Dr. Sebastian Berndt

sebastian.berndt@gmail.com http://seberndt.github.io @berndt_seb

Personal Data

Name	Sebastian Berndt
Date of Birth	27-04-1986
Postal Address	Selmsdorfer Weg 1 23568 Lübeck Germany
Phone	+49-151-23768013
Email	sebastian.berndt@gmail.com
Marital Status	Married, two children

Employment History

2020–·· **Postdoc,** Institute for IT Security (Prof. Dr. Thomas Eisenbarth), University of Lübeck

2017–2020 **Postdoc,** Department of Computer Science (Prof. Dr. Klaus Jansen), Kiel University

2012–2017 **Ph.D. Student,** Institute for Theoretical Computer Science (Prof. Dr. Rüdiger Reischuk), University of Lübeck

Education

2012 – 2018 **Ph.D.** in Computer Science (summa cum laude)
Thesis title: *New Results on Feasibilities and Limitations of Provable Secure Steganography.*
Advisor: Prof. Dr. Maciej Liśkiewicz

2010 – 2012 **MSc** in Computer Science, Kiel University.
Thesis title: *Robust Bin Packing — Theory and Praxis.*

2007 – 2010 **BSc** in Computer Science, Kiel University
Thesis title: *Robust Approximation Schemes for Online Bin Packing.*

Research Publications

Conference Proceedings

1. **Berndt**, **Sebastian**, Max A. Deppert, Klaus Jansen, and Lars Rohwedder. "Load Balancing: The Long Road from Theory to Practice". In: ***ALENEX***. SIAM, 2022, pp. 104–116. 🔗 DOI: 10.1137/1.9781611977042.9.

2. **Berndt**, **Sebastian**, Jan Wichelmann, Claudius Pott, Tim-Henrik Traving, and Thomas Eisenbarth. "ASAP: Algorithm Substitution Attacks on Cryptographic Protocols". In: ***AsiaCCS***. ACM, 2022, (accepted).

3. **Berndt**, **Sebastian**, Kilian Grage, Klaus Jansen, Lukas Johannsen, and Maria Kosche. "Robust Online Algorithms for Dynamic Choosing Problems". In: *Connecting with Computability - 17th Conference on Computability in Europe, **CiE** 2021, Virtual Event, Ghent, July 5-9, 2021, Proceedings*. Vol. 12813. Lecture Notes in Computer Science. Springer, 2021, pp. 38–49. 🔗 DOI: 10.1007/978-3-030-80049-9_4.

4. **Berndt**, **Sebastian**, Klaus Jansen, and Kim-Manuel Klein. "New Bounds for the Vertices of the Integer Hull". In: *4th Symposium on Simplicity in Algorithms, **SOSA** 2021, Virtual Conference, January 11-12, 2021.* SIAM, 2021, pp. 25–36. 🔗 DOI: 10.1137/1.9781611976496.3.

5. **Berndt**, **Sebastian**, Klaus Jansen, and Alexandra Lassota. "Tightness of Sensitivity and Proximity Bounds for Integer Linear Programs". In: ***SOFSEM** 2021: Theory and Practice of Computer Science - 47th International Conference on Current Trends in Theory and Practice of Computer Science, SOFSEM 2021, Bolzano-Bozen, Italy, January 25-29, 2021, Proceedings*. Vol. 12607. Lecture Notes in Computer Science. Springer, 2021, pp. 349–360. 🔗 DOI: 10.1007/978-3-030-67731-2_25.

6. Sieck, Florian, **Sebastian Berndt**, Jan Wichelmann, and Thomas Eisenbarth. "Util: : Lookup: Exploiting Key Decoding in Cryptographic Libraries". In: ***CCS** '21: 2021 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, Republic of Korea, November 15 - 19, 2021*. ACM, 2021, pp. 2456–2473. 🔗 DOI: 10.1145/3460120.3484783.

7. Wichelmann, Jan, **Sebastian Berndt**, Claudius Pott, and Thomas Eisenbarth. "Help, My Signal has Bad Device! - Breaking the Signal Messenger's Post-Compromise Security Through a Malicious Device". In: *Detection of Intrusions and Malware, and Vulnerability Assessment - 18th International Conference, **DIMVA** 2021, Virtual Event, July 14-16, 2021, Proceedings*. Vol. 12756. Lecture Notes in Computer Science. Springer, 2021, pp. 88–105. 🔗 DOI: 10.1007/978-3-030-80825-9_5.

8. Bannach, Max, **Sebastian Berndt**, Marten Maack, Matthias Mnich, Alexandra Lassota, Malin Rau, and Malte Skambath. "Solving Packing Problems with Few Small Items Using Rainbow Matchings". In: *45th International Symposium on Mathematical Foundations of Computer Science, **MFCS** 2020, August 24-28, 2020, Prague, Czech Republic*. Vol. 170. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 11:1–11:14. 🔗 DOI: 10.4230/LIPIcs.MFCS.2020.11.

9. Bannach, Max, **Sebastian Berndt**, Martin Schuster, and Marcel Wienöbst. "PACE Solver Description: Fluid". In: *15th International Symposium on Parameterized and Exact Computation, **IPEC** 2020, December 14-18, 2020, Hong Kong, China (Virtual Conference)*. Vol. 180. LIPIcs. (*invited paper*). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 27:1–27:3. 🔗 DOI: 10.4230/LIPIcs.IPEC.2020.27.

10. Bannach, Max, **Sebastian Berndt**, Martin Schuster, and Marcel Wienöbst. "PACE Solver Description: PID*". In: *15th International Symposium on Parameterized and Exact Computation, **IPEC** 2020, December 14-18, 2020, Hong Kong, China (Virtual Conference)*. Vol. 180. LIPIcs. (*invited paper*). Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 28:1–28:4. 🔗 DOI: 10.4230/LIPIcs.IPEC.2020.28.

11. Seker, Okan, **Sebastian Berndt**, Luca Wilke, and Thomas Eisenbarth. "SNI-in-the-head: Protecting MPC-in-the-head Protocols against Side-channel Analysis". In: ***CCS** '20: 2020 ACM SIGSAC Conference on Computer and Communications Security, Virtual Event, USA, November 9-13, 2020*. ACM, 2020, pp. 1033–1049. 🔗 DOI: 10.1145/3372297.3417889.

12. Bannach, Max and **Sebastian Berndt**. “Positive-Instance Driven Dynamic Programming for Graph Searching”. In: *Algorithms and Data Structures - 16th International Symposium, **WADS** 2019, Edmonton, AB, Canada, August 5-7, 2019, Proceedings*. Vol. 11646. Lecture Notes in Computer Science. Springer, 2019, pp. 43–56. 🔗 DOI: 10.1007/978-3-030-24766-9_4.

13. **Berndt**, **Sebastian**, Valentin Dreismann, Kilian Grage, Klaus Jansen, and Ingmar Knof. “Robust Online Algorithms for Certain Dynamic Packing Problems”. In: *Approximation and Online Algorithms - 17th International Workshop, **WAOA** 2019, Munich, Germany, September 12-13, 2019, Revised Selected Papers*. Vol. 11926. Lecture Notes in Computer Science. Springer, 2019, pp. 43–59. 🔗 DOI: 10.1007/978-3-030-39479-0_4.

14. **Berndt**, **Sebastian**, Leah Epstein, Klaus Jansen, Asaf Levin, Marten Maack, and Lars Rohwedder. “Online Bin Covering with Limited Migration”. In: *27th Annual European Symposium on Algorithms, **ESA** 2019, September 9-11, 2019, Munich/Garching, Germany*. Vol. 144. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, 18:1–18:14. 🔗 DOI: 10.4230/LIPIcs.ESA.2019.18.

15. Bannach, Max and **Sebastian Berndt**. “Practical Access to Dynamic Programming on Tree Decompositions”. In: *26th Annual European Symposium on Algorithms, **ESA** 2018, August 20-22, 2018, Helsinki, Finland*. Vol. 112. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018, 6:1–6:13. 🔗 DOI: 10.4230/LIPIcs.ESA.2018.6.

16. **Berndt**, **Sebastian**. “Computing Tree Width: From Theory to Practice and Back”. In: *Sailing Routes in the World of Computation - 14th Conference on Computability in Europe, **CiE** 2018, Kiel, Germany, July 30 - August 3, 2018, Proceedings*. Vol. 10936. Lecture Notes in Computer Science. (*invited paper*). Springer, 2018, pp. 81–88. 🔗 DOI: 10.1007/978-3-319-94418-0_8.

17. **Berndt**, **Sebastian** and Kim-Manuel Klein. “Using Structural Properties for Integer Programs”. In: *Sailing Routes in the World of Computation - 14th Conference on Computability in Europe, **CiE** 2018, Kiel, Germany, July 30 - August 3, 2018, Proceedings*. Vol. 10936. Lecture Notes in Computer Science. (*invited paper*). Springer, 2018, pp. 89–96. 🔗 DOI: 10.1007/978-3-319-94418-0_9.

18. **Berndt**, **Sebastian** and Maciej Liskiewicz. “On the Gold Standard for Security of Universal Steganography”. In: *Advances in Cryptology - **EUROCRYPT** 2018 - 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 - May 3, 2018 Proceedings, Part I*. Vol. 10820. Lecture Notes in Computer Science. Springer, 2018, pp. 29–60. 🔗 DOI: 10.1007/978-3-319-78381-9_2.

19. Bannach, Max, **Sebastian Berndt**, and Thorsten Ehlers. “Jdrasil: A Modular Library for Computing Tree Decompositions”. In: *16th International Symposium on Experimental Algorithms, **SEA** 2017, June 21-23, 2017, London, UK*. Vol. 75. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017, 28:1–28:21. 🔗 DOI: 10.4230/LIPIcs.SEA.2017.28.

20. **Berndt**, **Sebastian** and Maciej Liskiewicz. “Algorithm Substitution Attacks from a Steganographic Perspective”. In: *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, **CCS** 2017, Dallas, TX, USA, October 30 - November 03, 2017*. ACM, 2017, pp. 1649–1660. 🔗 DOI: 10.1145/3133956.3133981.

21. **Berndt**, **Sebastian**, Maciej Liskiewicz, Matthias Lutter, and Rüdiger Reischuk. “Learning Residual Alternating Automata”. In: *Proceedings of the Thirty-First **AAAI** Conference on Artificial Intelligence, February 4-9, 2017, San Francisco, California, USA*. AAAI Press, 2017, pp. 1749–1755.

22. **Berndt**, **Sebastian** and Maciej Liskiewicz. “Hard Communication Channels for Steganography”. In: *27th International Symposium on Algorithms and Computation, **ISAAC** 2016, December 12-14, 2016, Sydney, Australia*. Vol. 64. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, 16:1–16:13. 🔗 DOI: 10.4230/LIPIcs.ISAAC.2016.16.

23. **Berndt**, **Sebastian** and Maciej Liskiewicz. “Provable Secure Universal Steganography of Optimal Rate: Provably Secure Steganography does not Necessarily Imply One-Way Functions”. In: *Proceedings of the*

*4th ACM Workshop on Information Hiding and Multimedia Security, **IH&MMSec** 2016, Vigo, Galicia, Spain, June 20-22, 2016*. ACM, 2016, pp. 81–92. DOI: 10.1145/2909827.2930796.

24 **Berndt**, **Sebastian** and Rüdiger Reischuk. "Steganography Based on Pattern Languages". In: *Language and Automata Theory and Applications - 10th International Conference, **LATA** 2016, Prague, Czech Republic, March 14-18, 2016, Proceedings*. Vol. 9618. Lecture Notes in Computer Science. Springer, 2016, pp. 387–399. DOI: 10.1007/978-3-319-30000-9_30.

25 **Berndt**, **Sebastian**, Klaus Jansen, and Kim-Manuel Klein. "Fully Dynamic Bin Packing Revisited". In: *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques, **APPROX/RANDOM** 2015, August 24-26, 2015, Princeton, NJ, USA*. Vol. 40. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2015, pp. 135–151. DOI: 10.4230/LIPIcs.APPROX-RANDOM.2015.135.

Journal Articles

1 Bannach, Max and **Sebastian Berndt**. "Recent Advances in Positive-Instance Driven Graph Searching". In: ***Algorithms*** 15.2 (2022). DOI: 10.3390/a15020042.

2 Aranha, Diego F., **Sebastian Berndt**, Thomas Eisenbarth, Okan Seker, Akira Takahashi, Luca Wilke, and Greg Zaverucha. "Side-Channel Protections for Picnic Signatures". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst. (**CHES**)* 2021.4 (2021), pp. 239–282. DOI: 10.46586/tches.v2021.i4.239-282.

3 **Berndt**, **Sebastian**, Klaus Jansen, and Kim-Manuel Klein. "Fully dynamic bin packing revisited". In: ***Math. Program.*** 179.1 (2020), pp. 109–155. DOI: 10.1007/s10107-018-1325-x.

4 **Berndt**, **Sebastian** and Maciej Liskiewicz. "On the universal steganography of optimal rate". In: ***Inf. Comput.*** 275 (2020), p. 104632. DOI: 10.1016/j.ic.2020.104632.

5 Bannach, Max and **Sebastian Berndt**. "Practical Access to Dynamic Programming on Tree Decompositions". In: ***Algorithms*** 12.8 (2019), p. 172. DOI: 10.3390/a12080172.

Awards

2021 **Walter-Dosch teaching award** for the lecture "Advanced Cryptology"

2020 **Fourth place** (out of 15) in the exact track and **fifth place** (out of 10) in the heuristic tracks of the *PACE* challenge on parameterized algorithms (both descriptions were selected to appear in the *IPEC* 2020 proceedings)

2018 **Best Student Paper Award** for "Practical Access to Dynamic Programming on Tree Decompositions"

2017 **Third place** in "Track A: Treewidth" in the second *PACE* challenge on parameterized algorithms

2016 **Third place** in the track "sequential exact solver" and **third place** in the track "parallel heuristic solver" in the first *PACE* challenge on parameterized algorithms

Best Student Paper Award for "Provable Secure Universal Steganography of Optimal Rate"

Talks

2021 "Algorithm Substitution Attacks and Steganography", **Keynote ZITiS-Forschungsseminar**

"Kleine Veränderung, große Konsequenz: wie manipulierte Komponenten die Gesamtsicherheit aushebeln", **CAST Workshop**

2020 "New Bounds for the Vertices of the Integer Hull", **University of Göttingen**

"New Bounds for the Vertices of the Integer Hull", **University of Wrocław**

Talks (continued)

- ”ASAP: Algorithm Substitution Attacks on Cryptographic Protocols”, **University of Wuppertal**
- 2018 ”Computing Tree Width: Theory and Practice”, **University of Bergen**
- 2017 ”The PACE challenge: practical algorithms for tree width”, **Universidad de Chile**
- 2016 ”On the Relation between Steganography and Cryptography”, **Information Security Seminar, Queensland University of Technology**
- ”Computing tree decompostions via SAT solvers”, **Kiel University**
- 2015 ”Fully Dynamic Bin Packing Revisited”, **BIRS workshop Approximation Algorithms and Parameterized Complexity**
- ”Learnability does not imply Secure Steganography”, **Nordic Complexity Workshop**

Teaching

- **Lecturer** for ”Current Topics in IT Security” in 2021 teaching and designing half of the lectures (Lübeck)
- **Lecturer** for ”Advanced Cryptology” in 2021 teaching and designing the lectures (Lübeck)
- **Lecturer** for ”Introduction to IT Security and Reliability” in 2020 and 2021 teaching and designing half of the lectures (Lübeck)
- **Lecturer** for ”Secure Networks and Computer Forensics” in 2020 (winter and summer term) and 2021 teaching the forensics lectures (Lübeck)
- **Lecturer** for ”Introduction to Math for Dual-Subject Students” in 2018 and 2019 teaching and designing the lectures (Kiel)
- **Lecturer** for ”Online Algorithms” in 2018 teaching and designing the lectures (Kiel)
- Teaching Assistant for ”Algorithms and Datastructures” in 2018 and 2019 teaching tutorials and organizing the tutorials (Kiel)
- Teaching Assistant for ”Introduction to Operations Research” in 2017 and 2018 teaching tutorials (Kiel)
- **Lecturer** for ”Presentation and Documentation” in 2015 teaching four lectures (Lübeck)
- Teaching Assistant for ”Coding and Security” in 2013, 2014, 2015, and 2016 teaching tutorials and some of the lectures (Lübeck)
- Teaching Assistant for ”Introduction to IT Security and Reliability” in 2012, 2013, 2014, 2015, and 2016 teaching tutorials and some of the lectures (Lübeck)
- Teaching Assistant for ”Algorithm Design” in 2012, 2013, 2014, 2015, and 2016 teaching tutorials and some of the lectures (Lübeck)

Supervised Theses

- 2022 Master Thesis on ”Prevention of combined probing and fault attacks using active multiparty computation in the honest-majority setting” (ongoing)
- Master Thesis on ”Fault Attacks on BIKE” (ongoing)
- Master Thesis on ”Side-Channel Resistance of Sponge Constructions” (ongoing)
- Bachelor Thesis on ”Implementation of Cryptographic Reverse Firewalls” (ongoing)
- Bachelor Thesis on ”Experimental Evaluation of Knapsack Distributions” (ongoing)
- 2021 Master Thesis on ”Secure and Fast Outsourced Machine Learning” (now a Ph. D. student in Lübeck)
- Bachelor Thesis on ”Algorithm Substitution Attacks on Matrix”

Supervised Theses (continued)

- Bachelor Thesis on ”Comparison of AES-based MPCitH protocols”
- 2020 Master Thesis on ”Algorithms for Mixed Integer Linear Programs” (now a Ph. D. student in Frankfurt)
- Bachelor Thesis on ”Noncense - Algorithm Substitution Attacks on TLS”
- Bachelor Thesis on ”Algorithms for RSA Key Recovery”
- 2019 Master Thesis on ”Amortised Migration for Maximization Problems” (now a Ph. D. student in Göttingen)
- Bachelor Thesis on ”Deterministic Algorithms for Discrepancy Minimization”
- 2018 Bachelor Thesis on ”Mobility 4.0 - Optimizing Vehicle Planning by Scheduling Algorithms”
- Bachelor Thesis on ”Sensitivity Analysis with the Steinitz Lemma”
- 2015 Bachelor Thesis on ”Lower Bounds in Online Bin Packing Models”
- Bachelor Thesis on ”Secure Multiparty Computations in Bitcoin”
- Bachelor Thesis on ”Development and Examination of a Huffman-coding based Stegosystem” (now a Ph. D. student at Lübeck)

Academic Service

- I was on the program committee of the following conferences: *CHES* 2021, *INDOCRYPT* 2021, *COSADE* 2021, *ARES* 2021 and 2022, *S&P* 2021 (shadow committee)
- I was an external reviewer for the following conferences: *STOC, SODA, CRYPTO, EUROCRYPT, Usenix, S&P, ESA, ICALP, STACS, ISAAC, IPDPS, ALT, WG, LATIN, WAOA, SOFSEM, CIE, OPTA*
- I was a reviewer for the following journals: *Algorithmica, Int. J. Inform. Secur., IPL, JAIR, JCSS, JEA, Journal of Combinatorial Optimization, Journal of Optimization Theory and Applications, Journal of Scheduling, Trans. Inf. Forensics Secur.*

Extracurricular Activities

- 2021 Gave a public talk about steganography (Link)
- Taught parts of a four day summer course on IT security to a group of pupils from age 14 to 17 (Link)
- 2020 Helped with writing a grant proposal on secure open hardware
- Taught a week-long summer course on IT security to a group of pupils from age 14 to 17 (Link)
- 2019 Helped with writing a grant proposal on robust online algorithms
- Deputy Member of the ”Study Committee” (Studienausschuss) of the Department of Computer Science of Kiel University
- 2018 Co-organized the annual ”day of business informatics” (Link)
- Taught four lectures of one hour to a group of pupils (Link)
- 2017 Helped with writing a grant proposal on parameterized scheduling problems (accepted for about 300.000€) (Link)
- Taught a day-long course on algorithmics in the context of the ”Girls' Day” for female pupils from age 14 to 15 (Link)
- 2016 Taught a week-long summer course on algorithms to a group of pupils from age 14 to 17 based on *Computer Science Unplugged* (Link)

Extracurricular Activities (continued)

- Organizing Commitee of *Creative Mathematical Sciences Communication* (Link)
- 2012 – 2015 Received the “*Teaching Certificate II*” by taking more than ten courses in e. g. team leading, presentation techniques and others (Link)