University of Passau
Faculty of Computer Science and Mathematics

Chair of Computer Networks & Communications
Prof. Dr.-Ing. Hermann de Meer

Master Thesis

Pairings in Cryptography

Max W. Musterfrau

Date:	xx/xx/20xx
Supervisors:	Prof. Dr.-Ing. Hermann de Meer Prof. Dr. Franziska Mustermann Karl Müller, M. Sc.

Erklärung zur Master Thesis

→ *PLEASE choose either german or english!*

Name, Vorname des Studierenden/Name, first name of student: Musterfrau, Max W.

Universität/University Passau,
Fakultät für Informatik und Mathematik/Faculty of Computer Science and Mathematics

Hiermit erkläre ich, dass ich die Arbeit selbstständig verfasst, noch nicht anderweitig für Prüfungszwecke vorgelegt, keine anderen als die angegebenen Quellen oder Hilfsmittel benutzt, sowie wörtliche und sinngemäße Zitate auch als solche gekennzeichnet habe.

I hereby declare that I have written the present thesis independently, without assistance from external parties and without use of other resources than those indicated. The ideas taken directly or indirectly from external sources (including electronic sources) are duly acknowledged in the text. The material, either in full or in part, has not been previously submitted for grading at this or any other academic institution.

....
(Datum/Date) (Unterschrift des Studierenden/Signature of Student)

Supervisor Contacts:

Prof. Dr.-Ing. Hermann de Meer
Chair of Computer Networks & Communications
Universität Passau
E-Mail: demeer@fim.uni-passau.de
Web: http://www.net.fim.uni-passau.de/

Prof. Dr. Franziska Mustermann
Chair of XYZ
Universität Passau
E-Mail: xxx@fim.uni-passau.de
Web: http://www.xxx.fim.uni-passau.de/

Karl Müller, M. Sc.
Chair of Computer Networks & Communications
Universität Passau
E-Mail: xxx@fim.uni-passau.de
Web: http://www.xxx.fim.uni-passau.de/

Abstract

Kurze (ca. 1 Seite) Übersicht über die Problemstellung und das Thema der Arbeit.

Short (about 1 page) overview of the topic.

Inhaltsverzeichnis

1. Einleitung

Die Einleitung soll zum eigentlichen Themengebiet hinführen und die Motivation für die Arbeit liefern. Am Schluss der Einleitung wird weiterhin noch eine Übersicht über die restliche Arbeit gegeben. “Die Arbeit ist wie folgt gegliedert: Kapitel 3 beschreibt xy, Kapitel z zeigt die Ergebnisse etc.”

The introduction leads to the actual subject area and describes the Motivation for the work. At the end of the introduction, an overview of the thesis’ structure is provided. “The remainder of the work is as follows: Chapter 3 describes xy, Chapter z shows the results etc.”

2. Background

Je nachdem wie sehr das Thema in die Tiefe geht, kann es notwendig sein, Hintergrundwissen hier zu beschreiben. Kann auch als Unterkapitel der Einleitung gestaltet werden.

Depending on how complex your topic is, it could be necessary to explain background information here. This chapter can also be a section in the introduction.

3. Ein Kapitel des Hauptteils

3.1. Inhalte

Im Hauptteil werden aufbauend die Vorgehensweise zur Problemlösung und Ergebnisse der Arbeit im Detail vorgestellt. Dazu kann der Hauptteil in verschiedene Abschnitte (section) oder sogar in mehrere Kapitel (chapter) unterteilt werden.

Einleitung und Hauptteil sollen eine in sich geschlossene Abhandlung darstellen. Der Leser der Arbeit soll ohne zusätzliche Literatur in der Lage sein, die Arbeit im Zusammenhang zu verstehen. Gutes wissenschaftliches Arbeiten (Referenzen angeben, konkrete Sprache etc.) ist ein Muss!

Grob könnte ein Aufbau so aussehen:

- Problembeschreibung
- Annahmen: Dieser Abschnitt ist sehr wichtig! Hier beschreibt ihr die Grenzen und Annahmen die ihr trefft, damit euer Ansatz funktioniert
- Simulationsaufbau/Problemlösung
- Ergebnisse: Schaubilder, Grafiken, Tabellen etc.
- Evaluation: Was bedeuten die konkreten Ergebnisse?
- Ggf. Diskussion der Ergebnisse: Warum diese Werte und nicht andere? War euer Aufbau valide? Was könnte verbessert werden?

3.2. Goldene 6 $\times$ C - Regel

Da Verfassen von wissenschaftlichen Arbeiten ein wichtiger Teil an der Universität ist, folgt bitte den goldenen 6 x C Regeln:

1. Clarity (Klarheit)
2. Correctness (Korrektheit)
3. Conciseness (Prägnanz)
4. Consistency (Konsistenz)

5. Connectedness (Verbindung)
6. Completeness (Vollständigkeit)

Die 6Cs werden bei allen akademischen Texten wie Papern, Doktorarbeiten, Seminararbeiten, Bachelor-und Masterarbeiten angewendet. Bitte haltet euch an diese Regeln und übt diese.

3.3. Struktur des Dokuments

Die Arbeit sollte wie folgt strukturiert sein:

1. Abstract / Kurzfassung
2. Einleitung
   Hier wird ein Überblick über die Arbeit gegeben und das Projekt/Problem beschrieben
3. (Verwandte Arbeiten)
4. Hauptteil (gegliedert in mehrere Kapitel oder Abschnitte)
5. Verwandte Arbeiten (Related Work)
6. Zusammenfassung, Bewertung und Ausblick
7. Referenzen / Literatur

Alle Abbildungen in der Arbeiten müssen einen **Titel und eine Legende/Achsenbeschriftung** haben! Alle Abbildungen und Gleichungen müssen nummeriert sein, genauso wie Abschnitte, Unterabschnitte und Kapitel.

Referenzen zu Abbildungen, Gleichungen, Abschnitten etc. müssen explizit geschehen, also mit direkten Verweisen anstatt ein unkonkreter Beschreibung.

3.4. Einreichen

Bitte folgt den Informationen auf dieser Seite `http://www.net.fim.uni-passau.de/hints`.

Bitte sprecht vorher mit eurem Betreuer ob ihr alle Anforderungen verstanden habt. Vor der Abgabe muss verifiziert werden, dass alle Kopien unterschrieben sind und die elektronische Fassung aktuell ist.

3.4.1. Archivierung

Für die Archivierung sind alle Dateien der Arbeit (auch der Vorträge) dem Betreuer zur Verfügung zu stellen. Weiterhin soll noch ein BibTeX-Eintrag der Arbeit erstellt werden (die Felder in eckigen Klammern sind dabei auszufüllen):

```
@MastersThesis{<Nachname des Autors><Jahr>,
type =          {<Bachelor- oder Masterarbeit>},
title =         {{<Thema der Arbeit>}},
school =        {Institute of Communication Networks~(LKN),
Munich University of Technology~(TUM)},
author =        {<Nachname des Autors>, <Vorname des Autors>},
annote =        {<Nachname des Betreuers>, <Vorname des Betreuers>},
month =         {<Monat>},
year =          {<Jahr>},
key =           {<Mehrere Suchschlüssel>}
}
```

4. A Chapter of the main part

In the main part, the procedure how the problem was solved and the obtained results of the work are presented in detail. For this purpose, the main part can be divided into different sections or even into several chapters.

Introduction and main part must be written in a conclusive and coherent way. The reader of the work should be able to read and understand the thesis without additional literature. Good scientific work (giving references, concrete language etc.) is a must!

Roughly, a structure can be:

- Problem description
- Assumptions: This section is very important! Here, the limits and assumptions are described which are used for your approach
- Simulationsetup/how to solve the problem
- Results: Figures, Tables etc.
- Evaluation: What do the results mean?
- Discussion of results: Why those values? Was your setup valid? What could be improved?

4.1. Golden 6 $\times$ C - Rule

Since your are all getting more and more involved into writing, please follow strictly the golden rule of 6 x C :

This should be explained to you by your supervisor and is about how to choose your arguments carefully.

1. Clarity
2. Correctness
3. Conciseness
4. Consistency

5. Connectedness
6. Completeness

The 6Cs apply to all academic texts alike: Papers, PhD theses, Diploma theses, reports etc. So please practice yourself and teach the students you are supervising these golden rules as well.

4.2. Document Structure

The project thesis has to be structured according the following standard:

1. Abstract
2. Introduction
   This should include an overview of the thesis / project description (what is explained in which section/chapter)
3. (Verwandte Arbeiten)
4. Main body of work description, divided in several sections/chapters
5. Related Work
6. Conclusions and Future Work
7. References

All figures in project descriptions / theses must have a **title and a legend/description of axes!** All figures and equations must be numbered, as well as sections (reports), subsections and chapters (books). Please provide also a short description of the message of the figures/tables etc.

References to any object (figures, equations, sections etc.) must be done explicitly, that is, with pointers, rather than by means of loose connections as in shown above. That should be avoided all together.

4.3. Submittal Form

Please follow the current information provided online at `http://www.net.fim.uni-passau.de/hints`.

Please check with our supervisor beforehand to ensure you understand all the requirements. Before hand-in, verify that all copies have been signed and that the electronic version is up-to-date.

4.3.1. Archive

For the archive, all files of the work (also presentations) should be made available for the supervisor. Furthermore, a BibTeX-entry of the thesis should be created (fill in the fields in square brackets):

```
@MastersThesis{<Last name of the author><year>,
type =          {<Bachelor-/ or Master Thesis>},
title =         {{<Topic of the thesis>}},
school =        {Institute of Communication Networks~(LKN),
Munich University of Technology~(TUM)},
author =        {<last name of author>, <first name of author>},
annote =        {<last name of supervisor>, <first name of supervisor>},
month =         {<Month>},
year =          {<Year>},
key =           {<Several key words>}
}
```

5. How To in Deutsch

For english version, see below.

Hier kann beschrieben werden, wie man das Problem gelöst hat und alle Schritte auf dem Weg zum Ergebnis.

5.1. How To: Wie man eine Abschlussarbeit schreibt

In diesem Abschnitt werden einige hilfreiche Tipps und Tricks für das Schreiben und im Umgang mit Latex vorgestellt. Für Überschriften kann man einheitliches "Titlecase" verwenden.

5.2. Latex-Umgebung

Fast jeder Texteditor eignet sich dazu, um Latex zu schreiben. Empfehlenswert ist aber eine Entwicklungsumgebung wie z.B. TeXStudio.

5.3. Beispiel für eine Abbildung

Abbildung 5.1.: Beispiel für eine Beschriftung.

Durch die `\label` kann auf die Bilder mit `\ref` verwiesen werden. Es ist wichtig, im Text kurz die Abbildung zu beschreiben. Zum Beispiel: In Abbildung 6.1 sieht man das Logo des Lehrstuhls, das als Beispiel einer Abbildung dienen soll. In blau ist der Text dargestellt, in schwarz das Symbol des Lehrstuhls.

Die Tilde sorgt dafür, dass kein Umbruch zwischen Abbildung und Zahl vorkommt.

Ranking	Letter
1	A
2	B
3	C
4	D
5	E
6	F
7	G

Tabelle 5.1.: Ranking der Buchstaben im Alphabet.

5.4. Beispiel für eine Tabelle

Klar strukturierte Tabellen lassen sich mit dem Booktabs-Paket erstellen, wie man in Tabelle 6.1 sehen kann.

5.5. Beispiele für Referenzen

Die Literaturhinweise werden im Text z.B. folgendermaßen verwendet:
"..., wie in [AdMD+04] gezeigt." Der Stil der Referenz kann in der Datei "ThesisCNaCC.tex" angepasst werden (z.b. nur Zahlen anzeigen). Bei den meisten Papern kann direkt eine Bibtex-Quelle heruntergeladen werden (z.B. auf Google Scholar, Springer etc.). Zur Verwaltung der Literatur bieten sich Programme wie Jabref, Mendeley etc. an.

5.6. Schrifttypen

Als Schrifttyp wird Arial oder Roman empfohlen. Bitte beachten, dass Größen und Einheiten eine eigene Schreibweise haben:

Kursivschrift: physikalische Größen (z.B. U für Spannung), Variablen (z.B. x), sowie Funktions- und Operatorzeichen, deren Bedeutung frei gewählt werden kann (z.B. $f(x)$)

Matheformeln im Mathemodus: $\frac{1}{1} \cdot 3 = 3$

5.7. Code der Arbeit

5.7.1. GitLab

Am Lehrstuhl gibt es ein GitLab. Hier könnt ihr euren Code mit Versionskontrolle verwalten, und am Ende kann euer Betreuer ebenfalls auf den Code zugreifen.

Kontaktiert bei Interesse euren Betreuer, dieser wird euch weitere Details geben!

5.7.2. Hardware

Falls ihr mehr Rechenpower für euren Code/Simulationen benötigt, wendet euch bitte an euren Betreuer!

5.7.3. Code einfügen

Bitte kopiert nicht euren gesamten Code in die Arbeit! An manchen Stellen kann es aber sinnvoll sein, kurze Abschnitte zu zeigen. Das geht am besten mit Listings, as shown in Listing 6.1:

Listing 5.1: Hello World in Java

```
public static void main (String[] args) {
System.print.out("Hello World");
}
```

Man kann den Code auch direkt aus einer Datei darstellen (Datei ist nicht vorhanden, daher auskommentiert).

Falls die Darstellung noch nicht gefällt, kann es angepasst werden: `https://en.wikibooks.org/wiki/LaTeX/Source_Code_Listings#Settings`

5.8. Abkürzungen

Falls man viele fachspezifische Abkürzungen in der Arbeit verwendet, bieten sich Latex-Pakete zur Unterstützung an, zum Beispiel acronym oder glossary. Beispiel acronym-Paket: Eine Virtual Machine (VM) wird benutzt. Mehrere VMs sind besser als eine VM. Das ist eine lange Abkürzung: sehr sehr lange Abkürzung (ssla), bei der der Plural anders ist: ssla'en.

6. How To in English

Here, you can describe how the problem was solved and the steps taken to obtain the results.

6.1. Latex-Environment

Almost every text editor can be used to write latex. However, an IDE is recommended e.g TeXStudio.

6.2. How To: Write a Thesis

In this section, some useful tricks for writing and for using latex are presented. For headings in general, you can use “Titlecase” for a consistent appearance.

6.3. Example for a Figure

Abbildung 6.1.: Example for a title of a figure.

With the help of `\label`, figures and tables can be addressed with the command `\ref` It is important, to describe the figure in the text. For example: In Fig. 6.1, one can see the logo of the chair. The text is shown in blue, and the in black the symbol of the chair.

The tilde prevents a linebreak between Figure and the number.

Ranking	Letter
1	A
2	B
3	C
4	D
5	E
6	F
7	G

Tabelle 6.1.: Ranking of letters in the alphabet.

6.4. Example for a table

Clearly structured tables can be realized with the packet booktabs as you can see in Table 6.1.

6.5. Example for References

The literature reference in the text are used as follows:
"..., as shown in [AdMD+04]." The Style of the reference can be adapted in the file "ThesisCNaCC.tex" (e.g. show only numbers). For the most papers, you can directly download the Bibtex source (e.g. at Google Scholar, Springer etc.). For an easier management, you can use programs like Jabref, Mendeley etc.

6.6. Fonts

As font, Arial or Roman is recommended. Please note that some units have their own font:

Italic: physical units(e.g. V for Voltage), Variables (e.G. x), and functions and operators (e.G. $f(x)$)

Mathematical formulas in math mode: $\frac{1}{1} \cdot 3 = 4$

6.7. Code of the Thesis

6.7.1. GitLab

At the chair, there is a GitLab you can use for managing your code with version control. In the end, your supervisor can easily access this code.

If interested, please contact your supervisor!

6.7.2. Computing Power

If you need hardware for your code/simulations, please contact your supervisor!

6.7.3. Insert Code

Please do not copy your complete code in the thesis! But on some points it can be helpful to show snippets. You can use Listings:

Listing 6.1: Hello World in Java

```
public static void main (String[] args) {
System.print.out("Hello World");
}
```

You can import the code directly from a file, too (File does not exist here)

The appearance can be adapted: `https://en.wikibooks.org/wiki/LaTeX/Source_Code_Listings#Settings`

6.8. Abbreviations

If you are using many abbreviations, you can use latex-packages like acronym or glossary. For exmaple a VM is used. More VMs are better than one VM. This is a very long abbreviation in german: ssla, with a different plural: ssla'en.

7. Ergebnisse/Results

Hier werden die Ergebnisse gezeigt und beschrieben. Vergesst nicht eine ordentliche Beschriftung zu erstellen!

Here, results are shown and described. Do not forget proper labels for figures!

8. Related Work

Dieses Kapitel kann entweder nach der Einleitung oder vor der Zusammenfassung stehen. Wenn viel Vorwissen für das Verständnis der verwandten Arbeiten benötigt wird, dann empfiehlt sich das letztere. Hier werden Paper genannt, die ähnliche Probleme untersuchen. Es muss deutlich werden, inwiefern sich die Arbeit zu diesen Papern unterscheidet und was hier besser gemacht wird.

This chapter can be either after the introduction or before the conclusion. If a lot of knowledge is necessary to understand this chapter, the latter is recommended. Here, papers are mentioned that describe similar problems. It should be clarified why the thesis is different from those paper and what is performed better.

9. Zusammenfassung

Am Schluss werden noch einmal alle wesentlichen Ergebnisse zusammengefasst. Hier können auch gemachte Erfahrungen beschrieben werden. Am Ende der Zusammenfassung folgt ein Ausblick, der die zukünftige Entwicklung der behandelten Thematik aus der Sicht des Autors darstellt.

In the end, all relevant results are summarized. All experiences can described. At the end, future work is described. i.e. the future research questions and the development of the problem.

A. Abkürzungsverzeichnis

VM Virtual Machine

CD Compact Disc

ssla sehr sehr lange Abkürzung

B. Ein Beispiel für einen Anhang

Beispiel für eine Tabelle:

left	center	right
entry	entry	entry
entry	entry	entry
entry	entry	entry

Tabelle B.1.: Beispiel für eine Beschriftung.

Abbildungsverzeichnis

Tabellenverzeichnis

Literaturverzeichnis

[AdMD+04] Frank-Uwe Andersen, Hermann de Meer, Ivan Dedinski, Cornelia Kappler, Andreas Mäder, Jens Oberender, and Kurt Tutschku. An architecture concept for mobile p2p file sharing services. In *Workshop at Informatik 2004 - Algorithms and Protocols for Efficient Peer-to-Peer Applications*, pages 229–233, Ulm, 9 2004.