

Practicalities and Topic Assignment

Dr. Michael Kirsten

Chair of Theoretical Computer Science and
Theorem Proving

Version of October 13, 2026



Goals of this Seminar

- ▶ Read a research paper
- ▶ Search and understand the background concepts
- ▶ Understand the paper contribution
- ▶ Elaborate on the key elements in your own words
- ▶ Provide new explanations or examples that you missed from the paper

NB: The talks and paper may be either in English or in German.

Schedule

When	What
2026-10-13	Practicalities and topic assignment
2026-10-20	Introduction to security
2026-10-27	Introduction to logic for security
2026-12-01	Lightning talks
2026-12-15	Draft submission
2026-12-22	Review submission
2027-01-19	Talks
2027-01-26	Talks
2027-02-02	Talks
2027-03-27	Paper submission

Topic Assignment

Overview paper: “Formalization of security” by Barthe (2026)

Topic Assignment

Overview paper: “Formalization of security” by Barthe (2026)

1. Information-flow control (Li et al., 2021)
2. Language-based security for imperative features (Silver et al., 2023)
3. Language-based security for higher-order languages (Gregersen et al., 2021)
4. Automated side-channel analysis of cryptographic protocol implementations (Nasrabadi, Künnemann, and Nemati, 2025)
5. Resource usage (Avanzini et al., 2024)
6. Access control and capabilities (Cutler et al., 2024)
7. Secure compilation (El-Korashy et al., 2022)
8. EasyCrypt is a rich resource-aware module system (Barbosa, Barthe, Grégoire, et al., 2023)
9. CryptHOL (Butler, Aspinall, and Gascón, 2020) to verify oblivious transfer protocols

Topic Assignment II

10. SSProve (Haselwarter et al., 2023) is a Rocq library for state-separating proofs
11. Interactive probabilistic dependency logic (Gancher et al., 2023)
12. Squirrel (Baelde et al., 2021) is a domain-specific proof assistant using the Bana–Comon approach
13. Security proofs against quantum adversaries using qRHL (Unruh, 2019)
14. Security proofs against quantum adversaries using EasyCrypt for post-quantum cryptography (Barbosa, Barthe, Fan, et al., 2021)
15. Security proofs in the symbolic model (Braje et al., 2022) formalize a model of cryptographic protocols with built-in safety checks
16. Correctness proofs (Erbsen et al., 2024) use Fiat-Crypto to verify a formally verified bare metal server that uses elliptic curve cryptography
17. Correctness proofs using the Verified Software Toolchain to establish the correctness of the TweetNaCl implementation of Curve 25519 (Schwabe et al., 2021)

Topic Assignment: Procedure

Send me your list of preferred topics, starting with your most-preferred choice, as a message on Moodle until 19 October.

The main focus for each topic is the cited paper, but additional references may be used and adjustments are possible if agreed with me in advance.

Alternative topics are also permitted if they are coordinated with me beforehand.

Lightning Talk

The *lightning talk* is short (i.e., **150 seconds** and **two slides**).

You should present your topic and answer the following questions:

- ▶ **What** is the paper about?
- ▶ **Why** is it relevant?
- ▶ **How** does the paper achieve its goal?

Seminar Paper Draft

You will submit an incomplete *draft* of your seminar paper.
The draft will be peer-reviewed.

The following sections must be complete:

- ▶ **Title**
- ▶ **Abstract**
- ▶ **Table of contents**
- ▶ **Introduction**

The “**content**” **sections** may be incomplete, but must contain **bullet points** of what should go there. The “Background” and “Related work” sections may be empty.

Good sources to help you prepare your paper:

- ▶ Lecture R2 “Structure” of the seminar “Scientific and Technical English”

Reviews

Each student will be given two drafts to review.

The *reviews* should be between 0.5 and 1 pages long and contain the following:

- ▶ **Summary of the draft:** This is for the authors to ensure that the reviewers understood the text as expected.
- ▶ **General comments:** Start by praising what you liked about the draft. Then go on with constructive critiques of things you liked less. Finally, you can ask the author to add things to the draft that would have helped you understand the content better.
- ▶ **Nitpicking:** Write small comments about specific phrases, definitions, formulas, code listings, tables, figures, etc.
e.g., In § 3.2, you write that “the optimized program was faster by 55 %” while Table 3 only shows an improvement of 5 %; one of these two numbers is probably wrong.

Seminar Talk

The *talk* must be 25 **minutes** long and will be followed by 5 minutes of questions. This means, that you should prepare 10 **to** 20 **slides**.

You should integrate the feedback to your talk into you seminar paper.

Good sources to help you prepare for your talk:

- ▶ Section “Abschlussvortrag” of the “Leitfaden für Abschlussarbeiten”
- ▶ Lecture R12 “Slides and Posters” of the seminar “Scientific and Technical English”

Seminar Paper

The *seminar paper* must be 7000 **to** 14 000 **symbols** long.
Whitespaces do not count as symbols.

Good sources to help you prepare your paper:

- ▶ Section “Schriftliche Arbeit” of the “Leitfaden für Abschlussarbeiten”
- ▶ Lecture R11 “Theses and Papers” of the seminar “Scientific and Technical English”

Grading

To pass this seminar, you need to:

- ▶ be **present** at the first meetings, at the lightning talks, and the final talks;
- ▶ hold a **lightning talk** (i.e., not graded);
- ▶ submit a **paper draft** before the specified deadline (i.e., not graded);
- ▶ submit two **reviews** before the specified deadline (i.e., not graded);
- ▶ pass the **seminar talk** (i.e., with a grade of 4.0 or better); and
- ▶ pass the **seminar paper** (i.e., with a grade of 4.0 or better).

The seminar talk counts for 40 % and the seminar paper for 60 % of the *final grade*.

References I

- [1] Martin Avanzini, Gilles Barthe, Benjamin Grégoire, Georg Moser, and Gabriele Vanoni. “Hopping Proofs of Expectation-Based Properties: Applications to Skiplists and Security Proofs”. In: *Proc. ACM Program. Lang.* 8.OOPSLA1 (2024), pp. 784–809. DOI: [10.1145/3649839](https://doi.org/10.1145/3649839).
- [2] David Baelde, Stéphanie Delaune, Charlie Jacomme, Adrien Koutsos, and Solène Moreau. “An Interactive Prover for Protocol Verification in the Computational Model”. In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 537–554. DOI: [10.1109/SP40001.2021.00078](https://doi.org/10.1109/SP40001.2021.00078).

References II

- [3] Manuel Barbosa, Gilles Barthe, Xiong Fan, Benjamin Grégoire, Shih-Han Hung, Jonathan Katz, Pierre-Yves Strub, Xiaodi Wu, and Li Zhou. “EasyPQC: Verifying Post-Quantum Cryptography”. In: *CCS '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. Ed. by Yongdae Kim, Jong Kim, Giovanni Vigna, and Elaine Shi. ACM, 2021, pp. 2564–2586. DOI: 10.1145/3460120.3484567.
- [4] Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Adrien Koutsos, and Pierre-Yves Strub. “Mechanized Proofs of Adversarial Complexity and Application to Universal Composability”. In: *ACM Trans. Priv. Secur.* 26.3 (2023), 41:1–41:34. DOI: 10.1145/3589962.
- [5] Gilles Barthe. “Formalization of security”. In: *CoRR abs/2607.28551* (2026). DOI: 10.48550/arXiv.2607.28551. arXiv: 2607.28551.

References III

- [6] Timothy M. Braje, Alice R. Lee, Andrew Wagner, Benjamin Kaiser, Daniel Park, Martine Kalke, Robert K. Cunningham, and Adam Chlipala. “Adversary Safety by Construction in a Language of Cryptographic Protocols”. In: *35th IEEE Computer Security Foundations Symposium, CSF 2022, Haifa, Israel, August 7-10, 2022*. IEEE, 2022, pp. 412–427. DOI: [10.1109/CSF54842.2022.9919638](https://doi.org/10.1109/CSF54842.2022.9919638).
- [7] David Butler, David Aspinall, and Adrià Gascón. “Formalising oblivious transfer in the semi-honest and malicious model in CryptHOL”. In: *Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020*. Ed. by Jasmin Blanchette and Catalin Hritcu. ACM, 2020, pp. 229–243. DOI: [10.1145/3372885.3373815](https://doi.org/10.1145/3372885.3373815).

References IV

- [8] Joseph W. Cutler, Craig Disselkoen, Aaron Eline, Shaobo He, Kyle Headley, Michael Hicks, Kesha Hietala, Eleftherios Ioannidis, John H. Kastner, Anwar Mamat, Darin McAdams, Matt McCutchen, Neha Rungta, Emina Torlak, and Andrew Wells. “Cedar: A New Language for Expressive, Fast, Safe, and Analyzable Authorization”. In: *Proc. ACM Program. Lang.* 8.OOPSLA1 (2024), pp. 670–697. DOI: 10.1145/3649835.
- [9] Akram El-Korashy, Roberto Blanco, Jérémy Thibault, Adrien Durier, Deepak Garg, and Catalin Hritcu. “SecurePtrs: Proving Secure Compilation with Data-Flow Back-Translation and Turn-Taking Simulation”. In: *35th IEEE Computer Security Foundations Symposium, CSF 2022, Haifa, Israel, August 7-10, 2022*. IEEE, 2022, pp. 64–79. DOI: 10.1109/CSF54842.2022.9919680.

References V

- [10] Andres Erbsen, Jade Philipoom, Dustin Jamner, Ashley Lin, Samuel Gruetter, Clément Pit-Claudel, and Adam Chlipala. “Foundational Integration Verification of a Cryptographic Server”. In: *Proc. ACM Program. Lang.* 8.PLDI (2024), pp. 1704–1729. DOI: [10.1145/3656446](https://doi.org/10.1145/3656446).
- [11] Joshua Gancher, Kristina Sojakova, Xiong Fan, Elaine Shi, and Greg Morrisett. “A Core Calculus for Equational Proofs of Cryptographic Protocols”. In: *Proc. ACM Program. Lang.* 7.POPL (2023), pp. 866–892. DOI: [10.1145/3571223](https://doi.org/10.1145/3571223).
- [12] Simon Oddershede Gregersen, Johan Bay, Amin Timany, and Lars Birkedal. “Mechanized logical relations for termination-insensitive noninterference”. In: *Proc. ACM Program. Lang.* 5.POPL (2021), pp. 1–29. DOI: [10.1145/3434291](https://doi.org/10.1145/3434291).

References VI

- [13] Philipp G. Haselwarter, Exequiel Rivas, Antoine Van Muylder, Théo Winterhalter, Carmine Abate, Nikolaj Sidorenko, Catalin Hritcu, Kenji Maillard, and Bas Spitters. “SSProve: A Foundational Framework for Modular Cryptographic Proofs in Coq”. In: *ACM Trans. Program. Lang. Syst.* 45.3 (2023), 15:1–15:61. DOI: [10.1145/3594735](https://doi.org/10.1145/3594735).
- [14] Shih-Wei Li, Xupeng Li, Ronghui Gu, Jason Nieh, and John Zhuang Hui. “A Secure and Formally Verified Linux KVM Hypervisor”. In: *42nd IEEE Symposium on Security and Privacy, SP 2021, San Francisco, CA, USA, 24-27 May 2021*. IEEE, 2021, pp. 1782–1799. DOI: [10.1109/SP40001.2021.00049](https://doi.org/10.1109/SP40001.2021.00049).
- [15] Faezeh Nasrabadi, Robert Künnemann, and Hamed Nemati. “Automated Side-Channel Analysis of Cryptographic Protocol Implementations”. In: *CoRR abs/2511.11385* (2025). DOI: [10.48550/arXiv.2511.11385](https://doi.org/10.48550/arXiv.2511.11385). arXiv: [2511.11385](https://arxiv.org/abs/2511.11385).

References VII

- [16] Peter Schwabe, Benoît Viguié, Timmy Weerwag, and Freek Wiedijk. “A Coq proof of the correctness of X25519 in TweetNaCl”. In: *34th IEEE Computer Security Foundations Symposium, CSF 2021, Dubrovnik, Croatia, June 21-25, 2021*. IEEE, 2021, pp. 1–16. DOI: [10.1109/CSF51468.2021.00023](https://doi.org/10.1109/CSF51468.2021.00023).
- [17] Lucas Silver, Paul He, Ethan Cecchetti, Andrew K. Hirsch, and Steve Zdancewic. “Semantics for Noninterference with Interaction Trees”. In: *37th European Conference on Object-Oriented Programming, ECOOP 2023, Seattle, Washington, United States, July 17-21, 2023*. Ed. by Karim Ali and Guido Salvaneschi. Vol. 263. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2023, 29:1–29:29. DOI: [10.4230/LIPIcs.ECOOP.2023.29](https://doi.org/10.4230/LIPIcs.ECOOP.2023.29).
- [18] Dominique Unruh. “Quantum relational Hoare logic”. In: *Proc. ACM Program. Lang.* 3.POPL (2019), 33:1–33:31. DOI: [10.1145/3290346](https://doi.org/10.1145/3290346).