SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

# Thesis title

Andreas Korb

SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY — INFORMATICS

TECHNISCHE UNIVERSITÄT MÜNCHEN

Master's Thesis in Informatics

# Thesis title

# Titel der Abschlussarbeit

| | |
|---|---|
| Author: | Andreas Korb |
| Supervisor: | Prof. Claudia Eckert |
| Advisor: | Albert Stark |
| Submission Date: | 15.11.2023 |

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

Munich, 15.11.2023 Andreas Korb

# Acknowledgments

# Abstract

# Contents

# 1 Introduction

## 1.1 Section

Citation test [Lam94].

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 |

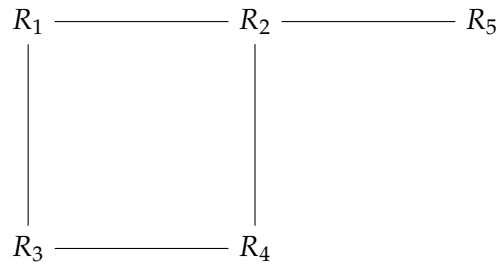


Figure 1.1: An example for a simple drawing.

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

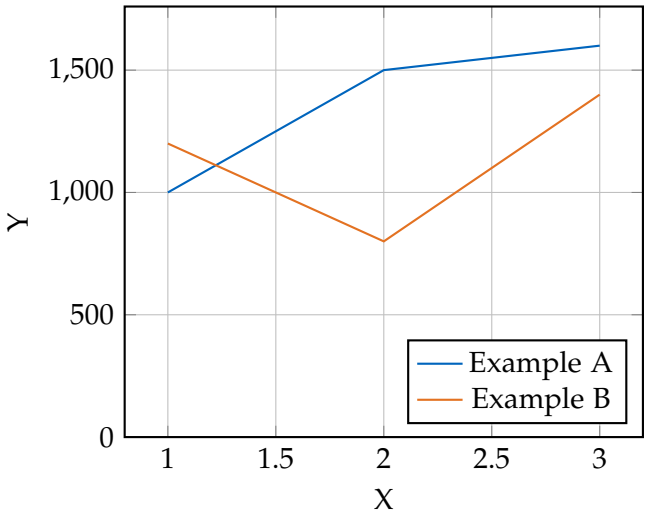


Figure 1.2: An example for a simple plot.

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

Figure 1.3: An example for a source code listing.

# 2 Background

## 2.1 Trusted execution environment

## 2.2 Trusted Platform Module

### 2.2.1 dTPM

### 2.2.2 vTPM

### 2.2.3 fTPM

## 2.3 Attestation

### 2.3.1 Local attestation

### 2.3.2 Remote attestation

# 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.