Author name(s)

Book title

– Monograph –

February 3, 2016

Springer

Use the template dedic.tex *together with the Springer document class SVMono for monograph-type books or SVMult for contributed volumes to style a quotation or a dedication at the very beginning of your book in the Springer layout*

Foreword

Use the template *foreword.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your foreword in the Springer layout.

The foreword covers introductory remarks preceding the text of a book that are written by a *person other than the author or editor* of the book. If applicable, the foreword precedes the preface which is written by the author or editor of the book.

Place, month year *Firstname Surname*

Preface

Use the template *preface.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your preface in the Springer layout.

A preface is a book's preliminary statement, usually written by the *author or editor* of a work, which states its origin, scope, purpose, plan, and intended audience, and which sometimes includes afterthoughts and acknowledgments of assistance.

When written by a person other than the author, it is called a foreword. The preface or foreword is distinct from the introduction, which deals with the subject of the work.

Customarily *acknowledgments* are included as last part of the preface.

Place(s), *Firstname Surname*
month year *Firstname Surname*

Acknowledgements

Use the template *acknow.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) if you prefer to set your acknowledgement section as a separate chapter instead of including it as last part of your preface.

Contents

Acronyms

Use the template *acronym.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your list(s) of abbreviations or symbols in the Springer layout.

Lists of abbreviations, symbols and the like are easily formatted with the help of the Springer-enhanced `description` environment.

ABC	Spelled-out abbreviation and definition
BABI	Spelled-out abbreviation and definition
CABR	Spelled-out abbreviation and definition

Part I
Part Title

Use the template *part.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your part title page and, if desired, a short introductory text (maximum one page) on its verso page in the Springer layout.

Chapter 1
Chapter Heading

Abstract Each chapter should be preceded by an abstract (10–15 lines long) that summarizes the content. The abstract will appear *online* at www.SpringerLink.com and be available with unrestricted access. This allows unregistered users to read the abstract as a teaser for the complete chapter. As a general rule the abstracts will not appear in the printed version of your book unless it is the style of your particular book or that of the series to which your book belongs.

Please use the 'starred' version of the new Springer `abstract` command for typesetting the text of the online abstracts (cf. source file of this chapter template `abstract`) and include them with the source files of your manuscript. Use the plain `abstract` command if the abstract is also to appear in the printed version of the book.

1.1 Section Heading

Use the template *chapter.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style the various elements of your chapter content in the Springer layout.

1.2 Section Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

Use the standard `equation` environment to typeset your equations, e.g.

$$a \times b = c\,, \tag{1.1}$$

however, for multiline equations we recommend to use the `eqnarray` environment[1].

$$\begin{aligned} a \times b &= c \\ \mathbf{a} \cdot \mathbf{b} &= \mathbf{c} \end{aligned} \tag{1.2}$$

1.2.1 Subsection Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

> Please do not use quotation marks when quoting texts! Simply use the `quotation` environment – it will automatically render Springer's preferred layout.

1.2.1.1 Subsubsection Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.1, see also Fig. 1.1[2]

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

Paragraph Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

---

[1] In physics texts please activate the class option `vecphys` to depict your vectors in ***boldface-italic*** type - as is customary for a wide range of physical subjects.

[2] If you copy text passages, figures, or tables from other works, you must obtain *permission* from the copyright holder (usually the original publisher). Please enclose the signed permission with the manucript. The sources must be acknowledged either in the captions, as footnotes or in a separate section of the book.

For typesetting numbered lists we recommend to use the `enumerate` environment – it will automatically render Springer's preferred layout.

1. Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.
   a. Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.
   b. Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.
2. Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.

Subparagraph Heading

In order to avoid simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2, see also Fig. 1.2.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

For unnumbered list we recommend to use the `itemize` environment – it will automatically render Springer's preferred layout.

- Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development, cf. Table 1.1.
  – Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.
  – Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.
- Livelihood and survival mobility are oftentimes coutcomes of uneven socioeconomic development.

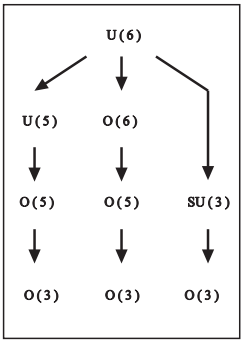

Fig. 1.1 If the width of the figure is less than 7.8 cm use the `sidecapion` command to flush the caption on the left side of the page. If the figure is positioned at the top of the page, align the sidecaption with the top of the figure – to achieve this you simply need to use the optional argument `[t]` with the `sidecaption` command

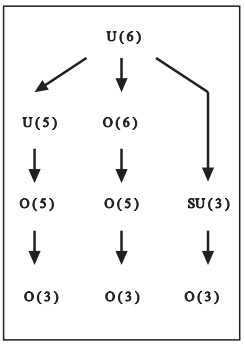

Fig. 1.2 Please write your figure caption here

Run-in Heading Boldface Version Use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

Run-in Heading Italic Version Use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

Table 1.1 Please write your table caption here

Classes	Subclass	Length	Action Mechanism
Translation	mRNA[a]	22 (19–25)	Translation repression, mRNA cleavage
Translation	mRNA cleavage	21	mRNA cleavage
Translation	mRNA	21–22	mRNA cleavage
Translation	mRNA	24–26	Histone and DNA Modification

[a] Table foot note (with superscript)

1.3 Section Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

If you want to list definitions or the like we recommend to use the Springer-enhanced `description` environment – it will automatically render Springer's preferred layout.

Type 1 That addresses central themes pertainng to migration, health, and disease. In Sect. 1.1, Wilson discusses the role of human migration in infectious disease distributions and patterns.

Type 2 That addresses central themes pertainng to migration, health, and disease. In Sect. 1.2.1, Wilson discusses the role of human migration in infectious disease distributions and patterns.

1.3.1 Subsection Heading

In order to avoid simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Use the LaTeX automatism for all your cross-references and citations citations as has already been described in Sect. 1.2.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

If you want to emphasize complete paragraphs of texts we recommend to use the newly defined Springer class option `graybox` and the newly defined environment `svgraybox`. This will produce a 15 percent screened box 'behind' your text.

If you want to emphasize complete paragraphs of texts we recommend to use the newly defined Springer class option and environment `svgraybox`. This will produce a 15 percent screened box 'behind' your text.

1.3.1.1 Subsubsection Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

Theorem 1.1. *Theorem text goes here.*

Definition 1.1. Definition text goes here.

Proof. Proof text goes here. □

Paragraph Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the

LaTeX automatism for all your cross-references and citations as has already been described in Sect. 1.2.

Note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

Theorem 1.2. *Theorem text goes here.*

Definition 1.2. Definition text goes here.

Proof. Proof text goes here. □

Acknowledgements If you want to include acknowledgments of assistance and the like at the end of an individual chapter please use the `acknowledgement` environment – it will automatically render Springer's preferred layout.

Appendix

When placed at the end of a chapter or contribution (as opposed to at the end of the book), the numbering of tables, figures, and equations in the appendix section continues on from that in the main text. Hence please *do not* use the `appendix` command when writing an appendix at the end of your chapter or contribution. If there is only one the appendix is designated "Appendix", or "Appendix 1", or "Appendix 2", etc. if there is more than one.

$$a \times b = c \tag{1.3}$$

Problems

1.1. A given problem or Excercise is described here. The problem is described here. The problem is described here.

1.2. Problem Heading
(a) The first part of the problem is described here.
(b) The second part of the problem is described here.

References

In view of the parallel print and (chapter-wise) online publication of your book at www.springerlink.com it has been decided that – as a genreral rule – references should be sorted chapter-wise and placed at the end of the individual chapters. However, upon agreement with your contact at Springer you may list your references

in a single seperate chapter at the end of your book. Deactivate the class option `sectrefs` and the `thebibliography` environment will be put out as a chapter of its own.

References may be *cited* in the text either by number (preferred) or by author/year.[3] The reference list should ideally be *sorted* in alphabetical order – even if reference numbers are used for the their citation in the text. If there are several works by the same author, the following order should be used:

1. all works by the author alone, ordered chronologically by year of publication
2. all works by the author with a coauthor, ordered alphabetically by coauthor
3. all works by the author with several coauthors, ordered chronologically by year of publication.

The *styling* of references[4] depends on the subject of your book:

- The *two* recommended styles for references in books on *mathematical, physical, statistical and computer sciences* are depicted in [1, 2, 3, 4, 5] and [6, 7, 8, 9, 10].
- Examples of the most commonly used reference style in books on *Psychology, Social Sciences* are [11, 12, 13, 14, 15].
- Examples for references in books on *Humanities, Linguistics, Philosophy* are [16, 17, 18, 19, 20].
- Examples of the basic Springer style used in publications on a wide range of subjects such as *Computer Science, Economics, Engineering, Geosciences, Life Sciences, Medicine, Biomedicine* are [21, 22, 24, 23, 25].

1. Broy, M.: Software engineering — from auxiliary to key technologies. In: Broy, M., Dener, E. (eds.) Software Pioneers, pp. 10-13. Springer, Heidelberg (2002)
2. Dod, J.: Effective substances. In: The Dictionary of Substances and Their Effects. Royal Society of Chemistry (1999) Available via DIALOG. http://www.rsc.org/dose/title of subordinate document. Cited 15 Jan 1999
3. Geddes, K.O., Czapor, S.R., Labahn, G.: Algorithms for Computer Algebra. Kluwer, Boston (1992)
4. Hamburger, C.: Quasimonotonicity, regularity and duality for nonlinear systems of partial differential equations. Ann. Mat. Pura. Appl. **169**, 321–354 (1995)
5. Slifka, M.K., Whitton, J.L.: Clinical implications of dysregulated cytokine production. J. Mol. Med. (2000) doi: 10.1007/s001090000086

6. J. Dod, in *The Dictionary of Substances and Their Effects*, Royal Society of Chemistry. (Available via DIALOG, 1999), http://www.rsc.org/dose/title of subordinate document. Cited 15 Jan 1999
7. H. Ibach, H. Lüth, *Solid-State Physics*, 2nd edn. (Springer, New York, 1996), pp. 45-56
8. S. Preuss, A. Demchuk Jr., M. Stuke, Appl. Phys. A **61**
9. M.K. Slifka, J.L. Whitton, J. Mol. Med., doi: 10.1007/s001090000086
10. S.E. Smith, in *Neuromuscular Junction*, ed. by E. Zaimis. Handbook of Experimental Pharmacology, vol 42 (Springer, Heidelberg, 1976), p. 593

[3] Make sure that all references from the list are cited in the text. Those not cited should be moved to a separate *Further Reading* section or chapter.

[4] Always use the standard abbreviation of a journal's name according to the ISSN *List of Title Word Abbreviations*, see http://www.issn.org/en/node/344

11. Calfee, R. C., & Valencia, R. R. (1991). *APA guide to preparing manuscripts for journal publication.* Washington, DC: American Psychological Association.
12. Dod, J. (1999). Effective substances. In: The dictionary of substances and their effects. Royal Society of Chemistry. Available via DIALOG.
http://www.rsc.org/dose/Effective substances. Cited 15 Jan 1999.
13. Harris, M., Karper, E., Stacks, G., Hoffman, D., DeNiro, R., Cruz, P., et al. (2001). Writing labs and the Hollywood connection. *J Film* Writing, 44(3), 213–245.
14. O'Neil, J. M., & Egan, J. (1992). Men's and women's gender role journeys: Metaphor for healing, transition, and transformation. In B. R. Wainrig (Ed.), *Gender issues across the life cycle* (pp. 107–123). New York: Springer.
15. Kreger, M., Brindis, C.D., Manuel, D.M., Sassoubre, L. (2007). Lessons learned in systems change initiatives: benchmarks and indicators. *American Journal of Community Psychology*, doi: 10.1007/s10464-007-9108-14.

16. Alber John, Daniel C. O'Connell, and Sabine Kowal. 2002. Personal perspective in TV interviews. *Pragmatics* 12:257–271
17. Cameron, Deborah. 1997. Theoretical debates in feminist linguistics: Questions of sex and gender. In *Gender and discourse*, ed. Ruth Wodak, 99–119. London: Sage Publications.
18. Cameron, Deborah. 1985. *Feminism and linguistic theory.* New York: St. Martin's Press.
19. Dod, Jake. 1999. Effective substances. In: The dictionary of substances and their effects. Royal Society of Chemistry. Available via DIALOG.
http://www.rsc.org/dose/title of subordinate document. Cited 15 Jan 1999
20. Suleiman, Camelia, Daniel C. O?Connell, and Sabine Kowal. 2002. 'If you and I, if we, in this later day, lose that sacred fire...?': Perspective in political interviews. *Journal of Psycholinguistic Research*. doi: 10.1023/A:1015592129296.

21. Brown B, Aaron M (2001) The politics of nature. In: Smith J (ed) The rise of modern genomics, 3rd edn. Wiley, New York
22. Dod J (1999) Effective Substances. In: The dictionary of substances and their effects. Royal Society of Chemistry. Available via DIALOG.
http://www.rsc.org/dose/title of subordinate document. Cited 15 Jan 1999
23. Slifka MK, Whitton JL (2000) Clinical implications of dysregulated cytokine production. J Mol Med, doi: 10.1007/s001090000086
24. Smith J, Jones M Jr, Houghton L et al (1999) Future of health insurance. N Engl J Med 965:325–329
25. South J, Blass B (2001) The future of modern genomics. Blackwell, London

Chapter 2
Contiki OS

Assuming this is the structure...

2.1 Security in Contiki OS

Implementing security protocols poses great difficulty in IoT devises due to the constrained resources and variant applications. In this section, we will cover two security components that has so far been implemented in Contiki OS, namely LLSEC and DTLS respectively.

2.1.1 LLSEC: noncoresec

Link Layer Security, or LLSEC, is a security mechanism at Link Layer level. In Contiki OS, noncoresec is the 802.15.4 security instantiation that has been implemented. Its design goal is to provide:

- Data confidentiality over MAC layer payload.
- Authenticity and integrity over MAC header and MAC payload.

noncoresec is disabled by default. When enabled, different security level can be configured from no security, to encryption / authentication only, then to full encryption and authentication.

To be more specifically, noncoresec has the following implemented:

Block Cipher
As specified by 802.15.4 specification, AES-128 is chosen as the underlying block cipher. Contiki OS implements a software AES, but on those platforms with an AES coprocessor, such as CC2538, it can be switched to use the hardware implementation instead. The benefit for doing so is to have a better time

and energy efficiency as well as to gain potential protections against side channel analysis attacks.

Mode of Operation

Also specified by 802.15.4 specification, the AES block cipher is used in CCM* mode, i.e. CTR mode with CBC-MAC. The asterisk symbol implies the additional support of security levels and additional requirement to encode the security level into the nonce.

Key Management

A hard coded 128 bit AES key is shared among the whole network in LLSEC. This effectively means that the same key will be used for all incoming and outgoing data frames on every node.

Replay Protection

noncoresec has implemented the replay protection by comparing the received frame counter with the last frame counter from the same source.

Therefore in general, noncoresec has the following benefits:

- It prevents an eavesdropper from seeing the plaintext of MAC Layer payload.
- It prevents illegal nodes from joining the network, as nodes without knowledge of the network shared key cannot forge a message.
- It can be implemented efficiently on most platforms, especially with hardware support.
- Multicast and broadcast is supported by the nature of 802.15.4.

However, the following factors should also be taken into concern when adopting noncoresec as the security measures:

- Lack of flexibility. This is mostly due to the fact that the key is hard coded.
- Fixed key. As there is yet no key updating scheme implemented.
- Reused nonce. Since in CCM mode, the difference of two ciphertext is exactly the same of their according plaintext and knowing that can lead to breach of data confidentiality in many cases. The reuse may occur when the 4 bytes frame counter rounds up, or when the devices reboots which resets the frame counter back to 0.
- The 802.15.4 frame header is not encrypted.

More discussion of 802.15.4 security can be found in [1].

2.1.2 DTLS

DTLS is derived from the widely used TLS protocol on Internet. As of TLS, DTLS also provides encryption and authentication between two nodes.

The main difference is that TLS is based on TCP whilst DTLS is based on UDP protocol, where the later one is more adapted to IoT applications. In addition, DTLS also provides a simple reliable transmission mechanism as a result for providing data integrity.

In Contiki OS, DTLS is provided by a third party implementation named tinydtls[2]. The current version of tinydtls supports two cipher suites:

TLS_PSK_WITH_AES_128_CCM_8
aaa

TLS_ECHDE_ECHSA_WITH_AES_128_CCM_8
bbb

Comparing to noncoresec which uses a hard coded network shared key, DTLS is a stateful session based protocol. This implies that:

- A handshake must be performed between two nodes before any data can be transmitted.
- Different session keys are derived for each session during the handshake.

References

1. Sastry N, Wagner D (2004) Security Considerations for IEEE 802.15.4 Networks. Proceedings of the 3rd ACM Workshop on Wireless Security 32–42
2. tinydtls.
http://tinydtls.sourceforge.net/

Appendix A
Chapter Heading

All's well that ends well

Use the template *appendix.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style appendix of your book in the Springer layout.

A.1 Section Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations.

A.1.1 Subsection Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the LaTeX automatism for all your cross-references and citations as has already been described in Sect. A.1.

For multiline equations we recommend to use the `eqnarray` environment.

$$\begin{aligned} \mathbf{a} \times \mathbf{b} &= \mathbf{c} \\ \mathbf{a} \times \mathbf{b} &= \mathbf{c} \end{aligned} \tag{A.1}$$

A.1.1.1 Subsubsection Heading

Instead of simply listing headings of different levels we recommend to let every heading be followed by at least a short passage of text. Furtheron please use the

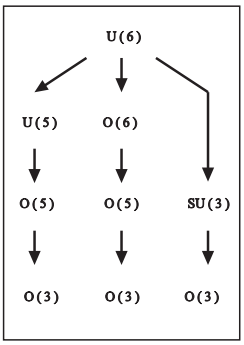

Fig. A.1 Please write your figure caption here

LaTeX automatism for all your cross-references and citations as has already been described in Sect. A.1.1.

Please note that the first line of text that follows a heading is not indented, whereas the first lines of all subsequent paragraphs are.

Table A.1 Please write your table caption here

Classes	Subclass	Length	Action Mechanism
Translation	mRNA[a]	22 (19–25)	Translation repression, mRNA cleavage
Translation	mRNA cleavage	21	mRNA cleavage
Translation	mRNA	21–22	mRNA cleavage
Translation	mRNA	24–26	Histone and DNA Modification

[a] Table foot note (with superscript)

Glossary

Use the template *glossary.tex* together with the Springer document class SVMono (monograph-type books) or SVMult (edited books) to style your glossary in the Springer layout.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

glossary term Write here the description of the glossary term. Write here the description of the glossary term. Write here the description of the glossary term.

Solutions

Problems of Chapter 1

1.1 The solution is revealed here.

1.2 Problem Heading
(a) The solution of first part is revealed here.
(b) The solution of second part is revealed here.