchange of commands and data, synchronization, etc. Operations like benchmarking or performing database transactions add another overhead as well
*** Sentence 2423: Replace "etc." by "and so on" in:
In distributed computing, there is always an overhead that computing nodes require for communication, i.e., the interchange of commands and data, synchronization, etc. Operations like benchmarking or performing database transactions add another overhead as well
*** Sentence 2425: Replace "utilized" by "used" in:
In other words, describes how well the processors are utilized
*** Sentence 2433: Replace "for the purpose of" by "for" in:
Adaptability - For the purpose of my research, I assume a potentially changing computing environment
*** Sentence 2442: Replace "do not have to" by "need not" in:
They do not have to be a part of a dedicated HPC cluster
*** Sentence 2443: Replace "gpus" by "graphical processing units" in:
The system should run on personal computers with consumer-grade GPUs and commonly used operating systems like Microsoft Windows or Linux
*** Sentence 2444: Replace "research purposes" by "research" in:

Open-source code - For research purposes and further development, all parts of the system should be publicly available under open-source licenses
*** Sentence 2444: Replace "publicly available" by "public" in:
Open-source code - For research purposes and further development, all parts of the system should be publicly available under open-source licenses
*** Sentence 2445: Replace "to contribute to" by "for" in:
Meeting this condition allows smooth reproduction of experimental results and enables any enthusiast to contribute to the system by creating additional modules and improvements
*** Sentence 2450: Replace "vs." by "versus" in:
We can categorize them by the network topology (centralized/de-centralized, star, ring, hierarchical, etc.), by the type of communication (synchronous vs. asynchronous), and other aspects [108]
*** Sentence 2452: Replace "local area networks" by "local-area networks" in:
Cracking tasks may run not only in local area networks (LAN) but also in larger computer grids with nodes in different locations
*** Sentence 2453: Replace "utilize" by "use" in:
The system may utilize both dedicated GPU servers and personal computers
*** Sentence 2453: Replace "gpu" by "graphical processing unit" in:
The system may utilize both dedicated GPU servers and personal computers
*** Sentence 2457: Replace "selection" by "choice" in:
The selection of frameworks is inspired by the previous work of Kasabov et al., who compared BOINC with MPI and CLara [103]
*** Sentence 2458: Replace "in addition to" by "besides" in:
In addition to these three frameworks, I also discuss VirtualCL and Apache Hadoop
*** Sentence 2459: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Naturally, there are other existing solutions that are not included in the comparison for various reasons
*** Sentence 2465: Replace "that allow for" by "for" in:
Hadoop supports porting to many languages, including C and C++, that allow for creating compiled and highly-optimized applications
*** Sentence 2467: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Nevertheless, it is not designed for tasks whose processing lasts long as there is a limit in seconds for each function call
*** Sentence 2480: Replace "is performed" by "is done" in:
Message passing is performed by calling functions named MPI routines
*** Sentence 2480: Replace "performed by" by "done by" in:
Message passing is performed by calling functions named MPI routines
*** Sentence 2488: Replace "employed" by "used" in:
For instance, Apostal et al. employed the MPI in the CUDA-based password cracker [17]
*** Sentence 2490: Replace "larger amounts of" by "more" in:
However, it seems the MPI may not be an obstacle even for larger amounts of data
*** Sentence 2493: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
There are multiple existing implementations of MPI, both open-source like OpenMPI24
*** Sentence 2494: Replace "e.g.," by "for example," in:
or MPICH25, and commercial, e.g., Intel MPI26
*** Sentence 2495: Replace "etc." by "and so on" in:
OpenMPI includes various fault-tolerance techniques: local or distributed checkpoints, network failure detection, etc. In Section 3.3, I defined the proposed cracking system should support adding new computing nodes during runtime
*** Sentence 2499: Replace "not detected" by "undetected" in:
Unfortunately, new nodes are not detected automatically, so the programmer needs to create an extra process that detects new connections
*** Sentence 2499: Replace "needs to" by "must" or "should" if "needs" is a verb in:
Unfortunately, new nodes are not detected automatically, so the programmer needs to create an extra process that detects new connections

*** Sentence 2501: Replace "paradigms" by "concepts" in:
Programming of interconnected cluster applications with MPI often requires advanced communication paradigms that increase the programming effort for code writing
*** Sentence 2501: Replace "programming effort" by "programming" in:
Programming of interconnected cluster applications with MPI often requires advanced communication paradigms that increase the programming effort for code writing
*** Sentence 2503: Replace "would have to" by "must" in:
All such security mechanisms would have to be implemented manually by the application programmer
*** Sentence 2507: Replace "paradigm" by "concept" in:
The paradigm works as follows
*** Sentence 2512: Replace "final result" by "result" in:
#"<-#2, and produces the final result
*** Sentence 2530: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
The main discussed advantages contain the distributed file system with integrated data replication management, adding new nodes on-the-fly, and a set of useful tools for data analysis and management [170]
*** Sentence 2532: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
It is easy-to-use, well-designed for working with Big Data, and offers a set of useful integrated tools for data analysis and system management
*** Sentence 2534: Replace "in contrast to" by "compared to" in:
In contrast to MPI, Hadoop allows adding new nodes at runtime
*** Sentence 2535: Delete "there were" and insert "occurred" or "were possible" or similar word later in:
Although there were approaches30 on distributed computing of hashing algorithms using Hadoop and MapReduce, I do not the password cracking process an appropriate candidate for the MapReduce model
*** Sentence 2539: Replace "located on" by "on" in:
It allows applications to use OpenCL devices located on different computing nodes in the same way as they were connected locally to the computer
*** Sentence 2539: Replace "in the same way as" by "the same as" in:
It allows applications to use OpenCL devices located on different computing nodes in the same way as they were connected locally to the computer
*** Sentence 2540: Replace "any additional" by "additional" in:
Such use does not require any additional modifications to the native OpenCL application [21]
*** Sentence 2540: Replace "modifications" by "changes" in:
Such use does not require any additional modifications to the native OpenCL application [21]
*** Sentence 2541: Replace "limiting factor" by "obstacle" or "constraint" in:
VCL uses a custom protocol over TCP/IP, and the network latency is the main limiting factor
*** Sentence 2542: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
A set of SHOC benchmarking tests showed that the overhead of VCL is nonnegligible, especially with bigger chunks of input data [51]
*** Sentence 2543: Replace "seem to be" by "appear" or "appear as" in:
The latest version 1.25 of VCL was released in 2017, and the project does not seem to be develop anymore
*** Sentence 2549: Replace "seem to be" by "appear" or "appear as" in:
However, the NVIDIA drivers did not seem to be supported anymore since the cards were not visible from the host machine
*** Sentence 2549: Replace "not visible" by "invisible" in:
However, the NVIDIA drivers did not seem to be supported anymore since the cards were not visible from the host machine
*** Sentence 2550: Replace "gpu" by "graphical processing unit" in:
After switching to AMD R9 290X, the remote GPU became accessible from the host machine, but it was impossible to use the device with hashcat version 2 or higher
*** Sentence 2552: Replace "in addition to" by "besides" in:
In addition to the compatibility issues, password cracking with VirtualCL adds an un-desirable amount of overhead compared to running a standalone password cracker remotely
*** Sentence 2554: Replace "utilizing" by "using" in:

Utilizing a tool like hashcat or JtR only requires the controlling node to specify the attack settings, e.g., in the form of command-line ar-guments
*** Sentence 2554: Replace "e.g.," by "for example," in:
Utilizing a tool like hashcat or JtR only requires the controlling node to specify the attack settings, e.g., in the form of command-line ar-guments
*** Sentence 2557: Replace "etc." by "and so on" in:
As I detected, practically all existing GPU-supported password crackers require a periodi-cal low-latency host-to-GPU communication to synchronize the work, monitor the device, verify the success of password verification, etc. Even the Wrathion that I proposed in my preliminary research [81] works in iterations, each verifying a vector of candidate passwords
*** Sentence 2559: Replace "gpu" by "graphical processing unit" in:
Hashcat uses a similar concept with two nested cycles, where the base loop (see Section 3.6.4) runs on the host#'s CPU, while the modifier loop is implemented within the OpenCL GPU kernels
*** Sentence 2562: Replace "similar to" by "like" in:
Similar to VirtualCL, CLara is a framework that allows accessing graphic processors over IP networks
*** Sentence 2563: Replace "paradigm" by "concept" in:
Compared to VCL, the concept of CLara is more general as it uses the #"many-to-many#" communication paradigm where any computer in the network may access an OpenCL device to any other computer
*** Sentence 2566: Replace "e.g.," by "for example," in:
A provider is a computer that offers its OpenCL devices, e.g., one or more GPUs
*** Sentence 2566: Delete "one or more" in:
A provider is a computer that offers its OpenCL devices, e.g., one or more GPUs
*** Sentence 2566: Replace "gpus" by "graphical processing units" in:
A provider is a computer that offers its OpenCL devices, e.g., one or more GPUs
*** Sentence 2570: Replace "could potentially" by "could" in:
I assume a password cracking system built over CLara could potentially run multiple cracking sessions initiated at different points of the network
*** Sentence 2570: Replace "initiated" by "started" in:
I assume a password cracking system built over CLara could potentially run multiple cracking sessions initiated at different points of the network
*** Sentence 2584: Delete "one or more" in:
The architecture resembles a client-server model where the network consists of a server and one or more hosts
*** Sentence 2585: Replace "is responsible for" by "handles" or "causes" in:
The server is responsible for the management, planning, and scheduling of tasks
*** Sentence 2588: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
A problem or a set of problems is described as a project
*** Sentence 2592: Replace "is responsible for creating" by "creates" in:
The project server is responsible for creating and scheduling tasks, keeping track of clients, maintaining data storage, etc.
*** Sentence 2592: Replace "keeping track of" by "tracking" in:
The project server is responsible for creating and scheduling tasks, keeping track of clients, maintaining data storage, etc.
*** Sentence 2592: Replace "etc." by "and so on" in:
The project server is responsible for creating and scheduling tasks, keeping track of clients, maintaining data storage, etc.
*** Sentence 2594: Replace "illustrates" by "shows" in:
Figure 3.4 illustrates the communication between the project server and a client that is required for solving a single workunit
*** Sentence 2598: Delete "one or more" in:
For solving the task, a client may need one or more applications
*** Sentence 2605: Replace "api" by "applications programming interface" or "interface" in:

The framework provides two options for running client-side programs: i) using BOINC Wrapper, ii) using BOINC API
*** Sentence 2608: Replace "via" by "by" in:
The communication is possible via redirecting the program#'s input
*** Sentence 2612: Replace "app" by "program" in:
The communication between the BOINC core client and the app uses shared memory and message passing
*** Sentence 2613: Replace "api" by "applications programming interface" or "interface" in:
Compared with the wrapper, the API provides many advanced features like progress reporting, checkpointing, critical section handling, atomic operations, pausing, or using time handlers [16]
*** Sentence 2614: Delete "is designed to" and change following verb to present tense singular in:
Unlike MPI or VCL, BOINC is designed to distribute tasks over the Internet
*** Sentence 2615: Delete "use of" in:
It provides the optional use of built-in security mechanisms for untrusted environments: authentica-tion, user account management, digital signatures, and public-key encryption
*** Sentence 2617: Replace "cpu" by "processor" in:
Users can even specify the percentage of CPU or GPU power assigned to a BOINC task, network upload or download limits, disk, and memory size utilization assigned to the computing
*** Sentence 2617: Replace "gpu" by "graphical processing unit" in:
Users can even specify the percentage of CPU or GPU power assigned to a BOINC task, network upload or download limits, disk, and memory size utilization assigned to the computing
*** Sentence 2617: Replace "utilization" by "use" in:
Users can even specify the percentage of CPU or GPU power assigned to a BOINC task, network upload or download limits, disk, and memory size utilization assigned to the computing
*** Sentence 2618: Replace "etc." by "and so on" in:
It is also possible to define at which time the computing should start, restrict the computing to concrete days in week, etc.
*** Sentence 2619: Replace "be used for" by "be for" in:
Crumpacker et al. showed BOINC can be used for password cracking and created a sim-ple proof-of-concept tool for distributing attack with John the Ripper tool [47]
*** Sentence 2625: Replace "crucial" by "key" in:
Table 3.2 compares the above-described solutions based on criteria that I consider crucial for distributed password cracking to meet the requirements from Section 3.3
*** Sentence 2629: Replace "not the case" by "false" in:
The primary advantages are working with big data and the MapReduce model, which is not the case
*** Sentence 2631: Replace "not compatible" by "incompatible" in:
However, the projects are abandoned and mostly are not compatible with today#'s hardware and software
*** Sentence 2650: Replace "app" by "program" in:
cracking without additional app
*** Sentence 2681: Replace "gpu" by "graphical processing unit" in:
Designing custom GPU kernels from scratch, as I did for the Wrathion tool, is unnecessary since there already are existing tools with well-optimized implementations of the password verification routines
*** Sentence 2681: Replace "i did" by "we did" in:
Designing custom GPU kernels from scratch, as I did for the Wrathion tool, is unnecessary since there already are existing tools with well-optimized implementations of the password verification routines
*** Sentence 2686: Replace "gpu" by "graphical processing unit" in:
Performance - The solution must provide GPU acceleration
*** Sentence 2689: Replace "etc." by "and so on" in:
Attack modes - The solution should support not only the dictionary and brute-force attack but should also cover advanced attack with password-mangling rules, word combinations, etc.
*** Sentence 2695: Replace "gpu" by "graphical processing unit" in:
Those include OS and integration support, GPU acceleration, supported formats and algorithms, attack modes, development, and licensing
*** Sentence 2739: Replace "gui" by "graphical user interface" in:

* #--only for agent (worker), ** #--without GUI
*** Sentence 2741: Replace "gpu" by "graphical processing unit" in:
GPU acceleration
*** Sentence 2889: Replace "api" by "applications programming interface" or "interface" in:
Cain & Abel and commercial tools like Elcomsoft or AccessData software are monolithic applications with proprietary API and communication protocols
*** Sentence 2890: Replace "via" by "by" in:
Their source code is not publicly available, and the only way of controlling their operations is via the provided graphical user interface
*** Sentence 2898: Replace "gpu" by "graphical processing unit" in:
Moreover, it is the only tool from the list that offers full GPU support
*** Sentence 2899: Replace "cpus" by "processors" in:
Recent versions of hashcat have all cryptographic algorithms implemented within OpenCL kernels, allowing GPU-accelerated cracking but does not restrict using OpenCL-compatible CPUs
*** Sentence 2900: Replace "gpu" by "graphical processing unit" in:
The rule engine for mangling dictionary words is, unlike in any other tool, implemented for GPU as well
*** Sentence 2902: Replace "did not have" by "lacked" in:
On the other hand, John still offers some features that hashcat did not have in the current 6.1.1 release: the Single crack attack mode or support for RAR 3 archives without an encrypted header
*** Sentence 2906: Replace "includes support for" by "supports" in:
The development version already includes support for RAR3-p hash mode for cracking both compressed and uncompressed RAR version 3 archives without the encrypted header [95]
*** Sentence 2911: Replace "it is necessary to" by "one must" in:
It is necessary to either use the internal MPI support, define the keyspace splitting manually in the configuration file, or use an external password generator [12]
*** Sentence 2914: Replace "allows to" by "allows one to" or "allows them", etc. in:
This integrated feature allows to easily create chunks of work and distribute them between the computing nodes
*** Sentence 2919: Replace "frequently" by "often" in:
The tool is maintained and improved over time, well-documented, and is surrounded by a large community of supporters that frequently discuss its features on web forums35
*** Sentence 2926: Replace "amongst" by "among" in:
This section discusses the principles of dividing workload amongst multiple cracking nodes
*** Sentence 2927: Replace "terminology" by "terms" and make a following verb plural in:
First, I describe the general principles and unify the terminology
*** Sentence 2929: Replace "utilized" by "used" in:
Finally, I contribute with a proposal of job processing with BOINC and hashcat utilized in the Fitcrack system
*** Sentence 2942: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
Keyspace ### = |#" | where #" is the set of all password candidates
*** Sentence 2983: Replace "terminology" by "terms" and make a following verb plural in:
In the terminology of Fitcrack, a job represents a single cracking task added by the ad-ministrator
*** Sentence 2984: Delete "one or more" in:
Each job is defined by an attack mode (see Section 3.8), attack settings (e.g., which dictionary should be used), and one or more password hashes of the same type (e.g., SHA-1)
*** Sentence 2991: Replace "are capable of" by "can" change following word to a verb in:
Since tools like hashcat or John the Ripper are capable of cracking multiple hashes for each can-didate password while the candidate hash is only generated once, I do not consider hash distribution to be an efficient method for dividing the workload
*** Sentence 2992: Replace "deals with" by "concerns" or "handles" or "encounters" in:
I suppose it only makes sense if cryptographic salt is used or if one deals with exceptionally large hashlists

*** Sentence 2993: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
Otherwise, there is no need to calculate the hash more than once from each candidate password
*** Sentence 2994: Replace "shown in figure" by "in figure" in:
An example of hash distribution is shown in Figure 3.5(a)
*** Sentence 2997: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
al [112] divides the set of all candidate passwords into a number of chunks and assignes a chunk to each client
*** Sentence 2997: Replace "a number of" by "several" in:
al [112] divides the set of all candidate passwords into a number of chunks and assignes a chunk to each client
*** Sentence 3000: Replace "has to be" by "must be" in:
If a chunk is lost, it has to be recomputed from the beginning, if no method of checkpointing is implemented
*** Sentence 3003: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
The set of password candidates is, however, split into three chunks with sizes set accordingly to the performance of each computer
*** Sentence 3003: Replace "accordingly" by "so" in:
The set of password candidates is, however, split into three chunks with sizes set accordingly to the performance of each computer
*** Sentence 3011: Replace "is illustrated" by "is shown" in:
An example is illustrated in Figure 3.5(c)
*** Sentence 3011: Replace "illustrated in" by "shown in" in:
An example is illustrated in Figure 3.5(c)
*** Sentence 3018: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
the set of all candidate passwords
*** Sentence 3025: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
the set of all candidate passwords
*** Sentence 3038: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
the set of all candidate passwords
*** Sentence 3057: Replace "terminology" by "terms" and make a following verb plural in:
Fitcrack adopts the same terminology
*** Sentence 3064: Replace "denoted" by "meant" or "indicated" or "represented" in:
The index ranges are also denoted in Figure 3.5
*** Sentence 3070: Replace "informs" by "tells" or "affects" in:
One of candidate passwords is correct (or more, if we crack multiple hashes) - the client informs the server that it has found the correct password
*** Sentence 3079: Replace "it is necessary to" by "one must" in:
Since Fitcrack uses the hashcat tool as the internal cracking engine, it is necessary to consider its design and properties
*** Sentence 3086: Replace "i.e." by "in other words" in:
While --skip corresponds to ############, --limit defines the keyspace to be processed within a workunit, i.e. should be equal to #######" #### ############
*** Sentence 3087: Delete "the use of" if followed by a gerund or noun describing an action in:
Whereas for a dictionary attack without the use of password-mangling rules (see Section 3.8.1), hashcat#'s keyspace equals the actual number of candidate passwords, for other attack modes, it may not match
*** Sentence 3092: Replace "gpu" by "graphical processing unit" in:
modifier loop is implemented within OpenCL GPU kernels
*** Sentence 3093: Replace "be different from" by "differ from" in:

Hashcat#'s keyspace is equal to the number of iterations of the base loop and could be different from the actual number of password guesses
*** Sentence 3099: Replace "is used for" by "is for" in:
And in our database (see Section 3.7.8), we store both hashcat#'s keyspace which is used for distributing work, and the actual keyspace, to inform the user about the actual number of passwords processed
*** Sentence 3099: Replace "inform" by "tell" or "affect" in:
And in our database (see Section 3.7.8), we store both hashcat#'s keyspace which is used for distributing work, and the actual keyspace, to inform the user about the actual number of passwords processed
*** Sentence 3118: Replace "taken into account" by "considered" or "accounted for" in:
For better or worse, these deviations from a traditional password index concept should be taken into account
*** Sentence 3122: Replace "utilize" by "use" in:
This section shows how to utilize this principle in BOINC and calculate the proper size of workunits
*** Sentence 3123: Replace "one of the" by "one" if followed by a plural noun, and make it singular in:
One of the main reasons for choosing BOINC is the integrated technique called targeting that defines which workunit is assigned to which host
*** Sentence 3128: Replace "will be described" by "is described" or "are described" in:
This approach is used in Fitcrack, and will be described in the following paragraphs
*** Sentence 3131: Replace "in addition," by "also," in:
In addition, the performance of a node can change over time
*** Sentence 3134: Replace "utilize" by "use" in:
Utilize as many available hosts as possible #--ideally, all of them
*** Sentence 3135: Replace "utilized" by "used" in:
Make all hosts utilized most of the time #--ideally, all the time
*** Sentence 3135: Replace "most of the" by "most" if followed by a plural noun in:
Make all hosts utilized most of the time #--ideally, all the time
*** Sentence 3139: Replace "time it would take to" by "time to" in:
The algorithm#'s idea is to estimate how much time it would take to verify the remaining candidate passwords on all the active clients
*** Sentence 3156: Replace "above-shown" by "previously shown" in:
The above-shown description purposedly omits an important step #--choosing the workunit processing time ######
*** Sentence 3162: Replace "suitable for" by "for" in:
Such a setting is more suitable for an unsta-ble environment where clients are more likely to fail, frequently disconnect or change their performance
*** Sentence 3162: Replace "frequently" by "often" in:
Such a setting is more suitable for an unsta-ble environment where clients are more likely to fail, frequently disconnect or change their performance
*** Sentence 3163: Replace "impact of" by "effect of" in:
And thus, the impact of a lost workunit is lower, and the task can be assigned to another client
*** Sentence 3167: Replace "in case of" by "for" or "for when" in:
In case of lost connection, recovery is longer
*** Sentence 3169: Replace "e.g.," by "for example," in:
E.g., suppose 20 clients where only 10 nodes are computing
*** Sentence 3170: Replace "since there is" by "with" in:
These active nodes will be computing for another hour while others stop working since there is no more task assigned to them
*** Sentence 3170: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
These active nodes will be computing for another hour while others stop working since there is no more task assigned to them
*** Sentence 3171: Replace "entire task" by "task" in:
In Hashtopolis, the ###### is defined purely by a user and is constant throughout an entire task
*** Sentence 3183: Delete "the use of" if followed by a gerund or noun describing an action in:
This approach also respects the use of cryptographic salt

*** Sentence 3185: Replace "can not" by "cannot" in:
The workunits are created on-demand so that the system can not predict the future
*** Sentence 3188: Replace "enormously" by "very" in:
Creating enormously large workunits is a much more significant problem
*** Sentence 3190: Replace "terminate" by "end" or "finish", except if referring to employment in:
Not only the user may get annoyed, but the system may also terminate the process due to an exceeded deadline that is set for each workunit
*** Sentence 3194: Replace "gpu" by "graphical processing unit" in:
Potential failures range from GPU overheat-ing, lack of memory, through network problems up to possibly compromised nodes
*** Sentence 3196: Replace "utilized" by "used" in:
Secondly, if the hosts are not assigned to another running job simultaneously, they may not be utilized well at the end
*** Sentence 3197: Replace "illustrates" by "shows" in:
An example is described in Figure 3.6(a), which illustrates the keyspace distribution
*** Sentence 3198: Delete "there is" and insert "occurs" or "is" or a similar word later in:
There is a total of five hosts, each having assigned a workunit of its color
*** Sentence 3198: Replace "a total of five" by "five" in:
There is a total of five hosts, each having assigned a workunit of its color
*** Sentence 3200: Replace "since there is" by "with" in:
Since there is no more keyspace left to distribute, they do not receive any work
*** Sentence 3200: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
Since there is no more keyspace left to distribute, they do not receive any work
*** Sentence 3201: Replace "employed" by "used" in:
Even if it takes hours for hosts 1 and 3 to finish, the other nodes are not employed
*** Sentence 3204: Replace "most of the" by "most" if followed by a plural noun in:
The solution is called ramp-down, and the goal is to ensure all hosts compute most of the time
*** Sentence 3205: Replace "is illustrated" by "is shown" in:
The solution is illustrated in Figure 3.6(b) and allows for more efficient utilization of network resources
*** Sentence 3205: Replace "illustrated in" by "shown in" in:
The solution is illustrated in Figure 3.6(b) and allows for more efficient utilization of network resources
*** Sentence 3205: Replace "utilization" by "use" in:
The solution is illustrated in Figure 3.6(b) and allows for more efficient utilization of network resources
*** Sentence 3254: Replace "e.g.," by "for example," in:
E.g., #"s# = 0.1 means that maximally 10% of the remaining keyspace #" #" is assigned
*** Sentence 3256: Delete "there is" and insert "occurs" or "is" or a similar word later in:
additional hosts connect to the network, there is always a piece of work for them
*** Sentence 3259: Replace "illustrated in" by "shown in" in:
The motivation for the ramp-down was discussed above and illustrated in Figure 3.6
*** Sentence 3272: Replace "impact of" by "effect of" in:
The actual impact of the algorithm is shown by experiments in Section 3.9.2
*** Sentence 3276: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Yet, there are many other factors in the game that influence the actual performance
*** Sentence 3277: Replace "utilization" by "use" in:
Those include the settings of the attack, disk i/o speed, amount of available memory, utilization by different running processes, and others
*** Sentence 3289: Replace "so that they can" by "to" in:
The hosts literally wait for new candidate passwords so that they can verify them
*** Sentence 3294: Replace "at the time" by "then" in:
At the time the host is processing a workunit, it can be downloading another one
*** Sentence 3300: Replace "would need to" by "should" in:
The user either has to configure the client manually, or Fitcrack would need to use a modified version of the BOINC client

*** Sentence 3301: Replace "together with" by "with" in:
In 2020, together with my fellow researchers, I later discovered an alternative solution
*** Sentence 3303: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Even if multiple Runner processes are started, there is maximally one hashcat process
*** Sentence 3308: Replace "utilized" by "used" in:
The initial release37 utilized custom OpenCL and CUDA kernels for cracking PDF, ZIP, 7z, RAR, and MS Office up to version 2003
*** Sentence 3314: Replace "illustrates" by "shows" in:
Figure 3.7 illustrates the architecture of the Fitcrack system
*** Sentence 3316: Replace "lan" by "local-area network" in:
The server and clients are interconnected by a TCP/IP network, not necessarily only LAN which makes it possible to run a cracking task over-the-Internet on nodes in geographically distant locations
*** Sentence 3316: Replace "makes it possible to" by "enables" and change verb to a gerund in:
The server and clients are interconnected by a TCP/IP network, not necessarily only LAN which makes it possible to run a cracking task over-the-Internet on nodes in geographically distant locations
*** Sentence 3319: Replace "is responsible for managing" by "manages" in:
Server - The server is responsible for managing cracking jobs and assigning work to clients
*** Sentence 3321: Delete "one or more" in:
Each job is defined by an attack mode (see Section 3.8), attack set-tings (e.g., which dictionary should be used), and one or more password hashes of the same type (e.g., SHA-1)
*** Sentence 3323: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
In terms of the client-server ar-chitecture, the server provides a workunit assignment service since hosts actively ask for new work
*** Sentence 3327: Replace "at least one" by "a" or "an" in:
A Fitcrack host can be any machine with Windows or Linux OS, and at least one OpenCL-compatible device with proper drivers installed
*** Sentence 3328: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
The only piece of software that needs to be installed is the BOINC Client (see Section 3.7.9), and optionally the BOINC Manager (see Section 3.7.10) providing a graphical user interface to the BOINC Client
*** Sentence 3338: Replace "api" by "applications programming interface" or "interface" in:
REST API MySQL
*** Sentence 3353: Replace "gui" by "graphical user interface" in:
GUI
*** Sentence 3360: Replace "pipe" by "send" if a verb in:
PIPE
*** Sentence 3382: Delete "use of" in:
To achieve an efficient use of network#'s resources, it employs the Adaptive scheduling algorithm [81] described in Section 3.6.5
*** Sentence 3382: Replace "employs" by "uses" in:
To achieve an efficient use of network#'s resources, it employs the Adaptive scheduling algorithm [81] described in Section 3.6.5
*** Sentence 3386: Replace "etc." by "and so on" in:
For example, it performs the fragmentation of dictionaries, calculates the appropriate password index boundaries, loads the preterminal structures for the PCFG attack, etc.
*** Sentence 3387: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
There are three types of workunits: a) regular cracking tasks, b) benchmark workunits, and c) a complete benchmark
*** Sentence 3388: Replace "are used to" by "can" in:
Regular workunits are used to verify a set of candidate passwords
*** Sentence 3388: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
Regular workunits are used to verify a set of candidate passwords
*** Sentence 3394: Replace "is performed" by "is done" in:
It is performed automatically at the time a completely new host connects

*** Sentence 3394: Replace "at the time" by "then" in:
It is performed automatically at the time a completely new host connects
*** Sentence 3403: Replace "is ready to" by "anticipates" in:
Job is ready to be started
*** Sentence 3406: Delete "one or more" in:
Job is finished, one or more hashes cracked
*** Sentence 3437: Replace "encountered" by "met" or "saw" or "seen" in:
The host encountered an error during the computation
*** Sentence 3441: Replace "not running" by "stopped" in:
Numbers above 10 mean the job is not running
*** Sentence 3443: Replace "is illustrated" by "is shown" in:
The lifetime of a job is illustrated in Figure 3.8
*** Sentence 3443: Replace "illustrated in" by "shown in" in:
The lifetime of a job is illustrated in Figure 3.8
*** Sentence 3447: Delete "there is" and insert "occurs" or "is" or a similar word later in:
If there is at least one non-cracked hash and no error or user action occurs, the job eventually proceeds to the Finishing state
*** Sentence 3447: Replace "at least one" by "a" or "an" in:
If there is at least one non-cracked hash and no error or user action occurs, the job eventually proceeds to the Finishing state
*** Sentence 3452: Replace "in case of" by "for" or "for when" in:
In case of a non-recoverable error (e.g., the database gets corrupted), the job switches to the Malformed state
*** Sentence 3453: Replace "are allowed to" by "may" in:
In Fitcrack, three subsystems are allowed to change the state of the job: the Generator, when a host asks for a new workunit, the Assimilator if a workunit result is received, and the Webadmin at an event of user#'s action
*** Sentence 3457: Replace "shown in table" by "in table" in:
The host codes are shown in Table 3.5
*** Sentence 3458: Replace "illustrated" by "showed" or "shown" in:
The Generator daemon runs in a loop illustrated by Algorithm 2
*** Sentence 3459: Delete "there is" and insert "occurs" or "is" or a similar word later in:
It takes care that for each running job, there is always at least a single workunit assigned
*** Sentence 3461: Replace "needs to" by "must" or "should" if "needs" is a verb in:
Each participating host needs to perform a benchmark workunit first
*** Sentence 3472: Replace "at the time" by "then" in:
At the time the second workunit is processed, another one can be transferred over the network
*** Sentence 3473: Replace "deals with" by "concerns" or "handles" or "encounters" in:
The daemon also deals with disconnected hosts and computation errors
*** Sentence 3474: Replace "pre-defined" by "predefined" in:
When a host delivers an incorrect workunit result, or when the processing reaches a pre-defined deadline, the workunit is tagged with retry flag, and a the Generator reassigns it by creating a copy of the original workunit
*** Sentence 3481: Replace "replicated" by "copied" or "simulated" in:
If the job replication is active, i.e., a single workunit is assigned to more than one host, the Validator verifies if the replicated results match
*** Sentence 3519: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
There are three options, how a workunit could end:
*** Sentence 3522: Delete "one or more" in:
If the host cracked one or more hashes, the passwords are saved to the database
*** Sentence 3523: Replace "terminated" by "ended" or "finished", except if referring to employment in:
If all hashes are cracked, the entire job is considered done, and all ongoing workunits are terminated
*** Sentence 3532: Replace "ok" by "adequate" or "enough" when used as an adjective in:

if Result is OK (code 0) then
*** Sentence 3537: Delete "one or more" in:
if One or more passwords found (code 0)) then
*** Sentence 3553: Replace "ok" by "adequate" or "enough" when used as an adjective in:
if Result is OK (code 0) then
*** Sentence 3559: Replace "obtains" by "gets" in:
However, the only information about the workunit#'s progress the server obtains when the host finishes its work and sends a report
*** Sentence 3561: Replace "via" by "by" in:
Via this API, each host periodically sends XML-based Trickle messages that
*** Sentence 3563: Replace "inform" by "tell" or "affect" in:
inform the server about partial progress
*** Sentence 3568: Replace "denoted" by "meant" or "indicated" or "represented" in:
Besides the previously denoted applications, Fitcrack uses the following subsystems43 which are part of the BOINC:
*** Sentence 3569: Replace "in order to" by "to" in:
Transitioner - controls the state transitions of workunits and their results in order to keep the database synchronized
*** Sentence 3578: Replace "consists of two" by "has two" in:
It consists of two parts: frontend and backend connected interconnected via a REST API
*** Sentence 3578: Replace "via" by "by" in:
It consists of two parts: frontend and backend connected interconnected via a REST API
*** Sentence 3578: Replace "api" by "applications programming interface" or "interface" in:
It consists of two parts: frontend and backend connected interconnected via a REST API
*** Sentence 3586: Replace "back-end" by "backend" in:
For each one, the frontend offers graphical components for user interaction, while the back-end provides a series of endpoints that communicate with the database and implement the underlying operations
*** Sentence 3593: Replace "selection" by "choice" in:
The second step is the selection of an attack mode and attack options
*** Sentence 3594: Replace "need to be" by "must be" if "need" is a verb in:
While in the Hashtopolis tool, the attack settings need to be specified manually as hashcat#'s command line
*** Sentence 3598: Replace "selection" by "choice" in:
The settings cover the selection of wordlists for dictionary-based attacks, password-mangling rules, masks for brute-force and hybrid attacks, custom character sets, Markov model parameters, and much more
*** Sentence 3599: Replace "notifies" by "tells" in:
As the user creates the job, the WebAdmin in real-time notifies the user about the current keyspace and estimated worst-case cracking time
*** Sentence 3600: Delete "one or more" in:
Once the attack is configured, the user assigns one or more hosts to perform the attack
*** Sentence 3603: Replace "various statistics" by "statistics" in:
For each job, the user sees the current progress and various statistics
*** Sentence 3610: Delete "one or more" in:
The user may assign each job to one or more bins
*** Sentence 3611: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
For instance, the bins may refer to individual cases in terms of forensic investigation
*** Sentence 3619: Replace "conducted" by "did" or "done" in:
The lookup is conducted at job creation time
*** Sentence 3620: Replace "notified" by "told" in:
Users are notified if they attempt to create a job with hash that was already cracked
*** Sentence 3620: Replace "attempt to" by "try to" in:
Users are notified if they attempt to create a job with hash that was already cracked
*** Sentence 3623: Replace "via" by "by" in:

Fitcrack supports three ways of adding new dictionaries: a) importing directly from the server; b) uploading new via HTTP; c) uploading using SFTP/SCP, if configured
*** Sentence 3631: Replace "utilize" by "use" in:
The brute-force attack mode allows the user to utilize up to four user-defined character sets
*** Sentence 3645: Replace "allows to" by "allows one to" or "allows them", etc. in:
User Management - allows to create, modify, and delete user accounts
*** Sentence 3647: Replace "provides an overview of" by "surveys" or "summarizes" in:
Server Monitor - provides an overview of the entire system
*** Sentence 3647: Replace "entire system" by "system" in:
Server Monitor - provides an overview of the entire system
*** Sentence 3648: Replace "utilization" by "use" in:
It displays the status of all server daemons and the utilization of the server#'s resources
*** Sentence 3651: Delete "one or more" in:
The user may assign one or more jobs to an export
*** Sentence 3656: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
For some operations, the WebAdmin backend uses a set of external utilities:
*** Sentence 3661: Replace "etc." by "and so on" in:
etc. For the media formats, where it is possible (e.g., ZIP and RAR archives, or Office documents), it detects the signature and contents of the file and calls one of the existing scraper scripts (e.g., office2hashcat.py) which extracts the hash
*** Sentence 3661: Replace "one of the" by "one" if followed by a plural noun, and make it singular in:
etc. For the media formats, where it is possible (e.g., ZIP and RAR archives, or Office documents), it detects the signature and contents of the file and calls one of the existing scraper scripts (e.g., office2hashcat.py) which extracts the hash
*** Sentence 3662: Replace "is used for" by "is for" in:
Hcstat2gen from the hashcat-utils46 repository is used for generating *.hcstat2 files from existing password dictionaries
*** Sentence 3664: Replace "is used for" by "is for" in:
Princeprocessor on the server is used for calculating the keyspace of PRINCE at-tacks, described in Section 3.8.6
*** Sentence 3669: Replace "employs" by "uses" in:
For each running attack, the server employs a single instance of the PCFG Manager server that creates preterminal structures [213] from the desired grammar
*** Sentence 3674: Delete "there is" and insert "occurs" or "is" or a similar word later in:
This tool ensures there is always a running instance of the PCFG Manager server for each running PCFG attack job
*** Sentence 3682: Replace "referred to as" by "called" in:
The BOINC Client, also referred to as a core client, is an application that handles the communication between the client and the server
*** Sentence 3683: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
It is the only application that needs to be installed manually to a newly-connected host
*** Sentence 3694: Replace "etc." by "and so on" in:
In BOINC Manager, the user can set #"when to compute#" by defining certain conditions, including times and days of the week, limits on CPU, memory, disk usage, etc.
*** Sentence 3701: Replace "to use for" by "for" in:
The Runner can optionally use a local configuration file, where the user can specify which OpenCL devices to use for computation, their workload profile, etc. The Runner also reports partial workunit progress using the Trickle messages processed by the server#'s Trickler daemon, described in Section 3.7.4
*** Sentence 3701: Replace "etc." by "and so on" in:
The Runner can optionally use a local configuration file, where the user can specify which OpenCL devices to use for computation, their workload profile, etc. The Runner also reports partial workunit progress using the Trickle messages processed by the server#'s Trickler daemon, described in Section 3.7.4
*** Sentence 3704: Replace "employs" by "uses" in:

It employs various OpenCL kernels that implement a GPGPU-based cracking of more than 300 different cryptographic algorithms supported by Fitcrack
*** Sentence 3708: Replace "in case of" by "for" or "for when" in:
In case of failure (e.g., GPU overheating, computation error), the Runner generates a report for the server
*** Sentence 3708: Replace "gpu" by "graphical processing unit" in:
In case of failure (e.g., GPU overheating, computation error), the Runner generates a report for the server
*** Sentence 3712: Replace "utilizes" by "uses" in:
Fitcrack utilizes it for PRINCE attacks
*** Sentence 3713: Replace "located on" by "on" in:
The princeprocessor is located on both the client and server sides
*** Sentence 3721: Replace "employ the use of" by "use" in:
Some advanced techniques employ the use of probability to guess passwords more precisely
*** Sentence 3724: Replace "while there is" by "despite" in:
While there is no unified naming convention, each software uses its unique terminology
*** Sentence 3724: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
While there is no unified naming convention, each software uses its unique terminology
*** Sentence 3724: Replace "terminology" by "terms" and make a following verb plural in:
While there is no unified naming convention, each software uses its unique terminology
*** Sentence 3729: Replace "in addition to" by "besides" in:
In addition to the integrated password generating mechanisms, some tools can read candidate passwords directly from standard input
*** Sentence 3730: Replace "employ" by "use" in:
This option allows the user to employ an external password generator and perform attacks that are not natively supported by the tool
*** Sentence 3736: Replace "utilization" by "use" in:
Therefore, my contribution lies in the utilization of these methods in a distributed password cracking network
*** Sentence 3746: Replace "should be able to" by "could" or "should" in:
Precision #--The system should be able to specify workunit sizes as precisely as possible, ideally, in the units of individual passwords
*** Sentence 3747: Replace "crucial" by "key" in:
This is crucial for the adaptive scheduling algorithm, described in Section 3.6.5
*** Sentence 3748: Replace "utilization" by "use" in:
Sensible network utilization #--With each workunit, the system should only trans-fer data that is necessary
*** Sentence 3749: Replace "be performed" by "be done" in:
Server-friendly computing #--Complex computing operations should be performed by hosts, not the server
*** Sentence 3749: Replace "performed by" by "done by" in:
Server-friendly computing #--Complex computing operations should be performed by hosts, not the server
*** Sentence 3750: Replace "utilization" by "use" in:
High utilization of server processors and memory is undesir-able
*** Sentence 3755: Replace "referred to as" by "called" in:
A dictionary attack, also referred to as a wordlist attack or a straight attack, uses a text file called the password dictionary
*** Sentence 3761: Delete "the use of" if followed by a gerund or noun describing an action in:
Fitcrack supports the use of one or multiple password dictionaries
*** Sentence 3773: Delete "the use of" if followed by a gerund or noun describing an action in:
The attack can be enhanced by the use of password-mangling rules
*** Sentence 3775: Replace "modifications" by "changes" in:
Password-mangling rules define various modifications of candidate passwords
*** Sentence 3776: Replace "etc." by "and so on" in:
Such alterations include replacing and swapping of characters and substrings, password truncation, padding, etc. Hashcat currently supports over 7051 different rules
*** Sentence 3777: Replace "illustrates" by "shows" in:

Table 3.6 illustrates their practical use on a few examples
*** Sentence 3778: Replace "needs to" by "must" or "should" if "needs" is a verb in:
To use password-mangling rules, the user needs to specify a text file called ruleset
*** Sentence 3779: Replace "pre-defined" by "predefined" in:
Several pre-defined rulesets are also present in hashcat#'s repository
*** Sentence 3779: Replace "are also present" by "also occur" or "also are" in:
Several pre-defined rulesets are also present in hashcat#'s repository
*** Sentence 3780: Delete "one or more" in:
Each line of the file contains one or more mangling rules separated by whitespace
*** Sentence 3786: Replace "be performed on" by "be done on" in:
The number of lines in the ruleset signifies how many mangling steps will be performed on each password
*** Sentence 3850: Replace "pre-loaded" by "preloaded" in:
If the dictionary is pre-loaded on all nodes, the workload distribution is possible by setting different offset and guess limits to different nodes
*** Sentence 3851: Replace "via" by "by" in:
An alternative may be a dictionary accessible via a shared network drive
*** Sentence 3854: Replace "it is necessary to" by "one must" in:
In general, it is necessary to distribute the password candidates from the server to clients, i.e., the computing nodes
*** Sentence 3855: Replace "lead to" by "cause" or "enable" or "find" in:
Unfortunately, this effort has significant overhead, and for less-complex hash algorithms could lead to an inefficient distributed attack [86, 84]
*** Sentence 3858: Replace "via" by "by" in:
If it does not exist locally, the client downloads it from the server via HTTP
*** Sentence 3861: Replace "while there is" by "despite" in:
While there is no broadcast in HTTP, the server needs to send the same file multiple times using different connections
*** Sentence 3861: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
While there is no broadcast in HTTP, the server needs to send the same file multiple times using different connections
*** Sentence 3861: Replace "needs to" by "must" or "should" if "needs" is a verb in:
While there is no broadcast in HTTP, the server needs to send the same file multiple times using different connections
*** Sentence 3861: Replace "multiple times" by "many times" in:
While there is no broadcast in HTTP, the server needs to send the same file multiple times using different connections
*** Sentence 3863: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
There are use cases where this strategy may be beneficial
*** Sentence 3863: Replace "be beneficial" by "help" in:
There are use cases where this strategy may be beneficial
*** Sentence 3864: Replace "pre-loaded" by "preloaded" in:
For instance, if the dictionaries are pre-loaded on all nodes or saved on network storage accessible via high-speed links in a computer cluster
*** Sentence 3864: Replace "via" by "by" in:
For instance, if the dictionaries are pre-loaded on all nodes or saved on network storage accessible via high-speed links in a computer cluster
*** Sentence 3873: Replace "shown in figure" by "in figure" in:
A simplified scheme of this strategy is shown in Figure 3.11
*** Sentence 3879: Delete "the use of" if followed by a gerund or noun describing an action in:
Another challenge is the use of password-mangling rules
*** Sentence 3882: Delete "the use of" if followed by a gerund or noun describing an action in:
The use of rules increase the actual number of password guesses, but hashcat applies them in the modifier loop, and therefore hashcat#'s keyspace remains the same as if no rules were used

*** Sentence 3884: Replace "that is used for" by "for" in:
As mentioned in Section 3.6.4, Fitcrack distinguishes between hashcat#'s keyspace that is used for setting the program parameters and the actual keyspace that is used for calculating the size of a workunit for a concrete client
*** Sentence 3886: Replace "the estimation of" by "the estimate of" in:
The estimation of computing time thus uses the actual number of password guesses
*** Sentence 3893: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
The hash algorithm thus needs to be calculated 100 times
*** Sentence 3897: Replace "referred to as" by "called" in:
A combination attack, also referred to as a combinator attack, uses two separate password dictionaries: a left dictionary, and a right dictionary
*** Sentence 3897: Replace "two separate" by "two" in:
A combination attack, also referred to as a combinator attack, uses two separate password dictionaries: a left dictionary, and a right dictionary
*** Sentence 3898: Replace "crafted" by "made" in:
Candidate passwords are crafted using a string concatenation: passwords from the left dictionary are extended by passwords from the right one
*** Sentence 3900: Replace "shown in figure" by "in figure" in:
An example of a combination attack is shown in Figure 3.12
*** Sentence 3909: Replace "in addition to" by "besides" in:
Note, in addition to the basic combination attack, enhanced alternatives exist
*** Sentence 3912: Delete "there is" and insert "occurs" or "is" or a similar word later in:
For chaining multiple dictionary words, there is also an advanced combination attack called PRINCE that is decribed in Section 3.8.6
*** Sentence 3950: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
Second, it increases the amount of data that needs to be transferred over the network
*** Sentence 3954: Replace "deal with" by "concern" or "handle" or "encounter" in:
To deal with this issue, Fitcrack uses a different solution
*** Sentence 3958: Replace "utilize" by "use" in:
Moreover, it may utilize the #"skip/limit#" arguments to reduce the number of left-hand strings if necessary
*** Sentence 3960: Delete "the process of" in:
Algorithm 4 describes the process of calculating workunit size
*** Sentence 3966: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
For example, if the desired keyspace is 100 and there are 101 passwords remaining, it assigns the host all 101 in a single workunit instead of creating two workunits with 100 and 1 password
*** Sentence 3967: Delete "essentially," in:
Essentially, there are three possible situations:
*** Sentence 3967: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Essentially, there are three possible situations:
*** Sentence 3976: Replace "over and over" by "again" or "repeatedly" in:
See that the proposed strategy iterates through the left dictionary over and over until all passwords from the right one are processed
*** Sentence 4002: Replace "illustrates" by "shows" in:
Figure 3.13 illustrates an example of distribution with the proposed strategy
*** Sentence 4009: Replace "not necessary" by "unnecessary" in:
The --skip and --limit parameters were not necessary
*** Sentence 4013: Replace "along with" by "with" in:
Since the left dictionary is fragmented, the host receives one password from the right dictionary along with hashcat argument --skip 40, the ##########" --# sub #### increases to 1, and #######" -#" --### is reset to 0
*** Sentence 4015: Delete "a total of" in:
The left dictionary is not fragmented so that this host can receive multiple passwords from the right dictionary (for a total of 1000 candidate passwords)

*** Sentence 4021: Replace "referred to as" by "called" in:
An incremental attack is a classic version of the brute-force attack with three parameters: the minimal password length, the maximal password length, and the alphabet, also referred to as the character set, or charset
*** Sentence 4022: Replace "that are used for" by "for" in:
The alphabet is an ordered set of characters that are used for generating candidate passwords
*** Sentence 4055: Replace "above-shown" by "previously shown" in:
The above-shown example is only one of the possible implementations
*** Sentence 4055: Replace "one of the" by "one" if followed by a plural noun, and make it singular in:
The above-shown example is only one of the possible implementations
*** Sentence 4059: Replace "modifications" by "changes" in:
As mentioned above, different tools use different modifications of the password-guessing algorithm
*** Sentence 4060: Delete "the use of" if followed by a gerund or noun describing an action in:
More advanced techniques involve Markovian models (see Section 4.2.2) and the use of probability to generate certain sequences of characters first
*** Sentence 4071: Replace "in addition to" by "besides" in:
Later versions of John the Ripper contain a #"mask attack mode#" as well, in addition to the classic incremental mode
*** Sentence 4073: Delete "one or more" in:
A user may define one or more masks for the attack
*** Sentence 4076: Delete "one or more" in:
Masks have the form of strings containing one or more symbols
*** Sentence 4081: Replace "can be used to" by "can" in:
Such a mask can be used to generate candidate passwords in the form of #" <-1#" <-2...#" <-### where #" <-### is the ###-th symbol of the candidate password
*** Sentence 4084: Replace "is:" by "is" in:
###, the ###### symbol in the mask is:
*** Sentence 4127: Replace "used in combination with" by "combined with" in:
Custom character sets may contain both ASCII and non-ASCII characters - i.e., may be used in combination with various national encodings
*** Sentence 4129: Replace "is illustrated" by "is shown" in:
An example of generating passwords using a mask is illustrated by Figure 3.14
*** Sentence 4130: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
If there are concrete characters in a mask, the same characters at the same positions are used in the generated candidate passwords #--i.e., if for all ### [1, ###], if ###### = #" <-###, character #" <-### is used at the ###-th position in all generated passwords
*** Sentence 4132: Delete "there is" and insert "occurs" or "is" or a similar word later in:
If there is more than one one substitute symbol, candidate passwords are generated as a cartesian product of all used corresponding character sets
*** Sentence 4168: Replace "illustrate" by "show" in:
To illustrate the difference, Figure 3.15 shows an example of candidate passwords generated using the classic incremental approach and Markov chains
*** Sentence 4170: Replace "follow after" by "after" in:
Generating characters is based on conditional probability #" (#"<-# #"<-#) that character #"<-# will follow after character #"<-#
*** Sentence 4180: Replace "etc." by "and so on" in:
In the example, the most probable character on the first position is #"n#", the second most probable is #"p#", etc. The other rows show characters which will most probably succeed after a certain character (entitling the row)
*** Sentence 4180: Replace "a certain" by "a" or "an" in:
In the example, the most probable character on the first position is #"n#", the second most probable is #"p#", etc. The other rows show characters which will most probably succeed after a certain character (entitling the row)

*** Sentence 4182: Replace "etc." by "and so on" in:
The second most probable successor of #"a#" is #"a#", the third one is #"e#", etc.
*** Sentence 4263: Replace "etc." by "and so on" in:
Once all passwords starting with n are generated, the next sequence contains passwords starting with letter #"p#", etc. For each character #"c#" generated, the algorithm looks at the row entitled by #"c#", and the next character will be generated from that row
*** Sentence 4263: Replace "looks at" by "studies" if "looks" is a verb in:
Once all passwords starting with n are generated, the next sequence contains passwords starting with letter #"p#", etc. For each character #"c#" generated, the algorithm looks at the row entitled by #"c#", and the next character will be generated from that row
*** Sentence 4265: Replace "can be used to" by "can" in:
In hashcat, however, it is possible to define a threshold value which can be used to limit the depth of character lookup
*** Sentence 4273: Replace "in case of" by "for" or "for when" in:
In case of mask ?l?l?l, the keyspace would be
*** Sentence 4283: Replace "two different" by "two" in:
For brute-force attack with Markov chains, hashcat supports two different models:
*** Sentence 4287: Replace "utilizes" by "uses" in:
It utilizes the idea that character probability is influ-enced not only by the previously generated character, but also by the position in the password
*** Sentence 4289: Replace "etc." by "and so on" in:
If the first character is generated, the first matrix is used, for the second chracter, the second matrix is used, etc. Such an enhancement makes sense because users often follow specific password-creation patterns, e.g., numbers will more likely be at the end of the password than at the beginning [35, 212]
*** Sentence 4289: Replace "e.g.," by "for example," in:
If the first character is generated, the first matrix is used, for the second chracter, the second matrix is used, etc. Such an enhancement makes sense because users often follow specific password-creation patterns, e.g., numbers will more likely be at the end of the password than at the beginning [35, 212]
*** Sentence 4292: Replace "employ" by "use" in:
For example, commercial tools from Elcomsoft54 employ the classic incremental brute-force (see Section 3.8.3) and provide the #"Start from#" and #"End at#" columns where a user can specify the range using concrete passwords
*** Sentence 4294: Replace "e.g.," by "for example," in:
In such a case, without modification of the program, the options are very limited55, e.g., letting different nodes generate passwords of different lengths, etc.
*** Sentence 4294: Replace "etc." by "and so on" in:
In such a case, without modification of the program, the options are very limited55, e.g., letting different nodes generate passwords of different lengths, etc.
*** Sentence 4299: Replace "since there is" by "with" in:
The overhead to the attack is minimal since there is no need to transfer strings via the network
*** Sentence 4299: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
The overhead to the attack is minimal since there is no need to transfer strings via the network
*** Sentence 4299: Replace "via" by "by" in:
The overhead to the attack is minimal since there is no need to transfer strings via the network
*** Sentence 4303: Replace "gpu" by "graphical processing unit" in:
In the brute-force attack mode, part of the mask is processed on GPU and cannot be managed by users
*** Sentence 4304: Replace "cpu" by "processor" in:
Using command-line arguments, users can only control the part of the mask that is generated in the base loop on a CPU
*** Sentence 4312: Replace "is used to determine" by "investigates" in:
This value is used to determine the range of allowed password indexes
*** Sentence 4316: Replace "informing" by "telling" in:

This value serves for estimation of the cracking time, specifying workunit sizes, and informing the user
*** Sentence 4342: Delete "is used to" and change following verb to present tense singular in:
The -a 3 parameter corresponds to the brute-force attack mode, while the time utility is used to measure real time of running
*** Sentence 4343: Replace "conducted" by "did" or "done" in:
The experiment was conducted on a system with the above mentioned GPU, Intel(R) Core(TM) i7-8700 CPU, and 16 GB RAM
*** Sentence 4343: Replace "ram" by "memory" in:
The experiment was conducted on a system with the above mentioned GPU, Intel(R) Core(TM) i7-8700 CPU, and 16 GB RAM
*** Sentence 4364: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Depending on a concrete network, there is additional overhead for network communication, BOINC, and other factors
*** Sentence 4365: Replace "employed in" by "used in" or "in" in:
The scheduling algorithm employed in Fitcrack, however, adapts to such impacts without problems since it measures the overall time between assigning each workunit and receiving its result
*** Sentence 4366: Replace "taken into account" by "considered" or "accounted for" in:
All additional delays are thus taken into account
*** Sentence 4372: Replace "illustrated in" by "shown in" in:
Both cases are illustrated in Figure 3.18
*** Sentence 4376: Replace "is:" by "is" in:
The resulting keyspace is:
*** Sentence 4397: Replace "need to" by "must" if "need" is a verb in:
Sim-ilarly to the combination attack, we need to combine every left-hand password with every right-hand one
*** Sentence 4399: Delete "there is" and insert "occurs" or "is" or a similar word later in:
If there is a dictionary, the parameters control the number of dictionary passwords
*** Sentence 4402: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
There is no way to generate only part of the mask-created strings
*** Sentence 4405: Replace "allows to" by "allows one to" or "allows them", etc. in:
This approach allows to precisely control the size of each workunit, but at the cost of efficiency
*** Sentence 4406: Replace "enormous" by "very large" in:
The overhead for generating and transmitting password guesses would be enormous
*** Sentence 4409: Replace "was transformed" by "changed" in:
Then, the attack was transformed into a combination attack, and the distribution followed the same strategy as proposed in Section 3.8.2
*** Sentence 4414: Replace "in the same way as" by "the same as" in:
An advantage of the solution was that Fitcrack could the use the left and right password-mangling rules (see Section 3.8.1) in the same way as with the combination attack, although rules are normally not supported in hybrid attacks
*** Sentence 4420: Replace "there is no need" by "it is unnecessary" in:
Hashcat runs in the native hybrid attack mode, and there is no need for the maskprocessor utility since no strings are pre-generated anymore
*** Sentence 4422: Replace "in the same manner" by "in the same way" in:
For the hybrid mask + wordlist attack, the dictionary on the right side is frag-mented in the same manner as in the combination attack
*** Sentence 4426: Replace "shown in figure" by "in figure" in:
An example of the workunit distribution is shown in Figure 3.20
*** Sentence 4427: Replace "is transformed" by "changed" or "changes" in:
For the hybrid wordlist + mask, the mask on the right is transformed into multiple masks with lower keyspace using the newly-proposed Algorithm 6
*** Sentence 4430: Replace "shown in figure" by "in figure" in:
An example of workunit distribution with mask slicing is shown in Figure 3.21

*** Sentence 4531: Replace "illustrate" by "show" in:
I illustrate the principle using two examples
*** Sentence 4533: Replace "that we want to" by "to" in:
Suppose that we want to send a mask with 20 passwords
*** Sentence 4538: Replace "two times" by "twice" in:
The desired keyspace is two times higher, so we leave the first symbol intact and proceed to the second one
*** Sentence 4556: Replace "need to" by "must" if "need" is a verb in:
Since the first 160 strings were already generated, we only need to change a for b as the next symbol from the ?l character set
*** Sentence 4561: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
In this case, there are two options: either fragmenting the left dictionary or slicing the mask
*** Sentence 4568: Delete "the use of" if followed by a gerund or noun describing an action in:
The use of probabilistic context-free grammars (PCFG) for password cracking was originally proposed by Weir et al. [213] The attack is based on the previous knowledge of user pass-words whose structure is represented by a grammar
*** Sentence 4570: Replace "denote" by "mean" or "indicate" or "represent" in:
Rewrite rules have probability values assigned to denote what fragments of symbols will more occur in candidate pass-words
*** Sentence 4644: Replace "need to" by "must" if "need" is a verb in:
Similarly to the other attack modes, we need to deliver the passwords to the cracking nodes somehow
*** Sentence 4649: Replace "a significant amount of" by "much" or "significant" in:
The process may take a significant amount of time, and often the grammar cannot be processed entirely
*** Sentence 4654: Replace "utilizes" by "uses" in:
The idea utilizes the fact that each preterminal structure produces passwords with the same probability
*** Sentence 4657: Replace "obtaining" by "getting" in:
Fitcrack supports two ways of obtaining the grammar
*** Sentence 4661: Replace "via" by "by" in:
Both sides can communicate via gRPC13 and Protocol buffers14, as described in Section 4.8.1
*** Sentence 4662: Replace "utilized" by "used" in:
The concept is utilized in Fitcrack as well with slight modifications since the client-server communication in BOINC is based on passing input/output files
*** Sentence 4662: Replace "modifications" by "changes" in:
The concept is utilized in Fitcrack as well with slight modifications since the client-server communication in BOINC is based on passing input/output files
*** Sentence 4664: Delete "one or more" in:
preterminals - the file contains one or more preterminal structures that are used for generating password guesses within the workunit
*** Sentence 4664: Replace "that are used for" by "for" in:
preterminals - the file contains one or more preterminal structures that are used for generating password guesses within the workunit
*** Sentence 4666: Replace "is performed" by "is done" in:
The serialization is performed by the Pcfg endpoint in WebAdmin backend (see Section 3.7.6) at the time the grammar is created
*** Sentence 4666: Replace "performed by" by "done by" in:
The serialization is performed by the Pcfg endpoint in WebAdmin backend (see Section 3.7.6) at the time the grammar is created
*** Sentence 4666: Replace "at the time" by "then" in:
The serialization is performed by the Pcfg endpoint in WebAdmin backend (see Section 3.7.6) at the time the grammar is created
*** Sentence 4671: Replace "allows to" by "allows one to" or "allows them", etc. in:
This allows to run multiple PCFG attack at the same time
*** Sentence 4673: Replace "obtain" by "get" in:

When creating a workunit, the Generator invokes GetNextItems() call to obtain one or more preterminal structures
*** Sentence 4673: Delete "one or more" in:
When creating a workunit, the Generator invokes GetNextItems() call to obtain one or more preterminal structures
*** Sentence 4674: Replace "to enable" by "for" in:
With the call, the Generator also specifies a keyspace value that is necessary to enable the adaptive scheduling (see Section 3.6.5)
*** Sentence 4676: Replace "is illustrated" by "is shown" in:
An example is illustrated in Figure 3.23
*** Sentence 4676: Replace "illustrated in" by "shown in" in:
An example is illustrated in Figure 3.23
*** Sentence 4677: Replace "can not" by "cannot" in:
The exact match can not be guaranteed because different PTs may generate different number of password guesses
*** Sentence 4679: Replace "together with" by "with" in:
The preterminals file together with the grammar file represent the input data for the new workunit
*** Sentence 4714: Replace "that can be used for" by "for" in:
PRINCE (PRobability INfinite Chained Elements) is a modern password generation algo-rithm that can be used for advanced combination attacks
*** Sentence 4715: Replace "two different" by "two" in:
Jens Steube designed this al-gorithm to use only one vocabulary instead of two different dictionaries and then generate chains of combined words
*** Sentence 4758: Replace "shown in table" by "in table" in:
Keyspaces of some chains from the RockYou dictionary are shown in Table 3.9
*** Sentence 4800: Replace "at the time of" by "at" or "during" in:
At the time of writing this thesis, the latest release of princeprocessor is version 0.22
*** Sentence 4804: Replace "pre-defined" by "predefined" in:
Besides, the tool provides some additional options like calculating output password length distribution, eliminating duplicate words, saving state, or storing the output into a pre-defined text file
*** Sentence 4819: Replace "employs" by "uses" in:
The PRINCE is another attack mode of Fitcrack that employs an external password gen-erator
*** Sentence 4820: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
The input of the attack is a password dictionary and a set of options
*** Sentence 4821: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
For workload distribution, there are few possible strategies
*** Sentence 4823: Replace "massive" by "large" in:
Such a strategy, however, puts a significant load on the server and creates a massive overhead for network communication
*** Sentence 4824: Replace "e.g.," by "for example," in:
Another approach is to divide the password creation by length, e.g., let one node generate passwords of one length and another node passwords of another length, etc. Nevertheless, the length-based distribution would create chunks of significantly different keyspaces
*** Sentence 4824: Replace "etc." by "and so on" in:
Another approach is to divide the password creation by length, e.g., let one node generate passwords of one length and another node passwords of another length, etc. Nevertheless, the length-based distribution would create chunks of significantly different keyspaces
*** Sentence 4825: Replace "be used for" by "be for" in:
Such a method could not be used for fine-grained workunit tailoring
*** Sentence 4826: Replace "similar to" by "like" in:
Luckily, the princeprocessor utility supports the --skip and --limit parameters, so it is possible to use a strategy similar to the mask attack
*** Sentence 4827: Replace "illustrated in" by "shown in" in:

Therefore, Fitcrack runs the princeprocessor utility on the client and supplies hashcat with passwords using a pipe, as illustrated in Figure 3.7
*** Sentence 4836: Replace "shown in figure" by "in figure" in:
An example of attack distribution is shown in Figure 3.24
*** Sentence 4838: Replace "together with" by "with" in:
The server receives the configuration of the job together with the user-specified dictionary
*** Sentence 4874: Replace "illustrate" by "show" in:
Using different scenarios, I illustrate the practical impact of the algorithms integrated to Fitcrack#'s subsystems
*** Sentence 4874: Replace "impact of" by "effect of" in:
Using different scenarios, I illustrate the practical impact of the algorithms integrated to Fitcrack#'s subsystems
*** Sentence 4875: Replace "present" by "show" or "give" or "offer" if a transitive verb in:
Moreover, I present a series of comparisons with the Hashtopolis tool
*** Sentence 4876: Replace "at the time of" by "at" or "during" in:
At the time of writing this thesis, Hashtopolis is most likely the only other maintained open-source hashcat-based distributed password cracking solution
*** Sentence 4876: Replace "is most likely" by "is likely" in:
At the time of writing this thesis, Hashtopolis is most likely the only other maintained open-source hashcat-based distributed password cracking solution
*** Sentence 4877: Replace "different aspects" by "aspects" in:
The experiments are structured into multiple sections that analyze different aspects of the system
*** Sentence 4879: Replace "cpu" by "processor" in:
It analyzes both CPU and GPU-based networks and answers what kind of assignments are worth distributing
*** Sentence 4881: Replace "illustrates" by "shows" in:
Section 3.9.2 illustrates the practical impacts of the adaptive scheduling algorithm proposed in Section 3.6.5
*** Sentence 4881: Replace "impacts of" by "effects of" in:
Section 3.9.2 illustrates the practical impacts of the adaptive scheduling algorithm proposed in Section 3.6.5
*** Sentence 4882: Delete "the problem of" in:
It discusses the problem of benchmark accuracy and its impacts
*** Sentence 4886: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
I compare different attack modes in terms of password guessing complexity, the overhead for network transfer, and feasibility for cracking simple and complex hash algorithms
*** Sentence 4889: Replace "if and when" by "when" in:
The goal is to analyze if and when the attack is worth distribution, the difference between CPU and GPU nodes, and the scalability of such attacks
*** Sentence 4889: Replace "cpu" by "processor" in:
The goal is to analyze if and when the attack is worth distribution, the difference between CPU and GPU nodes, and the scalability of such attacks
*** Sentence 4889: Replace "gpu" by "graphical processing unit" in:
The goal is to analyze if and when the attack is worth distribution, the difference between CPU and GPU nodes, and the scalability of such attacks
*** Sentence 4892: Replace "i did" by "we did" in:
Unfortunately, at that time, I did not have access to that high number of GPU nodes
*** Sentence 4892: Replace "did not have" by "lacked" in:
Unfortunately, at that time, I did not have access to that high number of GPU nodes
*** Sentence 4892: Replace "have access to" by "access" in:
Unfortunately, at that time, I did not have access to that high number of GPU nodes
*** Sentence 4892: Replace "gpu" by "graphical processing unit" in:
Unfortunately, at that time, I did not have access to that high number of GPU nodes
*** Sentence 4893: Replace "most of the" by "most" if followed by a plural noun in:
Therefore, most of the hosts are CPU-based

*** Sentence 4897: Replace "were performed" by "were done" in:
The experiments were performed using 2, 4, 8, 16, 37, and 55 CPU hosts and using 1, 2, and 4 GPUs on a single GPU host
*** Sentence 4897: Replace "performed using" by "done by" in:
The experiments were performed using 2, 4, 8, 16, 37, and 55 CPU hosts and using 1, 2, and 4 GPUs on a single GPU host
*** Sentence 4897: Replace "cpu" by "processor" in:
The experiments were performed using 2, 4, 8, 16, 37, and 55 CPU hosts and using 1, 2, and 4 GPUs on a single GPU host
*** Sentence 4897: Replace "gpus" by "graphical processing units" in:
The experiments were performed using 2, 4, 8, 16, 37, and 55 CPU hosts and using 1, 2, and 4 GPUs on a single GPU host
*** Sentence 4897: Replace "gpu" by "graphical processing unit" in:
The experiments were performed using 2, 4, 8, 16, 37, and 55 CPU hosts and using 1, 2, and 4 GPUs on a single GPU host
*** Sentence 4899: Replace "gpu" by "graphical processing unit" in:
The last line shows the password cracking performance of a single GPU
*** Sentence 4902: Replace "employment" by "use" if not referring to labor in:
The employment of CPU nodes was from top to bottom, e.g., A 37-node attack used 16 nodes with Intel i5-4460, and 21 with Intel i3-4340, etc. We can also see that the benchmarked performance of the GPU node is much higher
*** Sentence 4902: Replace "cpu" by "processor" in:
The employment of CPU nodes was from top to bottom, e.g., A 37-node attack used 16 nodes with Intel i5-4460, and 21 with Intel i3-4340, etc. We can also see that the benchmarked performance of the GPU node is much higher
*** Sentence 4902: Replace "e.g.," by "for example," in:
The employment of CPU nodes was from top to bottom, e.g., A 37-node attack used 16 nodes with Intel i5-4460, and 21 with Intel i3-4340, etc. We can also see that the benchmarked performance of the GPU node is much higher
*** Sentence 4902: Replace "etc." by "and so on" in:
The employment of CPU nodes was from top to bottom, e.g., A 37-node attack used 16 nodes with Intel i5-4460, and 21 with Intel i3-4340, etc. We can also see that the benchmarked performance of the GPU node is much higher
*** Sentence 4902: Replace "gpu" by "graphical processing unit" in:
The employment of CPU nodes was from top to bottom, e.g., A 37-node attack used 16 nodes with Intel i5-4460, and 21 with Intel i3-4340, etc. We can also see that the benchmarked performance of the GPU node is much higher
*** Sentence 4916: Replace "gpu" by "graphical processing unit" in:
GPU
*** Sentence 4922: Replace "i tested" by "we tested" in:
In the first scenario, I tested the worst-case cracking time, i.e., the time required to generate and verify all candidate passwords
*** Sentence 4927: Replace "need to" by "must" if "need" is a verb in:
For example, with a maximum length of 5, we need to test 26 + 262 + 263 + 264 + 265 = 12, 356, 630 different passwords
*** Sentence 4928: Replace "exponentially" by "at an accelerating rate" except if you mean the math function in:
The complexity grows exponentially with each extra position
*** Sentence 4929: Replace "cpu" by "processor" in:
I ran these five jobs using the following network configurations: a server + 2, 4, 8, 16, 27, and 55 CPU nodes; and a single node with 1, 2, and 4 GPUs
*** Sentence 4929: Replace "gpus" by "graphical processing units" in:

I ran these five jobs using the following network configurations: a server + 2, 4, 8, 16, 27, and 55 CPU nodes; and a single node with 1, 2, and 4 GPUs
*** Sentence 4953: Replace "gpu" by "graphical processing unit" in:
1 GPU
*** Sentence 4954: Replace "gpu" by "graphical processing unit" in:
2 GPU
*** Sentence 4955: Replace "gpu" by "graphical processing unit" in:
4 GPU
*** Sentence 5007: Replace "cpu" by "processor" in:
The most time-exhausting experiment was the maximum length of 9 on 8 CPU hosts, which took over 23 hours
*** Sentence 5009: Replace "extreme" by "high" in:
See also the opposite extreme
*** Sentence 5012: Replace "gpus" by "graphical processing units" in:
Cracking with four GPUs was even longer than with one or two since the computer spent time with a pointless initialization of another two cards
*** Sentence 5013: Replace "cpu" by "processor" in:
Table 3.12: Time (in seconds) of distributed CPU and GPU-based password cracking First, I analyze the distributed CPU-based approach
*** Sentence 5017: Replace "substantial" by "large" in:
up to the maximum length of 6, the cracking is so quick that adding new nodes does not add any substantial acceleration
*** Sentence 5020: Replace "employed" by "used" in:
The 8-character job, however, employed 27 hosts without any problem
*** Sentence 5023: Replace "evident" by "clear" in:
For 9-character passwords, the advantage of distributed computing is evident
*** Sentence 5024: Replace "cpu" by "processor" in:
Cracking on two or four CPU nodes is impossible to perform within a day
*** Sentence 5030: Replace "cpu" by "processor" in:
Figure 3.25: Worst-case cracking time on CPU nodes
*** Sentence 5032: Replace "gpu" by "graphical processing unit" in:
For jobs up to the length of 8, Figure 3.26(a) shows the cracking time, but this time on GPU
*** Sentence 5033: Replace "employed" by "used" in:
On the X-Axis, we see the number of employed GPU units
*** Sentence 5033: Replace "gpu" by "graphical processing unit" in:
On the X-Axis, we see the number of employed GPU units
*** Sentence 5034: Replace "gpu" by "graphical processing unit" in:
The 5 and 6-character passwords were cracked almost instantly, even with a single GPU
*** Sentence 5035: Replace "advantageous" by "desirable" or "helpful" in:
Similarly to the distributed solution, multi-GPU cracking was advantageous for passwords of 7 characters and longer
*** Sentence 5036: Replace "gpu" by "graphical processing unit" in:
The absolute cracking time of 8-character passwords on one GPU processor corresponds was close to the result obtained with 16 CPU nodes
*** Sentence 5036: Replace "cpu" by "processor" in:
The absolute cracking time of 8-character passwords on one GPU processor corresponds was close to the result obtained with 16 CPU nodes
*** Sentence 5039: Replace "gpu" by "graphical processing unit" in:
9-character passwords can be processed within 49 196 secs (13.6 hours) on 1 GPU and in 12 379 secs (3.4 hours) on 4 GPUs
*** Sentence 5039: Replace "gpus" by "graphical processing units" in:
9-character passwords can be processed within 49 196 secs (13.6 hours) on 1 GPU and in 12 379 secs (3.4 hours) on 4 GPUs

*** Sentence 5040: Replace "utilization" by "use" in:
While the measured cracking times provide a basic overview of the cracking networks#' capabilities, they do not directly document the actual utilization
*** Sentence 5063: Replace "employ" by "use" in:
The efficiency of cracking short passwords is low since the jobs are too easy and employ more resources than needed
*** Sentence 5064: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
Therefore, the overhead for the initial benchmark-ing, sending workunit assignments, and reporting results, is much higher in terms of the entire job
*** Sentence 5066: Replace "gpu" by "graphical processing unit" in:
Also, the single-machine GPU approach is more efficient because there is no overhead for intra-node communication
*** Sentence 5066: Replace "because there is" by "with" in:
Also, the single-machine GPU approach is more efficient because there is no overhead for intra-node communication
*** Sentence 5066: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
Also, the single-machine GPU approach is more efficient because there is no overhead for intra-node communication
*** Sentence 5067: Replace "no matter what" by "whatever" in:
We can see, no matter what cracking network we have, the trend is ascending in all cases
*** Sentence 5067: Replace "in all cases" by "always" in:
We can see, no matter what cracking network we have, the trend is ascending in all cases
*** Sentence 5069: Replace "employ" by "use" in:
In other words, for every cracking network, we can find a task difficult enough to employ it efficiently
*** Sentence 5070: Replace "utilize" by "use" in:
If a job is too easy to utilize all nodes efficiently, we can use only some of them
*** Sentence 5072: Replace "gpus" by "graphical processing units" in:
We also see the high potential of GPUs
*** Sentence 5073: Replace "gpu" by "graphical processing unit" in:
In this case, a single powerful GPU node could beat an entire network of CPU nodes
*** Sentence 5073: Replace "cpu" by "processor" in:
In this case, a single powerful GPU node could beat an entire network of CPU nodes
*** Sentence 5074: Replace "employed" by "used" in:
However, this experiment purposedly employed a relatively simple algorithm and had an alphabet limited to lowercase letters
*** Sentence 5075: Replace "would need to" by "should" in:
For more complex algorithms or stronger passwords, we would need to use multiple GPU nodes
*** Sentence 5075: Replace "gpu" by "graphical processing unit" in:
For more complex algorithms or stronger passwords, we would need to use multiple GPU nodes
*** Sentence 5076: Replace "gpu" by "graphical processing unit" in:
Down below in this chapter, I also show various experiments with the actual distributed cracking on GPU nodes using different attack modes
*** Sentence 5080: Replace "is required to" by "must" in:
The previous scenario analyzed the worst-case time that is required to process the entire keyspace
*** Sentence 5081: Replace "not necessary" by "unnecessary" in:
In real cases, this is often not necessary since the correct password could be found much earlier
*** Sentence 5085: Replace "ten different" by "ten" in:
For each host configuration and password length, I generated ten different random passwords
*** Sentence 5090: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
Hence, there is no correlation between the number of hosts and cracking time
*** Sentence 5096: Replace "very similar to" by "much like" in:
This expected trend is very similar to the previous experiment
*** Sentence 5101: Replace "cpu" by "processor" in:

Concretely, CPU nodes 1 to 16 and a host with GPUs from Table 3.10
*** Sentence 5101: Replace "gpus" by "graphical processing units" in:
Concretely, CPU nodes 1 to 16 and a host with GPUs from Table 3.10
*** Sentence 5103: Replace "provides an overview of" by "surveys" or "summarizes" in:
Table 3.13 provides an overview of the cost of working nodes based on 2015 prices
*** Sentence 5110: Replace "gpu" by "graphical processing unit" in:
unit price of GPU solutions is lower when inserting additional GPU cards
*** Sentence 5112: Replace "taken into account" by "considered" or "accounted for" in:
The motherboard, disks, RAM, PSU, and other parts are taken into account as well
*** Sentence 5115: Replace "cpu" by "processor" in:
Also note, with a change of PSU and RAM, each CPU node from the cluster is upgradeable to a GPU one
*** Sentence 5115: Replace "gpu" by "graphical processing unit" in:
Also note, with a change of PSU and RAM, each CPU node from the cluster is upgradeable to a GPU one
*** Sentence 5144: Replace "gpu" by "graphical processing unit" in:
1 GPU
*** Sentence 5148: Replace "gpu" by "graphical processing unit" in:
2 GPU
*** Sentence 5152: Replace "gpu" by "graphical processing unit" in:
4 GPU
*** Sentence 5160: Replace "similar to" by "like" in:
The table shows that the power consumption of the 16-node cluster is similar to a 4-GPU node
*** Sentence 5161: Replace "gpu" by "graphical processing unit" in:
However, the prices of energy consumed to perform the jobs are lower on GPU because of faster computing
*** Sentence 5197: Replace "gpu" by "graphical processing unit" in:
1 GPU
*** Sentence 5202: Replace "gpu" by "graphical processing unit" in:
2 GPU
*** Sentence 5207: Replace "gpu" by "graphical processing unit" in:
4 GPU
*** Sentence 5215: Replace "cpu" by "processor" in:
The total power consumption spent on cracking password of length 5 to 8 on CPU and GPU nodes is shown in Figure 3.29
*** Sentence 5215: Replace "gpu" by "graphical processing unit" in:
The total power consumption spent on cracking password of length 5 to 8 on CPU and GPU nodes is shown in Figure 3.29
*** Sentence 5215: Replace "shown in figure" by "in figure" in:
The total power consumption spent on cracking password of length 5 to 8 on CPU and GPU nodes is shown in Figure 3.29
*** Sentence 5217: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
In terms of power consumption, the password cracking is generally more efficient on GPU cards than CPU units
*** Sentence 5217: Replace "gpu" by "graphical processing unit" in:
In terms of power consumption, the password cracking is generally more efficient on GPU cards than CPU units
*** Sentence 5217: Replace "cpu" by "processor" in:
In terms of power consumption, the password cracking is generally more efficient on GPU cards than CPU units
*** Sentence 5218: Replace "cpu" by "processor" in:
An interesting observation is that when we add new CPU nodes, the total power consumption #" ##########" #### softly rises
*** Sentence 5219: Replace "gpu" by "graphical processing unit" in:
On the GPU machine, adding new units decreases the total consumption
*** Sentence 5221: Replace "gpu" by "graphical processing unit" in:

Another cause is that in the experiments, GPU units shared the same motherboard and PSUs
*** Sentence 5221: Replace "shared the same" by "shared the" in:
Another cause is that in the experiments, GPU units shared the same motherboard and PSUs
*** Sentence 5222: Replace "gpu" by "graphical processing unit" in:
Adding a new GPU did not require starting another computer
*** Sentence 5225: Replace "illustrates" by "shows" in:
Firstly, it illustrates the impact of the algorithm in different phases of a job
*** Sentence 5225: Replace "impact of" by "effect of" in:
Firstly, it illustrates the impact of the algorithm in different phases of a job
*** Sentence 5232: Replace "utilizes" by "uses" in:
While Hash-topolis strictly respects the user-entered chunk size and uses the same tailoring mechanism from the very start till the end, Fitcrack utilizes the ramp-up and ramp-down techniques
*** Sentence 5234: Replace "illustrates" by "shows" in:
Figure 3.30 illustrates the practical impact of the original scheduling algorithm using an experiment with a brute-force attack on SHA-1 hash
*** Sentence 5234: Replace "impact of" by "effect of" in:
Figure 3.30 illustrates the practical impact of the original scheduling algorithm using an experiment with a brute-force attack on SHA-1 hash
*** Sentence 5235: Replace "employed" by "used" in:
The attack employed 8 hosts with NVIDIA GTX 1050 Ti GPU and a password mask made of 10 lowercase letters (10x ?l)
*** Sentence 5235: Replace "gpu" by "graphical processing unit" in:
The attack employed 8 hosts with NVIDIA GTX 1050 Ti GPU and a password mask made of 10 lowercase letters (10x ?l)
*** Sentence 5243: Replace "illustrates" by "shows" in:
The chart in Figure 3.30(a) illustrates how workunit size changes over time
*** Sentence 5245: Replace "gpus" by "graphical processing units" in:
This is an anticipated result since all nodes had the same GPUs and no link outage, or computation error occured
*** Sentence 5261: Replace "utilize" by "use" in:
Workunits get smaller again at the end of the job to utilize all hosts by all means
*** Sentence 5264: Replace "utilizes" by "uses" in:
If another process utilizes the computer, the cracking speed may suddenly drop
*** Sentence 5265: Replace "illustrate" by "show" in:
In this experiment, I illustrate that the system can react appropriately to such an event
*** Sentence 5268: Replace "cpus" by "processors" in:
To make the results comparable, I used faster CPUs and a slower GPU
*** Sentence 5268: Replace "gpu" by "graphical processing unit" in:
To make the results comparable, I used faster CPUs and a slower GPU
*** Sentence 5270: Replace "the reason for" by "why" in:
The reason for brute-force was to eliminate a possible impact of transferring dictionary passwords over the network
*** Sentence 5270: Replace "impact of" by "effect of" in:
The reason for brute-force was to eliminate a possible impact of transferring dictionary passwords over the network
*** Sentence 5291: Replace "cpu" by "processor" in:
We can see that despite the high potential of GPGPU, cracking on high-end CPU like Core i7-5930K can be faster than on low-end notebook graphics like Radeon R5 M255
*** Sentence 5293: Replace "cpu" by "processor" in:
At a marked time point, I intentionally added extra load to CPU threads of node B, causing its performance to go down
*** Sentence 5300: Replace "accordingly" by "so" in:
It calculates the worku-nit size accordingly to the performance of nodes

*** Sentence 5318: Replace "an additional" by "another" in:
Figure 3.31: Fitcrack#'s reaction to an additional load
*** Sentence 5321: Replace "gpus" by "graphical processing units" in:
To make a clear image, I performed a series of tests using different GPUs (NVIDIA, AMD) and hash algorithms (MD5 [172], SHA-1 [97], SHA-512 [76], and Whirlpool [188]) of a different computing complexity
*** Sentence 5324: Replace "gpu" by "graphical processing unit" in:
I intentionally chose different classes of cards from both manufacturers to provide a clearer image of how the GPU selection affects the cracking sessions
*** Sentence 5324: Replace "selection" by "choice" in:
I intentionally chose different classes of cards from both manufacturers to provide a clearer image of how the GPU selection affects the cracking sessions
*** Sentence 5329: Replace "shown in table" by "in table" in:
The measured cracking performances are shown in Table 3.17
*** Sentence 5331: Replace "a small fraction of" by "few" or "a few" if referring to a set in:
For the dictionary attack, the measured speed is only a small fraction of the benchmark result
*** Sentence 5332: Replace "needs to" by "must" or "should" if "needs" is a verb in:
This result makes sense since hashcat needs to load and cache dictionary passwords, making the cracking operations much slower
*** Sentence 5333: Replace "gpu" by "graphical processing unit" in:
Empty columns stand for OpenCL #"CL_OUT_OF_RESOURCES#" error, which occurred due to insufficient memory on the given GPU
*** Sentence 5335: Replace "encountered" by "met" or "saw" or "seen" in:
I encountered this problem when trying to compute Whirlpool on AMD Radeon RX 460 and AMD Radeon R9 Fury X.
*** Sentence 5336: Replace "gpu" by "graphical processing unit" in:
GPU
*** Sentence 5380: Replace "gpus" by "graphical processing units" in:
Table 3.16: Comparison of hardware specifications of used GPUs
*** Sentence 5382: Replace "gpu" by "graphical processing unit" in:
GPU
*** Sentence 5472: Replace "conducted" by "did" or "done" in:
To compare the old and new benchmarking methods, I conducted another series of ex-periments that show the practical impact on actual cracking tasks
*** Sentence 5476: Replace "employ" by "use" in:
The experiments employ three different formats and also explore the impact of a cryptographic salt
*** Sentence 5476: Replace "three different" by "three" in:
The experiments employ three different formats and also explore the impact of a cryptographic salt
*** Sentence 5476: Replace "impact of" by "effect of" in:
The experiments employ three different formats and also explore the impact of a cryptographic salt
*** Sentence 5479: Replace "was performed on" by "was done on" in:
Finally, MD5 is easiest-to-compute, but the attack was performed on 20 hashes, each with a unique salt
*** Sentence 5481: Replace "for the purpose of" by "for" in:
For the purpose of this experiment, the ramp-up was intentionally disabled to let the scheduling system create full-sized workunits from the very beginning
*** Sentence 5489: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
Every cryptographic salt means that the hash needs to be recomputed again
*** Sentence 5490: Replace "illustrated in" by "shown in" in:
The reason is discussed and illustrated in Section 3.1.1
*** Sentence 5492: Replace "state that" by "say" if "state" is a verb in:
Based on the results, I state that the improved benchmarking technique is definitely far more accurate
*** Sentence 5543: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
There is no mask or grammar, neither any special algorithm for generating guesses

*** Sentence 5545: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
As described in Section 3.8.1, there are two basic strategies
*** Sentence 5549: Replace "gpu" by "graphical processing unit" in:
To test both, I compare the two tools on a series of distributed GPU experiments
*** Sentence 5551: Replace "obtain" by "get" in:
To obtain comparable results in fair conditions, I measured the total time consisting of the: a) the benchmarking, b) data transfer, and c) the actual cracking
*** Sentence 5553: Replace "does not have" by "lacks" in:
Moreover, Hashtopolis does not have a #"start button#"
*** Sentence 5553: Replace "not have a" by "lack a" in:
Moreover, Hashtopolis does not have a #"start button#"
*** Sentence 5564: Replace "placed at" by "put at" in:
The correct password was, in all cases, intentionally placed at the end of each dictionary to force Fitcrack process it entirely
*** Sentence 5565: Replace "shown in table" by "in table" in:
The experimental results are shown in Table 3.19, where for each attack, I show the total time, and the number of chunks generated
*** Sentence 5576: Replace "the reason for" by "why" in:
The reason for such behavior is the inaccuracy of the hashcat#'s default benchmark mode
*** Sentence 5579: Delete "there was" and insert "occurred" or "was" or similar word later in:
Despite there was only a single node working, Fitcrack was still faster except using the smallest dictionary
*** Sentence 5580: Replace "a lot of" by "much" or "many" in:
Hashtopolis wasted a lot of time by sending the entire dictionary to all eight nodes, even though the smallest one could be processed relatively quickly using just a single node
*** Sentence 5697: Delete "there was" and insert "occurred" or "was" or similar word later in:
There was also a significant speedup for bigger dictionaries thanks to better utilization of resources
*** Sentence 5697: Replace "utilization" by "use" in:
There was also a significant speedup for bigger dictionaries thanks to better utilization of resources
*** Sentence 5698: Replace "helped to" by "helped" in:
The pipeline processing introduced in Fitcrack-3 helped to eliminate the overhead for wordlist transfer
*** Sentence 5701: Replace "illustrate" by "show" in:
To illustrate the influence of the wordlist size on the overall cracking time, I depicted the results in graphs
*** Sentence 5733: Replace "are performed" by "are done" in:
Since HTTP(S) has no broadcast by design, all server-host data transfers are performed using one unicast connection per host
*** Sentence 5733: Replace "performed using" by "done by" in:
Since HTTP(S) has no broadcast by design, all server-host data transfers are performed using one unicast connection per host
*** Sentence 5740: Replace "it is necessary to" by "one must" in:
So that, for 4.2 GB dictionary, it is necessary to transmit 8 4.2 GB = 33.6 GB of data
*** Sentence 5741: Replace "etc." by "and so on" in:
For 8.3 GB dictionary, the amount of transferred data equals 8 8.3 GB = 66.4 GB, etc. Thus, cracking with the 4.2 GB dictionary took around 4 minutes for Fitcrack, while Hashtopolis required between 11-12 minutes
*** Sentence 5742: Replace "most of the" by "most" if followed by a plural noun in:
For the 8.3 GB dictionary, the difference is even more significant #--5 minutes for Fitcrack and 32-47 minutes for Hashtopolis where most of the time is spent by data transfer
*** Sentence 5743: Replace "vast" by "large" in:
The distribution strategy used has a vast impact on scalability since lim#" i (#" ###) = #" ###, but lim#" i (#" i #" ###) = which makes the naive approach practicaly unusable for larger networks and bigger dictionaries
*** Sentence 5746: Replace "need to" by "must" if "need" is a verb in:
With each workunit, we only need to send hosts an attack configuration [87], and the indexes of candidate passwords

*** Sentence 5845: Replace "utilized" by "used" in:
In the main phase, the workunit assignment is standard, however, in the final phase, the count is increased, and the sizes are smaller, ensuring all nodes are utilized in every moment
*** Sentence 5854: Replace "together with" by "with" in:
The network bandwidth is not limiting since we only transfer a range of password indexes together with additional options
*** Sentence 5857: Replace "utilize" by "use" in:
However, to utilize hardware resources well, it is required to choose the keyspace of workunits wisely
*** Sentence 5857: Replace "is required to" by "must" in:
However, to utilize hardware resources well, it is required to choose the keyspace of workunits wisely
*** Sentence 5859: Replace "leads to" by "causes" or "enables" or "finds" in:
Hashtopolis preserves the similar keyspace to all workunits, which, as I detected, leads to shorter cracking times of less-complex jobs if the chunk size is set to a smaller value
*** Sentence 5860: Replace "employs" by "uses" in:
Fitcrack, on the other hand, employs the adaptive scheduling algorithm, which modifies the keyspace of workunits depending on the current progress
*** Sentence 5875: Replace "shown in table" by "in table" in:
The results are shown in Table 3.21
*** Sentence 5880: Replace "more difficult" by "harder" in:
The number iterations is thus 212 = 4, 096, which is much more difficult to crack
*** Sentence 5882: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
For each password, the hash only needs to be computed once, and testing the 100 different hashes is just string comparison
*** Sentence 5883: Replace "more difficult" by "harder" in:
Therefore, testing the entire hashlist is not significantly more difficult than testing a single hash
*** Sentence 5884: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
The BCrypt, on the other hand, uses cryptographic salt, so that the entire algorithm needs to be computed 100 times for each candidate password
*** Sentence 5885: Replace "i did" by "we did" in:
I did a short test with a brute-force attack with ?l?l mask on NVIDIA GTX 1050 Ti
*** Sentence 5914: Replace "in all cases" by "always" in:
While for SHA-1, the crack-ing performance highly depends on the attack mode, for BCrypt with cost 12, it is the same in all cases
*** Sentence 5918: Replace "needs to" by "must" or "should" if "needs" is a verb in:
The combination attack is also very fast since it only needs to load passwords only once
*** Sentence 5921: Replace "gpu" by "graphical processing unit" in:
With all attack modes, the GPU was not able to crack more than 32 hashes per second
*** Sentence 5921: Replace "was not able to" by "could not" in:
With all attack modes, the GPU was not able to crack more than 32 hashes per second
*** Sentence 5931: Replace "were performed on" by "were done on" in:
All three jobs were performed on 1, 2, and 4 hosts with a single NVIDIA GTX 1050 Ti GPU
*** Sentence 5931: Replace "gpu" by "graphical processing unit" in:
All three jobs were performed on 1, 2, and 4 hosts with a single NVIDIA GTX 1050 Ti GPU
*** Sentence 5932: Replace "needs to" by "must" or "should" if "needs" is a verb in:
The goal was to measure the attack efficiency and the time Fitcrack needs to process the entire keyspace
*** Sentence 5966: Replace "utilized" by "used" in:
Since BCrypt is a very complex algorithm, the hosts were highly utilized most of the time
*** Sentence 5966: Replace "most of the" by "most" if followed by a plural noun in:
Since BCrypt is a very complex algorithm, the hosts were highly utilized most of the time
*** Sentence 5969: Replace "illustrated" by "showed" or "shown" in:
The cracking time, also illustrated by the chart in Figure 3.35, scaled pretty well with the number of nodes
*** Sentence 5984: Replace "tb" by "terabytes" in:

However, since the total keyspace of combined passwords is about 168 109, the experiments do not test the dictionary attack because the prepared dictionary would have over 1 TB of size
*** Sentence 5985: Replace "were performed on" by "were done on" in:
The jobs were performed on 1, 2, 4, and 8 hosts with NVIDIA GTX 1050 Ti GPU
*** Sentence 5985: Replace "gpu" by "graphical processing unit" in:
The jobs were performed on 1, 2, 4, and 8 hosts with NVIDIA GTX 1050 Ti GPU
*** Sentence 6076: Delete "there is" and insert "occurs" or "is" or a similar word later in:
While the previous experiment explains there is always a limit on node count, it raises another question: What is the influence of the desired workunit processing time
*** Sentence 6083: Replace "gpu" by "graphical processing unit" in:
The jobs were processed on 8 hosts with NVIDIA GTX 1050 Ti GPU
*** Sentence 6125: Replace "employed" by "used" in:
The last job employed ten nodes with NVIDIA GTX 1050 Ti
*** Sentence 6176: Replace "gpus" by "graphical processing units" in:
The performance achievable with a single machine is always limited, even we equip it with multiple GPUs
*** Sentence 6178: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Yet, if it is, there is always a reasonable number of computing nodes we should employ to complete the job at the desired time
*** Sentence 6178: Replace "employ" by "use" in:
Yet, if it is, there is always a reasonable number of computing nodes we should employ to complete the job at the desired time
*** Sentence 6179: Replace "utilizing" by "using" in:
While underestimating the task#'s complexity results in delays, utilizing more machines than necessary may cause needless overhead and efficiency loss
*** Sentence 6180: Replace "needs to" by "must" or "should" if "needs" is a verb in:
The final decision is up to the system#'s operator, who needs to consider the complexity of algorithms, attack mode, network characteristics, and other aspects
*** Sentence 6181: Replace "does not need to" by "need not" in:
The choice, however, does not need to be based on manual calculations
*** Sentence 6181: Replace "need to be" by "must be" if "need" is a verb in:
The choice, however, does not need to be based on manual calculations
*** Sentence 6183: Replace "an estimation of" by "an estimate of" in:
Therefore, the Fitcrack system provides an estimation of the maximum cracking time when a job is created
*** Sentence 6186: Replace "employs" by "uses" in:
The system employs the adaptive scheduling algorithm to create fine-tailored workunits that match each hosts#' current per-formance
*** Sentence 6192: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Yet, there are differences since each attack mode has specific properties
*** Sentence 6197: Replace "gpu" by "graphical processing unit" in:
The brute-force attack provides the best performance since we generate the passwords directly on the GPU
*** Sentence 6198: Replace "utilization" by "use" in:
The network utilization is low because there is no need to transfer additional data
*** Sentence 6198: Replace "because there is" by "with" in:
The network utilization is low because there is no need to transfer additional data
*** Sentence 6198: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
The network utilization is low because there is no need to transfer additional data
*** Sentence 6201: Replace "need to" by "must" if "need" is a verb in:
But if so, we need to transfer a large amount of data from the server to hosts
*** Sentence 6201: Replace "a large amount of" by "much" in:
But if so, we need to transfer a large amount of data from the server to hosts
*** Sentence 6205: Replace "since there is" by "with" in:

is easy-to-implement, but since there is no broadcast in HTTP, it may require a lot of time, and the scalability is terrible
*** Sentence 6205: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
is easy-to-implement, but since there is no broadcast in HTTP, it may require a lot of time, and the scalability is terrible
*** Sentence 6205: Replace "a lot of" by "much" or "many" in:
is easy-to-implement, but since there is no broadcast in HTTP, it may require a lot of time, and the scalability is terrible
*** Sentence 6207: Replace "need to" by "must" if "need" is a verb in:
The link to the server becomes the bottleneck, and the more nodes we have, the longer we need to wait
*** Sentence 6209: Replace "was required to" by "must" in:
While it was required to put additional logic to the system, the initial overhead is much lower, and the cracking session in Fitcrack can start sooner
*** Sentence 6211: Replace "three different" by "three" in:
While Fitcrack supports three different dictionary-based attack modes, the PRINCE seems to be the most low-cost one in terms of network utilization
*** Sentence 6211: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
While Fitcrack supports three different dictionary-based attack modes, the PRINCE seems to be the most low-cost one in terms of network utilization
*** Sentence 6211: Replace "utilization" by "use" in:
While Fitcrack supports three different dictionary-based attack modes, the PRINCE seems to be the most low-cost one in terms of network utilization
*** Sentence 6215: Replace "is beneficial for" by "helps" in:
The classic dictionary attack, if performed in a distributed way, is beneficial for complex cryptographic algorithms
*** Sentence 6217: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
In terms of efficiency, the combination attack is in the middle between the dictionary and PRINCE
*** Sentence 6218: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
The amount of data that needs to be transferred to hosts is lower than with the classic dictionary attack but higher than with PRINCE
*** Sentence 6220: Replace "employed" by "used" in:
In all cases, I suggest that the decision about the employed solution to use should reflect the algorithm#'s complexity
*** Sentence 6223: Replace "more or less" by "approximately" in:
While machine-generated passwords are more or less random, if the choice is up to a human being, the situation is different
*** Sentence 6225: Replace "utilize" by "use" in:
Probabilistic methods utilize that knowledge to allow a better targeting of password cracking attacks
*** Sentence 6227: Replace "employment" by "use" if not referring to labor in:
The core of the chapter focuses on probabilistic context-free grammars and their employment in password cracking tasks
*** Sentence 6228: Replace "state-of-the-art" by "recent" in:
In the following sections, I describe the properties of state-of-the-art methods for grammar-based cracking and identify weak spots that com-plicate their use from the practical point of view
*** Sentence 6229: Replace "improve existing" by "improve" in:
I introduce a series of enhancements that improve existing concepts and allow guessing more passwords for the same time
*** Sentence 6231: Replace "methodology" by "method" or "methods" in:
I also propose a methodology for distributed password cracking with probabilistic grammars
*** Sentence 6232: Replace "together with" by "with" in:
Together with my fellow researchers, I created two proof-of-concept tools that demonstrate the discussed principles
*** Sentence 6237: Replace "e.g.," by "for example," in:

In reaction, system administrators and software developers introduce mandatory rules for password composition, e.g., #"use at least one special character.#" While password-creation policies force users to create stronger passwords [166, 207], recent leaks of credentials from various websites showed the reality is much more bitter
*** Sentence 6239: Replace "utilized" by "used" in:
This fact may be utilized by both malicious attackers and forensic investigators who seek for evidence in password-protected data
*** Sentence 6243: Replace "exponentially" by "at an accelerating rate" except if you mean the math function in:
exponentially with the length of the password, and one does not need to #"try everything#" to crack the password
*** Sentence 6243: Replace "does not need to" by "need not" in:
exponentially with the length of the password, and one does not need to #"try everything#" to crack the password
*** Sentence 6244: Replace "a limited number of" by "few" or "a few" in:
The dictionary attack, on the other hand, usually checks a limited number of commonly-used or previously-leaked passwords
*** Sentence 6247: Delete "the use of" if followed by a gerund or noun describing an action in:
Even with the use of the popular hashcat tool and a machine with 11 NVIDIA GTX 1080 Ti1 units, brute-forcing an 8-character alphanumeric password may take over 48 years
*** Sentence 6250: Delete "the use of" if followed by a gerund or noun describing an action in:
Over the years, the use of probability and statistics showed the potential for a rapid im-provement of attacks against human-created passwords [136, 213, 114]
*** Sentence 6251: Delete "the use of" if followed by a gerund or noun describing an action in:
Various leaks of credentials from websites and services provide an essential source of knowledge about user password creation habits [35, 212], including the use of existing words [63] or reusing the same credentials between multiple services [52]
*** Sentence 6253: Replace "over and over" by "again" or "repeatedly" in:
People across the world unwittingly follow common password-creation patterns over and over
*** Sentence 6254: Delete "the use of" if followed by a gerund or noun describing an action in:
One approach is the use of Markov chains which consider probabilities that a certain character will follow after another one
*** Sentence 6254: Replace "a certain" by "a" or "an" in:
One approach is the use of Markov chains which consider probabilities that a certain character will follow after another one
*** Sentence 6254: Replace "follow after" by "after" in:
One approach is the use of Markov chains which consider probabilities that a certain character will follow after another one
*** Sentence 6257: Delete "the use of" if followed by a gerund or noun describing an action in:
To work with larger password fragments, Weir et al. proposed the use of probabilistic context-free grammars (PCFG) that can describe the structure of passwords in an existing (training) dictionary
*** Sentence 6259: Replace "can not" by "cannot" in:
Then, by derivation using rewriting rules of the grammar, one can not only generate all passwords from the original dictionary, but produce many new ones that still respect password-creation patterns learned from the dictionary [213]
*** Sentence 6263: Replace "utilized" by "used" in:
Such knowledge has been utilized in multiple password cracking principles and adopted to exist-ing tools
*** Sentence 6265: Delete "the use of" if followed by a gerund or noun describing an action in:
The use of probabilistic methods for computer-based password cracking dates back to 1980
*** Sentence 6275: Replace "more or less" by "approximately" in:
Whereas a machine-generated password may be more or less random, human beings follow specific patterns we can describe mathemat-ically
*** Sentence 6276: Replace "frequently used" by "frequent" in:

Markov chains are stochastic models frequently used in natural language processing [169]
*** Sentence 6276: Replace "natural language processing" by "natural-language processing" in:
Markov chains are stochastic models frequently used in natural language processing [169]
*** Sentence 6281: Replace "look at" by "study" if "look" is a verb in:
Password guessing based on a zero-order model means we use more probable characters first, but do not look at the already-generated ones
*** Sentence 6283: Replace "utilize" by "use" in:
Higher-order models utilize one or more previous states as well [169, 136]
*** Sentence 6283: Delete "one or more" in:
Higher-order models utilize one or more previous states as well [169, 136]
*** Sentence 6286: Replace "follow after" by "after" in:
The method uses conditional probability #" (#"<-# #"<-#) that character #"<-# will follow after character #"<-#
*** Sentence 6288: Replace "utilized" by "used" in:
The technique was utilized in Hashcat tool which uses Markov chains for brute-force attacks by default
*** Sentence 6291: Replace "employed in" by "used in" or "in" in:
A modified model based on 3-grams is also employed in the Incremental attack mode of John the Ripper tool [57]
*** Sentence 6296: Delete "there is" and insert "occurs" or "is" or a similar word later in:
There is also an extended three-dimensional model where the next character relies not only on the current state but also on the position in the password
*** Sentence 6303: Replace "actual values" by "values" in:
We can thus omit the actual values and create a matrix by placing characters from the most probable to the least probable one
*** Sentence 6305: Replace "in case of" by "for" or "for when" in:
In case of mask ?l?l?l, the keyspace would be 26 26 26 = 17576, since there are 26 lowercase letters in the latin alphabet
*** Sentence 6305: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
In case of mask ?l?l?l, the keyspace would be 26 26 26 = 17576, since there are 26 lowercase letters in the latin alphabet
*** Sentence 6386: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
In 2015, Duermuth et al. presented Ordered Markov ENumerator (OMEN), a password guessing algorithm they claim to outperform all previous publicly available Markov-based password guessers
*** Sentence 6386: Replace "publicly available" by "public" in:
In 2015, Duermuth et al. presented Ordered Markov ENumerator (OMEN), a password guessing algorithm they claim to outperform all previous publicly available Markov-based password guessers
*** Sentence 6387: Replace "a number of" by "several" in:
The algorithm discretizes all probabilites into a number of bins, and iterates over the bins in an order of decreasing likelihood
*** Sentence 6389: Replace "state that" by "say" if "state" is a verb in:
Duermuth et al. state that unlike existing algorithms, the #"OMEN can output guesses in order of (approximate) decreasing frequency#" [57]
*** Sentence 6390: Replace "incorporates" by "includes" in:
While in hashcat, the brute-force attack is always related to a fixed password length defined by the mask, OMEN incorporates the probability of password length as well
*** Sentence 6398: Replace "in addition," by "also," in:
In addition, we add rules that rewrite the starting symbol (#") to base structures which are non-terminal sentential forms describing the structure of the password [213]
*** Sentence 6402: Delete "there is" and insert "occurs" or "is" or a similar word later in:
There is only one rule that rewrites #" since both passwords are described by the same base structure
*** Sentence 6403: Replace "were able to" by "could" in:

By using PCFG on MySpace dataset (split to training and testing part), Weir et al. were able to crack 28% to 128% more passwords in comparison with the default ruleset from John the Ripper (JtR) tool3 using the same number of guesses
*** Sentence 6436: Replace "etc." by "and so on" in:
While the previous techniques consider only the syntax of passwords, Veras et al. de-signed a semantics-based approach which divides password fragments into categories by semantic topics like names, numbers, love, sports, etc. With JtR in stdin mode feeded by a semantic-based password generator, Veras achieved better success rates than using Weir#'s approach or the default JtR wordlist [206]
*** Sentence 6438: Replace "a huge number of" by "very many" in:
By training and testing on a huge number of datasets, Ma showed that the improved Markov-based guessing could bring better results than PCFGs [114]
*** Sentence 6439: Replace "encountered" by "met" or "saw" or "seen" in:
Weir#'s PCFG-based technique encountered extensions as well
*** Sentence 6440: Delete "the use of" if followed by a gerund or noun describing an action in:
Houshmand et al. intro-duced keyboard patterns represented by additional rewrite rules that helped improve the success rate by up to 22%, proposed the use of Laplace probability smoothing, and cre-ated guidelines for choosing appropriate attack dictionaries [80]
*** Sentence 6441: Replace "utilize" by "use" in:
After that, Houshmand also introduced targeted grammars that utilize information about a user who created the password [79]
*** Sentence 6442: Replace "presented in" by "in" in:
The research presented in this thesis is based on the late 2018#'s PCFG Cracker (version
*** Sentence 6445: Replace "need to" by "must" if "need" is a verb in:
To prove the contribution of the proposed improvements, I de-cided not to mix PCFG with Markovian models, and thus when one creates a grammar, they need to set the --coverage 1.0 option of the PCFG Trainer
*** Sentence 6449: Replace "consists of two" by "has two" in:
The current version of Weir#'s PCFG Cracker consists of two separate tools: PCFG Trainer and PCFG Manager
*** Sentence 6449: Replace "two separate" by "two" in:
The current version of Weir#'s PCFG Cracker consists of two separate tools: PCFG Trainer and PCFG Manager
*** Sentence 6450: Delete "is used to" and change following verb to present tense singular in:
While PCFG Trainer is used to create a grammar from an existing password dictionary, PCFG Manager generates new password guesses from the grammar - i.e., gradually applies rewrite rules to the starting symbol and derived sentential forms
*** Sentence 6451: Replace "at the time of" by "at" or "during" in:
At the time of writing this thesis, both tools include the support for letter capitalization rules [211], keyboard patterns [80], as well as the ability to generate new password segments
*** Sentence 6454: Replace "the portion of" by "the part of" in:
In the training phase, a user can set a coverage value which defines the portion of guesses to be generated using rewrite rules only while the rest is generated using Markov-based brute-force
*** Sentence 6456: Replace "present" by "show" or "give" or "offer" if a transitive verb in:
Moreover, the tools contain the support for context-sensitive character sequences like #"<3#" or #"#1#" that, if present in the training data, form a separate set of rewrite rules
*** Sentence 6457: Replace "can be used to" by "can" in:
Such replacements can be used to describe special strings like smileys, arrows, and others
*** Sentence 6459: Replace "numerous" by "many" in:
Despite numerous improvements made by Houshmand [80], users still have to face slow password guessing speed which is currently the bottleneck of the entire process
*** Sentence 6461: Replace "the application of" by "applying" in:

While the creation of a probabilistic grammar is fast and straightforward (see Section 4.4.1), the application of rewriting rules takes a significant amount of processor time, and the number of generated passwords is overwhelming in comparison with the original dictio-nary
*** Sentence 6461: Replace "a significant amount of" by "much" or "significant" in:
While the creation of a probabilistic grammar is fast and straightforward (see Section 4.4.1), the application of rewriting rules takes a significant amount of processor time, and the number of generated passwords is overwhelming in comparison with the original dictio-nary
*** Sentence 6466: Replace "cpu" by "processor" in:
The first 10 and first 100 passwords of darkweb2017 7 dataset and darkweb2017-top100 can be both used for training and gener-ating within 1 minute on Core(TM) i7-7700K CPU
*** Sentence 6468: Replace "provide information about" by "report on" in:
Moreover, the version 3 of the PCFG Manager tools did not provide information about the keyspace, i.e., the number of possible password candidates, and thus the user had no clue about how long the guessing took
*** Sentence 6469: Replace "suitable for" by "for" in:
Thus, I decided to make PCFG-based password cracking suitable for practical use and propose methods how to guess password faster, transform PCFGs to more compact ones, and calculate an exact number of possible password guesses, aka the keyspace
*** Sentence 6469: Replace "aka" by "also known as" in:
Thus, I decided to make PCFG-based password cracking suitable for practical use and propose methods how to guess password faster, transform PCFGs to more compact ones, and calculate an exact number of possible password guesses, aka the keyspace
*** Sentence 6470: Replace "that contain an" by "with an" in:
It is, however, necessary to mention, that later, Weir extended the tool with status reports that contain an approximate calculation of keyspace
*** Sentence 6479: Replace "findings" by "results" in:
Motivated by the findings mentioned above, I focus on making PCFG-based password cracking suitable for practical use
*** Sentence 6479: Replace "suitable for" by "for" in:
Motivated by the findings mentioned above, I focus on making PCFG-based password cracking suitable for practical use
*** Sentence 6483: Replace "amount of time" by "time" in:
I created a faster #"password generator#" that produces more guesses in the same amount of time using the same hardware
*** Sentence 6487: Replace "allows it to" by "lets it" in:
Concretely, I described how it accelerates the process and allows it to end in the desired maximum amount of time
*** Sentence 6487: Replace "amount of time" by "time" in:
Concretely, I described how it accelerates the process and allows it to end in the desired maximum amount of time
*** Sentence 6490: Replace "are present in" by "are in" in:
d) the success rate for testing datasets, i.e., how many newly-generated passwords are present in existing password dictionaries
*** Sentence 6506: Replace "regardless of" by "despite" in:
The grammar is called context-free because we can substitute nonterminal #"<-# with the right side #"s# regardless of the context where #"<-# is.
*** Sentence 6514: Replace "there are no" by "no" and insert "occur" or "are" or similar word later in:
Each fragment is unique; i.e., there are no duplicities
*** Sentence 6556: Replace "etc." by "and so on" in:
From #"pa#" we crete rewriting rule #"#"<-#2 # - pa#", #"$$#" creates #"#" l2 # - $$#", etc.
*** Sentence 6560: Replace "e.g." by "for example," in:
The same calculation goes for other rules, e.g. #" (#"<-#2 # - 42) = 2/4 = 0.5, etc.
*** Sentence 6560: Replace "etc." by "and so on" in:
The same calculation goes for other rules, e.g. #" (#"<-#2 # - 42) = 2/4 = 0.5, etc.

*** Sentence 6625: Delete "the method of" in:
The method of creating a PCFG described in Section 4.4.1 does not distinguish between lowercase and uppercase letters
*** Sentence 6627: Replace "e.g." by "for example," in:
If an uppercase letter is used, it is usually at the beginning of the password or of a word contained within it [83], e.g. passwords like #"Golf-Mike#" or #"HelloKitty!#" from RockYou9 dataset
*** Sentence 6628: Replace "utilize" by "use" in:
We can utilize the knowledge by mangling the capitalization of letters in existing fragments
*** Sentence 6632: Delete "one or more" in:
For fragment length ###, we define one or more capitalization masks
*** Sentence 6667: Replace "it is essential to" by "one must" in:
It is essential to distinguish between the implementation of the methodology in existing tools and the mathematical basis behind it
*** Sentence 6667: Replace "methodology" by "method" or "methods" in:
It is essential to distinguish between the implementation of the methodology in existing tools and the mathematical basis behind it
*** Sentence 6670: Replace "need to" by "must" if "need" is a verb in:
Thus, we need to consider every letter fragment a nonterminal
*** Sentence 6678: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
For grammar G, the set of all candidate passwords is the language generated by the grammar [70]:
*** Sentence 6704: Replace "need to" by "must" if "need" is a verb in:
Therefore, we need to limit the guessing to ### most probable passwords
*** Sentence 6706: Replace "together with" by "with" in:
A naive solution is to generate all possible password guesses together with their proba-bilities, sort them by probability, and select ### most probable ones
*** Sentence 6709: Replace "lead to" by "cause" or "enable" or "find" in:
When we perform a series of derivation steps from the start nonterminal, sooner or later, we get a sentential form where all possible derivation steps lead to passwords of the same probability
*** Sentence 6714: Replace "utilized" by "used" in:
Such a fact can be utilized to divide the guessing process into two separates steps
*** Sentence 6717: Replace "together with" by "with" in:
The easiest way is to generate all preterminal structures together with their probabilities, sort them in a probability order, and take a number of the most probable ones to generate password guesses
*** Sentence 6717: Replace "a number of" by "several" in:
The easiest way is to generate all preterminal structures together with their probabilities, sort them in a probability order, and take a number of the most probable ones to generate password guesses
*** Sentence 6719: Replace "a large amount of" by "much" in:
processing a large amount of input data before we can even create the first password
*** Sentence 6720: Replace "not possible" by "impossible" in:
Using this method, it is also not possible to generate preterminal structures and password guesses consequently
*** Sentence 6721: Replace "pre-defined" by "predefined" in:
Another approach is to use the technique proposed by Narayanan et al., where we only generate preterminal structures with probability values above a pre-defined limit
*** Sentence 6727: Replace "taking into consideration" by "considering" in:
Taking into consideration the sizes of derivation trees of PCFGs created from real password datasets, the number of required backtracking operations would be enormous
*** Sentence 6727: Replace "enormous" by "very large" in:
Taking into consideration the sizes of derivation trees of PCFGs created from real password datasets, the number of required backtracking operations would be enormous
*** Sentence 6733: Replace "a number of" by "several" in:
4.4.1 produces a number of rewrite rules represented by set #"

*** Sentence 6749: Delete "the existence of" and adjust following verb number in:
The existence of probability groups in grammars is the core assumption for the Next algorithm described in the following section
*** Sentence 6753: Delete "serves to" and change following verb to present singular tense and proper number in:
The queue serves to store the preterminal structures temporarily when they are processed
*** Sentence 6824: Replace "denotes" by "means" or "indicates" or "represents" in:
Concretely, it denotes that in the password guessing phase, the given nonterminal will be gradually modified by all rules from the given probability group (see Section 4.4.4)
*** Sentence 6825: Replace "illustrate" by "show" in:
For demonstration purposes, I will illustrate this by displaying terminals that can be substituted, e.g., instead of 4#"<-#3$$, we write 4 #" <-#" ####, #" ####" --$$
*** Sentence 6825: Replace "e.g.," by "for example," in:
For demonstration purposes, I will illustrate this by displaying terminals that can be substituted, e.g., instead of 4#"<-#3$$, we write 4 #" <-#" ####, #" ####" --$$
*** Sentence 6827: Replace "is illustrated" by "is shown" in:
The functionality of the Next function is illustrated by algorithm 8
*** Sentence 6828: Replace "denotes" by "means" or "indicates" or "represents" in:
The PT identi-fier denotes a preterminal structure
*** Sentence 6834: Replace "denotes" by "means" or "indicates" or "represents" in:
decrement(PT, i) creates a new preterminal structure from PT by applying a next (less probable) rewrite rule at position ###, or denotes the use of a next (less probable) probability group at position ###
*** Sentence 6834: Delete "the use of" if followed by a gerund or noun describing an action in:
decrement(PT, i) creates a new preterminal structure from PT by applying a next (less probable) rewrite rule at position ###, or denotes the use of a next (less probable) probability group at position ###
*** Sentence 6835: Replace "is illustrated" by "is shown" in:
The functionality of the Next algorithm is illustrated in an example
*** Sentence 6835: Replace "illustrated in" by "shown in" in:
The functionality of the Next algorithm is illustrated in an example
*** Sentence 6859: Replace "together with" by "with" in:
creates the most probable PT and pushes it to the priority queue together with its size and probability
*** Sentence 6862: Replace "illustrated in" by "shown in" in:
The example grammar contains two base structures, and thus after the initial phase, the priority queue contains two elements, as illustrated in Table 4.6
*** Sentence 6866: Replace "be performed" by "be done" in:
The rewriting to final passwords will be performed later by the generate_passwords() function
*** Sentence 6877: Replace "is illustrated" by "is shown" in:
The contents of the queue after this operation is illustrated by Table 4.7
*** Sentence 6878: Replace "two different" by "two" in:
Note, two different rewrite rules were applied to the base structures for nonterminals #"<-#1 and #" l2
*** Sentence 6879: Replace "used again" by "reused" in:
Since rules #"<-#1 5 and #"<-#1 6 have the same probability, the entire probability group was used again
*** Sentence 6971: Delete "there is" and insert "occurs" or "is" or a similar word later in:
And thus, for each string generated by the grammar, there is only one subset of the set of rewrite rules that produces it
*** Sentence 6971: Replace "the set of" by "the" if followed by a plural noun, and change a following verb to plural in:
And thus, for each string generated by the grammar, there is only one subset of the set of rewrite rules that produces it
*** Sentence 6974: Replace "enormously" by "very" in:
Despite the Next algorithm being feasible for creating preterminal structures, generating from more complex PCFGs has enormously high memory requirements
*** Sentence 6987: Replace "the reason why" by "why" or "that why" in:

The reason why the original Next function has high memory requirements is illustrated in an example
*** Sentence 6987: Replace "is illustrated" by "is shown" in:
The reason why the original Next function has high memory requirements is illustrated in an example
*** Sentence 6987: Replace "illustrated in" by "shown in" in:
The reason why the original Next function has high memory requirements is illustrated in an example
*** Sentence 6989: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
At each position, there are three possible replacements: 1, 2, and 3
*** Sentence 6997: Replace "enormously" by "very" in:
However, the problem is that the size of the priority queue grows enormously
*** Sentence 7015: Replace "illustrated in" by "shown in" in:
As illustrated in Figure 4.3, when the Next function pops node 1 from the priority queue, it generates nodes 2 and 3 from it and pushes both to the priority queue
*** Sentence 7017: Replace "illustrated in" by "shown in" in:
Then, the function creates node 4 and pushes it into the priority queue, because node 4 is node 2#'s child, as illustrated in Figure 4.2
*** Sentence 7061: Replace "is illustrated" by "is shown" in:
How it works is illustrated in Figure 4.4
*** Sentence 7061: Replace "illustrated in" by "shown in" in:
How it works is illustrated in Figure 4.4
*** Sentence 7067: Replace "does not have" by "lacks" in:
4) Only node (1,3,2) is pushed into the queue since it does not have any other parent with probability lower than 10 %
*** Sentence 7079: Replace "in contrast to" by "compared to" in:
In contrast to the Next function, the elements inside the probability queue do not have the pivot values
*** Sentence 7079: Replace "do not have the" by "lack the" in:
In contrast to the Next function, the elements inside the probability queue do not have the pivot values
*** Sentence 7104: Replace "amount of space" by "space" in:
We can see that the Deadbeat dad algorithm reduces the necessary amount of space dramatically in contrast to the original Next function
*** Sentence 7104: Replace "in contrast to" by "compared to" in:
We can see that the Deadbeat dad algorithm reduces the necessary amount of space dramatically in contrast to the original Next function
*** Sentence 7127: Replace "the existing methods" by "methods" in:
By analyzing the existing methods and the behavior of Weir#'s proof-of-concept PCFG Cracker on various leaked password datasets, I observed the following:
*** Sentence 7130: Replace "utilized" by "used" in:
Thus, the processor cores are not utilized well
*** Sentence 7131: Replace "a lot of" by "much" or "many" in:
Processing long base structures like #"<-#1#"<-#1#"<-#2#"<-#2#"<-#3#"<-#3#"<-#4#"<-#4#"<-#5#"<-#5 is computationally complex and wastes a lot of time even if their probabilities are insignificant
*** Sentence 7136: Replace "employing" by "using" in:
Without additional implementation, the only way of employing multiple nodes is to generate a password wordlist offline using Weir#'s tool, split it to smaller ones and use each to perform a dictionary attack on a particular computing node
*** Sentence 7136: Replace "a particular" by "a" or "an" in:
Without additional implementation, the only way of employing multiple nodes is to generate a password wordlist offline using Weir#'s tool, split it to smaller ones and use each to perform a dictionary attack on a particular computing node
*** Sentence 7137: Replace "a lot of" by "much" or "many" in:
Such a solution, however, requires a lot of user effort
*** Sentence 7146: Delete "the use of" if followed by a gerund or noun describing an action in:
Therefore, I propose an enhanced design that supports parallel and distributed (see Section 4.8) computing to improve the use of available resources

*** Sentence 7151: Delete "there was" and insert "occurred" or "was" or similar word later in:
However, there was still enough space for optimization
*** Sentence 7152: Replace "operations performed by" by "operations by" in:
Within all operations performed by the PCFG Manager, generating password guesses from preterminal structures [213, 211] was the most computationally complex part
*** Sentence 7153: Replace "since there is" by "with" in:
Since there is no mutual dependence between the preterminals, I decided to modify the program and parallelize this part of the process
*** Sentence 7153: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
Since there is no mutual dependence between the preterminals, I decided to modify the program and parallelize this part of the process
*** Sentence 7234: Replace "illustrate" by "show" in:
I illustrate both approaches by simplified schematics that display goroutines and data transfer operations
*** Sentence 7243: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Every time a preterminal is created, it is sent to the buffered channel if there is enough space
*** Sentence 7245: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
There is no need to generate more preterminals at the time they cannot be processed
*** Sentence 7245: Replace "at the time" by "then" in:
There is no need to generate more preterminals at the time they cannot be processed
*** Sentence 7246: Replace "in contrast to" by "compared to" in:
In contrast to the original version, the proposed design allows to process multiple preterminals and generate passwords in parallel if ### > 1
*** Sentence 7246: Replace "allows to" by "allows one to" or "allows them", etc. in:
In contrast to the original version, the proposed design allows to process multiple preterminals and generate passwords in parallel if ### > 1
*** Sentence 7248: Replace "supplementary" by "additional" in:
This behavior could be resolved by adding a supplementary synchronization mechanism at the output, however, at the cost of performance loss
*** Sentence 7251: Replace "slowed down" by "slowed" in:
Additional profiling, revealed that even though the parallelization accelerated generating terminal structures, the new bottleneck was at the output, where simple I/O text opera-tions slowed down the entire process
*** Sentence 7254: Replace "is illustrated" by "is shown" in:
The final design is illustrated in Figure 4.6(c) and the experimental results in Section 4.9.1
*** Sentence 7254: Replace "illustrated in" by "shown in" in:
The final design is illustrated in Figure 4.6(c) and the experimental results in Section 4.9.1
*** Sentence 7256: Replace "a high number of" by "many" in:
Grammars created from real datasets of passwords often have a high number of rewriting rules
*** Sentence 7258: Replace "many of the" by "many" if followed by a plural noun in:
If such a limit is specified, many of the rules are never used
*** Sentence 7260: Replace "obtain" by "get" in:
Therefore, in this section, I propose methods of grammar filtering that remove selected rules from the grammar to: a) make guessing faster, b) obtain a compact grammar that can be processed entirely without defining a #"hard limit#" for password guesses
*** Sentence 7263: Replace "the application of" by "applying" in:
Every edge stands for the application of a rewriting rule that transforms a parent node to a child node
*** Sentence 7264: Replace "in terms of" by "in" or "as" or "as to" or "using" in:
In terms of probabilistic password cracking, terminal structures are password candidates, and base structures (e.g., #"<-#4#"<-#2#" l1) are located on the second level of the tree
*** Sentence 7268: Replace "is being" by "is" when followed by a past participle in:
I analyzed the algorithm and observed that the most expensive task is to find every possible parent of every node which is being inserted into the priority queue
*** Sentence 7269: Replace "present" by "show" or "give" or "offer" if a transitive verb in:

In Weir#'s PCFG Manager, the task is resolved by a function called dd_is_my_parent that runs in it-erations whose count is potentially increased by every non-terminal present in the processed
*** Sentence 7272: Delete "the use of" if followed by a gerund or noun describing an action in:
This behavior bears on the use of probability groups described in Section 4.4.3
*** Sentence 7281: Replace "exponentially" by "at an accelerating rate" except if you mean the math function in:
One can see, the number of iterations grows almost exponentially each time #"<-#1 is added to the base structure
*** Sentence 7329: Replace "in most cases" by "usually" in:
Such structures usually have low probability values since they are in most cases created from randomly generated strings, not created by users
*** Sentence 7330: Replace "speeds up" by "speeds" in:
As I as-sume and experimentaly prove in Section 4.9.2, removing such structures from the grammar speeds up password generation several times and does not noticeably decrease success rate at cracking sessions
*** Sentence 7333: Replace "presented in" by "in" in:
The exact calculation of possible password guesses from a PCFG is a currently missing feature that is, however, essential for tools presented in this chapter
*** Sentence 7354: Replace "located in" by "in" in:
non-terminal #" i = #" c### (see Section 4.4) is, in most cases, the number of lines in n.txt file located in a directory for fragments of type #" c
*** Sentence 7362: Replace "modifications" by "changes" in:
To increase speed even more, I experimented with various modifications of already-trained grammars
*** Sentence 7366: Replace "was able to" by "could" in:
At this point, I was able to generate much more passwords per time unit
*** Sentence 7367: Replace "amount of time" by "time" in:
However, without a manually-defined limit for password guesses, the total amount of time required for generating was still extensive
*** Sentence 7368: Delete "there is" and insert "occurs" or "is" or a similar word later in:
From a practical perspective, any limit to guess count means that there is always a part of the grammar that is never used and unnecessarily wastes memory during the guess generation
*** Sentence 7376: Replace "not necessary" by "unnecessary" in:
From a practical standpoint, such a correction is not necessary since the implementation
*** Sentence 7378: Replace "to ensure that" by "so that" in:
The goal of the filtering is to make the output dictionary more compact and to ensure that generating passwords will end in an acceptable time
*** Sentence 7380: Replace "massive" by "large" in:
Nevertheless, the strongest motivation for grammar filtering is a potentially massive saving of processor time
*** Sentence 7382: Replace "denoted" by "meant" or "indicated" or "represented" in:
As denoted above, rules for alpha characters, digits, and special symbols usually have similar probabilities, thus removing them leads to a considerable loss of information which decreases the success rate
*** Sentence 7382: Replace "leads to" by "causes" or "enables" or "finds" in:
As denoted above, rules for alpha characters, digits, and special symbols usually have similar probabilities, thus removing them leads to a considerable loss of information which decreases the success rate
*** Sentence 7405: Replace "it is essential to" by "one must" in:
It is essential to state that the proposed PCFG reduction algorithm represents a naive solution created for experimental purposes
*** Sentence 7405: Replace "state that" by "say" if "state" is a verb in:
It is essential to state that the proposed PCFG reduction algorithm represents a naive solution created for experimental purposes
*** Sentence 7408: Replace "tool called" by "tool" in:
To experimentally evaluate the technique#'s benefits, I propose a proof-of-concept tool called the PCFG Mower 12 which can:

*** Sentence 7409: Replace "inform" by "tell" or "affect" in:
Calculate the total number of possible password guesses from a PCFG and inform the user about achievable keyspace
*** Sentence 7411: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
Filter a PCFG by performing an automatic removal of rewriting rules based on a set of options entered by the user
*** Sentence 7412: Replace "as an alternative to" by "as well as" in:
If the results show that such filtering brings advantages and can serve as an alternative to a password guess count limit, it is possible to use a more systematic way
*** Sentence 7416: Delete "a set of" if followed by a plural noun, and change a following verb to plural in:
For distributed cracking, I assume a network consisting of a server and a set of clients, as illustrated in Figure 4.7
*** Sentence 7416: Replace "illustrated in" by "shown in" in:
For distributed cracking, I assume a network consisting of a server and a set of clients, as illustrated in Figure 4.7
*** Sentence 7417: Replace "is responsible for" by "handles" or "causes" in:
The server is responsible for handling client requests and assigning work
*** Sentence 7418: Delete "one or more" in:
Clients represent the cracking stations equipped with one or more OpenCL-compatible devices like GPU, hardware coprocessors, etc. In the proposal, I talk about a client-server architecture since the clients are actively asking for work, whereas the server is offering a #"work assignment service.#"
*** Sentence 7418: Replace "etc." by "and so on" in:
Clients represent the cracking stations equipped with one or more OpenCL-compatible devices like GPU, hardware coprocessors, etc. In the proposal, I talk about a client-server architecture since the clients are actively asking for work, whereas the server is offering a #"work assignment service.#"
*** Sentence 7418: Replace "talk about" by "discuss" in:
Clients represent the cracking stations equipped with one or more OpenCL-compatible devices like GPU, hardware coprocessors, etc. In the proposal, I talk about a client-server architecture since the clients are actively asking for work, whereas the server is offering a #"work assignment service.#"
*** Sentence 7421: Replace "gpus" by "graphical processing units" in:
GPUs
*** Sentence 7423: Replace "referred to as" by "called" in:
In PCFG-based attacks, a probabilistic context-free grammar represents the source of all password guesses, also referred to as candidate passwords
*** Sentence 7424: Replace "known as" by "called" in:
Each guess represents a string generated by the grammar, also known as a terminal structure [213, 211]
*** Sentence 7425: Replace "need to" by "must" if "need" is a verb in:
In a distributed environment, we need to deliver the passwords to the cracking nodes somehow
*** Sentence 7436: Delete "one or more" in:
Each chunk produced by the server contains one or more preterminal structures, from which the clients generate the password guesses
*** Sentence 7441: Replace "i did" by "we did" in:
I chose hashcat as a cracking engine for the same reasons as I did for the Fitcrack distributed password cracking system [84], mainly because of its speed and range of supported hash formats
*** Sentence 7442: Replace "two different" by "two" in:
The proposed tool supports two different modes of operation:
*** Sentence 7452: Replace "similar to" by "like" in:
The behavior is similar to the function of Gouroutine M from the parallel version (see Section 4.6) - it generates PT and tailors workunits for client nodes
*** Sentence 7453: Delete "one or more" in:
Each workunit, called chunk, contains one or more PTs
*** Sentence 7454: Replace "api" by "applications programming interface" or "interface" in:
As shown in listing 4.1, the server provides clients an API consisting of four methods

*** Sentence 7455: Replace "api" by "applications programming interface" or "interface" in:
Listing 4.2 shows an overview of input/output messages that are transferred with the calls of API methods
*** Sentence 7462: Replace "api" by "applications programming interface" or "interface" in:
Listing 4.1: Server API
*** Sentence 7488: Replace "together with" by "with" in:
In cracking mode, the message contains a map (an associative array) of cracked hashes together with corresponding plaintext passwords
*** Sentence 7490: Replace "informs" by "tells" or "affects" in:
With the ResultResponse message, the server then informs the client, if the cracking is over or if the client should ask for a new chunk by calling the GetNextItems() method
*** Sentence 7493: Replace "is illustrated" by "is shown" in:
The flow of messages between the server and a client is illustrated in Figure 4.8
*** Sentence 7493: Replace "illustrated in" by "shown in" in:
The flow of messages between the server and a client is illustrated in Figure 4.8
*** Sentence 7500: Replace "performed by" by "done by" in:
Client information - for each connected client, the server maintains its IP ad-dress, current performance, the total number of password guesses performed by the client, and information about the last chunk that the client completed: its keyspace and timestamps describing when the processing started and ended
*** Sentence 7505: Replace "that have not been" by "not" if followed by a past participle in:
List of non-cracked hashes (cracking mode only) - the list contains all input hashes that have not been cracked yet
*** Sentence 7506: Replace "together with" by "with" in:
List of cracked hashes (cracking mode only) - The list contains all hashes that have already been cracked, together with corresponding passwords
*** Sentence 7508: Replace "via" by "by" in:
Next, it checks the desired mode of operation and other configuration options #--the complete description is available via the tool#'s help
*** Sentence 7514: Delete "there is" and insert "occurs" or "is" or a similar word later in:
The process continues as long as there is free space in the channel, and the grammar allows new PTs to be created
*** Sentence 7517: Replace "be used for" by "be for" in:
In the ConnectResponse message, the client receives the grammar that should be used for generating passwords guesses
*** Sentence 7518: Replace "illustrated in" by "shown in" in:
In cracking mode, the server also sends the hashlist and hash mode identifying the algorithm that should be used, as illustrated in Figure 4.8
*** Sentence 7523: Delete "one or more" in:
The the server pops one or more PTs from the buffered channel and sends them to the client as a new chunk
*** Sentence 7524: Replace "denote" by "mean" or "indicate" or "represent" in:
Besides, the server updates the client information structure to denote what chunk is currently assigned to the client
*** Sentence 7542: Replace "via" by "by" in:
Once a client submits a result via the SendResult() call, the server updates the infor-mation about the last completed chunk inside the client information structure
*** Sentence 7543: Replace "together with" by "with" in:
For each cracked hash, the server removes it from the list of non-cracked hashes and adds it to the list of cracked hashes together with the resulting password
*** Sentence 7546: Replace "in case" by "if" or "for when" in:
The same happens in the cracking mode in case there is a non-cracked hash
*** Sentence 7546: Delete "there is" and insert "occurs" or "is" or a similar word later in:
The same happens in the cracking mode in case there is a non-cracked hash
*** Sentence 7552: Replace "obtain" by "get" in:
Then it calls the GetNextItems() method to obtain a chunk assigned by the server

*** Sentence 7555: Replace "it is necessary to" by "one must" in:
For the cracking mode, it is necessary to have a compiled executable of hashcat on the client node
*** Sentence 7615: Replace "informs" by "tells" or "affects" in:
In the end, the client eventually informs the server about the chunk completion using the SendResult() call
*** Sentence 7630: Replace "employed" by "used" in:
All employed datasets are enlisted in table 4.9
*** Sentence 7634: Replace "illustrate" by "show" in:
The other columns illustrate how a PCFG trained on the dataset looks like
*** Sentence 7638: Replace "were performed" by "were done" in:
All three experiments were performed using a computer with Intel(R) Core(TM) i7-4700HQ CPU with 8 GB RAM
*** Sentence 7638: Replace "performed using" by "done by" in:
All three experiments were performed using a computer with Intel(R) Core(TM) i7-4700HQ CPU with 8 GB RAM
*** Sentence 7638: Replace "cpu" by "processor" in:
All three experiments were performed using a computer with Intel(R) Core(TM) i7-4700HQ CPU with 8 GB RAM
*** Sentence 7638: Replace "ram" by "memory" in:
All three experiments were performed using a computer with Intel(R) Core(TM) i7-4700HQ CPU with 8 GB RAM
*** Sentence 7791: Replace "presented in" by "in" in:
The re-sults prove that the concept presented in Section 4.6 is usable and works well
*** Sentence 7793: Replace "massive" by "large" in:
The experiment showed the chosen method brings a massive accel-eration on a multi-core CPU since all cores can be utilized
*** Sentence 7793: Replace "cpu" by "processor" in:
The experiment showed the chosen method brings a massive accel-eration on a multi-core CPU since all cores can be utilized
*** Sentence 7793: Replace "utilized" by "used" in:
The experiment showed the chosen method brings a massive accel-eration on a multi-core CPU since all cores can be utilized
*** Sentence 7794: Replace "helped to" by "helped" in:
What also helped to achieve higher performance was compilation into machine language instead of using an interpreter
*** Sentence 7802: Replace "were performed" by "were done" in:
The experiments were performed using Intel(R) Core(TM) i7-7700K CPU with 32 GB RAM and an SSD
*** Sentence 7802: Replace "performed using" by "done by" in:
The experiments were performed using Intel(R) Core(TM) i7-7700K CPU with 32 GB RAM and an SSD
*** Sentence 7802: Replace "cpu" by "processor" in:
The experiments were performed using Intel(R) Core(TM) i7-7700K CPU with 32 GB RAM and an SSD
*** Sentence 7802: Replace "ram" by "memory" in:
The experiments were performed using Intel(R) Core(TM) i7-7700K CPU with 32 GB RAM and an SSD
*** Sentence 7804: Replace "was used for" by "was for" in:
The first column (tr) shows which dataset was used for training to create the PCFG
*** Sentence 7808: Replace "is performed" by "is done" in:
The mow-n modification means that longbase is performed first and then the ################ of the PCFG reduction algorithm is ### passwords
*** Sentence 7811: Replace "illustrates" by "shows" in:
Since the algorithm removes selected rules, the table illustrates the changes done to the grammars in each step
*** Sentence 7815: Replace "inform" by "tell" or "affect" in:
Next columns inform about password guessing
*** Sentence 7816: Replace "amount of time" by "time" in:

We display the amount of time required to generate the output dictionary (time), (or 10###* if it reached the time 10-minute limit), the size of the output dictionary (out size) and the number of its passwords in millions (mop)
*** Sentence 7828: Replace "modifications" by "changes" in:
I use ASRI to analyze the influence of the modifications
*** Sentence 7831: Replace "massive" by "large" in:
As we can see from results, removing long base structures resulted in a massive increase of password guessing speed which enabled to generate much more passwords within 10 minutes
*** Sentence 7832: Replace "enormously" by "very" in:
The highest acceleration was achieved on dw and r65 since they contain very complex passwords that create enormously long base structures
*** Sentence 7836: Replace "led to" by "caused" or "enabled" or "found" in:
From 16 testings, only 8 led to decrease by a maximum of 0.06 %
*** Sentence 7843: Replace "achieved the best results" by "performed best" in:
Again, we achieved the best results with dw and r65 datasets, where we were able to reduce the size from 12 GB (longbase) to 112 MB dictionary, and from 25 GB to 130 MB with a loss of success rate below 4 % in all cases
*** Sentence 7843: Replace "were able to" by "could" in:
Again, we achieved the best results with dw and r65 datasets, where we were able to reduce the size from 12 GB (longbase) to 112 MB dictionary, and from 25 GB to 130 MB with a loss of success rate below 4 % in all cases
*** Sentence 7843: Replace "in all cases" by "always" in:
Again, we achieved the best results with dw and r65 datasets, where we were able to reduce the size from 12 GB (longbase) to 112 MB dictionary, and from 25 GB to 130 MB with a loss of success rate below 4 % in all cases
*** Sentence 7845: Replace "modifications" by "changes" in:
For dw, the mow-1000M and mow-500M modifications produced the same results since the grammar remained the same
*** Sentence 7846: Replace "a high number of" by "many" in:
The dw-trained grammar contains a high number of base structures with similar probabilities
*** Sentence 7847: Replace "a lot of" by "much" or "many" in:
Thus, a lot of them was removed by mow-1000M modification, and no further filtering was necessary
*** Sentence 7849: Replace "at the time of" by "at" or "during" in:
Long base structures originate at the time of grammar creation
*** Sentence 7850: Delete "the existence of" and adjust following verb number in:
Their presence is caused by the existence of complex passwords in the training dictionary
*** Sentence 8079: Replace "not possible" by "impossible" in:
With larger grammars, generating every possible password guess is not possible in an ac-ceptable time
*** Sentence 8080: Replace "needs to be" by "must be" or "should be" if "needs" is a verb in:
And thus, the guessing needs to be limited somehow
*** Sentence 8083: Replace "as an alternative to" by "as well as" in:
Despite the PCFG filtering algorithm be-ing heuristical and very simple, the experiments show that the filtering can serve as an alternative to classic guess or time limit
*** Sentence 8087: Replace "conduct" by "do" if a verb in:
I conduct a number of experiments in order to prove several points
*** Sentence 8087: Replace "a number of" by "several" in:
I conduct a number of experiments in order to prove several points
*** Sentence 8087: Replace "in order to" by "to" in:
I conduct a number of experiments in order to prove several points
*** Sentence 8088: Replace "usage" by "use" in:
First, I want to show the proposed solution results in a higher cracking performance and lower network usage
*** Sentence 8143: Replace "impact of" by "effect of" in:

I discuss the differences among different grammars and the impact of scrambling the chunks during the computation
*** Sentence 8149: Replace "ram" by "memory" in:
8GB RAM
*** Sentence 8150: Replace "local area network" by "local-area network" in:
The nodes are in a local area network connected with links of 10, 100, and 1000 Mbps bandwidth
*** Sentence 8153: Replace "a number of" by "several" in:
With this setup, I perform a number of cracking tasks on different hash types and grammars
*** Sentence 8157: Replace "enormous" by "very large" in:
One can also notice the enormous number of generated passwords, especially with the myspace grammar
*** Sentence 8170: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Apart from the proposed solution being generally faster, there is a significant difference in speeds with the lower network bandwidths
*** Sentence 8172: Replace "impact of" by "effect of" in:
The impact of the network bandwidth limit is expected as the naive terminal distribution requires a significant amount of data in the form of a dictionary to be transmitted
*** Sentence 8172: Replace "a significant amount of" by "much" or "significant" in:
The impact of the network bandwidth limit is expected as the naive terminal distribution requires a significant amount of data in the form of a dictionary to be transmitted
*** Sentence 8175: Replace "illustrates" by "shows" in:
Figure 4.16 illustrates the network activity using both solutions
*** Sentence 8177: Replace "all of the" by "all" or "all the" if followed by a plural noun in:
Both runs use almost all of the bandwidth for the entire experiment
*** Sentence 8178: Replace "larger amount of" by "more" in:
Nevertheless, we may see that cracking with the naive terminal distribution took much longer and required the transfer of more than a 14 times larger amount of data
*** Sentence 8183: Replace "multiple times" by "many times" in:
The average cracking speeds are multiple times lower than with SHA3
*** Sentence 8184: Replace "can not" by "cannot" in:
In this case, the two solutions do not differ because the transferred chunks have much lower keyspace since clients can not verify as many hashes as was possible for SHA3
*** Sentence 8185: Replace "most of the" by "most" if followed by a plural noun in:
Most of the experiment time is used by hashcat itself, cracking the hashes
*** Sentence 8187: Replace "leverage" by "use" in:
This happens since smaller tasks cannot fully leverage the whole distributed net-work as the smallest task took only several seconds to crack
*** Sentence 8189: Delete "there is" and insert "occurs" or "is" or a similar word later in:
While for the smallest task, there is almost no difference with the increasing node count, for the largest task, the speed rises even between 8 and 16 nodes
*** Sentence 8199: Replace "ram" by "memory" in:
Generating passwords from the Darkweb2017 (dw17) grammar is also very memory demanding because of the long base structures at the beginning of the grammar, and 8GB RAM is not enough for the largest cracking task using the naive solution
*** Sentence 8199: Replace "is not enough" by "is insufficient" in:
Generating passwords from the Darkweb2017 (dw17) grammar is also very memory demanding because of the long base structures at the beginning of the grammar, and 8GB RAM is not enough for the largest cracking task using the naive solution
*** Sentence 8200: Replace "encounter" by "meet" or "see" in:
With the proposed preterminal-based solution, we encounter no such problem
*** Sentence 8208: Replace "fulfilled" by "done" in:
The goal of generating and verifying ### most probable passwords is fulfilled
*** Sentence 8231: Replace "be helpful in" by "help for" in:

This fact confirms the hypothesis of Weir et al., who suggested preterminal distribution may be helpful in a distributed password cracking trial [213]
*** Sentence 8235: Replace "massive" by "large" in:
As the experiments show, the new parallel solution provides a massive speedup in the password guessing performance
*** Sentence 8236: Replace "in contrast to" by "compared to" in:
In contrast to the original tool, the new concept can efficiently utilize all available processors
*** Sentence 8236: Replace "utilize" by "use" in:
In contrast to the original tool, the new concept can efficiently utilize all available processors
*** Sentence 8242: Replace "there is no" by "no" and insert "occurs" or "is" or similar word later in:
Experiments showed processing these structures creates a bottleneck, in which case there is no advantage of using SSD over HDD
*** Sentence 8247: Replace "similar to" by "like" in:
If configured carefully, the success rate can remain similar to the original
*** Sentence 8249: Replace "does not have to" by "needs not" in:
The password guessing performance is much higher when the algorithm does not have to process complex sentential forms
*** Sentence 8250: Replace "not possible" by "impossible" in:
With larger grammars, gen-erating every possible password guess is not possible in an acceptable time
*** Sentence 8251: Replace "trivial" by "easy" or "simple" in:
Further filtering of rules is a working alternative to a hard guess limit.#" It is, however, arguable what rules are unnecessary.#" While my experiments with the trivial algorithm indicate a possible way, I suppose practical use would require more profound research to find more systematic techniques
*** Sentence 8257: Replace "gpu" by "graphical processing unit" in:
While the GPU computes cryptographic algorithms, the CPU takes care of generating new candidate passwords, and the TCP/IP stack communicates with the server
*** Sentence 8257: Replace "cpu" by "processor" in:
While the GPU computes cryptographic algorithms, the CPU takes care of generating new candidate passwords, and the TCP/IP stack communicates with the server
*** Sentence 8258: Replace "a lot of" by "much" or "many" in:
The experiments showed that the proposed preterminal distribution saves a lot of network bandwidth, achieves much higher cracking performance, and better scala-bility over the naive solution
*** Sentence 8263: Replace "need to" by "must" if "need" is a verb in:
The more password guesses we make, the more effort we need to put forth for their verification
*** Sentence 8267: Replace "dealing with" by "concerning" or "handling" or "encountering" in:
Dealing with bcrypt hashes, VeraCrypt-secured disks, or newer Microsoft Office documents using the Agile Encryption is an entirely different story
*** Sentence 8269: Delete "there are" and insert "occur" or "are possible" or a similar phrase later in:
Luckily, there are ways to accelerate the process, and in the thesis, I described some of them
*** Sentence 8273: Delete "a collection of" in:
Buying a collection of high-end graphics cards is the number one option for a long-term password cracking solution
*** Sentence 8274: Delete "there is" and insert "occurs" or "is" or a similar word later in:
Yet, there is always a limit to the performance we can achieve with a single computer
*** Sentence 8276: Replace "employ" by "use" in:
Therefore, I studied existing solutions for distributed processing and possible techniques to employ multiple nodes in a single cracking task
*** Sentence 8282: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
I also presented the pipeline processing of workunits that reduces the overhead of attacks
*** Sentence 8287: Replace "pre-defined" by "predefined" in:
The experiments showed the proposed strategies work as intended and that the system meets the pre-defined requirements
*** Sentence 8288: Replace "findings" by "results" in:

Moreover, the results bring valuable findings to the password cracking area
*** Sentence 8292: Replace "a high number of" by "many" in:
For instance, the brute-force and dictionary attacks have the same achievable performance on the complex BCrypt with a high number of iterations
*** Sentence 8293: Replace "gpu" by "graphical processing unit" in:
However, for MD5 or SHA-1, the brute-force is much more efficient since it generates passwords directly on GPU
*** Sentence 8294: Replace "need to" by "must" if "need" is a verb in:
Logically, the more we can pre-load to the GPU, the less we need to provide on-the-fly
*** Sentence 8295: Replace "need to" by "must" if "need" is a verb in:
Therefore, the combination attack is more efficient than the classic dictionary attack, where we need to feed the GPU with new passwords continually
*** Sentence 8295: Replace "gpu" by "graphical processing unit" in:
Therefore, the combination attack is more efficient than the classic dictionary attack, where we need to feed the GPU with new passwords continually
*** Sentence 8299: Replace "previous experience" by "experience" in:
I suggest Hashtopolis could be an excellent choice for advanced users who have previous experience with hashcat
*** Sentence 8300: Replace "a lot of" by "much" or "many" in:
It offers a lot of flexibility and allows the user to craft attack com-mands directly
*** Sentence 8302: Replace "a lot of" by "much" or "many" in:
It provides a high level of abstraction and a lot of automation
*** Sentence 8303: Replace "employs" by "uses" in:
For each attack mode, Fitcrack employs a unique strategy that is optimized and fine-tailored for this exact use-case
*** Sentence 8304: Replace "utilize" by "use" in:
If appropriately configured, the Fitcrack can utilize the resources more efficiently
*** Sentence 8311: Replace "have the potential to" by "can" in:
Probabilistic methods undisputedly have the potential to help with cracking human-created passwords
*** Sentence 8312: Replace "employed in" by "used in" or "in" in:
In the thesis, I mapped the history from the early time-memory trade-off attack by Martin Hellman, through Markovian models employed in hashcat and John the Ripper tools, to probabilistic context-free grammars (PCFG)
*** Sentence 8318: Replace "numerous" by "many" in:
Despite numerous improvements, including the Deadbeat dad algorithm, state-of-the-art solutions were hardly usable for real attacks due to the low performance and missing solution for a parallel or distributed cracking
*** Sentence 8318: Replace "state-of-the-art" by "recent" in:
Despite numerous improvements, including the Deadbeat dad algorithm, state-of-the-art solutions were hardly usable for real attacks due to the low performance and missing solution for a parallel or distributed cracking
*** Sentence 8321: Replace "utilizing" by "using" in:
A modification of the existing method allowed parallel processing and therefore utilizing all available processor cores efficiently
*** Sentence 8327: Replace "massive" by "large" in:
A series of experiments showed that the proposed improvements introduced a massive speedup in password guessing performance
*** Sentence 8328: Replace "the state-of-the-art" by "the latest" in:
While the state-of-the-art tools were strictly single-machine, the new distributed solution allows employing a larger network of multiple GPU-equipped nodes
*** Sentence 8328: Replace "employing" by "using" in:
While the state-of-the-art tools were strictly single-machine, the new distributed solution allows employing a larger network of multiple GPU-equipped nodes

*** Sentence 8329: Replace "newly-created" by "new" in:
The newly-created tools also serve as modules for Fitcrack#'s PCFG attack
*** Sentence 8334: Replace "employing" by "using" in:
An alternative is employing ASIC chips like in the 1990s EFF DES cracker or the Antminer for bitcoin mining with SHA-256
*** Sentence 8336: Replace "gpu" by "graphical processing unit" in:
In contrast, building a large grid or cluster of GPU nodes is rela-tively easy, and only a matter of funding
*** Sentence 8338: Replace "there is no need to" by "no need to" and insert "occurs" or similar phrase later in:
Besides, there is no need to #"brute-force everything#" when cracking user passwords
*** Sentence 8340: Replace "utilizing" by "using" in:
Password guessing with Markovian chains, PRINCE, and PCFG, are only a few examples of utilizing such knowledge
*** Sentence 8342: Replace "presented" by "shown" or "given" or "gave" or "offered" in:
I hope the presented work will inspire other researchers and developers in the future
*** Sentence 8345: Replace "findings" by "results" in:
It should be possible to create a cracking system that learns over time and uses the findings from previously completed tasks to improve attacks
*** Sentence 8346: Replace "incorporate" by "include" in:
Moreover, Fitcrack may incorporate a subsystem for rainbow table attack, at least for most common algorithms like MD5, SHA1, or NTLM
*** Sentence 8348: Replace "in case of" by "for" or "for when" in:
In case of a match, it can crack the password almost immediately
*** Sentence 8349: Replace "in case" by "if" or "for when" in:
In case a company utilizes multiple Fitcrack servers, one might create an interface that allows for mutual synchronization, e.g., sharing the cache of cracked passwords, dictionaries, Markovian statistics, grammars, and others
*** Sentence 8349: Replace "utilizes" by "uses" in:
In case a company utilizes multiple Fitcrack servers, one might create an interface that allows for mutual synchronization, e.g., sharing the cache of cracked passwords, dictionaries, Markovian statistics, grammars, and others
*** Sentence 8349: Replace "that allows for" by "for" in:
In case a company utilizes multiple Fitcrack servers, one might create an interface that allows for mutual synchronization, e.g., sharing the cache of cracked passwords, dictionaries, Markovian statistics, grammars, and others
*** Sentence 8349: Replace "e.g.," by "for example," in:
In case a company utilizes multiple Fitcrack servers, one might create an interface that allows for mutual synchronization, e.g., sharing the cache of cracked passwords, dictionaries, Markovian statistics, grammars, and others
*** Sentence 8351: Delete "there is" and insert "occurs" or "is" or a similar word later in:
However, there is still space for improvements
*** Sentence 8353: Replace "e.g.," by "for example," in:
Users often create pass-words from multiple words that follow each other without any separator, e.g., #"Ilikeapples#" that would be handled as a whole
*** Sentence 8356: Replace "extremely" by "very" in:
Last but not least, current proba-bilistic methods are extremely powerful but mostly focus on the syntax of the password
*** Sentence 8357: Replace "extremely" by "very" in:
Semantical-based approaches are extremely rare and could be a subject of future research
Possible acronym to expand: FAKULTA
Possible acronym to expand: HESEL
Possible acronym to expand: RADEK
Possible acronym to expand: AUTOR

Possible acronym to expand: KOLITEL
Possible acronym to expand: SU
Possible acronym to expand: VG
Possible acronym to expand: ICT
Possible acronym to expand: NPU
Possible acronym to expand: LQ
Possible acronym to expand: GECOS
Possible acronym to expand: WRDPASS
Possible acronym to expand: LTPASS
Possible acronym to expand: PXPASS
Possible acronym to expand: WDPASS
Possible acronym to expand: XLSPASS
Possible acronym to expand: ASIC
Possible acronym to expand: ISHASHGPU
Possible acronym to expand: WF
Possible acronym to expand: PBKF
Possible acronym to expand: GPL
Possible acronym to expand: JTRDLL
Possible acronym to expand: FPGA
Possible acronym to expand: DSP
Possible acronym to expand: DDR
Possible acronym to expand: ASUS
Possible acronym to expand: IOSPACE
Possible acronym to expand: PCI
Possible acronym to expand: SXM
Possible acronym to expand: EVGA
Possible acronym to expand: RTX
Possible acronym to expand: UID
Possible acronym to expand: PS
Possible acronym to expand: MPICH
Possible acronym to expand: SHOC
Possible acronym to expand: CLI
Possible acronym to expand: GUI
Possible acronym to expand: SDK
Possible acronym to expand: RPC
Possible acronym to expand: CGI
Possible acronym to expand: NGINX
Possible acronym to expand: LZMA
Possible acronym to expand: TB
Possible acronym to expand: UUUUU
Possible acronym to expand: ULLLL
Possible acronym to expand: UULLL
Possible acronym to expand: ULULU
Possible acronym to expand: FIFO
Note: Present participles and gerunds usually end in "ing", past participles in "ed".