SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNICAL UNIVERSITY OF MUNICH

Bachelor's Thesis in Informatics

Formalizing the Kate-Zaverucha-Goldberg Polynomial Commitment Scheme

Tobias Rothmann

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNICAL UNIVERSITY OF MUNICH

Bachelor's Thesis in Informatics

Formalizing the Kate-Zaverucha-Goldberg Polynomial Commitment Scheme

Eine Formalisierung des Kate-Zaverucha-Goldberg Polynomiellen Commitment Verfahrens

Author:	Tobias Rothmann
Supervisor:	Prof. Tobias Nipkow
Advisor:	Katharina Kreuzer
Submission Date:	April 15, 2024

I confirm that this bachelor's thesis is my own work and I have documented all sources and material used.

Munich, April 15, 2024 Tobias Rothmann

Acknowledgments

Abstract

Contents

1 Introduction

1.1 Section

Citation test [Lam94] [Lan02].

Acronyms must be added in `main.tex` and are referenced using macros. The first occurrence is automatically replaced with the long version of the acronym, while all subsequent usages use the abbreviation.

E.g. `\ac{TUM}, \ac{TUM}` ⇒ Technical University of Munich (TUM), TUM

For more details, see the documentation of the `acronym` package[1].

1.1.1 Subsection

See Table 1.1, Figure 1.1, Figure 1.2, Figure 1.3.

Table 1.1: An example for a simple table.

A	B	C	D
1	2	1	2
2	3	2	3

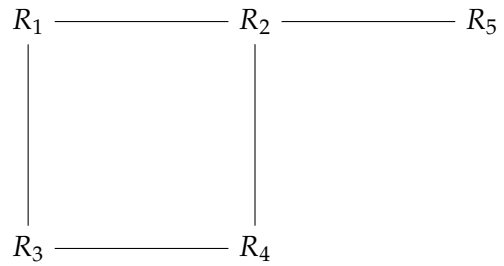

Figure 1.1: An example for a simple drawing.

[1] `https://ctan.org/pkg/acronym`

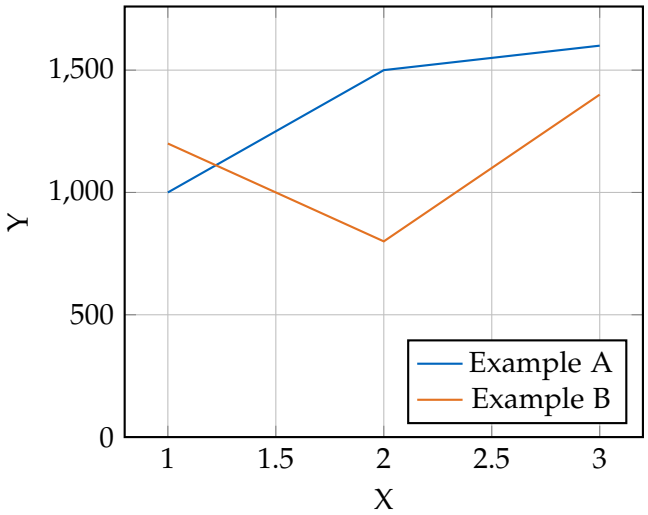

Figure 1.2: An example for a simple plot.

```
SELECT * FROM tbl WHERE tbl.str = "str"
```

Figure 1.3: An example for a source code listing.

2 related work

3 Prelimiaries

3.1 Mathematical Prelimiaries

In this section we introduce the notation used through out the paper, and capture the most important prerequisits in definitions.

We let p and q denote prime numbers if not explicitly stated otherwise. Groups are written in a multiplicate manner with the $\cdot$ operator and the abbreviation ab for $a \cdot b$. Furthermore we use the notation $\mathbb{Z}_p$ for a finite field of prime order p (note that the integers modulo p are isomorph to a finite field of prime order p [Lan02]).

Abbreviations

TUM Technical University of Munich

List of Figures

List of Tables

Bibliography

[Lam94] L. Lamport. *LaTeX : A Documentation Preparation System User's Guide and Reference Manual*. Addison-Wesley Professional, 1994.

[Lan02] S. Lang. *Algebra*. Vol. 3. Springer New York, NY, 2002.