

Review: Verifying Constant-Time Implementations

Mahyar Emami, Rishabh Iyer, Sahand Kashani
firstname.lastname@epfl.ch

November 11, 2021

1 Introduction

Say a few general words about the general context of the paper you chose. Explain why the topic is of interest, or where it can be applied. If it is about a piece of software or artifact, give a description of it. State the main result of the paper and why it is new or how it improves on previous state of knowledge. You can cite references using, for example [1] and make a succinct presentation of the organisation of your report.

2 Preliminaries

State the technical details that are necessary to understand the paper. It is generally a collection of definitions, concepts and notations with potentially a few preliminary results. It can be, for example the mathematical framework in which the topic of your paper is expressed. In particular, fix the notation you will be using for your review.

3 Body

Explain the paper, in your own words. Don't go into as many details as the original text, but the person reading your review should have a general understanding of the paper's results and how those results can be obtained. The structure and content of this section of course heavily depends on the paper itself. Don't hesitate to split it in multiple sections or subsections, for example:

3.1 An algorithm for whatever problem we try to solve

If your paper contains theorems, sketch the proofs of important theorems.

3.2 Benchmarks

If it contains benchmarks, show the key scores or results.

You can follow the structure of the paper you're reviewing, but write with your own words.

4 Conclusion

Recall briefly what the paper achieves, and how it is new. Express your critical skill on the paper and explain what you think are the strong and weak points of the paper. Also tell how you could potentially use the paper's results in your future project. You can also suggest further work or extensions to the paper.

References

- [1] Bibliography management in LaTeX.
https://overleaf.com/learn/latex/Bibliography_management_in_LaTeX.