

# Sebastian Berndt

---

Research Areas: algorithms, cryptography, it security

Publications: AAAI, APPROX, CCS, ESA, EUROCRYPT, SEA, ... ([Link](#))

Teaching: Algorithms and Datastructures, Algorithm Design, IT-Security, Coding Theory, ([Link](#))

Education: BSc, MSc, Ph.D. ([Link](#))

---

## Education

2018	Ph.D. in Computer Science, "New Results on Feasibilities and Limitations of Provable Secure Steganography", Advisor: Prof. Dr. Maciej Liśkiewicz (summa cum laude)
2012	MSc in Computer Science, Kiel University
2010	BSc in Computer Science, Kiel University

## Employment

2020–	Research Associate, Institute for IT Security (Prof. Dr. Thomas Eisenbarth), University of Lübeck
2017–2020	Research Associate, Department of Computer Science (Prof. Dr. Klaus Jansen), Kiel University
2012–2017	Research Associate, Ph.D. Student, Institute for Theoretical Computer Science (Prof. Dr. Rüdiger Reischuk), University of Lübeck

## Awards

2020	Fourth place (out of 15) in the exact track and fifth place (out of 10) in the heuristic tracks of the <i>PACE</i> challenge on parameterized algorithms (both descriptions chosen to appear in <i>IPEC</i> 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 <i>PACE</i> challenge on parameterized algorithms
2016	Third place in the tracks »sequential exact solver« and »parallel heuristic solver« in the first <i>PACE</i> challenge on parameterized algorithms
2016	Best Student Paper Award for "Provable Secure Universal Steganography of Optimal Rate"

email: [sebastian.berndt@gmail.com](mailto:sebastian.berndt@gmail.com)

URL: <http://seberndt.github.io/>

## Talks

- 2015a "Learnability does not imply Secure Steganography", Nordic Complexity Workshop
- 2015b "Fully Dynamic Bin Packing Revisited", [Approximation Algorithms and Parameterized Complexity](#)
- 2016a "Computing tree decompositions via SAT solvers", Kiel University
- 2016b "On the Relation between Steganography and Cryptography", Information Security Seminar, Queensland University of Technology
- 2017 "The PACE challenge: practical algorithms for tree width", Universidad de Chile
- 2018 "Computing Tree Width: Theory and Practice", University of Bergen
- 2020a "New Bounds for the Vertices of the Integer Hull", University of Göttingen
- 2020b "New Bounds for the Vertices of the Integer Hull", University of Wrocław
- 2020c "ASAP: Algorithm Substitution Attacks on Cryptographic Protocols", University of Wuppertal
- 2021a "Kleine Veränderung, große Konsequenz: wie manipulierte Komponenten die Gesamtsicherheit aushebeln", CAST Workshop
- 2021b "Algorithm Substitution Attacks and Steganography ", **Keynote** ZITIS-Forschungsseminar

## Publications

### Conference Proceedings

- 2015 Berndt, Sebastian and Jansen, Klaus and Klein, Kim-Manuel<sup>\*†</sup> (2015),  
"Fully Dynamic Bin Packing Revisited", *APPROX/RANDOM 2015*
- 2016a Berndt, Sebastian and Reischuk, Rüdiger<sup>\*</sup> (2016),  
"Steganography Based on Pattern Languages", *LATA 2016*
- 2016b Berndt, Sebastian and Liśkiewicz, Maciej<sup>\*</sup> (2016),  
"Provable Secure Universal Steganography of Optimal Rate", *ACM IH&MMSEC 2016*  
**Awarded Best Student Paper**
- 2016c Berndt, Sebastian and Liśkiewicz, Maciej<sup>\*</sup> (2016),  
"Hard Communication Channels for Steganography", *ISAAC 2016*
- 2017a Berndt, Sebastian and Liśkiewicz, Maciej and Lutter, Matthias<sup>†</sup> and Reischuk, Rüdiger<sup>\*</sup> (2017),  
"Learning Residual Alternating Automata", *AAAI 2017*
- 2017b Bannach, Max<sup>†</sup> and Berndt, Sebastian and Ehlers, Thorsten<sup>†\*</sup> (2017),  
"Jdrasil: A Modular Library for Computing Tree Decompositions", *SEA 2017*
- 2017c Berndt, Sebastian and Liśkiewicz, Maciej<sup>\*</sup> (2017),  
"Algorithm Substitution Attacks from a Steganographic Perspective", *CCS 2017*
- 2018a Berndt, Sebastian and Liśkiewicz, Maciej<sup>\*</sup> (2018),  
"On the Gold Standard for Security of Universal Steganography", *EUROCRYPT 2018*
- 2018b Berndt, Sebastian (2018),  
"Computing Tree Width: From Theory to Practice and Back", *CIE 2018* (invited)
- 2018c Berndt, Sebastian and Klein, Kim-Manuel<sup>\*</sup> (2018),  
"Using Structural Properties for Integer Programs", *CIE 2018* (invited)
- 2018d Bannach, Max<sup>†</sup> and Berndt, Sebastian<sup>\*</sup> (2018),  
"Practical Access to Dynamic Programming on Tree Decompositions", *ESA 2018*  
**Awarded Best Student Paper (Track B)**

---

<sup>\*</sup>The authors are alphabetically sorted

<sup>†</sup>This author was a Ph. D. student at time of writing

email: [sebastian.berndt@gmail.com](mailto:sebastian.berndt@gmail.com)

URL: <http://seberndt.github.io/>

- 2019a Bannach, Max† and Berndt, Sebastian\* (2019),  
"Positive-Instance Driven Dynamic Programming for Graph Searching", *WADS 2019*
- 2019b Berndt, Sebastian and Epstein, Leah and Jansen, Klaus and Levin, Asaf and Maack, Marten† and Rohwedder, Lars†\* (2019),  
"Online Bin Covering with Limited Migration", *ESA 2019*
- 2019c Berndt, Sebastian and Dreismann, Valentin‡ and Grage, Kilian† and Jansen, Klaus and Knof, Ingmar‡\* (2019),  
"Robust Online Algorithms for Certain Dynamic Packing Problems", *WAOA 2019*
- 2020a Bannach, Max and Berndt, Sebastian and Maack, Marten† and Mnich, Matthias and Lassota, Alexandra† and Rau, Malin and Skambath, Malte†\* (2020),  
"Solving Packing Problems with Few Small Items Using Rainbow Matchings", *MFCS 2020*
- 2020b Seker, Okan† and Berndt, Sebastian and Wilke, Luca† and Eisenbarth, Thomas (2020),  
"SNI-in-the-head: Protecting MPC-in-the-head Protocols against Side-channel Analysis", *CCS 2020*
- 2020c Bannach, Max and Berndt, Sebastian and Schuster, Martin and Wienöbst, Marcel†\* (2020),  
"PACE Solver Description: Fluid", *IPEC 2020* (invited)
- 2020d Bannach, Max and Berndt, Sebastian and Schuster, Martin and Wienöbst, Marcel†\* (2020),  
"PACE Solver Description: PID\*", *IPEC 2020* (invited)
- 2021a Berndt, Sebastian and Jansen, Klaus and Lassota, Alexandra†\* (2021),  
"Tightness of Sensitivity and Proximity Bounds for Integer Programs", *SOFSEM 2021*
- 2021b Berndt, Sebastian and Jansen, Klaus and Klein, Kim-Manuel\* (2021),  
"New Bounds for the Vertices of the Integer Hull", *SOSA 2021*
- 2021c Berndt, Sebastian and Grage, Kilian† and Jansen, Klaus and Johannsen, Lukas§ and Kosche, Maria†\* (2021),  
"Robust Online Algorithms for Dynamic Choosing Problems", *CIE 2021*
- 2021d Wichelmann, Jan† and Berndt, Sebastian and Pott, Claudius† and Eisenbarth, Thomas (2021),  
"Help, my Signal has bad Device! - Breaking the Signal Messenger's Post-Compromise Security through a Malicious Device", *DIMVA 2021*
- 2021e Aranha, Diego F. and Berndt, Sebastian and Eisenbarth, Thomas and Seker, Okan† and Takahashi, Akira† and Wilke, Luca† and Zaverucha, Greg\* (2021),  
"Side-Channel Protections for Picnic Signatures", *CHES 2021*
- 2021f Sieck, Florian† and Berndt, Sebastian and Wichelmann, Jan† and Eisenbarth, Thomas (2021),  
"Util::Lookup: Exploiting key decoding in cryptographic libraries", *CCS 2021*

## Journal Publications

- 2018 Berndt, Sebastian and Klein, Kim-Manuel and Jansen, Klaus (2018),  
"Fully Dynamic Bin Packing Revisited", *Math. Program.* 2020 179  
preliminary version was presented at *APPROX/RANDOM 2015*
- 2019 Bannach, Max† and Berndt, Sebastian (2019),  
"Practical Access to Dynamic Programming on Tree Decompositions", *Algorithms* 2019 12(8), 172  
preliminary version was presented at *ESA 2018*
- 2020 Berndt, Sebastian and Liśkiewicz, Maciej (2020),  
"On the universal steganography of optimal rate", *Information and Computation* 275  
preliminary version was presented at *ACM IH&MMSEC 2016*

---

†This author was a M.Sc. student at time of writing

§This author was a B.Sc. student at time of writing

## Non-Peer-Reviewed Works

2018 Bannach, Max† and Berndt, Sebastian and Ehlers, Thorsten† and Nowotka, Dirk (2018), "SAT-Encoding of Tree Decompositions", *SAT COMPETITION 2018*

## Teaching

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

## Supervised Theses

2015a Bachelor Thesis on "Lower Bounds in Online Bin Packing Models"

2015b Bachelor Thesis on "Secure Multiparty Computations in Bitcoin"

2015c Bachelor Thesis on "Development and Examination of a Huffman-coding based Stegosystem" (now a Ph. D. student at Lübeck)

2018a Bachelor Thesis on "Mobility 4.0 - Optimizing Vehicle Planning by Scheduling Algorithms"

2018b Bachelor Thesis on "Sensitivity Analysis with the Steinitz Lemma"

2019a Master Thesis on "Amortised Migration for Maximization Problems" (now a Ph. D. student in Göttingen)

2019b Bachelor Thesis on "Deterministic Algorithms for Discrepancy Minimization"

2020a Master Thesis on "Algorithms for Mixed Integer Linear Programs" (now a Ph. D. student in Frankfurt)

2020b Bachelor Thesis on "Noncense - Algorithm Substitution Attacks on TLS"

2020c Bachelor Thesis on "Algorithms for RSA Key Recovery"

email: [sebastian.berndt@gmail.com](mailto:sebastian.berndt@gmail.com)

URL: <http://seberndt.github.io/>

## Extracurricular Activities

2012–2015	Received the “ <i>Teaching Certificate II</i> ” by taking more than 10 courses in e.g. team leading, presentation techniques and others ( <a href="#">Link</a> )
2016	Organizing Committee of <i>Creative Mathematical Sciences Communication</i> ( <a href="#">Link</a> )
2016	Taught a week-long summer course on algorithms to a group of pupils from age 14 to 17 based on <i>Computer Science Unplugged</i> ( <a href="#">Link</a> )
2016	Developed the tool <i>Jdrasil</i> to compute tree decompositions ( <a href="#">Link</a> )
2018	Taught a day-long course on algorithmics in the context of the “Girls’ Day” for female pupils from age 14 to 15 ( <a href="#">Link</a> )
2017	Helped with writing a grant proposal on parameterized scheduling problems (accepted for about 300.000€)
2018	Taught four lectures of one hour to a group of pupils ( <a href="#">Link</a> )
2018	Co-organized the annual “day of business informatics” ( <a href="#">Link</a> )
2019	Deputy Member of the “Study Committee” (Studienausschuss) of the Department of Computer Science of Kiel University
2019	Helped with writing a grant proposal on robust online algorithms
2020	Taught a week-long summer course on IT security to a group of pupils from age 14 to 17 ( <a href="#">Link</a> )
2020	Helped with writing a grant proposal on secure open hardware

## Academic Service

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