TECHNISCHE
UNIVERSITÄT
DARMSTADT

A VERY COOL TOPIC

Am Fachbereich Informatik
der Technischen Universität Darmstadt
eingereichte

DISSERTATION

zur Erlangung des akademischen Grades
Doktor-Ingenieur (Dr.-Ing.)
von

NAME OF THE STUDENT

Erstreferent: Prof. Dr.-Ing. Matthias Hollick
Korreferent: Put name here

Darmstadt 1337
Hochschulkennziffer D17

Name of the Student, *A Very Cool Topic*, Dissertation, Technische Universität Darmstadt, 1337.

Fachgebiet Sichere Mobile Netze
Fachbereich Informatik
Technische Universität Darmstadt
Jahr der Veröffentlichung: 1337
Tag der mündlichen Prüfung: 1. Januar 1337
URN: urn:nbn:de:tuda-tuprints-83253

Ohana means family.
Family means nobody gets left behind, or forgotten.

— Lilo & Stitch

Dedicated to the loving memory of Rudolf Miede.

1939 – 2005

ABSTRACT

Short summary of the contents in English. . . a great guide by Kent Beck how to write good abstracts can be found here:

https://plg.uwaterloo.ca/~migod/research/beckOOPSLA.html

ZUSAMMENFASSUNG

Kurze Zusammenfassung des Inhaltes in deutscher Sprache. . .

ACKNOWLEDGMENTS

I would like to express my deepest gratitude to my parents and my family for supporting me in all the years of my studies and also while writing this thesis.

Special thanks for giving helpful advice while writing this thesis goes to Prof. Matthias Hollick and Adrian Loch.

Furthermore, I especially thank Sandrine Adélaïde and Adrian Loch for proofreading my thesis.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LISTINGS

ACRONYMS

SNR	signal-to-noise ratio

LIST OF PUBLICATIONS

During the course of writing this thesis, I co-authored several papers and articles that I list below.

JOURNAL AND MAGAZINE ARTICLES

[1] André Miede. "Theses and other Beautiful Documents with `classicthesis`." In: *TUGboat – The Communications of the TEX Users Group* 31.1 (2010), pp. 18–20. ISSN: 0896-3207.

[2] Hsin-Yi Tsai, Melanie Siebenhaar, André Miede, Yu-Lun Huang, and Ralf Steinmetz. "Threat as a Service? Virtualization's Impact on Cloud Security." In: *IEEE IT Professional* 14.1 (2012), pp. 32–37. ISSN: 1520-9202.

CONFERENCE AND WORKSHOP PAPERS

[3] Tobias Isenberg, André Miede, and Sheelagh Carpendale. "A Buffer Framework for Supporting Responsive Interaction in Information Visualization Interfaces." In: *Proceedings of the Fourth International Conference on Creating, Connecting, and Collaborating through Computing (C5 2006)*. IEEE, 2006, pp. 262–269. ISBN: 978-0-7695-2563-1.

[4] Ulrich Lampe, Markus Kieselmann, André Miede, Sebastian Zöller, and Ralf Steinmetz. "A Tale of Millis and Nanos: On the Accuracy of Time Measurements in Virtual Machines." In: *Proceedings of the Second European Conference on Service-Oriented and Cloud Computing (ESOCC 2013)*. Springer, 2013, pp. 172–179. ISBN: 978-3-642-40650-8.

[5] Ulrich Lampe, Qiong Wu, Ronny Hans, André Miede, and Ralf Steinmetz. "To Frag Or To Be Fragged – An Empirical Assessment of Latency in Cloud Gaming." In: *Proceedings of the Third International Conference on Cloud Computing and Services Science (CLOSER 2013)*. 2013, pp. 5–12. ISBN: 978-898-8565-52-5.

[6] André Miede, Gökhan Şimşek, Stefan Schulte, Daniel F. Abawi, Julian Eckert, and Ralf Steinmetz. "Revealing Business Relationships – Eavesdropping Cross-organizational Collaboration in the Internet of Services." In: *Proceedings of the Tenth International Conference Wirtschaftsinformatik (WI 2011)*. Vol. 2. 2011, pp. 1083–1092. ISBN: 978-1-4467-9236-0.

POSTERS AND DEMONSTRATORS

[7] Milan Stute, David Kreitschmann, and Matthias Hollick. "Demo: Linux Goes Apple Picking: Cross-Platform Ad hoc Communication with Apple Wireless Direct Link." In: *ACM Conference on Mobile Computing and Networking (MobiCom)*. Best Demo Award. **Part of this thesis**. Oct. 2018. DOI: 10.1145/3241539.3267716.

UNDER PEER REVIEW

[8] Milan Stute, Pranay Agarwal, Abhinav Kumar, Arash Asadi, and Matthias Hollick. "LIDOR: A Lightweight DoS-Resilient Communication Protocol for Safety-Critical IoT Systems." In: *IEEE Internet of Things Journal (IoT-J)* (submitted). **Part of this thesis.**

COLLABORATIONS AND MY CONTRIBUTION

Systematically investigating a technical research topic and engineering the required tools is a demanding and interdisciplinary process. Most achievements could never evolve without collaborations in which colleagues and international partners integrated their intellectual forces. When working in teams, accounting particular contributions and components of the resulting publications to individual collaborators becomes almost impossible. This situation also applies to several contents of this thesis, which arise from collaborations, thus, cover joint contributions. Many of these collaborations persisted even longer than the research projects and became a long-term strategic partnership. In our previous publications, all authors contributed by discussing ideas and debating on results throughout the whole project duration. Each of them has particular strengths that sometimes appear invisible. For this reason, I explicitly state and acknowledge—where possible—the contributions of my collaborators in the following.

In the following, I detail the contributions of my co-authors and myself per chapter. In addition, I follow the regulations of the Department of Computer Science at Technische Universität Darmstadt and give an account of the parts that include verbatim or revised fragments of previous publications that form this thesis as indicated in the preceding list of publications.[1]

Chapters 1 and 2 collate the contributions, background, and related work sections of the core papers that form this thesis [8, 7].

1 References in this chapter refer to my list of publications given on Pages xi to xii.

Part I

INTRODUCTION

The first chapter of this part gives an introduction and a motivation to this thesis, followed by a presentation of related work found in the area of physical layer security. In the third chapter, we present some definitions and background information to make it easier for the reader to quickly understand the subsequent parts of this thesis.

1 INTRODUCTION

Start a chapter with text and not with a section header. Open the *classicthesis-config.tex* file to insert the title of your thesis, the names of your supervisors and the hand-in date of your thesis.

1.1 FIRST SECTION

After a section there should always be text before the next section. The first paragraph is always without indentation. Starting from the second paragraph, there is an indentation.

Here is an equation without numbers for referencing:

$$\underbrace{\begin{pmatrix} \mathcal{B}_1 \\ \mathcal{B}_2 \\ \vdots \\ \mathcal{B}_R \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} H_{1,1} & H_{1,2} & \dots & H_{1,T} \\ H_{2,1} & H_{2,2} & \dots & H_{2,T} \\ \vdots & \vdots & \ddots & \vdots \\ H_{R,1} & H_{R,2} & \dots & H_{R,T} \end{pmatrix}}_{H_{A\to B}} \cdot \underbrace{\begin{pmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \\ \vdots \\ \mathcal{A}_T \end{pmatrix}}_{\mathcal{A}}$$

Here is an equation that you can reference:

$$\underbrace{\begin{pmatrix} \mathcal{B}_1 \\ \mathcal{B}_2 \\ \vdots \\ \mathcal{B}_R \end{pmatrix}}_{\mathcal{B}} = \underbrace{\begin{pmatrix} H_{1,1} & H_{1,2} & \dots & H_{1,T} \\ H_{2,1} & H_{2,2} & \dots & H_{2,T} \\ \vdots & \vdots & \ddots & \vdots \\ H_{R,1} & H_{R,2} & \dots & H_{R,T} \end{pmatrix}}_{H_{A\to B}} \cdot \underbrace{\begin{pmatrix} \mathcal{A}_1 \\ \mathcal{A}_2 \\ \vdots \\ \mathcal{A}_T \end{pmatrix}}_{\mathcal{A}} \tag{1}$$

1.1.1 *Referencing*

Take a look in the following list to reference sections, figures and equations:

- Section 1.1
- Figure 1
- Equation (1)

1.1.2 *Acronyms*

For acronyms you should use the *glossaries* package and put your acronyms in the *FrontBackmatter/acronyms.tex* file. The first acronym is

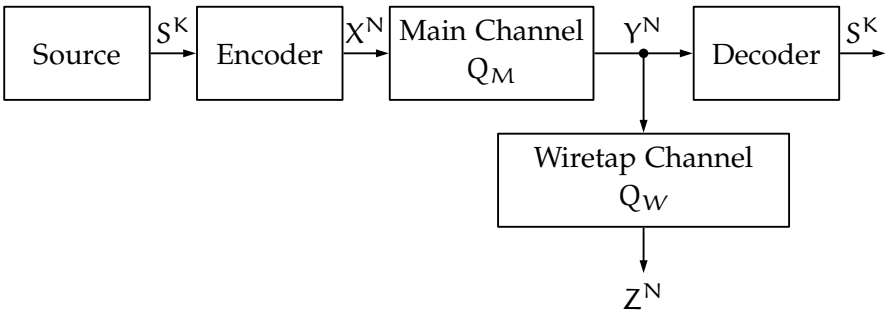

Figure 1: The wiretap channel (source: [1])

always written in it's long form, the following occurrences are abbreviated: first occurrence signal-to-noise ratio (SNR), second occurrence SNR, plural SNRs.

1.1.3 *Examples on Figures*

When using figures, use vector graphics whenever possible. In Figures 1 and 2 are some examples to generate vector graphics directly from LaTeXcode. The second example is based on the *matlab2tikz* script for matlab. You find an example in the *gfx/matlab/create_example_graph.m* file. TikZ is used to generate the graphics. As it takes some time and memory to recompile a graphic, pdflatex caches generated figures when the `--enable-write18` switch is set when calling `pdflatex`. Graphics are only recompiled when you uncomment the `\tikzset{external/remake next}` command. Figures should always appear after the first reference in the text or at the top of the same page as the reference, but never before the reference. Prefer placing figures on separate pages. Try to always have figures and text on each page. Or place enough figures to fill a page only with figures.

1.1.4 *Examples on Tables*

You can find an example table in Table 1 using the *tabular* environment. Note the use of horizontal lines from the *booktabs* package (`\toprule`, `\midrule`, and `\bottomrule`) and removed whitespace at both sides of the table (`@{}`) as proposed by Markus Püschel.[1]

1.2 MARGIN NOTES

Here you can add text to the margin. For example, to summarize the section next to it.

Especially in the standard SEEMOO template with wide margins, you are encouraged to insert text into the margins. If you decide to do so, plan to have at least one margin note per double page.

1 https://www.inf.ethz.ch/personal/markusp/teaching/guides/guide-tables.pdf

DISASTER	YEAR	COUNTRY	AREA (KM²)
Nepal earthquake	2015	Nepal	3 610
Cyclone Pam	2015	Vanuatu	12 190
Ludian earthquake	2014	China	1 487
Typhoon Haiyan	2013	Philippines	71 503
Christchurch earthquake	2011	New Zealand	1 426
East Africa drought	2011	East Africa	2 346 466
Tropical storm Washi	2011	Philippines	104 530
Tohoku earthquake	2011	Japan	83 955
Haiti earthquake	2010	Haiti	27 750
Afghanistan blizzard	2008	Afghanistan	652 864
Sichuan earthquake	2008	China	485 000
Cyclone Nargis	2008	Myanmar	676 578

Table 1: Large-scale natural disasters in the last ten years

1.3 SOME EXAMPLE TEXT

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor.

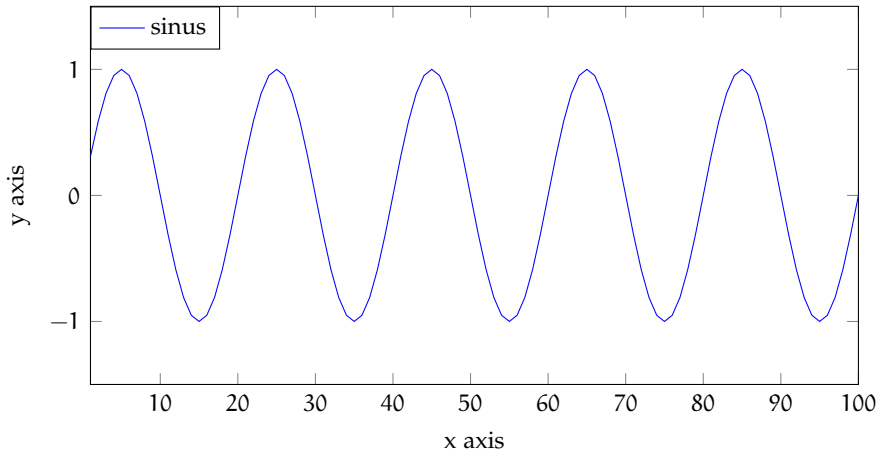

Figure 2: Caption of figure

Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

Suspendisse vitae elit. Aliquam arcu neque, ornare in, ullamcorper quis, commodo eu, libero. Fusce sagittis erat at erat tristique mollis. Maecenas sapien libero, molestie et, lobortis in, sodales eget, dui.

Morbi ultrices rutrum lorem. Nam elementum ullamcorper leo. Morbi dui. Aliquam sagittis. Nunc placerat. Pellentesque tristique sodales est. Maecenas imperdiet lacinia velit. Cras non urna. Morbi eros pede, suscipit ac, varius vel, egestas non, eros. Praesent malesuada, diam id pretium elementum, eros sem dictum tortor, vel consectetuer odio sem sed wisi.

2

RELATED WORK

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Part II

CONTRIBUTION

The contribution starts with a design chapter, where we mathematically describe the design of the physical layer security system, as well as the adaptive filter of the attacker. After the design follows the implementation on WARP nodes. Here we give an insight into the challenges of implementing the designed MIMO communication system. The last chapter concentrates on evaluating the performance of our proposed attack in simulation and practice.

3

DESIGN

Morbi luctus, wisi viverra faucibus pretium, nibh est placerat odio, nec commodo wisi enim eget quam. Quisque libero justo, consectetuer a, feugiat vitae, porttitor eu, libero. Suspendisse sed mauris vitae elit sollicitudin malesuada. Maecenas ultricies eros sit amet ante. Ut venenatis velit. Maecenas sed mi eget dui varius euismod. Phasellus aliquet volutpat odio. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Pellentesque sit amet pede ac sem eleifend consectetuer. Nullam elementum, urna vel imperdiet sodales, elit ipsum pharetra ligula, ac pretium ante justo a nulla. Curabitur tristique arcu eu metus. Vestibulum lectus. Proin mauris. Proin eu nunc eu urna hendrerit faucibus. Aliquam auctor, pede consequat laoreet varius, eros tellus scelerisque quam, pellentesque hendrerit ipsum dolor sed augue. Nulla nec lacus.

4

IMPLEMENTATION

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

5 EVALUATION

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Part III

DISCUSSION AND CONCLUSIONS

After the evaluation, we further discuss the results and give an outlook. In addition, we finish this work with conclusions.

6

DISCUSSION

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

7 CONCLUSIONS

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

Part IV

APPENDIX

A

SOME PROOF

Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Donec odio elit, dictum in, hendrerit sit amet, egestas sed, leo. Praesent feugiat sapien aliquet odio. Integer vitae justo. Aliquam vestibulum fringilla lorem. Sed neque lectus, consectetuer at, consectetuer sed, eleifend ac, lectus. Nulla facilisi. Pellentesque eget lectus. Proin eu metus. Sed porttitor. In hac habitasse platea dictumst. Suspendisse eu lectus. Ut mi mi, lacinia sit amet, placerat et, mollis vitae, dui. Sed ante tellus, tristique ut, iaculis eu, malesuada ac, dui. Mauris nibh leo, facilisis non, adipiscing quis, ultrices a, dui.

BIBLIOGRAPHY

[1] A. D. Wyner. "The Wire-tap Channel." In: *Bell Systems Technical Journal* 54.8 (1975), pp. 1355–1387.

ERKLÄRUNG ZUR DISSERTATIONSSCHRIFT

gemäß § 9 der Allgemeinen Bestimmungen der Promotionsordnung der Technische Universität Darmstadt vom 12. Januar 1990 (ABI. 1990, S. 658) in der Fassung der 8. Novelle vom 1. März 2018

Hiermit versichere ich, Name of the Student, die vorliegende Dissertationsschrift ohne Hilfe Dritter und nur mit den angegebenen Quellen und Hilfsmitteln angefertigt zu haben. Alle Stellen, die Quellen entnommen wurden, sind als solche kenntlich gemacht worden. Eigenzitate aus vorausgehenden wissenschaftlichen Veröffentlichungen werden in Anlehnung an die Hinweise des Promotionsausschusses Fachbereich Informatik zum Thema „Eigenzitate in wissenschaftlichen Arbeiten“ (EZ-2014/10) in Kapitel „*Collaborations and My Contribution*“ auf Seiten xiii bis xiii gelistet. Diese Arbeit hat in gleicher oder ähnlicher Form noch keiner Prüfungsbehörde vorgelegen. In der abgegebenen Dissertationsschrift stimmen die schriftliche und die elektronische Fassung überein.

Darmstadt, 1. Januar 1337

Name of the Student