Lebenslauf

Persönliche Daten

Name	Arkadius Kalka
Adresse	Stresemannstr. 6 44328 Dortmund
E-mail	arkadius.kalka@rub.de
Homepage	http://homepage.ruhr-uni-bochum.de/arkadius.kalka/
Telefon (mobil)	0157 52434754
Tel. (Festnetz)	0231 22395079

Stellen

02/2018 - 12/2021	Wissenschaftlicher Angestellter in der Statistik (bei Prof. Sonja Kuhnt) im Fachbereich Informatik an der Fachhochschule Dortmund.
11/2015 - 02/2016	Gast an der Bar-Ilan Universität in Ramat Gan, und Projekt-Koordinator für die mathematische Ausstellung IMAGINARY Israel in Bar-Ilan.
22/04/2013 - 10/2015	Postdoctoral Researcher an der Bar-Ilan Universität in Ramat Gan, Israel.
04/2012 - 03/2013	Postdoctoral Research Fellow an der School of Mathematics & Physics an der University of Queensland in Brisbane, Australien.
01/2012 - 03/2012	Gastwissenschaftler am Max-Planck-Institut für Mathematik, Bonn.
10/2010 - 12/2011	Researcher an der Bar-Ilan Universität in Ramat Gan. (Beurlaubt: Oktober 2010-Februar 2011)
10/2007 - 09/2010	Postdoctoral Research Fellow an der Bar-Ilan Universität in Ramat Gan.

Lebenslauf

Promotion

06/07/2007	Verteidigung der Doktorarbeit (Magna cum laude), Dissertation: *Representations of braid groups and braid-based cryptography* (eingereicht: 9. Mai 2007), Doktorvater: Prof. Lothar Gerritzen.
06/2003 - 07/2006	Wissenschaftlicher Mitarbeiter, Fakultät für Mathematik, Ruhr-Universität Bochum.
06/2003 - 05/2006	Stipendium des Graduiertenkollegs *Methods of Mathematics and Engineering for Secure Data Transmision and Information Transfer*, Sprecher: Prof. G. Frey.

Studium

28/03/2003	*Diplom-Mathematiker*, Note: *sehr gut*. Diplomarbeit: *Zopfgruppen und kryptographische Anwendungen*, Betreuer: Prof. L. Gerritzen.
11/2002	Studienabschlussstipendium der *Ruth und Gert-Massenberg Stiftung*.
10/2000 - 03/2003	Studium der Mathematik an der Ruhr-Universität Bochum.
10/1991 - 09/1996	Studium der Physik an der Universität Dortmund.

Forschungsgebiete

Algorithmische Algebra	Post-Quantum Kryptographie, Komplexitätstheorie, Effiziente Algorithmen, LOGSPACE Computation, kombinatorische Gruppentheorie, Zopfgruppen, Garsidegruppen, Artingruppen, Coxetergruppen, Selbstdistributive Systeme.
Statistik	Algebraische Statistik, Anwendungen der Statistik in Technometrie und Modellierung (Design of Experiment(DoE), Generalisierte Lineare Modelle (GLMs), Neuronale Netze, Kriging, Globale Sensitivitätsanalyse)

Arkadius Kalka, , 44328 Dortmund, Tel.: 0157 52434754

Maschinenbau	Thermisches Spritzen (HVOF- High Velocity Oxygen Fuel), Innenbeschichtung
Weitere Interessen	Quantum Computation, Optimierung, Kombinatorik, Theorie der Normalflächen, 3-Mannigfaltigkeiten, Knoten

Computer Skills

Computeralgebra	Ich habe Tausende von Programmen unter Verwendung von Computeralgebrasystemen (hauptsächlich MAGMA, auch GAP) geschrieben.
Statistiksoftware	Ich habe Hunderte von Programmen unter Verwendung von Statistiksoftware (hauptsächlich R, auch JMP) geschrieben
Programmiersprachen	Ich habe Programme in den Programmiersprachen C, JAVA, PASCAL, BASIC geschrieben. Da Programmierung letztlich nichts anderes als strukturiertes Denken ist, bin in der Lage jede Programmiersprache schnell zu erlernen.
Basics	Windows, Linux, MS Office, LaTeX, HTML

Hobbys

Schach (Internationaler Meister)

Dortmund, 5. September 2022

Arkadius Kalka, , 44328 Dortmund, Tel.: 0157 52434754

Anlagen

Publikationen und Preprints

- Arkadius Kalka, *Representation attacks on the braid Diffie-Hellman public key encryption*, Applicable Algebra in Engineering, Communication and Computing **17** (2006), 257-266.
  `http://www.springerlink.com/content/87245vg6725n8322/`
- Arkadius Kalka, *Representations of braid groups and braid-based cryptography*, PhD thesis, submitted: May 9th 2007. Doctoral examination: July 6th 2007 (Magna cum laude). Advisor: Prof. L. Gerritzen.
  `www-brs.ub.ruhr-uni-bochum.de/netahtml/HSS/Diss/KalkaArkadiusG/`
- Arkadius Kalka, Mina Teicher, and Boaz Tsaban, *Short expressions of permutations as products and cryptanalysis of the Algebraic Eraser*, Advances in Applied Mathematics **49**, issue 1 (July, 2012), 57-76.
  Preprint: `arxiv.org/abs/0804.0629`.
- Arkadius Kalka, *Improved linear time inversion heuristic for the Burau representation*, Preprint (2008): `homepage.ruhr-uni-bochum.de/arkadius.kalka/CompPreimBrShortVersionUsePackageAlg.tex.pdf`
- Arkadius Kalka, Eran Liberman, and Mina Teicher, *A note on the shifted conjugacy problem in braid groups*, Groups – Complexity – Cryptology **1**, no. 2 (2009), 227-230.
- Arkadius Kalka, Eran Liberman, and Mina Teicher, *Solution to the subgroup conjugacy problem for Garside subgroups of Garside groups*, Groups – Complexity – Cryptology **2**, no. 2 (2010), 157-174.
- Joel Hass, Arkadius Kalka, and Tahl Nowik, *Complexity of relations in the braid group*, preprint: `arXiv.org/abs/0906.0137`
- Arkadius Kalka, *Non-associative public-key cryptography*, Contemporary Mathematics **677** (2016), 85-112. Preprint: `arxiv.org/abs/1210.8270`
- Arkadius Kalka and Mina Teicher, *Non-associative key establishment for left distributive systems*, Groups – Complexity – Cryptology **5**, no. 2 (2013), 169-191.
  Preprint `http://arxiv.org/abs/1305.4401`

- Murray Elder and Arkadius Kalka, *Logspace-computations for rigid Garside groups*, preprint `http://arxiv.org/abs/1310.0933v2`, extended version of the following paper.
- Murray Elder and Arkadius Kalka, *Logspace-computations for Garside groups of spindle type*,
  preprint `http://arxiv.org/abs/1310.0933`.
- David Garber, Arkadius Kalka, Eran Liberman, and Mina Teicher, *Double centralizers for parabolic subgroups of braid groups*,
  preprint `http://arxiv.org/abs/1310.0936`.
- Arkadius Kalka and Mina Teicher, *Iterated LD-Problem in non-associative key establishment*,
  preprint `http://arxiv.org/abs/1312.6791`.
- Arkadius Kalka and Mina Teicher, *Non-associative key establishment protocols and their implementation*, Contemporary Mathematics **677** (2016), 113-128,
  preprint `http://arxiv.org/abs/1312.6794`.
- Arkadius Kalka, Boaz Tsaban and Gary Vinokur, *Complete simultaneous conjugacy invariants in Artin's braid groups*,
  preprint `http://arxiv.org/abs/1403.4622`.
- Arkadius Kalka, Mina Teicher and Boaz Tsaban, *On the Double Coset Problem for parabolic subgroups in braid groups*,
  preprint `http://arxiv.org/abs/1402.5541`
- Benjamin Burton, Murray Elder, Arkadius Kalka and Stephan Tillmann, *2-manifold recognition is in logspace*, Journal of Computational Geometry **7**, no. 1 (2016), 70-85.
  preprint `http://arxiv.org/abs/1412.1188`
- Adi Ben-Zvi, Arkadius Kalka and Boaz Tsaban, *Cryptanalysis via algebraic spans*, In: Shacham, H., Boldyreva, A. (eds) Advances in Cryptology - CRYPTO 2018. Lecture Notes in Computer Science **10991**, Springer, Cham.
  preprint `https://eprint.iacr.org/2014/041`
- Arkadius Kalka, *Power commutator groups*.
  Preprint (2015): `http://arxiv.org/abs/1510.02286`
- Arkadius Kalka and Sonja Kuhnt, *The numerical statistical fan for noisy experimental designs*, submited to Algebraic Statistics, under Review.
  Preprint `http://arxiv.org/abs/2005.04051` (2020)

Arkadius Kalka, , 44328 Dortmund, Tel.: 0157 52434754

- Sonja Kuhnt and Arkadius Kalka, *Global Sensitivity Analysis for the Interpretation of Machine Learning Algorithms*, In: Ansgar Steland, Kwok-Leung Tsui (editor), *Artificial Intelligence, Big Data and Data Science in Statistics* (2022).
- W. Tillmann, I. Baumann, A. Brinkhoff, S. Kuhnt, E.-C. Becker-Emden and A. Kalka, *Effect of the spray parameters on the particle behaviour and the coating properties during ID warm spraying of fine WC-12Co powders (-10 + 2 μm)*, Thermal Spray 2021: Proceedings from the International Thermal Spray Conference ITSC2021 (2021), 283-289.
- Wolfgang Tillmann, Sonja Kuhnt, Ingor Baumann, Arkadius Kalka, Eva-Christina Becker-Emden and Alexander Brinkhoff, *Statistical Comparison of Processing Different Powder Feedstock in an HVOF Thermal Spray Process*, Journal of Thermal Spray Technology **31** (2022), 1476-1489.

Tätigkeit als Reviewer

- Design, Codes and Cryptography. 4 papers (2022, 2022, 2021, 2020).
- Proceedings of ProvSec2018 (LNCS). 1 review (2018).
- Journal of Mathematical Cryptology. 1 paper (2018).
- Applicable Algebra in Engineering, Communication and Computing. 6 Papers (2015/6, 2015, 2015, 2013, 2011/2, 2011).
- Proceeedings of ISSAC 2016. 1 paper (2016).
- Groups – Complexity – Cryptology. 3 Papers (2015, 2015, 2008).
- Journal of Symbolic Computation. 1 paper (2013).
- Proceedings of Eurocrypt 2013. 1 paper (2012).
- IJAC (International Journal of Algebra and Computation). 2 papers (2010, 2009/10).
- Journal of the European Mathematical Society (JEMS). 1 paper (2010).
- SRX Mathematics. 1 paper (2009).
- Proceedings of the Conference *Combinatorial and Geometric Group Theory with Applications*, University of Dortmund (Germany), August 27-31, 2007. 1 paper (2008/9)

Vorträge auf Konferenzen/Workshops (eingeladen)

- *Non-associative public key cryptography*, Workshop on "Complexity and Group-based Cryptography", CRM (Centre de recherches mathematiques), CRM, Montreal, August 30-September 3, 2010.
- *Introduction to Garside calculus*, Workshop on knot theory, University Zürich and ETH, November 18-29, 2013.
- *Simultaneous conjugacy and double coset problem in braid and Garside groups*, Special session on Applications of Algebra in Cryptography, Second Joint Meeting of the AMS and the IMU, Israel, Juni 16-19, 2014.
- *The numerical statistical fan of a noisy experimental design*, Workshop on Optimality in Algebraic Statistics, FH Dortmund, Februar, 14-15, 2019.

Weitere Konferenzvorträge

- *Computing preimage braids for the Burau representation*, Workshop on *Algebraic Methods in Cryptography*, University of Dortmund (Germany), März 11-12, 2004.
- *Representation attacks in braid group cryptography*, Workshop on *Algebraic Methods in Cryptography*, Ruhr-University Bochum (Germany), November 17-18, 2005.
- *AAG-like key agreement scheme for magmas and shifted conjugacy in braid-based cryptography*, Conference *Combinatorial and Geometric Group Theory with Applications*, University of Dortmund (Germany), August 27-31, 2007.
- *Improved linear time inversion heuristic for the Burau representation*, Conference *Braids in Paris*, Paris, September 17-20, 2008.
- *The shifted conjugacy decision problem in braid groups and its generalizations*, Conference *Geometric and Asymptotic Group Theory with Applications*, Hoboken, NJ, Marz 9-12, 2009.
- *Subgroup conjugacy problem for parabolic subgroups of the braid group*, Workshop *Braids in Pau*, Pau (France), Oktober 5-8, 2009.
- *Subgroup conjugacy problem for Garside subgroups of Garside group*, Conference *Singularities, knots, and mapping class groups*, in memory of Bernard Perron, Dijon, September 6-9, 2010.
- *Conjugacy in Braid Groups and related Problems*, Workshop *Winter Braids II*, Caen (France), Dezember 12-15, 2011

- *Non-associative key establishment protocols and their implementation*, emac13: 11th Engineering Mathematics and Applications Conference, Queensland University of Technology (QUT), Dezember 1-4, 2013.
- *On some Artin- and Coxeter-like groups*, Conference *Geometric, Asymptotic and Combinatorial Group Theory and Applications* (*GAGTA-9*), CIRM, Luminy (Marseille), September 14-18, 2015.
- *On numerical fans for noisy experimental designs*, 11th International Conference of the ERCIM WG on Computational and Methodological Statistics (CMStatistics 2018), University of Pisa, Italy, Dezember 14-16, 2018.
- *The numerical statistical fan and model selection*, ENBIS-21 Online Conference, September 13-15, 2021.

Weitere Konferenzen/Workshops

- *Workshop on Complexity-theoretical and Algebraic Methods in Cryptography*, Ruhr-University Bochum, Germany, November 7-8, 2002.
- *Joint meeting of AMS, DMV, ÖMG*, Mainz, Juni 16-19, 2005.
- *Conference on Representations of Algebras, Groups and Semigroups*, Bar-Ilan University, Ramat Gan, Dezember 30, 2007 - Januar 3, 2008.
- *HIRZ80*, Bar-Ilan University, Ramat Gan, Mai 18-23, 2008.
- *Workshop on Cryptology*, Technion, Haifa, Mai 29, 2008.
- *Compression and Combinatorial Algorithms* (*CCA*), Haifa, Juli 8, 2008.
- *Israel CS Theory day*, Raanana (Israel), März 2, 2009.
- Workshop *Why Knot? The mathematics of knots, links and braids*, Technion, Haifa, September 6-10, 2009.
- Workshop on *Algebra and Geometry of Configuration Spaces and related structures*, Centro di Ricerca Matematica Ennio De Giorgi, Pisa, Juni 21-5, 2010.
- Workshop *Topics in Algorithmic and Geometric Group and Semigroup Theory*, CRM, Montreal, August 23-27, 2010.
- *The Fourth Israel CS Theory Day*, The Open University in Raanana (Israel), März 24, 2011.

- *A Celebration Commemorating 20 Years of the Great Aliya of Immigrant Scientists from the Former Soviet Union*, Bar-Ilan University, Ramat Gan, Juni 14, 2011.
- *The 2011 Meeting of the Israel Mathematical Union*, Bar-Ilan University, Ramat Gan, Juni 16, 2011.
- International Conference *Trends and Perspectives in Mathematics*, Tel-Aviv, November 14-15, 2011.
- *International Conference on Geometric, Combinatorial and Dynamics aspects of Semigroup and Group Theory*, Bar-Ilan University, Ramat Gan (Israel), Juni 11-14, 2013.
- *Summer School on Algebraic and Tropical Geometry*, TU Kaiserslautern, September 7-11, 2015.
- *16th Workshop on Quality Improvement Methods*, Esplanade-Hotel, Dortmund, Juni, 1-2, 2018.
- *SFB 823 Klausurtagung*, Hotel Mercure, Lüdenscheid, Oktober, 25-26, 2018.
- Workshop *Complexity Reduction in Algebraic Statistics*, Otto von Guericke Universität, Magdeburg, November 26-27, 2018.
- *Workshop on Optimality in Algebraic Statistics*, Februar, 14-15, 2019.
- Poster: *Numerical Statistical Fan of a Noisy Design* (with S. Kuhnt), *17th Workshop on Quality Improvement Methods*, Esplanade-Hotel, Dortmund, Juni 14-15, 2019.
- *SFB 823 - Strukturbruchtag*, Ruhr-University Bochum, Oktober 11, 2019.
- *SFB 823 Klausurtagung 2019*, Hotel Mercure, Lüdenscheid, Germany, November 25, 2019.
- *ENBIS-20 Online Conference*, 28 Sep - 1 Okt 2020.
- ENBIS Workshop *Interpretability for Industry 4.0*, University of Naples Federico II (Italy) & online, Juli 12-13, 2021.

Lehre: Übungsgruppenleiter an der RUB

- **WS 03/04** 150301 *Seminar über Kryptographie.*
- **SS 2004** 150103 *Übungen zu Höhere Mathematik für Ergänzungsstudiengänge.*
- **WS 04/05** 150101 *Übungen zu Mathematik I für Maschinenbau-, Bauingenieure und UTRM*
  150127 *Übungen zu Kryptographie I.*

- **WS 05/06** 150231 *Übungen zu Diskrete Mathematik I*.
- **WS 06/07** 150128 *Tutorium: Mathematik für Naturwissenschaftler*.

Vorlesungen an der Bar-Ilan Universität

- *Introduction to Quantum Computing*, Minikurs innerhalb des CGC Colloquium (WS 2009/10).
- *Coxeter groups* (SS 2010).

Weitere professionelle Aktivitäten

- Ich half bei der Organisation des Workshops über *Algebraic Methods in Cryptography*, Ruhr-Universität Bochum, November 17-18, 2005.
  Insbesondere habe ich die Konferenzwebseite erstellt:
  `www.ruhr-uni-bochum.de/ffm/Lehrstuehle/Lehrstuhl-VI/Workshop05.htm`
- Von 2009/10 bis Dezember 2011, und wieder März-Mai 2014, habe ich das *BIU Colloquium on Combinatorial Group theory and Cryptography* (*CGC*) koorganisiert.
  `http://u.math.biu.ac.il/~ kalkaa/CGCColloq.html`
- An der BIU habe ich informell die Masterarbeiten von Gary Vinokur (Supervisor: Boaz Tsaban und David Garber) und Adi Ben-Zvi (Supervisor: Boaz Tsaban) mitbetreut.
- Im Dezember 2015/ Januar 2016 habe ich die mathematische Ausstellung IMAGINARY vom Weizmann Institute zur Bar-Ilan Universität gebracht.
- I habe die Webseite für den *German-Israeli Workshop in Algebraic and Tropical Geometry* (Bar-Ilan University, Ramat Gan Januar 11-15, 2016) erstellt.
  `http://homepage.ruhr-uni-bochum.de/arkadius.kalka/workshopJan2016/`
- I half bei der Organisation des Workshops *Workshop on Optimality in Algebraic Statistics*, Februar 14-15, 2019.
- Mitorganisator des *17th Workshop on Quality Improvement Methods*, Esplanade-Hotel, Dortmund, June 14-15, 2019.