

# Bewerbung Sebastian Berndt

## Persönliche Daten

Name	Sebastian Berndt
Geburtsdatum	27-04-1986
Adresse	Selmsdorfer Weg 1 23568 Lübeck Germany
Telefon	+49-151-23768013
Email	sebastian.berndt@gmail.com
Familienstatus	Verheiratet, zwei Kinder

## Ausbildung

2012 – 2018	<b>Dr. rer. nat.</b> in Informatik (summa cum laude), Universität zu Lübeck. Titel: <i>New Results on Feasibilities and Limitations of Provable Secure Steganography</i> . Doktorvater: Prof. Dr. Maciej Liśkiewicz
2010 – 2012	<b>M.Sc.</b> in Informatik, Christian-Albrechts-Universität Kiel. Titel: <i>Robust Bin Packing — Theory and Praxis</i> .
2007 – 2010	<b>B.Sc.</b> in Informatik, Christian-Albrechts-Universität Kiel. Titel: <i>Robust Approximation Schemes for Online Bin Packing</i> .







## Akademische Positionen

2022–...	<b>Vertretungsprofessur</b> , Institut für Theoretische Informatik, Universität zu Lübeck
2022	<b>Ruf auf Assistant Professorship</b> , Services and Cybersecurity group, University of Twente (abgelehnt)
2020–2022	<b>Postdoc</b> , Institut für IT-Sicherheit (Prof. Dr. Thomas Eisenbarth), Universität zu Lübeck
2017–2020	<b>Postdoc</b> , Institut für Informatik (Prof. Dr. Klaus Jansen), Christian-Albrechts-Universität Kiel
2012–2017	<b>Doktorand</b> , Institut für Theoretische Informatik (Prof. Dr. Rüdiger Reischuk), Universität zu Lübeck
























## Forschungsinteressen

- Algorithmik, Kryptographie, IT-Sicherheit, Künstliche Intelligenz

## Auszeichnungen

- 2022  **Walter-Dosch-Lehrpreis** für Nachwuchs-Wissenschaftler der Universität zu Lübeck
- 2020  **Vierter Platz** im *Track A: Exact* und **fünfter Platz** im *Track B: Heuristic* der PACE challenge
- 2018  **Best Student Paper Award** für *Practical Access to Dynamic Programming on Tree Decompositions*, ESA 2018
- 2017  **Dritter Platz** im *Track A: Treewidth* in der zweiten PACE challenge
- 2016  **Dritter Platz** im *Track A: sequential exact solver* und **dritter Platz** im *Track B: parallel heuristic solver* in der ersten PACE challenge
-  **Best Student Paper Award** für *Provable Secure Universal Steganography of Optimal Rate*, ACM IH&MMSec 2016

## Lehre (inklusive Abschlussarbeiten)

- 2022  Dozent für *Codierung und Sicherheit* (Lübeck)
-  Dozent für *Cybersecurity* (Lübeck)
-  Dozent für *Algorithmik, Logik und Komplexität* (Lübeck)
-  Dozent für *Aktuelle Themen der IT-Sicherheit* (Lübeck)
- 2021, 2022  Dozent für *Advanced Cryptology* (Lübeck)
- 2020, 2021  Dozent für *Einführung in die IT-Sicherheit und Zuverlässigkeit* (Lübeck)
-  Dozent für *Sichere Netze und Computerforensik* (Lübeck)
- 2018, 2019  Dozent für *Mathematik für Algorithmiker* (Kiel)
- 2018  Dozent für *Online-Algorithmen* (Kiel)
- 2018, 2019  Assistent für *Algorithmen und Datenstrukturen* (Kiel)
-  Assistent für *Einführung in Operations Research* (Kiel)
- 2015  Dozent für *Präsentieren und Dokumentieren* (Lübeck)
- 2013–2016  Assistent für *Codierung und Sicherheit* (Lübeck)
- 2012–2016  Assistent für *Einführung in die IT-Sicherheit und Zuverlässigkeit* (Lübeck)
-  Assistent für *Algorithmen design* (Lübeck)
- 2022  Master Thesis, Sophie Ketelsen, *Fault attacks against BIKE* (in Bearbeitung)
-  Master Thesis, Julia Tönnies, *On the leakage resilience of XMSS with SHA-3* (in Bearbeitung)
-  Master Thesis, Paula Arnold, *Preventing combined probing and fault attacks using active MPC* (in Bearbeitung)
-  Master Thesis, Jonah Heller, *Using lattice predicates for the hidden number problem* (in Bearbeitung)
- 2021  Master Thesis, Jonas Sander, *Secure and Fast Outsourced Machine Learning* (jetzt Doktorand in Lübeck)
- 2020  Master Thesis, Leonie Krull, *Algorithms for Mixed Integer Linear Programs* (jetzt Doktorandin in Frankfurt)
- 2019  Master Thesis, Maria Kosche, *Amortised Migration for Maximization Problems* (jetzt Doktorandin in Göttingen)
- 2015–2022  Betreuung von fünfzehn Bachelor-Arbeiten

## Akademisches Engagement und weitere Aktivitäten

- Mitglied im Editorial Board von *Information Processing Letters*
  - Mitglied im Programm-Komitee: *CHES* 2021 und 2022, *INDOCRYPT* 2021, *COSADE* 2021, *ARES* 2021 und 2022, *S&P* 2021 (shadow committee)
  - Externer Gutachter für die folgenden Konferenzen: *STOC*, *SODA*, *CRYPTO*, *EUROCRYPT*, *Usenix*, *S&P*, *ESA*, *ICALP*, *STACS*, *ISAAC*, *IPDPS*, *ALT*, *WG*, *LATIN*, *WAOA*, *SOFSEM*, *CIE*, *OPTA*
  - Gutachter für die folgenden Zeitschriften: *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.*
  - Mitarbeit an unterschiedlichen Förderungsanträgen
- 
- 2021 ■ Dozent für einen viertägigen Sommerkurs für Schüler (Link)
  - 2020 ■ Dozent für einen viertägigen Sommerkurs für Schüler (Link)
  - 2019 ■ Stellvertretendes Mitglied des Studienausschusses des Instituts für Informatik der Christian-Albrechts-Universität Kiel
  - 2018 ■ Organisator des *Tag der Wirtschaftsinformatik* (Link)
  - Dozent für das Schnupperstudium für Schüler (Link)
  - 2017 ■ Dozent für einen Kurs über Algorithmen im Rahmen des *Girl's day* (Link)
  - 2016 ■ Dozent für einen einwöchigen Kurs über Algorithmen für Schüler (Link)
  - Co-Organisator des Workshops *Creative Mathematical Sciences Communication* (Link)
  - 2012 – 2015 ■ Besuch von mehr als zehn Kursen über verschiedenen Themen der Didaktik, der Teamleitung und anderen zum Erwerb des *Lehrzertifikat II*. (Link)






## Konferenzvorträge

- 2022 ■ *ASAP: Algorithm Substitution Attacks on Cryptographic Protocols*, **ASIACCS**
- 2021 ■ *Util::Lookup: Exploiting Key Decoding in Cryptographic Libraries*, **CCS**
- *New Bounds for the Vertices of the Integer Hull*, **SOSA**
- 2018 ■ *Computing Tree Width: From Theory to Practice and Back*, **CiE**
- 2017 ■ *Hard Communication Channels for Steganography*, **ISAAC**
- 2016 ■ *Provable Secure Universal Steganography of Optimal Rate: Provably Secure Steganography does not Necessarily Imply One-Way Functions*, **ACM IH&MMSec**
- *Steganography Based on Pattern Languages*, **LATA**
- 2015 ■ *Fully Dynamic Bin Packing Revisited*, **APPROX**




## Weitere Vorträge

- 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*, **Universität Göttingen**
- *New Bounds for the Vertices of the Integer Hull*, **University of Wrocław**
- *ASAP: Algorithm Substitution Attacks on Cryptographic Protocols*, **Universität Wuppertal**
- 2018 ■ *Computing Tree Width: Theory and Practice*, **University of Bergen**

## Weitere Vorträge (fortgesetzt)

- 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 decompositions via SAT solvers*, **Christian-Albrechts-Universität Kiel**
- 2015  *Fully Dynamic Bin Packing Revisited*, **BIRS workshop Approximation Algorithms and Parameterized Complexity**
-  *Learnability does not imply Secure Steganography*, **Nordic Complexity Workshop**

## Repräsentative Publikationen

- CCS 2020  In der Arbeit *SNI-in-the-head: Protecting MPC-in-the-head Protocols against Side-channel Analysis* haben wir das MPC-in-the-head Entwurfsmuster zur Konstruktion von Zero-Knowledge Beweisen untersucht, welches inzwischen in zahlreichen Anwendungen benutzt wird, unter anderem im Post-Quantum-Signaturverfahren **Picnic**. Wir waren zunächst in der Lage, einen konkreten Seitenkanalangriff auf nahezu alle Verfahren, die dieses Entwurfsmuster nutzen, zu finden. Als Gegenmaßnahme konnten wir das Verfahren so erweitern, dass eine große Klasse von Seitenkanalangriffen beweisbar ausgeschlossen werden kann. Dies ist das erste Verfahren, welches einen Schutz gegen Seitenkanalangriffe bereits auf der Protokoll-Ebene umsetzt.
- ESA 2019  In der Arbeit *Online Bin Covering with Limited Migration* haben wir uns mit einem Semi-Online-Szenario auseinander gesetzt. Hierbei erscheinen Objekte über die Zeit, dürfen aber, im Gegensatz zum reinen Online-Szenario, auch für gewisse Kosten umgepackt werden. Wir haben uns mit dem Problem **BIN COVERING** beschäftigt, welches als duales Problem zu **BIN PACKING** das Ziel hat, möglichst viele Behälter zu füllen. Hierbei haben wir alle vier möglichen Fälle (mit und ohne Löschen von Objekten und mit und ohne Amortisierung) untersucht und jeweils Algorithmen mit sehr beschränkten Umpackungskosten entwickelt. Weiterhin haben wir für alle vier Fälle zeigen können, dass diese Umpackungskosten asymptotisch optimal sind, also kein Algorithmus niedrigere Kosten haben kann.
- EUROCRYPT 2018  In der Arbeit *On the Gold Standard for Security of Universal Steganography* haben wir uns mit asymmetrischen Verfahren der Steganographie beschäftigt. Backes und Cachin hatten gezeigt, dass es ein asymmetrisches Stegosystem gibt, welches für viele Kommunikationskanäle einen relativ schwachen Sicherheitsbegriff erfüllt. In einer Nachfolgearbeit konnte Hopper zeigen, dass auch ein stärkerer Sicherheitsbegriff erfüllt werden kann, jedoch muss das Stegosystem hier auf den Kanal zugeschnitten werden. In unserer Arbeit konnten wir zeigen, dass dieser stärkere Sicherheitsbegriff auch durch ein universelles Stegosystem für viele Kanäle erreicht werden kann. Zusätzlich konnten wir zeigen, dass dies bestmöglich ist, indem wir diesen starken Sicherheitsbegriff für andere Kanäle ausschließen konnten. Dies ist ein starker Kontrast zu Kryptosystemen, bei denen seit langem bekannt ist, wie ein analoger starker Sicherheitsbegriff gewährleistet werden kann.

## Repräsentative Publikationen (fortgesetzt)

ESA 2018



In der Arbeit *Practical Access to Dynamic Programming on Tree Decompositions* haben wir uns mit dynamischer Programmierung auf sogenannten Baumzerlegungen beschäftigt. Diese Baumzerlegungen geben die Ähnlichkeit eines gegebenen Graphens zu einem Baum an und haben viele Anwendungen im Bereich der parametrisierten Komplexität. In dieser Arbeit haben wir ein Tool entwickelt, welches es erlaubt, solche dynamischen Programme sehr einfach zu beschreiben und direkt in Verbindung mit state-of-the-art-Solvern für Baumzerlegungen zu benutzen. Weiterhin waren wir in der Lage, ein Fragment der MSO-Logik zu formulieren, welches ausdrucksstark genug ist, um nahezu alle relevanten Fragestellungen zu Graphen mit beschränkter Baumweite zu formalisieren. Mithilfe unseres Tools können diese Fragestellungen nun direkt mit Algorithmen zur Baumzerlegung kombiniert werden und die so entstehenden Algorithmen sind kompetitiv mit vielen spezialisierten state-of-the-art Verfahren.

AAI 2017



In der Arbeit *Learning Residual Alternating Automata* haben wir uns mit dem aktiven Lernen von regulären Sprachen beschäftigt. Der erste entsprechende Algorithmus von Angluin war in der Lage, solche Sprachen als endliche deterministische Automaten darzustellen. Dieser Algorithmus wurde von Bollig, Habermehl, Kern und Leucker verallgemeinert, so dass er auch nichtdeterministische Automaten lernen kann, welche bewiesenermaßen exponentiell kleiner sein können. Angluin, Eisenstat und Fisman wiederum konnte dies auf alternierende Automaten übertragen, die wiederum exponentiell kleiner als nichtdeterministische Automaten sein können. Ein zentraler Begriff in all diesen Algorithmen ist der Begriff der Residualität, der es erlaubt, den einzelnen Zuständen der Automaten eine sinnvolle Semantik zuzuordnen. Angluin, Eisenstat und Fisman hatten in ihrer Arbeit die Vermutung aufgestellt, dass ihr Algorithmus ebenfalls solche residualen Automaten lernt. Wir konnten mittels eines komplexen Gegenbeispiels beweisen, dass diese Vermutung nicht der Wahrheit entspricht. Weiterhin waren wir in der Lage, einen Algorithmus zu konstruieren, der beweisbar nur residuale Automaten lernt und zu zeigen, dass diese auch weiterhin exponentiell kleiner als nichtdeterministische Automaten sein können.

Die übliche Konvention in der theoretischen Informatik ist die alphabetische Sortierung der Autoren.

## Schriftenverzeichnis

### Publications in peer reviewed conference proceedings

- 1 **Sebastian Berndt**, Klaus Jansen und Kim-Manuel Klein. „Fully Dynamic Bin Packing Revisited“. In: *APPROX-RANDOM*.
- 2 **Sebastian Berndt**, Max A. Deppert, Klaus Jansen und Lars Rohwedder. „Load Balancing: The Long Road from Theory to Practice“. In: 2022, (accepted).
- 3 **Sebastian Berndt**, Kilian Grage, Klaus Jansen, Lukas Johannsen und Maria Kosche. „Robust Online Algorithms for Dynamic Choosing Problems“. In: *CiE*. 2021.
- 4 **Sebastian Berndt**, Klaus Jansen und Kim-Manuel Klein. „New Bounds for the Vertices of the Integer Hull“. In: *SOSA*. 2021.
- 5 **Sebastian Berndt**, Klaus Jansen und Alexandra Lassota. „Tightness of Sensitivity and Proximity Bounds for Integer Linear Programs“. In: *SOFSEM*. Bd. 12607. Lecture Notes in Computer Science. Springer, 2021, S. 349–360.
- 6 **Sebastian Berndt**, Klaus Jansen und Alexandra Lassota. „Tightness of Sensitivity and Proximity Bounds for Integer Programs“. In: *SOFSEM*. 2021.
- 7 Florian Sieck, **Sebastian Berndt**, Jan Wichelmann und Thomas Eisenbarth. „Util: : Lookup: Exploiting Key Decoding in Cryptographic Libraries“. In: *CCS*. ACM, 2021, S. 2456–2473.
- 8 Jan Wichelmann, **Sebastian Berndt**, Claudius Pott und Thomas Eisenbarth. „Help, my Signal has bad Device! - Breaking the Signal Messenger’s Post-Compromise Security through a Malicious Device“. In: *DIMVA*. 2021.
- 9 Max Bannach, **Sebastian Berndt**, Marten Maack, Matthias Mnich, Alexandra Lassota, Malin Rau und Malte Skambath. „Solving Packing Problems with Few Small Items Using Rainbow Matchings“. In: *MFCs*. Bd. 170. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2020, 11:1–11:14.
- 10 Okan Seker, **Sebastian Berndt**, Luca Wilke und Thomas Eisenbarth. „SNI-in-the-head: Protecting MPC-in-the-head Protocols against Side-channel Analysis“. In: *ACM Conference on Computer and Communications Security*. 2020, (in print).
- 11 Max Bannach und **Sebastian Berndt**. „Positive-Instance Driven Dynamic Programming for Graph Searching“. In: *WADS*. Bd. 11646. Lecture Notes in Computer Science. Springer, 2019, S. 43–56.
- 12 **Sebastian Berndt**, Valentin Dreismann, Kilian Grage, Klaus Jansen und Ingmar Knof. „Robust Online Algorithms for Certain Dynamic Packing Problems“. In: *WAOA*. Bd. 11926. Lecture Notes in Computer Science. Springer, 2019, S. 43–59.
- 13 **Sebastian Berndt**, Leah Epstein, Klaus Jansen, Asaf Levin, Marten Maack und Lars Rohwedder. „Online Bin Covering with Limited Migration“. In: *ESA*. Bd. 144. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2019, 18:1–18:14.
- 14 Max Bannach und **Sebastian Berndt**. „Practical Access to Dynamic Programming on Tree Decompositions“. In: *ESA*. Bd. 112. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2018, 6:1–6:13.
- 15 **Sebastian Berndt**. „Computing Tree Width: From Theory to Practice and Back“. In: *CiE*. Bd. 10936. Lecture Notes in Computer Science. Springer, 2018, S. 81–88.
- 16 **Sebastian Berndt** und Kim-Manuel Klein. „Using Structural Properties for Integer Programs“. In: *CiE*. Bd. 10936. Lecture Notes in Computer Science. Springer, 2018, S. 89–96.

- 17 **Sebastian Berndt** und Maciej Liskiewicz. „On the Gold Standard for Security of Universal Steganography“. In: *EUROCRYPT (1)*. Bd. 10820. Lecture Notes in Computer Science. Springer, 2018, S. 29–60.
- 18 Max Bannach, **Sebastian Berndt** und Thorsten Ehlers. „Jdrasil: A Modular Library for Computing Tree Decompositions“. In: *SEA*. Bd. 75. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2017, 28:1–28:21.
- 19 **Sebastian Berndt** und Maciej Liskiewicz. „Algorithm Substitution Attacks from a Steganographic Perspective“. In: *ACM Conference on Computer and Communications Security*. ACM, 2017, S. 1649–1660.
- 20 **Sebastian Berndt**, Maciej Liskiewicz, Matthias Lutter und Rüdiger Reischuk. „Learning Residual Alternating Automata“. In: *AAAI*. AAAI Press, 2017, S. 1749–1755.
- 21 **Sebastian Berndt** und Maciej Liskiewicz. „Hard Communication Channels for Steganography“. In: *ISAAC*. Bd. 64. LIPIcs. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2016, 16:1–16:13.
- 22 **Sebastian Berndt** und Maciej Liskiewicz. „Provable Secure Universal Steganography of Optimal Rate: Provably Secure Steganography does not Necessarily Imply One-Way Functions“. In: *IH&MMSec*. ACM, 2016, S. 81–92.
- 23 **Sebastian Berndt** und Rüdiger Reischuk. „Steganography Based on Pattern Languages“. In: *LATA*. Bd. 9618. Lecture Notes in Computer Science. Springer, 2016, S. 387–399.

## Journal articles

- 1 Diego F. Aranha, **Sebastian Berndt**, Thomas Eisenbarth, Okan Seker, Akira Takahashi, Luca Wilke und Greg Zaverucha. „Side-Channel Protections for Picnic Signatures“. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2021.4 (2021), S. 239–282.
- 2 Thore Tiemann, **Sebastian Berndt**, Thomas Eisenbarth und Maciej Liskiewicz. „Ät natural!": Having a Private Chat on a Public Blockchain“. In: *IACR Cryptol. ePrint Arch.* (2021), S. 1073.
- 3 **Sebastian Berndt**, Klaus Jansen und Kim-Manuel Klein. „Fully dynamic bin packing revisited“. In: *Math. Program.* 179.1 (2020). Preliminary version was presented at APPROX-RANDOM 2015, S. 109–155.
- 4 **Sebastian Berndt**, Jan Wichelmann, Claudius Pott, Tim-Henrik Traving und Thomas Eisenbarth. „ASAP: Algorithm Substitution Attacks on Cryptographic Protocols“. In: *IACR Cryptol. ePrint Arch.* 2020 (2020), S. 1452.
- 5 Max Bannach und **Sebastian Berndt**. „Practical Access to Dynamic Programming on Tree Decompositions“. In: *Algorithms* 12.8 (2019). Preliminary version was presented at ESA 2018, S. 172.