UNIVERSITY NAME

DOCTORAL THESIS

Practical zk-SNARKS

Author:
Uroš Tešić

Supervisor:
Prof. Dr. Srđan Čapkun
SMITH

A thesis submitted in fulfillment of the requirements
for the degree of MSc in Computer Science

in the

System Security Group
D-INFK

March 5, 2019

Declaration of Authorship

I, Uroš Tešić, declare that this thesis titled, "Practical zk-SNARKS" and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed:

Date:

"Thanks to my solid academic training, today I can write hundreds of words on virtually any topic without possessing a shred of information, which is how I got a good job in journalism."

Dave Barry

UNIVERSITY NAME

Abstract

Faculty Name
D-INFK

MSc in Computer Science

Practical zk-SNARKS

by Uroš Tešić

The Thesis Abstract is written here (and usually kept to just this page). The page is kept centered vertically so can expand into the blank space above the title too...

Acknowledgements

The acknowledgments and the people to thank go here, don't forget to include your project advisor...

Contents

List of Figures

List of Tables

List of Abbreviations

LAH	**L**ist **A**bbreviations **H**ere
WSF	**W**hat (it) **S**tands **F**or

Physical Constants

Speed of Light $c_0 = 2.997\,924\,58 \times 10^8\,\mathrm{m\,s^{-1}}$ (exact)

List of Symbols

a	distance	m
P	power	W ($\mathrm{J\,s^{-1}}$)
ω	angular frequency	rad

For/Dedicated to/To my…

Chapter 1

Introduction

One of the biggest events in computer science in the last decade was the invention of Bitcoin. On the surface, Bitcoin offers perfect anonymity. Users can generate an arbitrary number of new addresses. Many parties also offer tumblers that transfer Bitcoin through thousands of different accounts and send laundered funds to the user (for a small fee). However, data in the blockchain is public. Transaction history can be combined with out-of-blockchain data to de-anonymize users of Bitcoin. Further graph analysis can be used to defeat tumblers as well.

ZCash is a fork of Bitcoin that tries to address this issue. It contains two types of addresses - transparent (t-addr) and shielded (z-addr). Transparent addresses behave like Bitcoin addresses - all transaction history (identities and amounts) are public. Shielded addresses encrypt this data to prevent leaks - the transactions reveal nothing about its users, or the amounts transferred. For transparent addresses, miners can easily check if the transaction is valid (eg. the account has enough money) by iterating through the previous transactions in the blockchain. For shielded addresses this isnt́ possible, so the party creating the transaction needs to provide one more piece of information - a zero-knowledge proof that the transaction is valid.

It isn't enough for a proving system to be zero-knowledge to be used in practice. It needs to be small because it will be stored in the blockchain. Furthermore, miners need to verify every transaction before they add it to the block, so it must be non-interactive and fast to verify. ZCash uses zk-SNARKS for this purpose, but these properties come at a cost - proof generation is extremely slow. Because of this many wallets don't support shielded transactions. Considering that many users have Bitcoin wallets on their phones, which are relatively weak, this is preventing more widespread use of zCash.

In this thesis we take a look at using graphics cards, present on many devices today, to accelerate zk-SNARKs. In order to make our solution cover as many platforms as possible (including mobile phones), we port performance critical code (scalar multi-exponentiation over curve BLS12-381) to OpenCL. We compare the differences, as well as difficulties in running cross-platform OpenCL code. We benchmark different algorithms for multi-exponentiation on different devices (Intel, NVIDIA and ARM), and compare the results.

The remainder of the thesis is organized as follows. The background and related research are presented in **??**. In **??**, we explain the anatomy of zCash and zk-SNARKs. **??** covers the architecture of OpenCL. Implementation details of different algorithms are covered in **??**. The benchmarking results, as well as their analyses, are presented in **??**.

Appendix A

Frequently Asked Questions

A.1 How do I change the colors of links?

The color of links can be changed to your liking using:

`\hypersetup{urlcolor=red}`, or
`\hypersetup{citecolor=green}`, or
`\hypersetup{allcolor=blue}`.

If you want to completely hide the links, you can use:

`\hypersetup{allcolors=.}`, or even better:
`\hypersetup{hidelinks}`.

If you want to have obvious links in the PDF but not the printed text, use:

`\hypersetup{colorlinks=false}`.