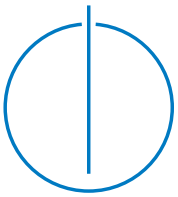
Department of Informatics
Technical University of Munich

Master's Thesis in Informatics

Multi-Party End-to-End Encryption for the Inverse Transparency Toolchain

Jonas Hagg



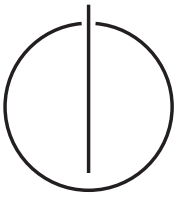
Department of Informatics
Technical University of Munich

Master's Thesis in Informatics

Multi-Party End-to-End Encryption for the Inverse Transparency Toolchain

Mehrparteien-Ende-zu-Ende-Verschlüsselung für die Inverse-Transparenz-Toolchain

Author: Jonas Hagg
Submission Date: December 15, 2022
Supervisor: Prof. Dr. Alexander Pretschner
Advisor: Valentin Zieglmeier



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

Garching, December 15, 2022 Jonas Hagg

Acknowledgments

Iff you want, you can use this section to thank your supervisors, your universities or just anybody else who has helped you writing your thesis. But for this template, I want to abuse this section for a little request: I want this template to be used for as many wonderful theses as possible. Therefore, this template needs advertisement. So, please tell your colleagues and supervisors about it. Thank you very much for your help!

Abstract

It 42654 is just a small template, that is hopefully helpful for writing your thesis. First, it gives a short introduction to its usage and the personalizations. Finally, it presents several examples of frequently used pieces of layout.

In general, it is a good idea to outline three things: (1) the problem you aim to solve, (2) the general solution to approach the problem and (3) your contribution on the way to establish the solution.

Finally, please do not forget to double check compliance to the official guidelines of your university/study program. They all differ in minor aspects and in addition change over time. Thereby, this template might not be fully accurate. **TODO$_1$: Assure compliance to the official guidelines and requirements** Ignoring this warning may require you to print your thesis again after your first try to hand in.

Contents

1 User manual

Indeed, another long manual for a tool [1] that aims for not requiring any guidance. However, it is highly recommended to read it thoroughly as it covers a lot of non-standard LaTeX features and helps you with getting the most out of this template. Have fun!

1.1 First steps

1.1.1 Compile it!

Before modifying any file, try if you can compile it! I – a long year Linux enthusiast – prefer vim and just running make in the project directory. But other toolchains works as well. For some files, I also use gummi – especially for drawing images –, but as long as you have LaTeX installed on your system, almost every editor should work as well. I have also tested it with TeXstudio. Although the navigation over the structure panel seems to be broken (it does not recognize the `\subfile` commands correctly), compilation works perfectly. As a workaround for broken navigation, I suggest compiling `main.tex` once, view the resulting PDF and use a right click on any text with "Go to Source" to jump to the corresponding `.tex`-file

1.1.2 Personalize the template

Your thesis is a very personal project, but – nevertheless – after all, it is an official document. Hence, there must be a lot of formal stuff in place. This template takes care of the layout, but you must provide the content. To add your personal information (e.g. your name, Topic, supervisors, etc.), just open `./myconfig.sty` with your favorite tex(t)-editor and edit the corresponding dummy data.

In the `./txt/`-directory you also find the dummy text for the abstract and the acknowledgments for the preface of the thesis. I do not suggest to start writing your thesis with those pieces of text, but if you want to add or adjust them later – now you know where they are waiting for you to fill them.

If you lack any LaTeX-package for some special purposes, feel free to add it to the package list in `./zxy/mypackages.sty`. The template does not split the package list into multiple files (e.g. for "template-packages" and "user-packages") to avoid double-listing of any package. Furthermore the order of the packages matters in rare corner cases you can solve some conflicts just by reordering. Inside the zyx-directory you also find all the internal files for setting up the cover and the surrounding pages. The average user should not be required to touch these files, but if something is broken, this is most likely the place to fix it.

1.1.3 Start writing

Of course, the biggest part of the thesis document is writing text. This template uses the `./txt`-directory for all of it. For the inclusion into the main document, you must put a corresponding entry into `main.tex`. The name of the file does not matter as the sequence of the entries in the tex-code determines the order of the included chapters.

Although I recommend adding a (not necessarily serial) number in front of the file names to represent the correct order in file browsers and across multiple editors. As a good starting point for new files just copy the `0-empty.tex` file and start writing in there. If you prefer having a subdirectory for each chapter, just create new folders inside the `txt`-directory. Afterward, adjust the file names inside `main.tex` corresponding to your subdirectory names and adapt the path to the main.tex in the \documentclass in the new/moved file (most likely to "`../..`" for one nested subdirectory).

1.2 Core ideas

1.2.1 Each `.tex`-file can be compiled on its own

Every file with a `.tex`-file extension can be compiled without any of the other `.tex`-files. If you want someone to read your abstract or only one of your chapters, just only compile the corresponding `.tex`-file and you get a single PDF only containing the current file. This is very convenient when drawing pictures with tikz (inside the img-folder) as they must be compiled and adjusted many times before they look perfect and having them separated speeds up their compile time immensely. Additionally, the generated pictures can be reused in other documents – for example in your final presentation.

1.2.2 Separate blown up LaTeX code from written text

Nothing is more distracting when reading text than huge blocks of random LaTeX macros spread between it. Hence, this templates does its best to split layout logic and the actual content into separate files. For example, the main file does not start with a few hundred lines of template and package stuff before you can organize your files. That also has a nice side effect: Everything inside the zyx directory requires a quite a decent LaTeX-skill, whereas adding new text becomes a fairly simple task.

1.2.3 Folder Structure

The root directory only contains few files, and the average user should not be required to add a new file there. `main.tex` is the entry point to your thesis. `Makefile`, `README.md`, `LICENSE` and `.gitignore` are needed to be at the top level to form a reasonable project setup. The `literature.bib` is the container for all the literature referenced anywhere in the thesis. Most scientific databases provide snippets in the BibTeX format that can directly be copied into it. However, be careful: Even the same database is not entirely consistent with the format of conference names and the longer the list becomes, the more likely it requires some manual adjustments. Finally, `make+docker.sh`, `.github/workflows/thesis-pdf.yml` and `.gitlab-ci.yml` are helper files for the continues integration pipeline. These can be ignored or deleted if the local build is working and you do not plan to use any external CI-Server.

img is the place for all images and pictures included in your thesis. The best way is to write your images as code and compile them, but having vector graphics in PDFs there is also fine (`git add -f name.pdf` may be helpful). You should avoid pixel based pictures like PNGs or JPGs wherever you can. If it is unavoidable provide at least 300dpi resolution for a high quality printout.

txt comprises all text files of your thesis, e.g. one file for each chapter or section in your thesis. Don't forget to register them in the `main.tex`.

zyx is a very strange name for a directory. It hides all LaTeX logic to compose the template and can be ignored by the average user. I choose this name because there exist no human word listed after this letters in a dictionary. Hence, it is always the last directory inside a directory what makes it easier to recognize and ignore it. Furthermore, it is still somehow pronounceable.

In case, you want to put tables, plots, code-snippets or whatever else into your thesis, I would recommend to create new folders in the root directory. This extends the original structure of the template and helps to keep the overview after months of work on your thesis document.

Nevertheless, feel free to adapt the directory structure to your needs and delete folders if you do not need them. There is no reason for keeping useless files or directories that only mess up your environment.

1.3 Minor Features

1.3.1 One or two sides per page

Depending on the amount of text you have written for your thesis, the final document will probably contain a lot of sides. Hence, I suggest printing two sides per page (one on the front and one on the back). In this way, the resulting book becomes not so thick and costs a lot less money for printing. If you want to use a single side per page layout instead, you can change this the `main.tex` by adjusting the `documentclass`. But no worry when you do not want to decide this now. The layout can also be adapted later as both setups have the same text dimensions and your text will look identical on both of them. No matter what design you chose, please don't forget to give a corresponding hint to the print shop. Finally, a small remark for all those, who look at this template with hawk eyes: The text is intentional not perfectly centered – instead the inner margin is a little bit bigger than the outer margin. That results in better readability after the pages are bound and glued to a book.

1.3.2 Integrated git version information

During writing your thesis, it is highly recommended to put your work under a version control system: to store older thoughts in case you need them later, for an easier backup and to proof that you have not copy-pasted your thesis. This template is prepared for git as it already provides a `.gitignore` file covering the most frequent use cases. So just initialize a new git repository in the root directory, and everything sets up automatically.

But there are even more benefits of using git for the template. It automatically adds the currently checked out branch and tag of the directory when the compilation starts as a keyword to the generated pdf document. That is particularly useful during the end phase of the thesis, where you most likely distribute some pdfs to different reviewers and it is quite easy to lost track, who has received which version, as some reviews arrive later than others. Depending on your pdf-viewer you can find it most likely somewhere under properties.

If you are not using the root directory of this template is the main directory of your git repository, you have to adjust the (relative) path to your git directory in the `./myconfig.sty`. In the rare case that your reviewer wants to print your thesis and returns a stack of paper with handwritten notes to you, the pdf meta-information is not helpful, but use the `wip` switch in the `main.tex` to print it on every page.

1.3.3 Create Submission Archive

After you are done with your thesis, your advisors may also want a copy of its source code. Of course, direct access to the git-repository is the best, but this also contains a lot of meta-data that arise privacy concerns (e.g. when exactly what part of the text was written). A good trade-off is to put all source files (i.e. all files under version control) and the final pdf into an archive. `make submit` creates such an archive.

1.3.4 Spell Checking

Detecting spelling and grammar errors inside multiple LaTeX documents is quite a complicated task because all the LaTeX commands obliterate the flow of the text. However, nothing can ruin a thesis as fast and gratuitous as spelling errors in each sentence. Of course, you can find somebody to proofread your thesis, but some automated tools as a first layer can be vital. Unfortunately, I am not aware of any flawless tool for this purpose.

First of all, you should set up your tex-editor to give you basic hints about wrong spelling. This is not a final solution, but a good starting point to prevent the most obvious errors. Most of the available editors support this feature—Just check the corresponding manual.

For more sophisticated grammar or text analysis, this template provides exports of the text from your thesis. If you have pandoc installed on your system or use docker, you can use "`make docx`" or "`make md`" for office or markdown exports. Although this output loses some text formatting, they can be imported in various professional checking tools. Of course directly in word, but some students also have used Grammarly or GrammarLookup. But keep in mind: the later are cloud-based systems, that most likely store a copy of your text permanently for further refinement of their tools. So expect all your text be read and evaluated by a third party, what is not an option for all situations.

Error: Cannot include ./txt/42-example.md. Please check your compiler toolchain

Bibliography

[1] Bithappens. *Template for Beautiful Theses*. 2016. URL: https://github.com/thesis-toolbox/template (visited on 02/20/2020).

A Lorem Ipsum

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.

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.

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.

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.

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.

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. 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.

Sed feugiat. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Ut pellentesque augue sed urna. Vestibulum diam eros, fringilla et, consectetuer eu, nonummy id, sapien. Nullam at lectus. In sagittis ultrices mauris.

Curabitur malesuada erat sit amet massa. Fusce blandit. Aliquam erat volutpat. Aliquam euismod. Aenean vel lectus. Nunc imperdiet justo nec dolor.

Etiam euismod. Fusce facilisis lacinia dui. Suspendisse potenti. In mi erat, cursus id, nonummy sed, ullamcorper eget, sapien. Praesent pretium, magna in eleifend egestas, pede pede pretium lorem, quis consectetuer tortor sapien facilisis magna. Mauris quis magna varius nulla scelerisque imperdiet. Aliquam non quam. Aliquam porttitor quam a lacus. Praesent vel arcu ut tortor cursus volutpat. In vitae pede quis diam bibendum placerat. Fusce elementum convallis neque. Sed dolor orci, scelerisque ac, dapibus nec, ultricies ut, mi. Duis nec dui quis leo sagittis commodo.

Aliquam lectus. Vivamus leo. Quisque ornare tellus ullamcorper nulla. Mauris porttitor pharetra tortor. Sed fringilla justo sed mauris. Mauris tellus. Sed non leo. Nullam elementum, magna in cursus sodales, augue est scelerisque sapien, venenatis congue nulla arcu et pede. Ut suscipit enim vel sapien. Donec congue. Maecenas urna mi, suscipit in, placerat ut, vestibulum ut, massa. Fusce ultrices nulla et nisl.

Etiam ac leo a risus tristique nonummy. Donec dignissim tincidunt nulla. Vestibulum rhoncus molestie odio. Sed lobortis, justo et pretium lobortis, mauris turpis condimentum augue, nec ultricies nibh arcu pretium enim. Nunc purus neque, placerat id, imperdiet sed, pellentesque nec, nisl. Vestibulum imperdiet neque non sem accumsan laoreet. In hac habitasse platea dictumst. Etiam condimentum facilisis libero. Suspendisse in elit quis nisl aliquam dapibus. Pellentesque auctor sapien. Sed egestas sapien nec lectus. Pellentesque vel dui vel neque bibendum viverra. Aliquam porttitor nisl nec pede. Proin mattis libero vel turpis. Donec rutrum mauris et libero. Proin euismod porta felis. Nam lobortis, metus quis elementum commodo, nunc lectus elementum mauris, eget vulputate ligula tellus eu neque. Vivamus eu dolor.

Nulla in ipsum. Praesent eros nulla, congue vitae, euismod ut, commodo a, wisi. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Aenean nonummy magna non leo. Sed felis erat, ullamcorper in, dictum non, ultricies ut, lectus. Proin vel arcu a odio lobortis euismod. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Proin ut est. Aliquam odio. Pellentesque massa turpis, cursus eu, euismod nec, tempor congue, nulla. Duis viverra gravida mauris. Cras tincidunt. Curabitur eros ligula, varius ut, pulvinar in, cursus faucibus, augue.

Nulla mattis luctus nulla. Duis commodo velit at leo. Aliquam vulputate magna et leo. Nam vestibulum ullamcorper leo. Vestibulum condimentum rutrum mauris. Donec id mauris. Morbi molestie justo et pede. Vivamus eget turpis sed nisl cursus tempor. Curabitur mollis sapien condimentum nunc. In wisi nisl, malesuada at, dignissim sit amet, lobortis in, odio. Aenean consequat arcu a ante. Pellentesque porta elit sit amet orci. Etiam at turpis nec elit ultricies imperdiet. Nulla facilisi. In hac habitasse platea dictumst. Suspendisse viverra aliquam risus. Nullam pede justo, molestie nonummy, scelerisque eu, facilisis vel, arcu.