Title

Dissertation Thesis

YOU

August 2024

Submitted in partial fulfillment of the requirements
for the degree of Doktor der Naturwissenschaften (Dr. rer. nat.)

to the

Department of Informatics
at Karlsruhe Institute of Technology

1st Reviewer	Prof. Dr. Meta
2nd Reviewer	Prof. Meta 2
3rd Reviewer	Prof. Meta 3

Acknowledgments

Thanks to people that put templates online.

Abstract

Zusammenfassung

Exchange this for an abstract in whatever language you want.

Publications

[BT21] Robin M. Berger and Marcel Tiepelt. "On Forging SPHINCS$^+$-Haraka Signatures on a Fault-Tolerant Quantum Computer". In: *Progress in Cryptology - LATINCRYPT 2021 - 7th International Conference on Cryptology and Information Security in Latin America, Bogotá, Colombia, October 6-8, 2021, Proceedings*. Ed. by Patrick Longa and Carla Ràfols. Vol. 12912. Lecture Notes in Computer Science. Springer, 2021, pp. 44–63. DOI: 10.1007/978-3-030-88238-9_3. URL: https://doi.org/10.1007/978-3-030-88238-9_3.

[Bin+24] Nina Bindel, Xavier Bonnetain, Marcel Tiepelt, and Fernando Virdia. "Quantum Lattice Enumeration in Limited Depth". In: *Advances in Cryptology – CRYPTO 2024*. Accepted at CRYPTO 2024. 2024.

[Boe+21] Franziska Boenisch, Reinhard Munz, Marcel Tiepelt, Simon Hanisch, Christiane Kuhn, and Paul Francis. "Side-Channel Attacks on Query-Based Data Anonymization". In: *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*. CCS '21. Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, pp. 1254–1265. ISBN: 9781450384544. DOI: 10.1145/3460120.3484751. URL: https://doi.org/10.1145/3460120.3484751.

[DAn+19] Jan-Pieter D'Anvers, Marcel Tiepelt, Frederik Vercauteren, and Ingrid Verbauwhede. "Timing Attacks on Error Correcting Codes in Post-Quantum Schemes". In: *Proceedings of ACM Workshop on Theory of Implementation Security, TIS at CCS 2019, London, UK, November 11, 2019*. Ed. by Begül Bilgin, Svetla Petkova-Nikova, and Vincent Rijmen. ACM, 2019, pp. 2–9. DOI: 10.1145/3338467.3358948. URL: https://doi.org/10.1145/3338467.3358948.

[Mäu+21] Nils Mäurer, Thomas Gräupl, Christoph Gentsch, Tobias Guggemos, Marcel Tiepelt, Corinna Schmitt, and Gabi Dreo Rodosek. "A Secure Cell-Attachment Procedure of LDACS". In: *IEEE European Symposium on Security and Privacy Workshops, EuroS&P 2021, Vienna, Austria, September 6-10, 2021*. IEEE, 2021, pp. 113–122. DOI: 10.1109/EuroSPW54576.2021.00019. URL: https://doi.org/10.1109/EuroSPW54576.2021.00019.

[TD20] Marcel Tiepelt and Jan-Pieter D'Anvers. "Exploiting Decryption Failures in Mersenne Number Cryptosystems". In: *Proceedings of the 7th on ASIA Public-Key Cryptography Workshop, APKC at AsiaCCS 2020, Taipei, Taiwan, October 6, 2020*. Ed. by Keita Emura and Naoto Yanai. ACM, 2020, pp. 45–54. DOI: 10.1145/3384940.3388957. URL: https://doi.org/10.1145/3384940.3388957.

[TES23] Marcel Tiepelt, Edward Eaton, and Douglas Stebila. "Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements". In: *Computer Security - ESORICS 2023 - 28th European Symposium on Research in Computer Security, The Hague, The Netherlands, September 25-29, 2023, Proceedings, Part I*. Ed. by Gene Tsudik, Mauro Conti, Kaitai Liang, and Georgios Smaragdakis. Vol. 14344. Lecture Notes in Computer Science. Springer, 2023, pp. 168–188. DOI: 10.1007/978-3-031-50594-2_9. URL: https://doi.org/10.1007/978-3-031-50594-2_9.

[TMM24] Marcel Tiepelt, Christian Martin, and Nils Maeurer. "Post-Quantum Ready Key Agreement for Aviation". In: *IACR Communications in Cryptology* 1.1 (Apr. 9, 2024). ISSN: 3006-5496. DOI: 10.62056/aebn2isfg. URL: https://doi.org/10.62056/aebn2isfg.

[TS19] Marcel Tiepelt and Alan Szepieniec. "Quantum LLL with an Application to Mersenne Number Cryptosystems". In: *Progress in Cryptology – LATINCRYPT 2019*. Ed. by Peter Schwabe and Nicolas Thériault. Cham: Springer International Publishing, 2019, pp. 3–23. ISBN: 978-3-030-30530-7.

[TS16] Marcel Kevin Tiepelt and Tilak Raj Singh. "Finding pre-production vehicle configurations using a Max-SAT framework". In: *Proceedings of the 18 th International Configuration Workshop*. 2016, pp. 117–123.

Open-Access Versions

[BT21] Robin M. Berger and Marcel Tiepelt. *On Forging SPHINCS+-Haraka Signatures on a Fault-tolerant Quantum Computer*. Cryptology ePrint Archive, Paper 2021/1484. https://eprint.iacr.org/2021/1484. 2021. DOI: 10.1007/978-3-030-88238-9_3. URL: https://eprint.iacr.org/2021/1484.

[Bin+23] Nina Bindel, Xavier Bonnetain, Marcel Tiepelt, and Fernando Virdia. *Quantum Lattice Enumeration in Limited Depth*. Cryptology ePrint Archive, Paper 2023/1423. https://eprint.iacr.org/2023/1423. 2023. URL: https://eprint.iacr.org/2023/1423.

[DAn+19] Jan-Pieter D'Anvers, Marcel Tiepelt, Frederik Vercauteren, and Ingrid Verbauwhede. *Timing attacks on Error Correcting Codes in Post-Quantum Schemes*. Cryptology ePrint Archive, Paper 2019/292. https://eprint.iacr.org/2019/292. 2019. URL: https://eprint.iacr.org/2019/292.

[Mäu+21] Nils Mäurer, Thomas Gräupl, Christoph Gentsch, Tobias Guggemos, Marcel Tiepelt, Corinna Schmitt, and Gabi Dreo Rodosek. "A Secure Cell-Attachment Procedure of LDACS". In: *IEEE European Symposium on Security and Privacy Workshops, EuroS&P 2021, Vienna, Austria, September 6-10, 2021*. IEEE, 2021, pp. 113–122. URL: https://elib.dlr.de/142721/1/2021___SRCNAS___A_Secure_Cell_Attachment_Procedure_of_LDACS.pdf.

[TD20] Marcel Tiepelt and Jan-Pieter D'Anvers. *Exploiting Decryption Failures in Mersenne Number Cryptosystems*. Cryptology ePrint Archive, Paper 2020/367. https://eprint.iacr.org/2020/367. 2020. DOI: 10.1145/3384940.3388957. URL: https://eprint.iacr.org/2020/367.

[TES23] Marcel Tiepelt, Edward Eaton, and Douglas Stebila. *Making an Asymmetric PAKE Quantum-Annoying by Hiding Group Elements*. Cryptology ePrint Archive, Paper 2023/1513. https://eprint.iacr.org/2023/1513. 2023. DOI: 10.1007/978-3-031-50594-2_9. URL: https://eprint.iacr.org/2023/1513.

[TMM24] Marcel Tiepelt, Christian Martin, and Nils Maeurer. *Post-Quantum Ready Key Agreement for Aviation*. Cryptology ePrint Archive, Paper 2024/1096. https://eprint.iacr.org/2024/1096. 2024. DOI: 10.62056/aebn2isfg. URL: https://eprint.iacr.org/2024/1096.

[TS19] Marcel Tiepelt and Alan Szepieniec. *Quantum LLL with an Application to Mersenne Number Cryptosystems*. Cryptology ePrint Archive, Paper 2019/1027. https://eprint.iacr.org/2019/1027. 2019. DOI: 10.1007/978-3-030-30530-7_1. URL: https://eprint.iacr.org/2019/1027.

Contents

ABSTRACT iii

ZUSAMMENFASSUNG iv

PUBLICATIONS v

CONTENTS vii

I NAME OF PART I 1

1 STRUCTURE 2

2 HOW TO USE THIS TEMPLATE 4

BIBLIOGRAPHY 8

ACRONYMS 9

LIST OF FIGURES 10

LIST OF TABLES 11

II APPENDIX 12

Part I

NAME OF PART I

1

Structure

Configuration

Template The main config are stored under

- /0_dissconfig

You should adapt /0_dissconfig/config.tex. There is space to add all your “custom” packages there.

Other The custom configs are stored under

- /0_customconfig

Currently, that holds acronyms and custom macros. I did not put the packages here, because I think keeping them as close to each other as possible makes it easier to avoid conflicts.

Bibliography

Bibliography files Bibliography files go into

- /bibliography

There are two special files for the Publication sections:

- /bibliography/own.bib to hold bibliography of you own publications.
- /bibliography/own_openaccess.bib to hold open-access (for instance, ePrint or arXiv) bibliography of you own publications.

Document The bibliography is added to the document via

- /FrontBackmatter/Biblipgraphy.tex
- /FrontBackmatter/Publications.tex

Biblatex If you use biblated with cryptobib in a folder called (say, in a folder called cryptobiblink), I strongly recommend to use Extract From Bibliography to extract the relevant entries via

```
python3 extract_from_bibliography.py diss
    .bcf cryptobiblink/crypto.bib
    cryptobiblink/dummy.bib  >
    bibliography/reduced_crypto.bib
```

I did not figure out what the 3rd input (“dummy.bib”) does, but the above worked flawlessly for me. This will significantly speed-up the compilation.

2

How to use this Template

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.[1] Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.[1]

[1] \footnote : This is a numbered and referenced footnote in the margin.

[1] \sidenote : This is a numbered but **un**referenced footnote in the margin.

\sidecomment : This is a unnumbered and unreferenced comment in the margin.

CITATION AND FLOATS Citations [BT21] appear as preview in the margin. Floats cannot have *direct* citations, you need to use \citeonly instead.

[BT21] Berger and Tiepelt, *On Forging SPHINCS+-Haraka Signatures on a Fault-tolerant Quantum Computer*

Floats include (but are not limited to):

- captions
- footnote, sidenote, sidecomment

The class offers a *full* citation:

- \fullfullcite

Marcel Tiepelt and Jan-Pieter D'Anvers. *Exploiting Decryption Failures in Mersenne Number Cryptosystems*. Cryptology ePrint Archive, Paper 2020/367. https://eprint.iacr.org/2020/367. 2020. DOI: 10.1145/3384940.3388957. URL: https://eprint.iacr.org/2020/367

There is also a command to present your contributions:

- \contentsource [TEXT]OFFICIAL CITETATIONOPEN CITETATIONContribution[IMPLEMENTATION]

Content Sources

TEXT.

Publication

Marcel Tiepelt and Jan-Pieter D'Anvers. "Exploiting Decryption Failures in Mersenne Number Cryptosystems". In: *Proceedings of the 7th on ASIA Public-Key Cryptography Workshop, APKC at AsiaCCS 2020, Taipei, Taiwan, October 6, 2020*. Ed. by Keita Emura and Naoto Yanai. ACM, 2020, pp. 45–54. DOI: 10.1145/3384940.3388957. URL: https://doi.org/10.1145/3384940.3388957

Open-Access Publication

Marcel Tiepelt and Jan-Pieter D'Anvers. *Exploiting Decryption Failures in Mersenne Number Cryptosystems*. Cryptology ePrint Archive, Paper 2020/367. https://eprint.iacr.org/2020/367. 2020. DOI: 10.1145/3384940.3388957. URL: https://eprint.iacr.org/2020/367

Implementation

LinktoGithub

Contribution Equal.

FIGURES AND CAPTIONS

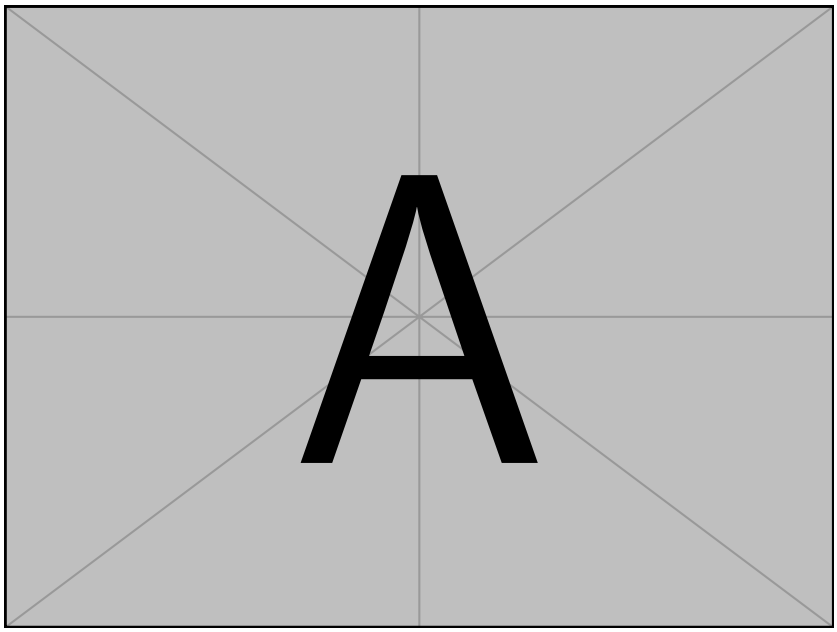


FIGURE 2.1: Linewidth Figure

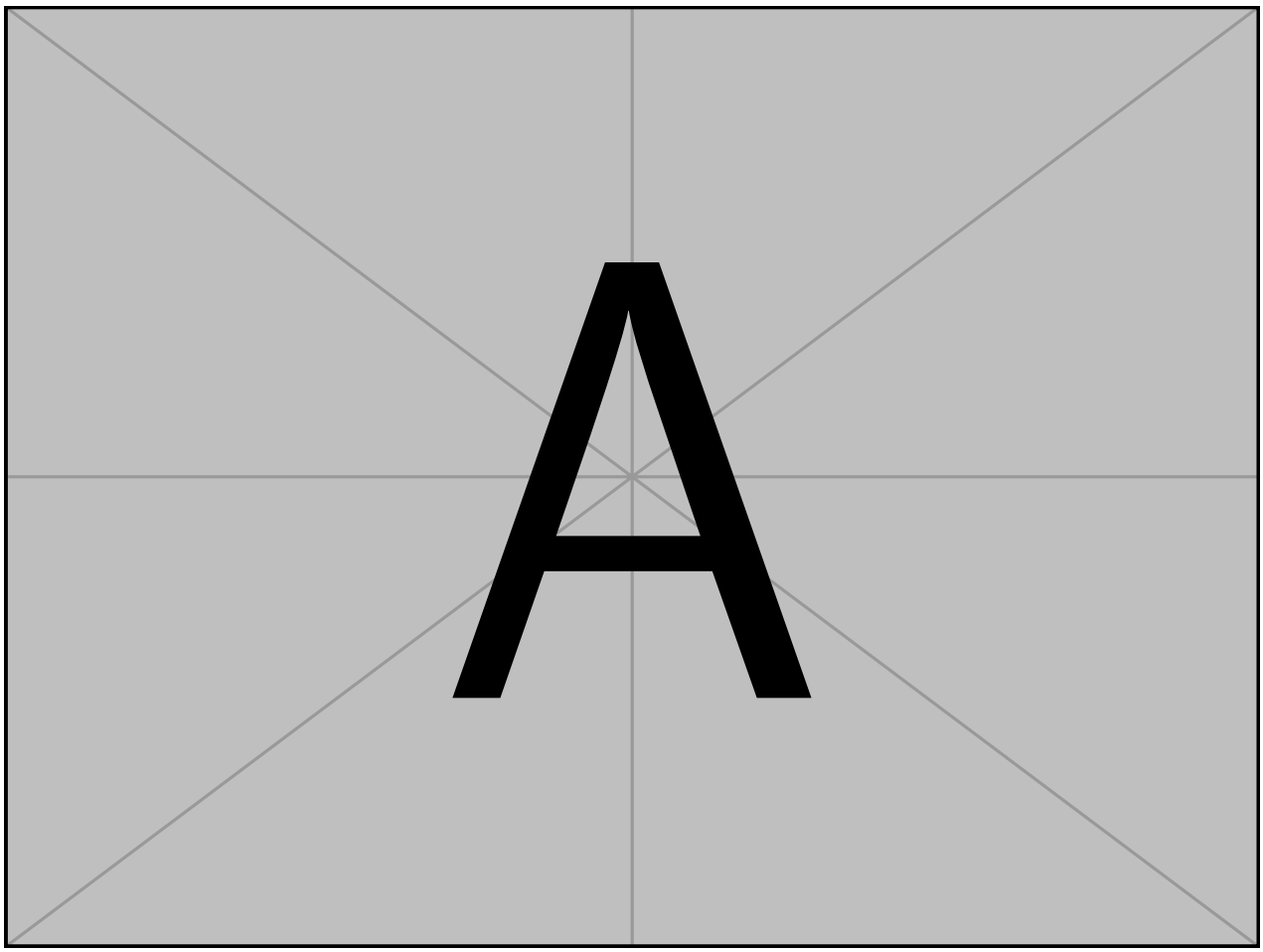


FIGURE 2.2: Fullwidth Figure

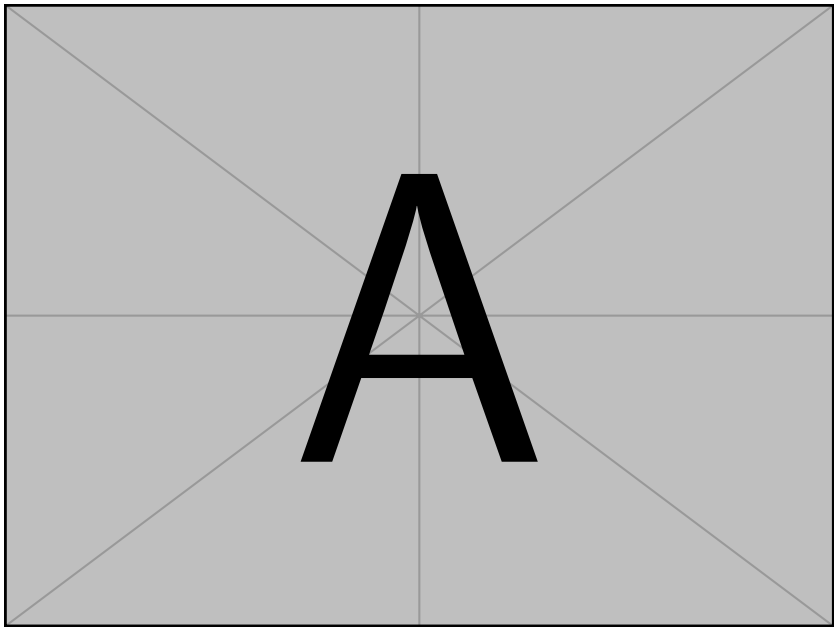
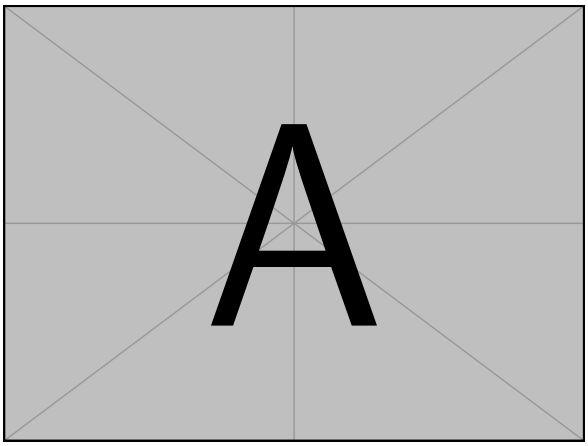
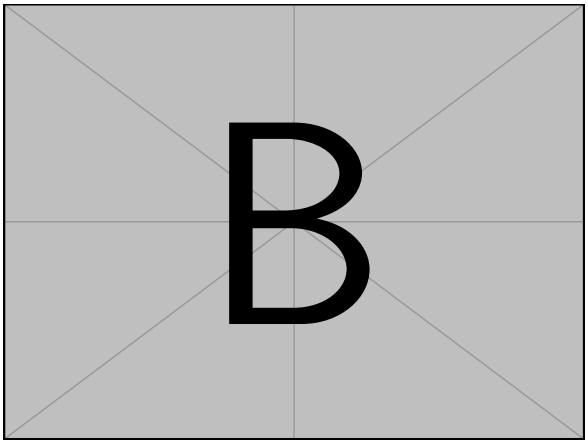


FIGURE 2.3: Sidecaption



(a) Subfigure in Memoir class



(b) Subfigure in Memoir class

FIGURE 2.4: Caption of subfigure in Memoir.

ACRONYMS This is a acronym: Advanced Encryption Standard (AES), where only the first occurence has a hyperlink to the reference.

- This should not have a hyperref: AES.
- You can reset the reference using \glsresetall , for example, after every new part. Not it should be referenced and expanded again: Advanced Encryption Standard (AES)
- If you want hyperlinks on every occurrence, search for "ACRONYMS" in 0_dissconfig/dissertationpackage.sty and remove the corresponding lines.

Bibliography

[BT21] Robin M. Berger and Marcel Tiepelt. *On Forging SPHINCS+-Haraka Signatures on a Fault-tolerant Quantum Computer*. Cryptology ePrint Archive, Paper 2021/1484. https://eprint.iacr.org/2021/1484. 2021. DOI: 10.1007/978-3-030-88238-9_3. URL: https://eprint.iacr.org/2021/1484 (cit. on p. 4).

[TD20a] Marcel Tiepelt and Jan-Pieter D'Anvers. *Exploiting Decryption Failures in Mersenne Number Cryptosystems*. Cryptology ePrint Archive, Paper 2020/367. https://eprint.iacr.org/2020/367. 2020. DOI: 10.1145/3384940.3388957. URL: https://eprint.iacr.org/2020/367 (cit. on pp. 4, 5).

[TD20b] Marcel Tiepelt and Jan-Pieter D'Anvers. "Exploiting Decryption Failures in Mersenne Number Cryptosystems". In: *Proceedings of the 7th on ASIA Public-Key Cryptography Workshop, APKC at AsiaCCS 2020, Taipei, Taiwan, October 6, 2020*. Ed. by Keita Emura and Naoto Yanai. ACM, 2020, pp. 45–54. DOI: 10.1145/3384940.3388957. URL: https://doi.org/10.1145/3384940.3388957 (cit. on p. 5).

Acronyms

AES Advanced Encryption Standard. 7

List of Figures

2.1 Linewidth Figure 5
2.2 Fullwidth Figure 6
2.3 Sidecaption 6
2.4 Caption of subfigure in Memoir. 7

List of Tables

Part II

APPENDIX

COLOPHON

This thesis was typeset using LaTeX and the `memoir` documentclass. The template[2] is based on Friedrich Wiemer's thesis [3], which itself is based Aaron Turon's thesis [4], itself again a mixture of `classicthesis`[5] by André Miede and `tufte-latex`[6], based on Edward Tufte's *Beautiful Evidence*.

The bibliography was processed by Biblatex. The body text is set 10/14pt (long primer) on a 26pc measure. The margin text is set 8/9pt (brevier) on a 12pc measure. Matthew Carter's Charter acts as both the text and display typeface. Monospaced text uses Jim Lyles's `Bitstream Vera Mono` ("Bera Mono").

[2] https://github.com/mtiepelt/dissertation

[3] https://github.com/pfasante/phd_thesis/tree/master

[4] https://people.mpi-sws.org/~turon/turon-thesis.pdf

[5] https://bitbucket.org/amiede/classicthesis/

[6] https://github.com/Tufte-LaTeX/tufte-latex