Zero-Knowledge Proof for attack prevention in the Ethereum Blockchain

Anders Malta Jakobsen
dept. of Computer Science
AAU
Aalborg, Denmark
amja23@student.aau.dk

Oliver Holmgaard
dept. of Computer Science
AAU
Aalborg, Denmark
oholmg20@student.aau.dk

***Abstract*—This is a placeholder abstract test. The whole template is used in semester projects at Aalborg University (AAU).**

I. Introduction

In this section we present some introductory ways to use the tools within LaTeX in general, and this template in particular. For example, this is a citation [1], while this is a multi-citation[1, 2].

The column width of the IEEE template is 3.5 inches, so if you generate your plots with this width or less, the output will be the best. For example, Listing 1 contains the code to generate the image in Figure 1 using Python with matplotlib, and exported as pgf (TeX).

```
import matplotlib.pyplot as plt

plt.rcParams.update({
    "pgf.texsystem": "pdflatex",
    "font.family": "serif",  # use serif/main font for text elements
    "pgf.preamble": "\n".join([
         r"\usepackage[utf8x]{inputenc}",
         r"\usepackage[T1]{fontenc}",
    ]),
})

fig, ax = plt.subplots(figsize=(3.5, 3.5))

ax.plot(range(5))
ax.text(0.5, 3., "serif")
ax.text(0.5, 2., "monospace")
ax.text(2.5, 2., "sans-serif")
ax.set_xlabel(r"µ is not $\mu$")

fig.tight_layout(pad=.5)
fig.savefig("graph.pgf")
```

Listing 1. Code to generate the graph.pgf

A. Tables and Figures

B. Algorithms, Theorems, and Proofs

There are a few different things outside the normal figure and table floats that are very relevant when writing a scientific paper or article. For example, you may wish to typeset theorems as in Theorem 1.

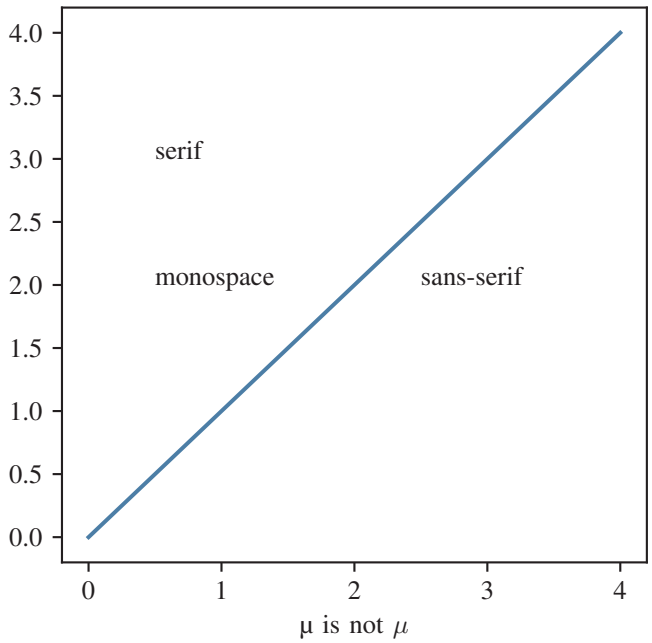

Fig. 1. An example graph drawn using Python's matplotlib library.

Theorem 1 (Pythagorean theorem)**.** *This is a theorem about right triangles and can be summarized in the next equation*

$$x^2 + y^2 = z^2$$

Or ref like Theorem 1 Similarly, for proofs:

Proof. To prove it by contradiction try and assume that the statement is false, proceed from there and at some point you will arrive to a contradiction. □

Note that proofs are not a numbered environment, and as such can't be referenced by default.

TABLE I
EXAMPLE OF A PRETTY, TWOCOLUMN TABLE.

	Klasser				
Hændelser	Reservation	Gæst	Borgerforening	Kalender	Betaling
Anmodet	✓	✓	✓		
Godkendt	✓		✓		
Afvist	✓		✓		
Redigeret	✓	✓	✓		
Annulleret	✓	✓	✓		✓
Betalt					✓
Refunderet					✓
Kvitteret		✓	✓		
Registreret	✓			✓	
Påmindet		✓	✓		

INSERTION-SORT(A, n)

```
1  for i = 2 to n
2      key = A[i]
3      // Insert A[i] into the sorted subarray A[1 : i − 1].
4      j = i − 1
5      while j > 0 and A[j] > key
6          A[j + 1] = A[j]
7          j = j − 1
8      A[j + 1] = key
```

Algorithm 1: Test

II. BACKGROUND

In this section we will go through some of the concepts that will be used in the rest of the paper as well as some surrounding context like attacks performed.

A. Ethereum and Proof of Stake

Ethereum is a blockchain platform that allows developers to create decentralized applications using smart contracts. Previously opperating with a Proof of Work (PoW) consensus algorithm, Ethereum transitioned to a Proof of Stake (POS) consensus algorithm in 2022. This transition was done to reduce the energy consumption of the network and to increase the scalability of the network. The transition was done in a series of upgrades called the Ethereum 2.0 upgrade. POS works by selecting validators to create new blocks based on the amount of cryptocurrency they have staked.

B. Zero-Knowledge Proofs

A Zero-Knowledge Proof (ZKP) is a cryptographic method that allows one party to prove to another party that something is ture without revealing any information.

Two of the subcategories of ZKPs are Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (ZK-SNARK) and Zero-Knowledge Scalable Transparent Argument of Knowledge (ZK-STARK). ZK-SNARK is the more common and of the two. It uses elliptic curve cryptography to create proofs based on the assumption that it is hard to find the discrete logarithm form the publicly known base point. ZK-SNARK has a start-up ritual which requires a trusted setup by all parties involved that the original proving key is destroyed as to not be able to create fake proofs. A criticism of ZK-SNARK is that it is not quantum resistant because of the reliance on elliptic curve cryptography.

ZK-STARK on the other hand is a newer and more complex ZKP. Despite not having non-interactive in its name, ZK-STARK is also non-interactive. Different form ZK-SNARK, ZK-STARK uses hashing functions to create proofs instead of elliptic curves. This method is post-quantum secure and does not require a trusted setup. It does however come with a higher computational cost and is not as widely used and dokumented as ZK-SNARK.

III. RELATED WORK

This is the Related Work section.

ACRONYMS

AAU Aalborg University. 1

POS Proof of Stake. 2
PoW Proof of Work. 2

ZK-SNARK Zero-Knowledge Succinct Non-Interactive Argument of Knowledge. 2
ZK-STARK Zero-Knowledge Scalable Transparent Argument of Knowledge. 2
ZKP Zero-Knowledge Proof. 2

REFERENCES

[1] M. Goossens, F. Mittelbach, and A. Samarin, *The LaTeX Companion*. Reading, Massachusetts: Addison-Wesley, 1993.

[2] G. D. Greenwade, "The Comprehensive Tex Archive Network (CTAN)," *TUGBoat*, vol. 14, no. 3, pp. 342–351, 1993.

APPENDIX A
COMPILING IN DRAFT

You can also compile the document in draft mode. This shows todos, and increases the space between lines to make space for your supervisors feedback.