DAVID MÖDINGER

Computer Science Researcher

david.moedinger@ketzu.net | Römerstr. 118, 89077 Ulm, Germany | Ulm, Germany
www.ketzu.net | @ketzu7 | ketzu

EXPERIENCE

Academic Employee

Ulm University

August 2015 – July 2021 | Ulm

During my time at Ulm University, I covered a wide range of roles and responsibilities. These include:

- Research and Development:
  - Generating and refining research questions and topics.
  - Developing simulations, research- and teaching prototypes.
  - Data analysis of simulation- and prototype results.
- Presentation:
  - Writing project reports as well as research publications.
  - Presenting research- and project results at conferences, project meetings, and other events.
- Supervision and Teaching:
  - Hiring and supervising student assistants for teaching and research tasks, e.g., programming work on prototype software.
  - Preparing and grading exercises and exams.
  - Supervising students for theses, projects, and seminars.

Research Assistant

Ulm University

June 2015 – July 2015 | Ulm

As a follow-up to my master's thesis on extending Aleknovich's algorithm to a new domain, we extended Gabidulin codes to characteristic zero fields. This short position culminated in a publication in the International Symposium on Information Theory.

PROJECTS

SORRIR - Fault-Tolerant IoT

Federal Ministry for Education and Research

3 Years

SORRIR is a collaboration project between Ulm University and University Passau, as well as industry partners. The goal of the project is to establish a framework for resilience and fault tolerance for IoT systems.
SORRIR provides a novel programming model, which is currently available as a TypeScript prototype. The SORRIR system allows for easy integration of fault-tolerance mechanisms and fault- and security monitoring services into an IoT system.

PriCloud - Privacy Preserving Cloud Storage

Baden-Württemberg Stiftung

3 Years

SKILLS

C++ | Python | Java | JavaScript | Docker | Git | LaTeX | Research | Django | Vuejs | Statistical Analysis | traefik

LANGUAGES

Deutsch (German) ●●●●●

English ●●●●○

한국어 **(Korean)** ●○○○○

EDUCATION

Ph.D. in Computer Science (Ongoing)

Ulm University

August 2015 – July 2021

Dissertation on privacy in blockchain transaction broadcasts.

M.Sc. in Computer Science

Ulm University

April 2012 – May 2015

Master's thesis on the extension of Aleknovich's algorithm for interleaved Gabidulin codes. It was later published as an extended version in "Algebraic and Combinatorial Coding Theory."

B.Sc. in Computer Science

Ulm University

April 2009 – April 2012

Bachelor's thesis on the evaluation of algorithms generating the k-Burrows-Wheeler transform in C++. This degree includes a minor in mathematics.

PriCloud is a completed research project for a privacy-preserving cloud storage. The system design is based on smart storage contracts managed through a blockchain system. Storage providers show they stored a file for the contractual promised time by providing a cryptographic proof-of-storage of the file at specific times of the contract. Failure to do so will refund the cost to the client. The project created various publications about the system design of PriCloud, its cryptographic novelties, and improvements in network privacy.

PUBLICATIONS

Journal Articles

- Mödinger, D., Lorenz, J.-H., van der Heijden, R. W., & Hauck, F. J. (2020). Unobtrusive monitoring: Statistical dissemination latency estimation in bitcoin's peer-to-peer network. *PLOS ONE*, *15*(12), 1–21.
- Tichy, M., Pietron, J., Mödinger, D., Juhnke, K., & Hauck, F. J. (2020). Experiences with an internal dsl in the iot domain.
- Puchinger, S., Müelich, S., Mödinger, D., né Nielsen, J. R., & Bossert, M. (2017). Decoding interleaved gabidulin codes using alekhnovich's algorithm. *Electronic Notes in Discrete Mathematics*, *57*, 175–180. Algebraic and Combinatorial Coding Theory - 2016.

Conference Proceedings

- Mödinger, D., Fröhlich, N., & Hauck, F. J. (2020). Pixy: A privacy-increasing group creation scheme. In *5th international conference on network security (icns)*.
- Mödinger, D., & Hauck, F. J. (2020). 3p3: Strong flexible privacy for broadcasts. In *4th international workshop on cyberspace security (iwcss 2020)*.
- Mödinger, D., Kopp, H., Kargl, F., & Hauck, F. J. (2018). A flexible network approach to privacy of blockchain transactions. In *Proc. of the 38th ieee int. conf. on distributed computing systems (icdcs)*, IEEE.
- Kopp, H., Mödinger, D., Hauck, F. J., Kargl, F., & Bösch, C. (2017). Design of a privacy-preserving decentralized file storage with financial incentives. In *Proceedings of ieee security & privacy on the blockchain (ieee s&b) (affiliated with eurocrypt 2017)*, IEEE.
- van der Heijden, R. W., Engelmann, F., Mödinger, D., Schönig, F., & Kargl, F. (2017). Blackchain: Scalability for resource-constrained accountable vehicle-to-x communication. In *Proceedings of the 1st workshop on scalable and resilient infrastructures for distributed ledgers* (4:1–4:5). Las Vegas, Nevada: ACM.
- Kraft, R., Erb, B., Mödinger, D., & Kargl, F. (2016). Using conflict-free replicated data types for serverless mobile social applications. In *Proceedings of the 8th acm international workshop on hot topics in planet-scale mobile computing and online social networking* (pp. 49–54). Paderborn, Germany: ACM.
- Müelich, S., Puchinger, S., Mödinger, D., & Bossert, M. (2016). An alternative decoding method for gabidulin codes in characteristic zero. In *2016 ieee international symposium on information theory (isit)* (pp. 2549–2553).

Further publications are currently under review or in preparation.

SIDE PROJECTS

Self Hosting

Services Repository

I host all my side projects and websites using docker-compose, a traefik reverse-proxy, including automated TLS via let's encrypt, and a simple services infrastructure-as-code repository.

Rough-Budget

Source Repository

Rough-Budget is a privacy-preserving Vuejs experiment using a very simple PHP back-end. The project helps people get into budgeting in a simple way, estimating expenses instead of tracking every cent.

Vocabulary REST API

k-Lang API

My current side project is a vocabulary study program focusing on writing sentences combined with spaced-repetition vocabulary studying. As a two-part project, Vuejs front-end and Django Rest Framework back-end, this repository presents the conceptually simple back-end.

Data Science Example

Eta-Adaption

Research often required data analysis, which can be presented nicely in a Python notebook. The repository is hosted via GitHub and run through Binder.