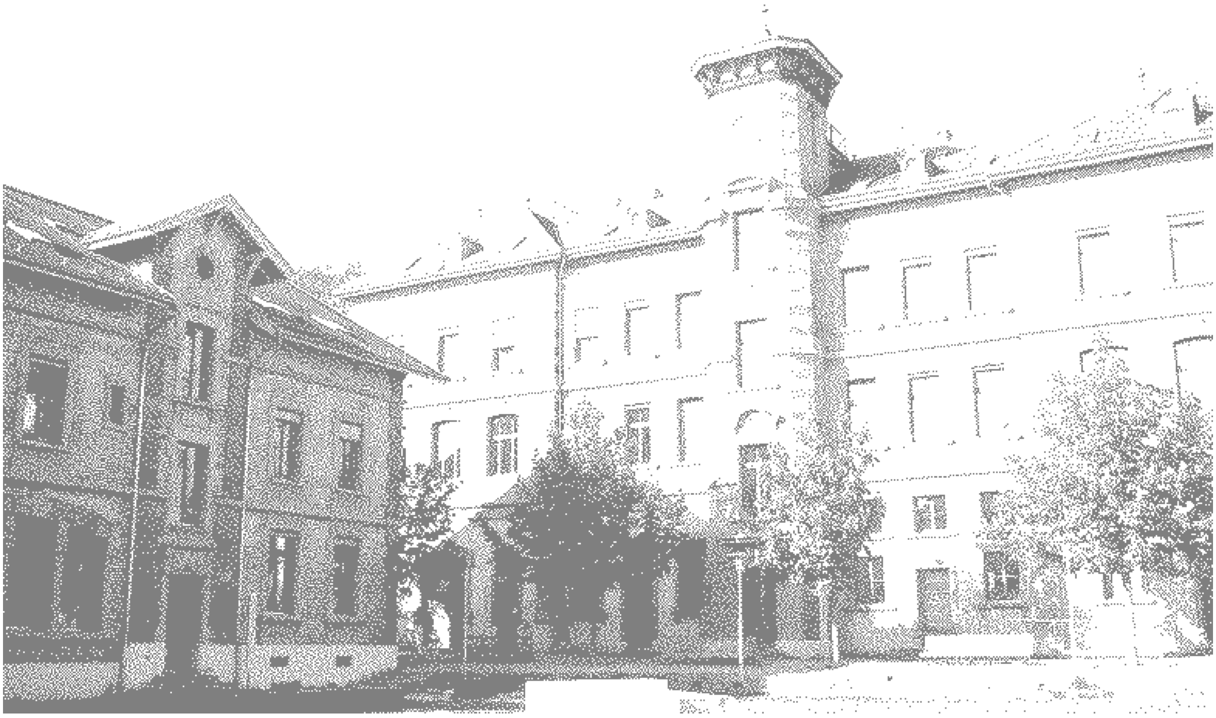
Institut für Informatik
Universität Bern

www.inf.unibe.ch

# INF Annual Report 2020/2021



# INF Annual Report

# Academic Year 2020/2021

September 15, 2021

# Contents

# 1 Institute of Computer Science (INF)

## 1.1 Address

Neubrückstrasse 10, 3012 Bern, Switzerland
Phone: +41 31 684 86 81
E-Mail: info@inf.unibe.ch
http://www.inf.unibe.ch

## 1.2 Personnel

### Members

Florence Aellen, Jesutofunmi Ajayi, Sigurd Alnes, Orestis Alpos, Ignacio Amores Sesar, Michael Bärtschi, Nina Baumgartner, Michael Baur, Pierre-Alexandre Beaufort, Marcel Behn, Lara Biehl, Adam Bielski, Prof. Dr. David Bommes, Dr. Peppo Brambilla, Prof. Dr. Torsten Braun, Nathalie Brugger, Patrick Brunner, Sabine Brunner, Marco Buchholz, Prof. Dr. Christian Cachin, Llukman Cerkezi, Bettina Choffat, Yannik Dällenbach, Aram Davtyan, Lucas De Sousa Pacheco, Dr. Antonio Di Maio, Negar Emami, Maria Fanger, Prof. Dr. Paolo Favaro, Mathias Fuchs, Pascal Gadient, Nicolas Gallego-Ortiz, Dr. Mohammad Ghafari, Francesca Giardina, Anthony Gillioz, Pinar Göktepe, Roman Gruber, Mohammadreza Hazhirpasand, Dragana Heinzen, Martin Heistermann, Dr. Benedikt Hitz-Gamper, Simon Jenni, Adrian Jörg, Simon Kafader, Rebeca Kehl, Eveline Lehmann, Abdelhak Lemkhenter, Manuel Leuenberger, Heng Liu, Thomas Lüthi, Dr. Giorgia Marson, Corina Masanti, Alisson Medeiros de Lima, Oscar Meier, Givi Meishvili, Hugo Melo dos Santos, Gerry Metzger, Jovana Mićić, Alejandro Nardo, Prof. Dr. Oscar Nierstrasz, Valentin Nigolian, Joël Niklaus, Dr. Jasmin Nussbaumer, Diego Oliveira Rodrigues, Nitish Patkar, Alex Pellegrini, Maurizio Piu, Kristelle Plüss, Simone Raimondi, Pooja Rani, PD Dr. Kaspar Riesen, Atefeh Rohani, Sepehr Sameni, Eric Samikwa, Alp Eren Sari, Daniela S. Schroth, Alec Schürmann, Dominic Schweizer, Nathalie Sinz, FH Prof. Dr. Ronny Standtke, Kerrie Stauffer, Nathalie Steinhauer, Prof. Dr. Thomas Strahm, Prof. Dr. Thomas Studer, Dr. Nataliia Stulova, Lionel Stürmer, PD Dr. Matthias Stürmer, Noe Leon Thalheim, Dr. Ruxandra Tivadar, Prof. Dr. Athina Tzovara, Adrian Wälchli, Jethro Warnett, Stefanie Weilenmann, Tobias Welz, Roland Widmer, Dimitrios Xenakis, Luca Zanolini, Lukas Zenger

## Administration

Bettina Choffat, Dragana Heinzen, Daniela Schroth, Nathalie Brugger

## Technical staff

Dr. Peppo Brambilla, Martin Heistermann, Adrian Wälchli

# 2 Teaching Activities

## 2.1 Courses for Major and Minor in Computer Science

### Autumn Semester 2020

- Bachelor 1st Semester

  Einführung in die Informatik (Die Dozenten der Informatik, 5 ECTS)

  Grundlagen der Technischen Informatik (T. Studer, 5 ECTS)

  Programmierung 1 (T. Studer, 5 ECTS)

- Bachelor 3rd Semester

  Diskrete Mathematik (C. Cachin, 5 ECTS)

  Computernetze (T. Braun, 5 ECTS)

  Einführung in Software Engineering (O. Nierstrasz, 5 ECTS)

- Bachelor 5th Semester

  Computergrafik (D. Bommes, 5 ECTS)

  Mensch-Maschine-Schnittstelle (K. Riesen, 5 ECTS)

  Machine Learning (P. Favaro, 5 ECTS)

  Digitale Nachhaltigkeit (M. Stürmer, 5 ECTS)

  Anleitung zu wissenschaftlichen Arbeiten (Die Dozenten der Informatik, 5 ECTS)

- Master Courses

  Software Modeling and Anaysis (O. Nierstrasz, 5 ECTS)

  Advanced Networking and Future Internet (T. Braun, 5 ECTS)

  Justification Logic (T. Studer, 5 ECTS)

Computer Vision (P. Favaro, 5 ECTS)

Applied Optimization (D. Bommes, 5 ECTS)

Cryptography (C. Cachin, 5 ECTS)

Seminar: Software Composition (O. Nierstrasz, 5 ECTS)

Seminar: Communication and Distributed Systems (T. Braun, 5 ECTS)

Seminar: Logic and Theoretical Computer Science (T. Studer, 5 ECTS)

Seminar: Machine Learning and Artificial Intelligence (P. Favaro, 5 ECTS)

Seminar: Computer Graphics (D. Bommes, 5 ECTS)

Seminar: Cryptography and Data Security (C. Cachin, 5 ECTS)

- Service Courses

Anwendungssoftware (K. Reisen, 3 ECTS)

Grundkurs Programmieren (M. Stürmer, 3 ECTS)

## Spring Semester 2021

- Bachelor 2nd Semester

Datenbanken (T. Studer, 5 ECTS)

Datenstrukturen und Algorithmen (D. Bommes, 5 ECTS)

Computer Architecture (P. Favaro, 5 ECTS)

Programmierung 2 (O. Nierstrasz, 5 ECTS)

- Bachelor 4th Semester

Praktikum in Software Engineering (T. Studer, 5 ECTS)

Betriebssysteme (T. Braun, 5 ECTS)

Berechenbarkeit und Komplexität (T. Strahm/J. Walker, 5 ECTS)

Algorithmen, Wahrscheinlichkeit und Information (C. Cachin, 5 ECTS)

- Bachelor 6th Semester

  Anleitung zu wissenschaftlichen Arbeiten (Die Dozenten der Informatik, 5 ECTS)

- Master Courses

  Internet of Things (T. Braun, 5 ECTS)

  Advanced Topics in Machine Learning (P. Favaro, 5 ECTS)

  3D Geometry Processing (D. Bommes, 5 ECTS)

  Cryptographic Protocols (C. Cachin, 5 ECTS)

  Programming Languages (O. Nierstrasz, 5 ECTS)

  Seminar: Communication and Distributed Systems (T. Braun, 5 ECTS)

  Seminar: Logic and Theoretical Computer Science (T. Studer, 5 ECTS)

  Seminar: Machine Learning and Artificial Intelligence (P. Favaro, 5 ECTS)

  Seminar: Computer Graphics (D. Bommes, 5 ECTS)

  Seminar: Cryptology and Data Security (C. Cachin, 5 ECTS)

  Seminar: Privatrecht und Informatik: Distributed Trust and Blockchain (C. Cachin, M. Eggen, 5 ECTS)

  Seminar: Software Compostition (O. Nierstrasz, 5 ECTS)

- Service Courses

  Anwendungssoftware (K. Riesen, 3 ECTS)

  Grundkurs Programmieren (M. Stürmer, 3 ECTS)

## 2.2 Colloquium in Computer Science

| | |
|---|---|
| 29.09.2020 | Vincent Gramoli - EPFL<br>Few Consensus Ideas to Improve Blockchains |
| 23.11.2020 | Claus Beisbart - University of Bern<br>Was sind ethische Algorithmen |

## 2.3 Students

- Major Subject Students: AS 2020: 281, SS 2021: 324
- Minor Subject Students: AS 2020: 179, SS 2021: 179
- Ph.D. Candidates: AS 2020: 47, SS 2021: 46

## 2.4 Degrees and Examinations

- PhD: 6
- Master: 26
- Bachelor: 22
- Completion of Minor Studies: 31 (90E:0, 60E:3, 30E:20, 15E:8, 900 ECTS)
- Semester Examinations AS 2020: 1095 (3852 ECTS)
- Bachelor's/Master's Theses AS 2020: 16 (240 ECTS)
- Semester Examinations FS 2021: 649 (2526 ECTS)
- Bachelor's/Masters Theses FS 2021: 17 (290 ECTS)

## 2.5 Activities

- Contribution to the "National Future Day for Girls and Boys", Bern, November 12, 2020 (Cancelled due to Covid19 pandemic)
- Contribution to the "Bachelor Infotage", December 1+2, 2020 (digital)
- Contribution to the "Master Infotage", March 10, 2021 (digital)
- Taster course for female students, Bern, May 6, 2021 (digital)
- Mini Symposium for the Nachfolge Nierstrasz, March 22-23, 2021
- Civil Law and Computer Science, May 26, 2021
- Seminar on Trusted Computing and Secure Protocols, September 8, 2020.

- Hyperledger Fabric Private Chaincode, Marcus Brandenburger, IBM Research - Zurich
- TZ4Fabric: Executing Smart Contracts with ARM TrustZone, Christian Göttel, Université de Neuchatel
- MQT-TZ: Hardening IoT Brokers Using ARM TrustZone, Valerio Schiavoni, Université de Neuchatel
- Consensus Beyond Thresholds: Generalized Byzantine Quorums Made, Orestis Alpos, University of Bern

# 3 Cognitive Computational Neuroscience Group

## 3.1 Personnel

| | | |
|---|---|---|
| **Head:** | Prof. Dr. A. Tzovara | Tel.: +41 31 511 7636<br>email: athina.tzovara@inf.unibe.ch |
| **Scientific Staff:** | Dr. R.I. Tivadar | +41 31 511 7636<br>email: ruxandra.tivadar@inf.unibe.ch |
| | Dr. Q. Hu | +41 31 511 7636<br>email: qiyang.hu@inf.unibe.ch |
| | F.M. Aellen | +41 31 511 7636<br>email: florence.aellen@inf.unibe.ch |
| | S.A. Alnes | +41 31 511 7636<br>email: sigurd.alnes@inf.unibe.ch |
| | P. Göktepe | +41 31 511 7636<br>email: pinar.goektepe@students.unibe.ch |
| | N. Norori | +41 31 511 7636<br>email: natalianorori@gmail.com |
| | G. Monachino | +41 31 511 7636<br>email: giuliana.monachino@inf.unibe.ch<br>(external PhD student) |

## 3.2 Overview

The Cognitive Computational Neuroscience group conducts research in the areas of neuroscience, machine learning and computational modeling. We use invasive and non-invasive electrophysiological recordings (scalp and intracranial electroencephalography and single-unit recordings), in combination with machine learning techniques to study neural functions of the human brain. The main areas of focus include: (a) machine learning techniques for neuroscience data and for assisting clinical decision making and (b) studying the neural correlates of sensory processing and predictions.

## 3.3 Research Projects

### Computational techniques for assisting clinical decision making and predicting outcome from coma

Coma after cardiac arrest is one of the most common causes of admission in intensive care units. Being able to predict the outcome of a patient in a coma is crucial for optimizing clinical care and improving patients' chances of survival. However, several of the available prognostication techniques rely on qualitative evaluations of patients' clinical signals, which are costly and require strong medical expertise.

The CCN group is developing novel computational approaches that can assist clinical decision making and automate outcome prediction from coma. To this aim, we are using electroencephalography (EEG) recordings of brain activity during the acute coma phase. We are combining EEG recordings with signal processing and machine learning techniques in order to identify markers that can predict patients' chances of awakening and surviving at 3 months. To this aim, we are focusing on EEG responses to auditory stimuli and we are quantifying patterns of neural synchrony (phase locking, transfer entropy) and complexity (Lempel Ziv complexity). The goal for this project is to develop novel markers of awakening from coma that complement current clinical investigations and support medical experts in making clinical decisions on the care of patients. Importantly, these novel markers emphasize interpretability.

**Research staff:** Florence Marcelle Aellen, Sigurd Alnes, Athina Tzovara

**Financial support:** Interfaculty Research Cooperation "Decoding Sleep: From Neurons to Health & Mind" of the University of Bern

### Identifying and mitigating bias in AI for healthcare

Artificial intelligence (AI) has an astonishing potential in assisting clinical decision-making and revolutionizing health care. The vast majority of medical fields can profit from the use of AI algorithms, which have promising applications on diagnosis of fine-grained disease phenotypes and on the design of personalized therapies. One of the next open challenges that AI will need to address before its integration in the clinical routine is that of algorithmic bias.

Most AI algorithms need big datasets to learn from, but several groups of the human population have a history of being absent or misrepresented in existing biomedical datasets. If the training data is misrepresentative of the population variability, AI is prone to reinforcing bias, which can lead to fatal outcomes, misdiagnoses, and lack of generalization.

In our work, we are investigating different facets of bias, manifesting as human, data, or algorithmic bias. Additionally, we are identifying key challenges in rendering AI algorithms fairer from the perspective of big data and algorithmic decision-making, and we propose concrete steps for quantifying and addressing bias in the field of medicine.

**Research staff:** Natalia Norori, Qiyang Hu, Florence Aellen

**Financial support:** Mozilla Foundation

## Neural mechanisms underlying sensory processing

The human brain has a remarkable capacity of learning streams of sensory events from our surroundings like sounds or images. Often, these events do not occur in a random way, but follow repetitive rules and patterns. Being able to learn these patterns and form predictions about future events before they occur is a key skill for survival, as violations of anticipated patterns can signal danger. Surprise, or prediction error (PE) signals can be recorded non invasively with the use of electro- or magnetoencephalography (E/MEG) techniques. PE signals are elicited in the brain not only when paying attention to environmental stimuli, but also when conscious perception fades away, for example during sleep. Interestingly, the presence and characteristics of PE signals can be associated to residual levels of consciousness and return of awareness, for example in patients with disorders of consciousness.

In our work, we are investigating the computational and electrophysiological substrates of PE signals in wakefulness and also during sleep. We are performing recordings of neural activity in humans via M/EEG, in order to study neural responses to anticipated sensory events such as sounds. These recordings are combined with machine learning techniques to extract patterns of neural responses to observed and/or anticipated events, like for example a sound that was anticipated but not delivered.

A better understanding of the neural circuits that are underlying sensory perception and PEs can shed light into predictive mechanisms in healthy conditions, and also their dysfunctions in various diseases, such as in patients with disorders of consciousness or patients with psychiatric disorders.

**Research staff:** Ruxandra Tivadar, Pinar Göktepe, Sigurd Alnes, Athina Tzovara

**Financial support:** Swiss National Science Foundation (320030_188737)

## Machine learning techniques for analyzing electrophysiological data

Recordings of neural activity from the human brain often result in large amounts of electrophysiological data. Multivariate Pattern Analysis (MVPA) is often used in neuroscience to extract patterns of neural responses to external stimuli. MVPA has been initially developed for imaging data, while more recent approaches are also focusing on electrophysiological data like electroencephalography (EEG). The majority of existing MVPA techniques consist of training and testing linear classifiers across time, and identifying periods of interest in a time-course of EEG signals. However, these techniques are only sensitive to time-locked information that appears at similar latencies across observations.

In our research, we are developing novel approaches for MVPA, based on convolutional neural networks (CNNs). These approaches have the advantage that they (a) learn from large populations of heterogeneous participants, and (b) disentangle neural processes that are not locked in space or time.

Our results show that compared to more 'traditional' machine learning techniques, CNNs provide a stronger classification performance, taking advantage of rich spatio-temporal EEG features. Crucially, features used by the networks to reach a decision have the advantage of being electrophysiologically interpretable. This work has future applications in the field of basic EEG research, for example for studying neural responses in large and diverse groups of participants, or for identifying fine-grained patterns that are relevant to experimental manipulations. Moreover, it has applications in clinical studies, where patient variability can be high due to different stages of disease progression, or different levels of brain injury.

**Research staff:** Florence Marcelle Aellen, Athina Tzovara

**Financial support:** Interfaculty Research Cooperation “Decoding Sleep: From Neurons to Health & Mind” of the University of Bern

## 3.4 Master’s Theses and Projects

- Fabian Loosli, University of Bern, Master’s Thesis: ”Predicting awakening from coma based on convolutional neural networks”, July 2021
- Shaikh Mohd Faraz, Technical University Dresden Germany, Master’s Research Project: ”Machine learning for detecting auditory sequences in Magnetoencephalography data”, April 2021

## 3.5 Bachelor’s Theses

- Mena Lerf, University of Fribourg Switzerland, Bachelor’s Thesis: ”Machine Learning for classifying EEG responses linked to neural predictive processing”, July 2021

## 3.6 Further Activities

### Presentations

**Athina Tzovara**

- Spatio-temporal structure and complexity of auditory processing in coma, Symposium organizer and symposium talk, Annual Meeting of the Organization for Human Brain Mapping, June 2021
- Data management for neuroscience studies, Lecture, Experimental Neurology Center, Inselspital, March 2021
- Neural dynamics of auditory processing in coma, Lecture, Benefri Neuroscience Workshop, February 2021
- Women in Computer Science and Engineering mentoring seminar, Lecture, University of Texas at Arlington, USA, February 2021
- unbAIsed: reducing bias in AI for healthcare, Workshop organizer and presenter, Mozilla Festival, March 2021
- Machine learning applications in neuroscience, Lecture, Bern Winter School on Machine Learning, University of Bern, February 2021

- Open access resources for applying machine learning techniques on neuroscience data, Lecture, Data Visualization Meeting, University of Bern, January 2021

- Introduction to machine learning for electrophysiological signals, Lecture, Experimental Neurology Center, Inselspital, January 2021

**Ruxandra Tivadar**

- Statistical Errors and Don’ts, Lecture, Experimental Neurology Center, Inselspital, July 2021

- EEG Responses to sound omissions are modulated by predictability, Poster Highlight Talk, Organization for Human Brain mapping, June 2021

- Digital Haptics in Vision Rehabilitation, Symposium Talk, Cognitive Neuroscience Society, January 2021

**Pinar Göktepe**

- Multivariate decoding of probabilistic auditory predictions, Short Talk, MEG NORD conference, May 2021

- Predictions of probabilistic sequences of environmental sounds, Poster Presentation, Organization for Human Brain Mapping June 2021

**Florence Aellen**

- Trade-offs between classification performance and interpretability in deep learning for EEG signals, Poster Presentation, Organization for Human Brain Mapping June 2021

**Sigurd Alnes**

- Complementary Roles for Neural Synchrony and Complexity in Acute Coma, Poster Presentation, Organization for Human Brain Mapping June 2021

## Conference and Scientific Committees

**Athina Tzovara**

- Committee on Best Practice in Data Analysis and Sharing (COBIDAS) for magnetic resonance imaging (MRI) data, member, 2021
- Organization for Human Brain Mapping (OHBM), past chair and member of Diversity and Gender Committee, 2020-2021
- Organization for Human Brain Mapping (OHBM), member of Awards Committee, 2020-2021

**Master Thesis Reviewer**
**Athina Tzovara**

- An Intracranial EEG Investigation of Long-Term memory: Coding of Associations in the Human Medial Temporal Lobe, Sepehrdad Rahimian, National Research University Higher School of Economics, Moscow, Russian Federation, 2020
- Spatial and Temporal Working Memory Identified by Distinct Oscillatory Activity, Riaz Abrar, National Research University Higher School of Economics, Moscow, Russian Federation, 2021

## Journal Committees

**Athina Tzovara**

- Handling Editor for open access publishing platform of the Organization for Human Brain Mapping, Aperture Neuro
- Editor for Frontiers for Young Minds

## Reviewing Activities

**Journal Reviews**
**Athina Tzovara**

- Computer Speech and Language
- European Journal of Neuroscience
- IEEE Journal of Biomedical and Health Informatics

- Journal of Neural Engineering
- Neuroimage
- Neuropsychologia

**Ruxandra Tivadar**

- Brain Topography
- Experimental Brain Research
- Psychophysiology
- The Leadership Quarterly

**Conference Abstracts Athina Tzovara**

- Organization for Human Brain Mapping

## 3.7 Publications

## Journal Publications

- Tivadar R., Knight R.T. Tzovara A. (2021). Automatic sensory predictions: a review of predictive mechanisms in the brain and their link to conscious processing. Frontiers in Human Neuroscience, doi: 10.3389/fnhum.2021.702520
- Norori N., Hu Q., Aellen F.M., Faraci F.D., Tzovara A. (2021). Addressing bias in big data and AI for health care: a call for open science. Patterns, doi: 10.1016/j.patter.2021.100347
- Schindler K.A., Nef T., Baud M.O., Tzovara A., Yilmaz G., Tinkhauser G., Gerber S.M., Gnarra O., Warncke J.D., Schütz N., Knobel S.E.J., Schmidt M.H., Krack P., Fröhlich F., Sznitman R., Rothen S., Bassetti C.L.A. (2021). NeuroTec Sitem-Insel Bern: Closing the Last Mile in Neurology. Clinical and Translational Neuroscience, doi: /10.3390/ctn5020013
- Llorens A.*, Tzovara A.*, Bellier L., Bhaya-Grossman I., Bidet-Caulet A., Chang W.K., Cross Z.R., Dominguez-Faus R., Flinker A., Fonken Y., Gorenstein M.A., Holdgraf C., Hoy C.W., Ivanova M.V., Jimenez

R.T., Jun S., Kam J.W.Y., Kidd C., Marcelle E., Marciano D., Martin S., Myers N.E., Ojala K., Perry A., Pinheiro-Chagas P., Ries S.K., Saez I., Skelin I., Slama K., Staveland B., Bassett D.S., Buffalo E.A., Fairhall A.L., Kopell N.J., Kray L.J., Lin J.J., Nobre A.C., Riley D., Solbakk A.K., Wallis J.D., Wang X.J., Yuval-Greenberg S., Kastner S., Knight R.T., Dronkers N.F. (2021). Gender bias in academia: A lifetime problem that needs solutions. Neuron, doi: 10.1016/j.neuron.2021.06.002 * equal contribution

- Dietmann A, Wenz E, van der Meer J, Ringli M, Warncke JD, Edwards E, Schmidt MH, Bernasconi CA, Nirkko A, Strub M, Miano S, Manconi M, Acker J, von Manitius S, Baumann CR, Valko PO, Yilmaz B, Brunner AD, Tzovara A, Zhang Z, Largiader CR, Tafti M, Latorre D, Sallusto F, Khatami R, Bassetti CLA. (2021). The Swiss Primary Hypersomnolence and Narcolepsy Cohort study (SPHYNCS): Study protocol for a prospective, multicentre cohort observational study. Journal of Sleep Research, doi: doi.org/10.1111/jsr.13296

- Tzovara A., Amarreh, I., Borghesani, V., Chakravarty, M. M., DuPre, E., Grefkes, C., Haugg A., Jollans L., Lee H.L., Newman S.D., Olsen R.K., Ratnanathern J. T., Rippon G., Uddin L., Q., Bringas Vega M.L., Veldsman M., White T., Badhwar, A. (2021). Embracing diversity and inclusivity in an academic setting: Insights from the Organization for Human Brain Mapping. Neuroimage, doi: 10.1016/j.neuroimage.2021.117742

- Turoman, N., Tivadar, R. I., Retsa, C., Maillard, A. M., Scerif, G., Matusz, P. J. (2021). The development of attentional control mechanisms in multisensory environments. Developmental cognitive neuroscience, doi: 10.1016/j.dcn.2021.100930

- Turoman, N., Tivadar, R. I., Retsa, C., Murray M.M., Matusz, P. J. (2021). Towards understanding how we pay attention in naturalistic visual search settings. NeuroImage. doi: 10.1016/j.neuroimage.2021.118556

## 3.8 Organization of Science Outreach Activities

- “Et si toi aussi tu devenais scientifique?” Scientific presentation for kids, Organization for Human Brain Mapping, June 2021.

- “Can your science pass a kid’s review”, Society for Neuroscience, Brain Awareness Week, March 2021.

# 4 Communication and Distributed Systems Group

## 4.1 Personnel

| | | |
|---|---|---|
| **Head:** | Prof. Dr. T. Braun | Tel.: +41 31 511 2631<br>Email: torsten.braun@inf.unibe.ch |
| **Office Manager:** | D. S. Schroth | Tel.: +41 31 684 8681<br>Email: daniela.schroth@inf.unibe.ch |
| **Scientific Staff:** | Dr. A. Di Maio | Tel.: +41 31 511 2639<br>Email: antonio.dimaio@inf.unibe.ch<br>(As of 01.09.20) |
| | J. Ajayi | Tel.: +41 31 511 2638<br>Email: jesutofunmi.ajayi@inf.unibe.ch |
| | L. De Sousa Pacheco | Tel.: +41 31 511 7631<br>Email: lucas.pacheco@inf.unibe.ch<br>(As of 15.09.20) |
| | N. Emami* | Tel.: +41 31 511 2633<br>Email: negar.emami@inf.unibe.ch |
| | E. Kalogeiton* | Email: eirini.kalogeiton@inf.unibe.ch<br>(Until 30.04.2020) |
| | A. Medeiros de Lima | Tel.: +41 31 511 2637<br>Email: alisson.medeiros@inf.unibe.ch |
| | H. Melo dos Santos | Email: hugo.santos@inf.unibe.ch<br>(Until: 31.12.20) |
| | D. Oliveira Rodrigues* | Email: diego.oliveira@inf.unibe.ch<br>(Until: 30.11.20) |
| | E. Samikwa | Tel.: +41 31 511 2634<br>Email: eric.samikwa@inf.unibe.ch<br>(As of 01.09.20) |
| | D. Xenakis* | Tel.: +41 31 511 7631<br>Email: dimitrios.xenakis@inf.unibe.ch |

**External Ph.D. Students:**

| | |
|---|---|
| G. Manzo (until February 2021) | Email: gaetanomanzo@gmail.com |
| J. Schaerer | Email: jakob.schaerer@abilium.com |
| P. Hammler (as of October 2020) | Email: patric.hammler@inf.unibe.ch |

*With financial support from a third party credit

## 4.2 Overview

The research group "Communication and Distributed Systems" has been investigating how multimedia and mixed reality applications and cloud computing services with high demands on the quality, reliability and energy efficiency can be supported by mobile communication systems and networks. Moreover, we are investigating localization mechanisms for wireless devices and new Future Internet paradigms such as Information-Centric Networking (ICN) as well as the Internet of Things (IoT). We are also working on mobility and trajectory prediction of mobile users and vehicles using advanced machine learning mechanisms. Distributed and Federated Machine Learning are emerging approaches for mobility prediction, mixed reality, and IoT.

## 4.3 Research Projects

### Multi-Echelon Inventory Optimization and Building Automation

This project started in December 2020 in collaboration with Hoffmann-La Roche and aims to apply Deep Reinforcement Learning (DRL) in several business areas such as building automation and supply chain optimization. Reinforcement Learning is a paradigm in the field of machine learning and its goal is to find an optimal policy. An agent applies actions to an environment by considering state information. After each interaction, the agent assesses the quality of specific state-action pairs and adjusts the model weights to maximize the expected reward. Deep Reinforcement Learning is associated with some promising characteristics: (1) DRL can handle high-dimensional state vectors. Many different factors can be taken into account in the control. (2) Using deep neural networks as function approximators is associated with a high representative capacity. This is particularly useful for stochastic control systems where the structure of the optimal controls is unknown.

Today's supply chains of multinational corporations are arranged in a network that can be interpreted as a multi-echelon inventory system. The products are stored in different processing stages. In the case of pharmaceutical companies, these can be divided into factory, global warehouses and local warehouses. Each of those stages represent one echelon and may consist of several inventory system instances. The reorder policy governs the reorder timing and the reorder quantity for each inventory

system. The goal of this project is to find the optimal reorder policy for a multi-echelon inventory system which minimizes the cost. The overall costs consist of holding-, shortage-, and reorder costs. From a research perspective, this project raises two interesting challenges: First, the environment needs to be modeled by considering several stochastic processes such as the demand and the lead times. Secondly, the agent needs to find an optimal policy. This is challenging due to the extremely high dimensional state and action spaces. In order to solve this scalability problem, the project's research will focus on a multi-agent reinforcement learning approach.
Another goal of this project is in the area of buildings and sustainability. The initial focus will be on the elevator system. Further steps then include also other building systems such as heating, cooling and ventilation. The underlying research question is whether Deep Reinforcement Learning can be used to control such systems for maximising comfort parameters (e.g. low average elevator waiting times) and minimizing energy consumption.

**Research staff:** P. Hammler, T. Braun.

## Efficient Distributed and Federated Machine Learning for Internet of Things

The Internet of Things (IoT) has gained a lot of importance in recent years. It encompasses infrastructure of software and hardware that connects the physical world with the Internet. Due to the explosive growth of interest in this paradigm, the number of IoT devices has increased dramatically in recent years. It has been estimated that by 2025, more than 75 billion devices will be connected to the Internet, leading to an economic impact on the global market. Machine Learning (ML) is an essential technology used in IoT applications, allowing them to infer higher-level information from a large amount of raw data collected by IoT devices. However, current state-of-the-art ML models often have significant demands on memory, computation, and energy. This contradicts the resource-constrained nature of IoT devices that is characterised by limited energy budget, memory, and computation capability. Typically, ML models are trained and executed on the cloud. This requires data from IoT systems to be sent to the cloud across networks for processing. The cloud-centric approach gives access to greater computing power and storage, but is principally disadvantageous in various ways. Firstly, the response time obtained from processing on geographically-distant data centers may not be sufficient to meet real-time requirements of latency-critical applications. Secondly, the cloud-centric methods risk potentially exposing private and sensitive information during data transmission and remote processing and storage. Thirdly, transferring the raw data to the centralized cloud increases the ingress bandwidth demand on the backhaul network. To overcome the aforementioned limitations, fog or edge computing has been proposed to make use of computation resources that are closer to data collection IoT end points through distributed computing. The objective of this research is to determine how to efficiently distribute ML tasks across different elements in IoT systems, taking into account computation and communication constraints. Initially, we propose a method for low latency and energy efficient ML inference in IoT systems through adaptive early exit of computation. We also propose a federated split learning mechanisms with clustering, for efficient privacy preserving training in resource-constrained environments.

**Research staff:** E. Samikwa, T. Braun.

## Managing Edge-enabled Mobile Virtual Reality Services with Service Chaining Graph

Virtual Reality (VR) enhances our physical environment by artificially rendering a real environment using audio and visual features possibly supplemented with other sensory devices. Although VR systems have attracted considerable attention in recent years, it has been considered a “killer” use case of 5G networks due to stringent application requirements. Despite expectations and investments, the use of tethered VR Head Mounted Displays (HMDs) imposes significant restrictions on VR technology’s application domain, e.g., Quality of Experience (QoE) for VR users. A primary latency bottleneck lies in the fact that VR systems are composed of multiple compute-intensive components. Furthermore, technical challenges for Mobile Virtual Reality (MVR) are posed by standalone VR HMDs that must be ergonomic, e.g., lightweight, leading to new challenges to meet the computing latency requirements for MVR merely by standalone VR HMD processing. VR has posed several challenges to the current VR HMD technology domain and the network infrastructure in supporting ultra-high throughput and ultra-low latency due to: (i) The current VR HMDs fail to satisfy the computing latency requirements for MVR applications; (ii) today’s VR HMDs do not support the necessary power demands;

and (iii) the cloud computing architecture does not support the network latency requirements for ultimate VR applications. The aforementioned challenges will become dramatically difficult to address once VR applications become advanced and are massively consumed. One way to overcome the challenges mentioned above is to use the MEC infrastructure to deploy the compute-intensive tasks of VR applications. We propose refactoring VR-intensive computing tasks into VR service functions, where they are chained and deployed throughout the MEC infrastructure. We aim to reduce the computing latency for future MVR applications. However, coordinating such a plethora of service functions brings to light several challenges: (i) How would VR refactoring overcome the computational power required by VR HMDs? (ii) What are the benefits of MEC to support VR-intensive computing tasks? (iii) How to manage several VR service functions, each featuring distinct policies and requirements? To answer these questions, we propose refactoring VR services into Service Chaining Graph (SCG). SCG is a graph-based structure to manage VR services deployed at MEC infrastructures. SCG seeks to support VR services' offloading as much as needed from the VR HMDs to the edge infrastructure to reduce the computation burden from VR HMDs. To deploy the VR services in the edge infrastructure we use REACT [Medeiros et al., 2021].

**Research staff:** A. Medeiros, A. Di Maio, T. Braun.

## Network Function Virtualization and Fog Service Support in 5G Networks

Fifth-generation wireless networks (*i.e.*, 5G) will need to provide connectivity for a wide range of services with heterogeneous requirements. These services can be designated into 3 main categorized, namely: enhanced Mobile Broadband (eMBB), massive Machine Type Communications (mMTC) and ultra-Reliable Low-Latency Communications (uRLLC). Of these three categories, network support for services needing low-latency and high reliability (*i.e.*, uRLLC) is anticipated to be the most challenging based on current deployments, which often rely on centralized processing (i.e. cloud data-centers) on specialized hardware. Following this, new innovations, which include a departure from the current hardware-centric network architecture, and a greater focus on network virtualization while bringing advanced computational capabilities to the edge (*i.e.*, Edge/Fog Computing), have been suggested as a means towards improving network support of such services.

In this research, we investigate ways to support services requiring low-latency communication *and* computation in virtualized & Edge-enabled 5G networks. Specifically, we look to develop novel resource allocation and orchestration approaches, based on network softwarization & virtualization, by focusing on support for services requiring Edge Computing capabilities in 5G networks. Initially, we propose the use of context-awareness to enhance the performance of edge-hosted services and improve resource utilization, by effectively allocating resources to services that are deployed over a common infrastructure, with the goal of meeting their service requirements while compensating for network uncertainty.

**Research staff:** J. Ajayi, T. Braun.

## Intelligent Mobility Services

Nowadays, huge amounts of data regarding pedestrian and vehicle mobility traces are available from Location Based Services (LBS). This data is pivotal for enabling intelligent mobility services such as navigation, localization and mobility prediction. In this project, we focus on developing improved methods to achieve that. More specifically, the research has been divided into two distinct aspects: localization and mobility prediction. Both these components are discussed below in more detail.

### *- Indoor & Outdoor Localization*

Different location-based services come with different positioning accuracy requirements. For outdoor applications (e.g. car navigation), most often, global navigation satellite systems (e.g. GPS) can inexpensively cover the needs. Yet, applications in indoor environments (e.g. COVID19 tracking indoors), where satellite signals are not available, are more challenging. Therefore, considering (i.e. fusing) many types of signal sources such as Bluetooth/Wi-Fi signals, magnetometer, accelerometer, gyroscope, etc. is critical for achieving accurate positioning indoors.

In accordance with the above and within the frame of the research that has been conducted by the communication and distributed systems group [Li et al., 2021], we propose a new methodology for enhancing the positioning accuracy in such systems by taking advantage of signals (e.g. Low Energy Bluetooth) that can be exchanged between different mobile devices (e.g. smartphones). With this new technique which has been named ARLCL (Anchor-free Ranging-Likelihood-based Cooperative

Localization) instead of tracking individually each mobile device, we consider at the same time all exchanged signals, eventually positioning them as a system (or a swarm of devices).

Exhaustive comparisons against the ”Mass-Spring” optimization, which is currently the most-respected approach for tackling the same problem, showed an overall improvement of 25% (for sparse deployments) and 6% (for thin deployments) at the 75th percentile of cases. A gain which is also correlated to both the swarm’s size and the signal’s noise.

***- Mobility & Congestion Prediction Services***

Today’s society is highly relying on mobility. Trajectory prediction plays a key role in enabling and enhancing the performance of a diverse range of applications. Managing traffic congestion, providing route recommendations, and emergency services on one hand, networking, collision prediction in autonomous cars, service migration, and handover optimization on the other hand, are only some of the many applications that immensely benefit from mobility prediction. Thanks to the availability of enormous location data which provides this possibility to analyze and infer mobile users’ daily behaviors and consequently the urban dynamics. The main focus and plans of this project are designing advanced machine learning and deep learning models in order to precisely predict the future location, trajectory, and traffic flow of both humans and vehicles. We have developed a Recurrent Neural Network-based mobility predictor and a Convolutional Neural Network-based predictor, which are compatible models for time-series data and can reach quite high accuracy with respect to the feed forward Neural Networks or non-Neural Networks. To automate and optimize the complex process of hyper-parameter selection, we have implemented a Reinforcement Learning-based model. However, the attained training time is still remarkable. We are trying to design other comparable models and means expecting to find a good compromise between accuracy and training time. We proposed a robust model that manages computational resources consumption by clustering similar trajectory users, training a single model per cluster based on few users data, and then transferring the pre-trained model to other group members. In this way, we are able to remarkably decrease the total training time and computational resources.

**Research staff:** D. Xenakis, N. Emami, T. Braun.

**Financial support:** Swiss National Science Foundation (SNSF) [Contract No. 184690]

## Context Awareness Engine

The Context Awareness Engine project funded by Orange SA explores network context information to discover, reason, and predict network and subscriber situations by appropriate computation and information modelling based on collected network data from various data sources (network nodes, devices, applications). The purpose is to propose recommendations or request actions (context awareness) using advanced machine learning and deep learning algorithms. We aim to find insights from observed phenomena and infer the root causes, such that future situation prediction can be achieved and further exploited to optimize network performance. The project is broken into 2 phases: Phase 1 includes use case definition (WP1) and functional architecture definition (WP2), and Phase 2 includes implementation architecture definition (WP3) and software development and demonstration (WP4).

From August 2020 to July 2021, the CDS group continued to work on the Orange data for other projects. We have extended the individual-level RL-LSTM mobility predictor to cluster-level RC-TL (Reinforcement Convolutional Transfer Learning) mobility predictor. The previously-suggested individual RL-LSTM brought high prediction accuracy, however, it was very expensive in terms of computational resource consumption and training time. Most state-of-the-art mobility predictors apply a same heuristically-designed neural network to different user datasets, which might be computationally effective, but does not guarantee the optimal performance. Thus, Reinforcement Learning as a self-learning approach can optimise the process of highest-performance neural architecture search. However, in big network scenarios, developing a single Reinforcement Learning scheme per user data is impossible due to limited computational resources. Therefore, in RC-TL we cluster similarly trajectory users, train a single Convolutional Neural Network (that is optimized through a single RL) per few users data, and then transfer the model to other group members. In this way, we can save up to 90% of total computational resources while, the average prediction accuracy drops only 3%.

**Research staff:** N. Emami, T. Braun.

**Financial support:** Orange Research Contract Number H09194

## Context- and Content-Aware Communications for QoS support in VANETs (CONTACT)

Vehicular Ad Hoc Networks (VANETs) are characterised by intermittent connectivity and path breaks between nodes since vehicles can travel with high speeds in different locations. These path breaks lead to high packet loss, reducing the Quality of Service (QoS) requirements that VANET applications demand. In our project named CONtext and conTent Aware CommunicaTions for QoS support in VANETs (CONTACT), we study three different architectures: Named Data Networking (NDN), Floating Content (FC) and Software Defined Networking (SDN). We apply these architectures in VANETs to achieve the QoS requirements of applications by using one or more combined paradigms.

This project aims to enable NDN in VANETs by using only vehicle to vehicle communication. We equip vehicles with directional antennas to provide directivity in message forwarding. This achieves higher and faster content retrieval, because vehicles that are outside of the spreading area of the message can perform other tasks. Furthermore, we combine SDN and NDN to study the impact that SDN have when applied in VANETs. SDN centralises the network, allowing the vehicles to follow the instructions provided by an SDN controller. The SDN controller is connected to RSUs that act as gateways and instructs them to change their transmission power to connect with more vehicles. The SDN controller, also, calculates routing paths between vehicles to achieve multi-hop connectivity between them.

Furthermore the project proposes a data-driven centralized approach to resource-efficient, QoS-aware dynamic management of FC. Our Deep Learning strategy employs a Convolutional Neural Network (CNN) to capture the relationships between patterns of users mobility, of content diffusion and replication, and FC performance in terms of resource utilization and of content availability within a given area. This project has already introduced a new version of FC, called Cellular Floating Content (CFC), which optimizes the use of bandwidth and memory [Rizzo et al., 2021] by adapting the content replication and storage strategies to the spatial distribution of users, and to their mobility patterns.

The project's final goal is to combine FC, NDN and SDN to address the issue of persistent partitioning that arises in VANETs. We propose DeepNDN [Manzo et al., 2020], a communication scheme that allows content retrieval in fragmented and highly dynamic network topologies with applications that require tight delay constraints. Our goal is to achieve the application's required hit ratio in an efficient, resource aware matter. To manage the DeepNDN algorithm we employ a CNN architecture for capturing the relations between spatio-temporal patterns of vehicular mobility and content requests of vehicles. The project's results about information-centric vehicular networks are summarized in the PhD thesis [Kalogeiton et al. 2020].

**Research staff:** E. Kalogeiton, G. Manzo, A. Di Maio, T. Braun.

**Financial support:** Swiss National Science Foundation Project No. 146376

## Software-Defined Service-Centric Networking in Urban Environments

Disruptive applications for mobile devices that can be enhanced by Edge Computing facilities are emerging, such as the Internet of Things, Immersive Media, and Connected and Autonomous Vehicles. These applications have strict requirements in order to properly work that are difficult to be fulfilled with current computing paradigm at the Cloud. In this context, Edge Computing is an architecture expected to aid on meeting requirements imposed these applications. This architecture aims to introduce computing capabilities in the path between the user and the Cloud to execute tasks closer to where they are consumed, thus mitigating issues, such as latency, context awareness, and mobility support. The present project aims to create models to understand urban mobility and its impact on mobile applications provisioned at the edge. We aim to model different aspects of mobility and analyse emerging classes of mobile applications. We expect to understand mobility and mobile applications to create better mobility management algorithms and protocols. Our initial efforts in this project concentrated on developing an origin-destination mobility flow clustering tool to model urban mobility [Rodrigues et al., 2021], and studying SDN-enabled handover mechanisms for cellular networks.

**Research staff:** D. O. Rodrigues, T. Braun

## Low Latency Service Management for Vehicular Fog Computing

Smart cities will enable the deployment of innovative applications, such as connected and autonomous vehicles. In this context, smart transportation and cooperative sensing services will be essential to improve traffic safety. The concept of Vehicular Fog Computing (VFC) expands cloud resources in the far edge with vehicles on-board units. We raise the challenges of stable quality of service provision, service migration schemes, and proactive VFC resources mapping for the continuous service execution. Specifically, we propose a mobility aware service management to automate the service assignment for mobile service requester and mobile fog nodes. We suggest a distributed clustering of fog nodes with similar trajectories at the same time into service zones. To validate the impact of the proposed service management approach, we consider vehicles interested in cooperative sensing services that share their trajectories plans and on-board cloud resources. For results, we expect to provide quality of service assurance for greedy and low latency services for VFC.

**Research staff:** H. Santos, T. Braun

## Mobility and Cloud Management with Federated and Distributed Learning

Service positioning becomes an increasingly important topic with the emergence of Multi-access Edge Computing (MEC) in modern networked scenarios. The presence of MEC signifies more fine-grained and distributed cloud computing capabilities. The computing and storage capabilities of the network are distributed across the scenario, such as across an entire region or city. In this context, users consume more demanding services, such as Virtual and Augmented Reality (VR and AR, respectively), which need to be allocated and served from locations close to the users themselves. As users move through the scenario, the services must follow their mobility patterns to maintain acceptable latencies and data rates according to the application requirements. The design and evaluation of tools for the migration and allocation of highly demanding services in MEC scenarios with multiple users and limited resources becomes increasingly important while challenging.

In this project, we have proposed two techniques for service migration and allocation of resources in MEC servers to maximize the end-to-end application throughput throughout the network and better serve the application requirements. Firstly, we propose a service migration for Connected Autonomous Vehicles (CAV) [Pacheco et al., 2021], which have extremely low latency requirements to be processed in instances in edge servers. Furthermore, we defined a service migration algorithm for environments with heterogenous applications with varying requirements

[Pacheco et al., 2021]. In both cases, the proposed solutions achieved superior performance compared to state-of-the-art solutions in terms of sufficing application requirements and maximizing network throughput. Furthermore, more investigation had been made in mobility prediction and mobility management in mobile networks, using service migration and advanced machine learning techniques [Zhao et al., 2020].

**Research staff:** L. Pacheco, T. Braun

## Distributed Public Key Infrastructure for the Internet of Things

The Internet of Things is growing fast. Recent improvements in the interoperability between smart devices enable new applications in the Industrial Internet of Things, Smart City, Smart Home, autonomous driving, and more. All these applications will require smart devices to exchange information with each other. However, the existing Public Key Infrastructures (PKI) do not adapt well to the decentralized architecture of the Internet of Things. Consequently, it becomes more challenging to verify the authenticity of exchanged data when the IoT is growing. Furthermore, many applications require auditability in all processes. To achieve this auditability it must be possible to prove that a specific smart device has measured a particular value or performed a certain action at a given time. Distributed Public Key Infrastructure (DPKI) based on Distributed Ledger Technology (DLT) is a promising approach to solve these challenges. In this project, we propose the framework Veritaa. Veritaa is a DPKI with a Signature Store. Veritaa comprises the Graph of Trust (GoT) and the Acyclic Block Confirmation Graph (ABCG). The GoT represents signed trust relations between identity claims. The ABCG is an application-specific BlockDAG optimized to store the graph transactions that build the GoT immutably and non-repudiable. Our initial work was to design, implement, and evaluate the basic Veritaa framework [Schaerer et al., 2020]. Furthermore, to validate Veritaa's applicability for the IoT, we build a real-world IoT testbed. And to evaluate distributed certification, we simulate different GoTs.

**Research staff:** J. Schärer, T. Braun.

## Testbeds

The CDS group possesses and operates a cloud infrastructure based on Dell Power Edge Servers. Currently on the institute we own five DELL machines: R320, R520R540. These support 212 parallel threads (106 cores) and 848 GB RAM. Furthermore, we operate two external Dell PowerVault MD3800i that provide us disk space of 35 TB in Raid 5 and Raid 6. The network backbone is based on Dell N4032 switches with 48x10 GbE-T ports and 80 Gb/s backbone connection. Together with the Lightweight Directory Access Protocol (LDAP) of the institute our infrastructure provides in the members of the CDS group the following services:

- Mirantis OpenStack 10.0 (IaaS research cloud)
- OwnCloud (shared storage between the CDS members)
- Wiki (information dissemination for the Institute and the CDS group)
- Etherpad (collaborative real-time editor)
- SVN (collaborative version management system)

For administrator purposes we use

- Teampass as a password management system

Finally for monitoring our infrastructure we use

- Nagios

The CDS group has its own IoT testbed that consists of:

- 40 MEMSIC Telsob by Crossbow (now Willow) sensors consisting of:
  - Texas Instruments 16 bit microprocessor (TI MSP 430)
  - 802.15.4 radio interface
  - Fixed Power Supply via the USB Interface
  - Temperature, humidity and light sensor
  - 1 MB external flash
- 7 MSB-430 Sensor Nodes consisting of:
  - Texas Instruments 16 bit microprocessor (TI MSP 430)
  - CC1020 radio interface
  - Temperature, humidity and acceleration sensor
  - SD memory interface

Hence, the CDS group built and operates a CDS testbed that consists of 47 nodes. These nodes are placed across the 4 floors of one building of the Institute of Computer Science of the University of Bern. The 7 MSB430 sensor nodes are placed indoors and one node is an outdoor node placed on a top window sill.

## 4.4 Ph.D. Theses

- Mariano de Souza, A. ”Towards a Personalized Multi-objective Vehicular Traffic Re-routing System”, May, 2021. URL: https://boris.unibe.ch/id/eprint/156641
- Karimzadeh, M. ”Prediction Models to Enhance Location Based Services in Urban Areas”, December, 2020. URL: https://boris.unibe.ch/id/eprint/149118
- Marandi, S. A. ”Bloom Filter-Based Content Discovery and Retrieval for Information-Centric Networks”, November, 2020. URL: https://boris.unibe.ch/id/eprint/147671
- Kalogeiton, E. ”Information-Centric Networking in Vehicular Ad-Hoc Networks”, October, 2020. URL: https://boris.unibe.ch/id/eprint/147670

## 4.5 Bachelor Theses

- Mordeniz, S. ”Veritaa: Signing Transactions on Arduino”, September, 2020. URL: https://tinyurl.com/abyyn5bk
- Würsten, M. ”Localization with LoRa - Independent of Network coverage Bachelor Thesis”, September, 2020. https://tinyurl.com/yncwnn4c
- Esposito, A. ”RL-CNN: Reinforcement Learning designed Convolutional Neural Network for Urban Traffic Flow Estimation Bachelor Thesis”, January, 2021. https://tinyurl.com/jzndxv39
- Schwegler, S.M. ”MTL-LSTM: Multi-Task Learning-based LSTM for Urban Traffic Flow Forecasting Bachelor Thesis”, January, 2021. https://tinyurl.com/nkrtn3mx

## 4.6 Awards

- Best Poster Award at Bern Science Day 2021: Negar Emami et al. ”Reinforcement-supported Artificial Neural Network-based Trajectory Prediction”

- Best Poster Award at Bern Science Day 2021: Lucas Pacheco et al. ”Distributed and Federated Learning Optimization with Federated Clustering of IID-users”

## 4.7 Further Activities

### Memberships

**Torsten Braun**

- Erweitertes Leitungsgremium Fachgruppe “Kommunikation und Verteilte Systeme”, Gesellschaft für Informatik
- SWITCH Stiftungsrat (until end of 2020)
- Kuratorium Fritz-Kutter-Fonds
- Expert for Bachelor Theses at Fachhochschule Bern
- Expert for Matura Exams at Gymnasium Langenthal
- Chair of thesis award committee of GI-KuVS

### Editorial Boards

**Torsten Braun**

- Editorial Board Member of Informatik Spektrum, Springer
- Editorial Board Member of MDPI (Multidisciplinary Digital Publishing Institute) Journal of Sensor and Actuator Networks

**Antonio Di Maio**

- The Hertz Journal of Engineering

### Public events

- **Study Week on Fascinating Informatics:** At this event, Jakob Schärer taught two high school students how to measure and analyse the Bluetooth messages sent by the SwissCovid app, 6-11 September, 2020.

- **BENEFRI Summer School 2020:** A 3-day seminar together with the HES-SO Fribourg and the University of Neuchâtel, at Münchenwiler, Switzerland, 31 August - 3 September, 2020.

## Conference Program Committees

### Torsten Braun

- 21st International Conference on Next Generation Wired/Wireless Networks and Systems (NEW2AN), August 26-28, 2020
- 13th conference on Internet of Things and Smart Spaces (ruSMART), August 26, 2020. St. Petersburg, Russia
- 21st IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM), August 31 - September 3, 2020
- 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), October 5-7, 2020
- 32th International Teletraffic Congress CONGRESS (ITC 32), September 22-14, 2020 Osaka
- 13th ICT Innovations Conference 2020, September 24-25, 2020
- IEEE 92nd Vehicular Technology Conference (VTC2020-Fall), November 18 - December 16, 2020
- IEEE International Conference on Internet of Things and Intelligence System (IoTaIS 2020), November 23-24, 2020, Bali
- IEEE Global Communications Conference (Globecom), December 8-10 2020, Taipei
- IEEE Consumer Communications and Networking Conference (CCNC), January 9-12, 2021
- 16th Wireless On-demand Network systems and Services Conference (WONS), March 9-11, 2021
- 36th ACM Symposium On Applied Computing Gwangju (SAC), March 22-26, 2021, South Korea

- IEEE Wireless Communications and Networking Conference (WMNC), March 29 - April, 1, 2021, Nanjing, China
- IEEE International Conference on Communications (ICC), June 14-23, 2021, Montreal
- IEEE/ACM International Symposium on Quality of Service (IWQoS), June 25–28, 2021
- 3rd International Workshop on Urban Computing, July 14-16, 2021

### Antonio Di Maio

- The 3rd ACM International Symposium on Blockchain and Secure Critical Infrastructure (ACM BSCI 2021), 7-11 June 2021, Hong Kong, China.
- The 17th IEEE International Conference on Advanced and Trusted Computing (IEEE ATC 2020), 8-10 December 2020, Melbourne, Australia.
- The 8th IEEE International Conference on Smart City and Informatization (IEEE iSCI 2020), 29 December 2020 - 1 January 2021, Guangzhou, China.
- The 19th International Conference on Ad Hoc Networks and Wireless (AdHoc-Now 2020), 19-21 October 2020, Bari, Italy.

## Project and Person Reviewing Activities

### Torsten Braun

- Research Council of Norway
- Research Foundation Flanders
- Luxembourg National Research Fund (CORE Panel chair)
- Academy of Finland
- European Science Foundation
- Swiss National Science Foundation
- Deutsche Forschungsgemeinschaft

- Italian Ministry for University and Research
- University of Luxembourg, Accreditation of Computer Science Programs

## Journal Article Reviewing Activities

### Torsten Braun

- IEEE Communications Magazine
- IEEE/ACM Transactions on Networking
- IEEE Transactions on Network and Service Management
- IEEE Wireless Communications Magazine
- IEEE Sensors Journal
- ACM Transactions on Multimedia Computing Communications and Applications

### Antonio Di Maio

- IEEE Transactions on Vehicular Technologies
- Elsevier Computer Networks
- Elsevier Computer Communications
- Elsevier Information Science
- Elsevier Journal of Network and Computer Applications
- MDPI Sensors
- MDPI Electronics
- MDPI Applied System Innovation
- IET Communications
- PeerJ

## Talks and Tutorials

### Torsten Braun

- Panelist “Session 4: Pedagogy: techniques and tips.“ at ACM Sigcomm 2020 workshop “Online Networking Education Community Discussion“
- Keynote Talk “Mobile Edge Computing: Research Challenges“ at VIII Oteima Tecnofest “La Revolucion del Cloud Computing“, Universidad Tecnologica Oteima, David, Panama, June 30, 2021

## PhD Committee Memberships

### Torsten Braun

- Cristian Hernandez Benet (PhD Jury), Karlstad University, June 3, 2021

# 4.8 Publications

**Disclaimer:** The publication list only includes publications published during the academic year, but does not include submitted and not yet published papers.

### Journal Papers

- Rizzo G., Marsan. M.A., Braun T., Manzo G. (2021). Optimal strategies for floating anchored information with partial infrastructure support. In *Vehicular Communications*, http://dx.doi.org/10.1016/j.vehcom.2020.100287, August 2020.
- Medeiros A., Braun T., Maio D.A., Neto A. (2021). REACT: A Solidarity-based Elastic Service Resource Reallocation Strategy for Multi-access Edge Computing. Physical communications, 47, p. 101380. Elsevier https://doi.org/10.1016/j.phycom.2021.101380

- Oliveira R. D., Maia G., Braun T., Loureiro A. A. F., Peixoto M. L.M., Villas L. A. (2021). Exploring Hybrid-Multimodal Routing to Improve User Experience in Urban Trips. In *Applied Sciences*, https://doi.org/10.3390/app11104523, May 2021.

- Li Z., Zhao X., Zhao Z., Braun T. (2021). WiFi-RITA Positioning: Enhanced Crowdsourcing Positioning based on Massive, Noisy User Traces. IEEE transactions on wireless communications, 20(6), pp. 3785-3799. IEEE 10.1109/TWC.2021.3053582

- Zhao Z., Karimzadeh M., Pacheco L., Santos H., Rosário D., Braun T., Cerqueira E. (2020). Mobility Management with Transferable Reinforcement Learning Trajectory Prediction. IEEE Transactions on Network and Service Management, 17(4), pp. 2102-2116. IEEE 10.1109/TNSM.2020.3034482.

- Esposito C., Zhao Z., Rak J. (2020). Reinforced Secure Gossiping Against DoS Attacks in Post-Disaster Scenarios. IEEE Access, 8, pp. 178651-178669, IEEE https://doi.org/10.1109/ACCESS.2020.3027150

## Book Chapters

- Dao N.N., Dinh N.T., Pham Q.V., Phan T.V., Cho S., Braun T. (2021). Vulnerabilities in Fog/Edge Computing from Architectural Perspectives. In: Chang, Wei, Wu, Jie (eds.) Fog/Edge Computing For Security, Privacy, and Applications. Advances in Information Security: Vol. 83 (pp. 193-212). Springer Nature Switzerland 10.1007/978-3-030-57328-7_8

## Conference Papers

- Pacheco L., Oliveira H., Rosário D., Cerqueira E., Villas L., Braun T. (2020). Service Migration for Connected Autonomous Vehicles. In: IEEE Symposium on Computers and Communications (pp. 1-6). IEEE 10.1109/ISCC50000.2020.9219592

- Karimzadeh M., Aebi R., Souza M.D.A., Zhao Z., Braun T., Sargento S., Villas L. (2021). Reinforcement Learning-designed

LSTM for Trajectory and Traffic Flow Prediction. In: IEEE Wireless Communications and Networking Conference (pp. 1-6). IEEE 10.1109/WCNC49053.2021.9417511

- Manzo G., Kalogeiton E., Di Maio A., Braun T., Palattella M. R., Turcanu I., Soua R., Rizzo G. (2020). DeepNDN: Opportunistic Data Replication and Caching in Support of Vehicular Named Data. In *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM 2020)*, Virtual Conference, https://doi.org/10.1109/WoWMoM49955.2020.00051, August 31 - September 03, 2020.

- Kalogeiton E., Braun T. (2020). On the Impact of SDN for Transmission Power Adaptation and FIB Population in NDN-VANETs. In: 18th ACM International Symposium on Mobility Management and Wireless Access (MobiWac'20) (pp. 57-66). ACM, https://doi.org/10.1145/3416012.3424617, November 16, 2020.

- Pacheco L., Rosario D., Cerqueira E., Villas L., Braun T., Loureiro A.F.A. (2021). Distributed User-centric Service Migration for Edge-Enabled Networks. In *2021 IFIP/IEEE International Symposium on Integrated Network Management (IM 2021)*, 618-622.

- Schaerer J., Zumbrunn S., Braun T. (2020). Veritaa - The Graph of Trust. In *IEEE Blockchain Research & Applications for Innovative Networks and Services (BRAINS 2020)*, Virtual Conference, https://doi.org/10.1109/BRAINS49436.2020.9223289, September 28-30, 2020.

# 5 Computer Graphics Group

## 5.1 Personnel

| | | |
|---|---|---|
| **Head:** | Prof. Dr. D. Bommes | Tel.: +41 31 631 3301<br>email: david.bommes@inf.unibe.ch |
| **Office Manager:** | D. Heinzen | Tel.: +41 31 631 4914<br>email: dragana.heinzen@inf.unibe.ch |
| **Scientific Staff:** | P.-A. Beaufort | Tel.: +41 31 511 76 01<br>email: pierre-alexandre.beaufort@inf.unibe.ch |
| | N. Gallego-Ortiz | Tel.: +41 31 511 76 01<br>email: nicolas.gallego@inf.unibe.ch |
| | M. Heistermann | Tel.: +41 31 511 76 01<br>email: martin.heistermann@inf.unibe.ch |
| | H. Liu | Tel.: +41 31 511 76 01<br>email: heng.liu@inf.unibe.ch |
| | V. Nigolian | Tel.: +41 31 511 76 01<br>email: valentin.nigolian@inf.unibe.ch |
| | S. Raimondi | Tel.: +41 31 511 76 06<br>email: simone.raimondi@inf.unibe.ch |

## 5.2 Overview

The research activities of the Computer Graphics Group are mainly located in the area of *geometry processing*, which is one of the central topics of *computer graphics*. Geometry processing is concerned with the development of concepts and algorithms to represent, generate, analyze, and modify the shape of objects. Resulting from the physical space we live in, omnipresent classes of shapes include curves, surfaces and volumetric bodies embedded in 3D, or 4D for time-varying shapes. Nowadays, such geometric objects are fundamental in numerous disciplines, inducing a strong scientific impact of geometry processing far beyond computer graphics. Applications as for instance numerical simulation in engineering or computational geology, anomaly detection or surgery planning in medicine, shape matching in computational biology, or the design of smart materials in additive manufacturing (e.g. 3D printing) only become feasible if accurate geometric representations of the involved shapes are available.

Currently, the group focuses on the generation of discrete geometry representations in the form of semi-structured meshes with quadrilateral elements for surfaces and hexahedral elements for volumetric objects. Such meshes combine the advantages of unstructured simplicial meshes and fully structured Cartesian grids. In contrast to previous methods, e.g. based on local operations, we focus on (global) variational formulations that enable a superior structure of the resulting meshes. There is empirical evidence that following this approach, for the first time algorithms are able to generate meshes that are comparable to manually designed ones. The variational formulation leads to involved nonlinear mixed-integer optimization problems. Hence, one goal of our research is the design of better formulations and parametrizations of the problem that pave the way for efficient solution strategies. In general, our research is driven by the idea of successively addressing the fundamental research questions that are critical from the practitioners perspective, and eventually come up with practically relevant meshing solutions.

## 5.3 Research Projects

### Locally Hexmeshable 3D Frame Fields

Hexahedral meshes are widely used in computational engineering, e.g. industrial applications, due to their superior numerical behavior than other volumetric meshes, e.g. reaching the same accuracy for much fewer elements. Among all hexahedral meshing algorithms, the frame field based method produces hexahedral meshes with superior quality and it is capable of generating meshes aligned to internal structures in addition to the boundary of the volume. It consists of three major steps: (1) generation of a surface-aligned 3D frame field, (2) construction of an integer-grid map that best aligns to the frame field, and (3) extraction of integer grids that explicitly form a hexahedral mesh. Being one of the most promising directions, however, it suffers from robustness issues that mainly come from frame field defects. The non-meshablity of the 3D frame field, from the singular graph point of view, can be categorized as (1) global topological inconsistencies such as twisted singular arcs on a cube topology, and (2) local topological inconsistencies, e.g. complex singular arc types, and non-meshable singular node types.

In this project, instead of solving the global inconsistencies, we focus on obtaining frame fields that are locally hex-meshable everywhere in the one-ring neighborhood in the discretized setting. To be locally hex-meshable, the one-ring has to meet two conditions: (1) one of the frame axes aligns to any singular edge or feature edge, and (2) the singularity has to be one of the 11 hex-meshable singularity types which we enumerated in our last publication. We develop an algorithm which on one hand includes both remeshing and relocation of singular vertices to align the singular graph to the frame field and eliminate complex singular edges; on the other hand, it decomposes non-meshable singular nodes by detaching singular arcs and turning points from it until it becomes meshable. At the end of the first stage, the only invalid nodes are turning points which in the second stage we split to a pair of valence +1 and valence -1 singular arcs and propagate to the boundary. In the end, the algorithm results in a 3D frame field that is locally hex-meshable.

**Research staff:** Heng Liu, David Bommes

**Financial support:** European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program, project AlgoHex, No. 853343

## HEXME – Dataset of Representative Inputs for Hexahedral Meshers

Since a while, the meshing community tries to build full conforming hexahedral meshes that are as regular as possible (i.e. structured) for geometries of interest. Those meshes are highly desired for fast and accurate simulations, and smooth and neat rendering. Even though some progress has been achieved, hex meshing remains - nowadays - a challenging task. Surprisingly, there is no dataset available to perform an objective analysis of state-of-the-art algorithms. Beyond yielding a fair comparison, enabling such a dataset would allow identifying common difficulties, and where improvements should be done.
Most of hexahedral meshers rely on a tetrahedral mesh faithfully representing the geometry. We therefore provide HEXME, the first dataset of tetrahedral meshes with feature entities. The feature entities are special points, curves and/or surfaces constraining the alignment of hexahedra. The tetrahedral meshes have been produced by using Gmsh, from three classes of computer-aided design models: simple, nasty and industrial. For the simple geometries, a hexahedral mesher should be able to generate a hexahedral mesh with optimal topology (the geometry of hexahedra

may be invalid). The nasty models seem to have a simple geometry, but are actually quite hard to be hex meshed. Finally, the industrial geometries correspond to cases whose hexahedrization is immensely valuable for simulations.

The resolution of a tetrahedral mesh likely affects the output quality of a hexahedral mesher. Hence, HEXME provides two resolutions per geometry: coarse and uniform. The coarse resolution is such that the number of tetrahedra is minimized while maintenaing the geometry. The size of tetrahedra may then change, in order to adapt to the geometry. On the other hand, the uniform resolution is such that the tetrahedra have more and less the same size, likely resulting in many tetrahedra.

The tetrahedral meshes are exported as vtk datafile version 2, in ASCII mode. In addition to the tetrahedral cells, other types of cell (vertex, edge, triangle) may be defined in order to represent the corresponding feature entities. A feature entity is identified thanks to a color, i.e. an integer corresponding to the cell data.

The pipeline generating the tetrahedral meshes from the computer-aided design models is orchestrated by Snakemake, a workflow management system. The pipeline is then fully transparent, and may easily be reproduced, maintained, and applied to new geometries. Specific parameters may be applied to some geometries, thanks to meta data file. A Snakemake html report may be produced, which yields details and timings related to the tetrahedrization, plus a pdf sheet per mesh summarizing the topology, geometry and quality of the mesh. This pdf report is published online https://cgg.unibe.ch/hexme/ as a preview of the dataset.

We plan to publish the Snakemake worklow on a public GitHub repository, along with the computer-aided design models (with their corresponding license), the meta data file and the compressed meshes. Each mesh is compressed with its log file into a zip file. The inflation may be done by using Snakemake, or manually. If relevant, the AlgoHex results could be published along.

**Research staff:** Pierre-Alexandre Beaufort, Heng Liu, David Bommes

**Financial support:** European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program, project AlgoHex, No. 853343

## Robust Volumetric Maps

Mapping an arbitrary volumetric domain to another one in an injective way is a challenging problem. If the domain is decomposed into tetrahedra, current methods tend to create “flipped” elements, making the mapping locally non-injective. While most mapping methods generally take a global approach by trying to minimize a particular energy, some others focus on local operations, i.e. changing the mesh’s topology.

Such a method called “Progressive Embeddings” focuses on two local operations, namely ”edge collapsing” and ”vertex splitting” to solve this issue on surfaces. By successively collapsing edges, one can reduce a surface mesh to its boundary and a single interior vertex. This interior vertex can then be split in successions, carefully placing the new vertex in a way that does not create flipped triangles. At the end of this second step, the mesh presents the same topology as the original surface but without any flipped triangles, making it an injective mapping.

However, this method cannot directly be applied to volumetric domains because collapsing edges can create blocking situations where collapsing additional edges would change the topology of the mesh. Additionally, the “vertex splitting” operation, the basis for the inverse process of “uncollapsing” the mesh reduced to a single interior vertex, cannot be guaranteed to be valid in the original domain. Indeed, we have identified cases where splitting vertices is guaranteed to be impossible, thus making this approach a dead-end.

Considering those limitations, we take a purely geometrical approach where “edge collapsing” is replaced by “edge shrinking”. This new operation moves one of the edge’s tips to the same location as the other one, thus shrinking the tetrahedra surrounding the edge. Not modifying the topology, this operation can be used freely for all interior edges, resulting in a mesh where all interior vertices are clustered together inside the mesh’s boundary. Vertices are then iteratively “pulled apart” or “expanded” from the cluster, gradually making tetrahedra have positive volume.

The main difference between our approach and the original “Progressive Embedding” method is that we do not modify the mesh’s topology in the shrinking sequence, but only during the “expansion” sequence by splitting edges. Since splitting edges is always allowed geometrically and topologically, we no longer have to worry about the validity of our mapping in the original domain. We currently have two main challenges to guarantee the success of our method. First, to establish whether or not we can alway guarantee to be able to expand cluster of vertices by merging their expansion cones. Secondly, to find a method that guarantees to be able to modify a non-star-shaped expansion cone to make it star-shaped and thus to be able to find a new valid position for the vertex or cluster.

**Research staff:** Valentin Nigolian, David Bommes

**Financial support:** European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program, project AlgoHex, No. 853343

## Flow-based T-Mesh Quantisation

In the generation of Quadrilateral surface meshes as well as quad layouts, a state-of-the-art algorithmic pipeline consists of the computation of frame fields that define desired local quad orientations, which is used to create a seamless parameterization. In this seamless parameterization, a motorcycle graph created by tracing along isolines defines a surface decomposition into non-conforming quadrilaterals, which we call a T-mesh. To obtain a conforming quadrilateral mesh or a quad layout, the edge lengths of all arcs of the T-mesh must be assigned non-negative integer lengths that are as close as possible to the original (real-valued) lengths in the parameterization, but also fulfill certain compatibility conditions, which yields a non-trivial global problem. This process is known as quantisation. Given a valid quantisation, each patch can be reparameterized and subdivided to obtain a pure-quadrilateral mesh, or (after optional geometric optimization) used as a quad layout.

In prior work, this crucial task is usually performed using greedy approaches or by solving an integer linear program. The former approach has no known guarantees on optimality, while the latter approach can be solved to optimality, but has exponential worst-case runtime complexity.

In our project, we aim to solve the quantisation problem using generalizations of minimum cost flow problems, which can be understood as special cases of integer linear programs. We investigate several flow-based formulations of the problem, including a generalization of the quantisation problem that relaxes hard constraints in the main solver step and fixes the allowed limited constraint violations in a post-processing step. We can approximately (with guarantees on approximation quality) solve our generalized flow problems with simple algorithms in polynomial time, and perhaps more important from a practical standpoint, negligible runtime compared to other steps of the overall pipeline.

Currently we are focused on quadrilateral surface meshes, however, hexahedral volume meshing can also be implemented using a similar pipeline, so we expect our results to be useful in future volume meshing pipelines.

**Research staff:** Martin Heistermann, David Bommes

**Financial support:** European Research Council (ERC) under the European Union's Horizon 2020 research and innovation program, project AlgoHex, No. 853343

## Quad Mesh Generation for Computer Graphics and Simulation

Quad meshes are discrete surface representations. Consider for example the surface of the earth tessellated by parallel and meridian lines. If we sample the coordinates in space of the points of intersection of parallel and meridian lines and replace the arcs that joined them by straight line segments, we obtain a discrete quad mesh of the earth's surface. Except for the poles, all vertices of this quad mesh are regular, they are adjacent to four quadrilateral faces. Singular vertices are those with more or less than four adjacent faces. Apart from cartography of the earth, which is already a well-understood problem, many applications require similarly a coordinate system on the surface, that can be easily subdivided, and oriented to salient features or curvature lines for example, or design constraints like a budget on the number of quadrilaterals while keeping a good approximation of the original surface.

This project aims to produce algorithms that support such designer or domain-specific constraints for the generation of quad meshes, with the appropriate degree of control over the different quality criteria. State-of-the-art methods decompose the generation of quad meshes into frame field generation followed by its parametrization. In simple words two linearly independent vector fields representing the desired orientations of the quad mesh edges and its lengths at every sampling point are prescribed or computed from the constraints, then the integration of the frame field produces a parameterization, that may be similar or arbitrarily different from the frame field depending on how integrable the frame field was.

We focus on the computation of integrable frame fields that are meshable with low alignment errors. We have decided to work on the frame-field based approach because it allows the most flexible setting to consider the user's constraints. Formulating and optimizing integrability energies is

a promising approach for the quad meshing problem. In this project we target a direct optimization of integrability via an elegant formulation in a polar representation of the frame field.
Currently we have a formulation amable for solving for integrable frame fields conforming to alignment and isotropic sizing constraints. Recently we have focused on the singularity relocation aspect of the problem. We have formulated a custom greedy algorithm to relocate existing singularities. Our next steps include formulation of a heuristic to place new singularities, and that together with the relocation strategy would complete the toolkit for optimizing integrable fields with control on singularities.

**Research staff:** Nicolas Gallego-Ortiz, David Bommes

## Fast Frame Field generation in two and three dimensions using a Multi-Grid approach

In geometry processing, many algorithms require the generation of a frame field. For example in Quad Meshing a two dimensional frame field defined over the surface is used to guide the generation of elements. Similarly, for Hex Meshing, a three dimensional field is used to guide the generation of the hexahedral elements in the whole volume. For this reason, algorithms able to quickly generate high quality fields are required.
In this project we explore a new approach based on a modified MBO method to solve the Heat Equation to generate a frame field both for two and three dimensions. Our work is inspired by the previous work from D. Palmer et al. *A*lgebraic Representations for Volumetric Frame Fields. In our method we use a Multi-Grid approach based on a tree data structure. This allows us to generate high quality fields adapting the resolution depending on a condition, for example the angle between adjacent frames. To solve the Heat Equation, we use the Divergence theorem to derive an explicit integration method that allow for a very simple computational approach which is trivial to parallelize. Thereafter, the performance of our method is very competitive and the small error introduced by our approximation does not influence the final solution too much. This is because of two reasons: first, after running a few integration steps, we end up with a representation of the frame, both for two and three dimensions, that is not valid. We correct it with a projection step where we find the closest point in the allowed space. Second, the error we introduce depends on how the tree is refined, meaning how many cells have a number of neighbors on

one side that is higher than one. Because of our refinement scheme, this number is generally low so the error is already contained.
The first results in two dimension are very promising both in terms of number and placement of the singularities and in terms of timings. We are now exploring its application to the three dimensional domain, hoping to be able to provide a new very fast and accurate algorithm to generate frame fields.

**Research staff:** Simone Raimondi, David Bommes

## 5.4 Bachelor's Theses

- Corina Danja Masanti, "Flesh Simulation with Application to Character Animation", January 2021.
- Lukas Seeholzer, "Feature Detection in Triangle Meshes", March 2021.

## 5.5 Awards

- Best paper award at Symposium on Geometry Processing (SGP) 2021, Philip Trettner, David Bommes, Leif Kobbelt: *G*eodesic Distance Computation via Virtual Source Propagation.

## 5.6 Further Activities

### Invited Talks

**David Bommes**

- "Quadrilateral and Hexahedral Mesh Generation with Integer-Grid Maps". Geometry & Mesh Generation Series, Siemens Digital Industries Software, online, April 2021.

### Editorial Boards

**David Bommes**

- Computer Graphics Forum (CGF) Journal, Associate Editor

- Graphical Models (GMOD) Journal, Associate Editor
- Computers & Graphics (CAG), Associate Editor

## Conference Organization

### David Bommes

- FRAMES 2020, Conference Co-Chair, December 9, 2020, online

## Conference Program Committees

### David Bommes

- EUROGRAPHICS (EG) 2021
- Symposium on Geometry Processing (SGP) 2020 & 2021
- Geometric Modeling and Processing (GMP) 2020 & 2021
- Solid and Physical Modeling (SPM) 2020 & 2021
- Shape Modeling International (SMI) 2021
- Vision, Modeling and Visualization (VMV) 2020 & 2021

## Reviewing Activities

### David Bommes

- ACM Transactions on Graphics
- ACM SIGGRAPH
- ACM SIGGRAPH Asia conference
- Computer-Aided Design (CAD)
- Computer Aided Geometric Design (CAGD)
- Computer Graphics Forum (CGF)
- Pacific Graphics
- Replicability Stamp
- UniBE Initiator Grants
- UniBE DocMobility

### Public events

- Study Week on Fascination Informatics 2020: Nicolas Gallego Ortiz supervised two students in the development of algorithms for the optimization of papercraft layouts.

## 5.7 Publications

## Journal Publications

- Philip Trettner, David Bommes, Leif Kobbelt: Geodesic Distance Computation via Virtual Source Propagation, Computer Graphics Forum, Volume 40(5), (Presented at SGP, **best paper award**), 2021.
- David Palmer, David Bommes, Justin Solomon: Algebraic representations for volumetric frame fields, ACM Transactions on Graphics, Volume 39(2), (Presented at ACM SIGGRAPH), 2020.
- Paul Zhang, Josh Vekhter, Edward Chien, David Bommes, Etienne Vouga, Justin Solomon: Octahedral Frames for Feature-Aligned Cross Fields, ACM Transactions on Graphics, Volume 39(3), (Presented at ACM SIGGRAPH), 2020.

# 6 Computer Vision Group

## 6.1 Personnel

| | | |
|---|---|---|
| **Heads:** | Prof. Dr. P. Favaro | Tel.: +41 31 631 4451<br>email: paolo.favaro@inf.unibe.ch |
| **Office Managers:** | D. Heinzen | Tel.: +41 31 631 4914<br>email: dragana.heinzen@inf.unibe.ch |
| **Scientific Staff:** | A. Bielski | Tel.: +41 31 511 76 05<br>email: adam.bielski@inf.unibe.ch |
| | A. Lemkhenter | Tel.: +41 31 511 76 03<br>email: abdelhak.lemkhenter@inf.unibe.ch |
| | G. Meishvili | Tel.: +41 31 511 76 01<br>email: givi.meishvili@inf.unibe.ch |
| | X. Wang | Tel.: +41 31 511 76 04<br>email: xiaochen.wang@inf.unibe.ch |
| | A. Wälchli | Tel.: +41 31 511 76 03<br>email: adrian.waelchli@inf.unibe.ch |
| | L. Cerkezi | Tel.: +41 31 511 76 04<br>email: llukman.cerkezi@inf.unibe.ch |
| | A. Davtyan | Tel.: +41 31 511 76 04<br>email: aram.davtyan@inf.unibe.ch |
| | S. Sameni | Tel.: +41 31 511 76 05<br>email: sepehr.sameni@inf.unibe.ch |
| | A. E. Sari | Tel.: +41 31 511 76 04<br>email: alp.sari@inf.unibe.ch |
| | L. Fiorillo | Tel.: +41 58 666 65 71<br>email: luigi.fiorillo@students.unibe.ch<br>(external PhD student) |
| **Visitors:** | T. Watanabe | Tel.: +41 31 511 76 24<br>email: tomoki.watanabe@inf.unibe.ch |

## 6.2 Overview

Prof. Dr. P. Favaro joined the Institute of Computer Science and established the Computer Vision group in June 2012. The Computer Vision group conducts research on the broad areas of machine learning, computer vision, image processing, and imaging and sensor design by employing models, algorithms and analysis tools from optimization theory, probability theory, and applied mathematics. Our general aim is to extract high-level information from images by using digital processing. Such high-level information can be in the form of geometric or photometric quantities about objects in the scene, or semantic attributes such as their category, their function, etc. In order to achieve this aim, we use a systematic approach based on three steps: modeling, inference and experimental validation. The first step in digital processing requires modeling sensors and distortions of their measured signals such as optical aberrations (defocus and motion blur), noise, spatial loss of resolution and quantization. Moreover, a careful analysis of models allows us to design novel imaging architectures that can more efficiently and accurately capture visual data. For instance, light field cameras allow for single-snapshot digital refocusing (i.e., the ability to change the focus plane of an image after capture via digital processing) by incorporating a microlens array in conventional cameras. Models also allow us to infer their parameters or a distribution of their parameters by assuming some stochastic description of the data. Parameter estimation can then be performed via optimization techniques, which require a careful selection of suitable algorithms and understanding of their behavior. Finally, both sensor and data models are validated experimentally by using synthetic and real data. Currently, our efforts in imaging have been devoted to problems in: inverse imaging (deblurring, blind deconvolution, super resolution), 3D estimation (multi view stereo, photometric stereo, coded aperture photography), motion estimation (structure from motion, tracking). We are also working extensively in unsupervised learning with the purpose of building useful feature representations of images. In our approaches a good representation is one that makes future learning easier. Currently, we use neural networks to solve tasks and because of their compositional architecture, a feature is naturally identified as one of many possible intermediate outputs of the trained model. The questions we focus on are then: How do we build a feature that can be used as input to a weak classifier or regressor for different unknown tasks? How do we use the least amount of annotation to build general purpose features?

## 6.3 Research Projects

### Blind 3D Face Deblurring

The aim of this project is to restore images depicting blurred faces. Parents like to capture pictures of important events of their little ones: a birthday party, the first day at school, the first time on a bicycle and so on. However, these ever so special memories are often completely spoiled by motion blur. Typically, the details that matter the most to parents, such as the face, are completely blurred. This blurriness is not caused by the shaky hands of the photographer, but by the subjects, with whom cooperation cannot always be established.

The main difficulty with removing blur from an articulated or deforming body is that blur is typically non-smooth, space-varying and characterized by occlusions. Consider for example the picture of a rotating head. The area around the nose will be the combination of a partial occlusion and disocclusion process. Another issue is that the blurry input image provides limited and low-quality data to make decisions about the 3D geometry of an object, its 3D motion trajectory, and its texture. Thus, the challenge is that the process is highly nonlinear, one needs to determine its model with high precision, and there is only limited and ambiguous information (the blurry input image) to make such decisions.

We study this category of blind deconvolution problems with a model-based approach by exploiting user interaction and efficient search in parameter space. We envision a system where the user can help select and align (to different degrees) a 3D model on top of the blurry image. Given the 3D model, we then design an efficient algorithm to find the motion parameters of the model and to recover its texture. To cope with the data limitations and to break down the parameter search complexity, we consider building and using datasets of sharp images of faces.

**Research staff:** Givi Meishvili, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 165845

## Face Super-Resolution

We developed a novel method to perform extreme (16x) face super-resolution by exploiting audio. Super-resolution is the task of recovering a high-resolution image from a low-resolution one. When the resolution of the input image is too low (e.g., 8x8 pixels), the loss of information is so dire that the details of the original identity have been lost. However, when the low-resolution image is extracted from a video, the audio track is also available. Because the audio carries information about the face identity, we propose to exploit it in the face reconstruction process. Towards this goal, we propose a model and a training procedure to extract information about the identity of a person from her audio track and to combine it with the information extracted from the low-resolution input image, which relates more to pose and colors of the face. We demonstrate that the combination of these two inputs yields high-resolution images that better capture the correct identity of the face. In particular, we show that audio can assist in recovering attributes such as the gender and the identity, and thus improve the correctness of the image reconstruction process. Our procedure does not make use of human annotation and thus can be easily trained with existing video datasets. Moreover, we show that our model allows one to mix low-resolution images and audio from different videos and to generate realistic faces with semantically meaningful combinations.

**Research staff:** Givi Meishvili, Simon Jenni, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 165845

## Unsupervised Learning of Image Representations

Recent developments in deep learning have demonstrated impressive capabilities in learning useful features from images, which could then be transferred to several other tasks. These systems rely on large annotated datasets, which require expensive and time-consuming human labor. To address these issues self-supervised learning methods have been proposed. These methods learn features from images without annotated data by introducing a pretext task. The design of these pretext tasks appears to be mostly based on intuition and trial and error. The recognition of image transformations has emerged as one successful principle for SSL tasks in the literature (e.g., classifying image rotations, recognizing artifacts, or classifying arrangements of patches). We studied why such pretext tasks learn good features. We observe that common to these tasks is that recognizing the image transformation is not possible by only observing local image patches (i.e., local image statistics), but rather requires modeling global image statistics, e.g., the shape of objects. Indeed, we find experimentally that such tasks do not perform well on datasets where the tasks can be solved based on local statistics alone (e.g., recognizing image rotations on images of faces). Following this insight, we design a novel learning-based image transformation called Limited Context Inpainting (LCI). In LCI a random image patch is extracted, inpainted based on only a thin border of context pixels, and pasted back in the image. The result is an image with natural local statistics but unnatural global statistics. Our experiments show that recognizing LCI, image warpings, and image rotations combined leads to state-of-the-art unsupervised feature performance.

**Research staff:** Simon Jenni, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 169622

## Self-Supervised Video Representation Learning

Supervised representation learning on video data via action recognition has a tendency to focus on appearance rather than motion features. This is due to the fact that action categories can often be recognized based on a singe video frame. To build features that accurately represent motion features we design self-supervised learning tasks by recognizing transformations of the temporal domain. To build temporal transformations we consider not only alterations of the natural frame order, but also alterations of the playback speed. We thus train a 3D-CNN to recognize if videos are played at different speeds, exhibit random re-orderings, show periodic motions, or have a warped temporal evolution, i.e., a temporally varying playback speed. Networks pre-trained using this SSL task achieve state-of-the-art performance on action recognition benchmarks. We also demonstrate that these representations perform better on time-related tasks such as video synchronization or recognizing the order of two non-overlapping video sequences.

**Research staff:** Simon Jenni, Givi Meishvili, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 169622

## Self-Supervised Feature Learning for 3D Human Pose Estimation

Annotations for 3D human pose estimation require calibrated multi-view setups with specialized motion capture sensors and are thus expensive to obtain. We explore the use of self-supervised learning to reduce the amount of necessary 3D annotations. To this end, we exploit multi-view synchronized video data of a shared scene of a person performing different actions. As a self-supervised learning task, we pose the task of recognizing whether two different views are synchronized or not and whether they underwent the same horizontal flipping or not. To solve this task a network has to recognize non-rigid deformations in the human pose (assuming movement between un-synchronized frames). This in turn should require accurate modeling of the underlying 3D pose. We find that the learned features outperform prior SSL methods by a large margin when transferred to monocular 3D pose estimation with small amounts of labeled data.

**Research staff:** Simon Jenni, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 169622

## Self-supervised Learning of Optical Flow

Optical Flow, the problem of recovering a vector field that describes the motion in every pixel from one image to the next, as for example in a video, is one of the oldest problems in Computer Vision. Applications of Optical Flow can be found in almost any system that deals with motion, e.g., in video compression, video frame interpolation (high frame rate), motion segmentation, 3D reconstruction and more. To this date researchers are trying to develop methods that estimate Optical Flow faster, with greater accuracy or with more robustness to ambiguities. One major challenge that the prior work tries to address is the estimation of Optical Flow in regions with ambiguity, e.g., regions that are being occluded, disoccluded or have less to no texture. We believe that with a data-driven approach we can overcome the limitations of prior works and learn to handle the aforementioned challenges. Since Optical Flow does not naturally emerge as annotation from real datasets, and synthetically generated videos/flows limit the generalization to real data, we must strive towards an unsupervised approach, i.e., we do not rely on labelled data. In this project, we investigate several possible generalizations of Optical Flow that naturally handle occlusions and have subpixel accuracy. The approach is self-supervised, hence the only training data are frames from high frame rate video recordings and no other annotation is needed.

**Research staff:** Adrian Wälchli, Paolo Favaro

**Financial support:** CVG

## Generative Adversarial Learning via Kernel Density Discrimination

We introduce Kernel Density Discrimination GAN (KDD GAN), a novel method for generative adversarial learning. KDD GAN formulates the training as a likelihood ratio optimization problem where the data distributions are written explicitly via (local) Kernel Density Estimates (KDE). This is inspired by the recent progress in contrastive learning and its relation to KDE. We define the KDEs directly in feature space and forgo the requirement of invertibility of the kernel feature mappings. In our approach, features are no longer optimized for linear separability, as in the original GAN formulation, but for the more general discrimination of distributions in the feature space. We analyze the gradient of our loss with respect to the feature representation and show that it is better behaved than that of the original hinge loss. We perform experiments with the proposed KDE-based loss, used either as a training loss or a regularization term, on both CIFAR10 and scaled versions of ImageNet. We use BigGAN/SA-GAN as a backbone and baseline, since our focus is not to design the architecture of the networks. We show a boost in the quality of generated samples with respect to FID from 10% to 40% compared to the baseline.

**Research staff:** Abdelhak Lemkhenter, Paolo Favaro

**Financial support:** Computational Platform Project No. 38-817. This research is supported by the Interfaculty Research Cooperation “Decoding Sleep from Neurons to Health & Mind” of the University of Bern.

## Unsupervised Learning of Object Segmentation From Perturbed Generative Models

We introduce an approach to learn object segmentation from a large collection of images without any manual annotation. The key idea is to build a synthetic training set for segmentation (i.e., where each sample consists of an input image and the corresponding segmentation mask) through a generative model. This dataset is then used to train a segmentation network in a supervised fashion. To obtain the synthetic samples for the dataset, we train a generative model such that it learns to output triplets consisting of a foreground image and mask and a background image. Each triplet is mapped to a so-called composite image through the convex combination of the foreground and background by using the foreground mask. To achieve realism, the generative model is trained in an adversarial fashion against a discriminator. During the adversarial training, we perturb the output of the generative model by introducing a random shift of the foreground relative to the background, which results in valid data augmentations for the composite images. We demonstrate on several datasets that models trained on the generated data are able to generalize well on real images

**Research staff:** Adam Bielski, Paolo Favaro

**Financial support:** CVG

## Sleep Physician Assistant System (SPAS)

The ultimate goal of the project is to develop a platform to empower the sleep physicians and to simplify effectively their work. SPAS will act like a young apprentice, taking care of tedious job and learning continuously from the expert physician. A new personalized approach for the polysomnography (PSG) scoring and a data miner for whole data exploitation will ease the scoring procedure and will improve general diagnosis and treatment. Existing automated and semi-automated scoring software cannot provide personalized scores in the same way as the expert physician's judgement. Sleep scoring is the procedure of classifying PSG recordings (EEG, EOG and EMG). The whole night recording is divided into 30-s windows and the physician has to classify each epoch into one of the five sleep stages: awake W, stage N1, stage N2, stage and stage REM. Since 1960 several techniques have been employed to solve this task automatically. However, up to now, no system has proven to be a valid substitute for the sleep physician. The goal is to improve and optimize the recent deep learning-based scoring systems. SPAS aims to develop an automatic sleep scoring algorithm able to interactively query the sleep physician and to learn from his knowledge. In order to release an optimized interactive system, we focused on three closely related challenges: clustering sleep recordings – the deep learning architectures need to be trained on subgroups of PSG recordings; confidence estimation methods for sleep scoring neural networks – the system gives in output the final sleep scores along with the degree of confidence; query the physician and update the network – detect the uncertain forecast, the sleep physician corrects the uncertain (not-confident) answers of the network and the network will be updated (fine-tuning) by using this external knowledge. Considering the architecture for an application in real-time, we are developing a scoring network that needs to process only temporal information related to the one preceding and the one succeeding epoch. A reduced memory requirement (less parameters to be trained) and low-latency characteristic may be advantageous in a real-time implementation.

**Research staff:** Luigi Fiorillo, Paolo Favaro

## Unsupervised Disentanglement of Factors of Variation

The aim of the project is to develop better-disentangled representations for image data in an unsupervised fashion. We aim to build a better representation for a generative model so that it would achieve more interpretable representation with high image quality. In fact, a disentangled representation provides us to the ability to easily manipulate the properties of the generated images such as texture, object locations, etc. We also aim to explore a set of inductive biases to help disentangled representations for generative models which may guide the training. This is crucial since the inductive bias grants the necessary guidance in an unsupervised setting.

**Research staff:** Alp Eren Sari, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 188690

## Unsupervised 3D Shape Learning

In this project, we aim to learn a generative model that learns different 3D models of an object category from a collection of random images without any supervision. The typical choice for the 3D representation includes meshes, voxels, and point clouds. In this project, we chose meshes as a representation as they are efficient and flexible in terms of vertex transformations. Once the 3D model is generated by a neural network, the final image is obtained via a differentiable renderer. The generated images should capture the underlying distribution of the dataset and the corresponding 3D models should be multiview consistent. Generating valid 3D shapes could lead us manipulating 3D objects easily thus providing rich variability in terms of affine transformations. Although there are several works in this direction, almost all of them rely on some kind of supervision signal such as known foreground mask, known camera parameters, etc. We aim to use only raw images as training data and handle all other aspects via 3D consistency properties.

**Research staff:** Llukman Cerkezi, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 188690

## Unsupervised Learning of Object Interactions

In this project we are given a dataset of videos capturing an agent/agents interacting with the environment. From this data we aim to learn a transition model, that would predict the next frame of the video given the current frame. There are plenty of works on video generation in the literature. However, in our project the main focus is made on capturing object interactions occurring in the scene. For this purpose we condition the transition model on a set of abstract action codes assigned to each of the agents in the scene. All the components of the model, including the transition model itself as well as the scene decomposition and the action space, are learnt in an unsupervised way. On the contrast to the other works in this field, that train on simple synthetic data, we consider the multi agent complex data setup, aiming to generalize to real videos.

**Research staff:** Aram Davtyan, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 188690

## Unsupervised 3D Scene Learning via Implicit Neural Representation

The aim of this project is to learn a generative model for 3D scenes using implicit neural representation. Recently, implicit neural representation based methods have shown great success in many applications. In this approach, a signal is parametrized as a continuous function that maps the domain of the signal to some quantity of interest e.g. mapping a pixel coordinate to an RGB value. We believe that we can build a generative model for 3D scenes based on the implicit neural representation that is computationally lightweight and being able to generate multiview consistent complex scenes. We also aim to make a generative model being able to disentangle between different aspects of the scene i.e. background, foreground, shape, and texture.

**Research staff:** Llukman Cerkezi, Sepehr Sameni, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 188690

### Improving Self-Supervised Contrastive Representation Learning Using Generative Models

The aim of this project is to implicitly distill the representation learned with generative models into a self-supervised contrastive learner. Each model with its own architecture and objective function learns different aspects of the data, by combining contrastive learning and generative models we hope to bring some of the benefits of generative models into contrastive learners. We are using a pretrained BigBiGAN to synthesis nontrivial positive pairs in contrastive learning because the generated samples are just semantically related to the real image but not necessarily close in the RGB space, which encourages the model to learn more robust semantic features.

**Research staff:** Sepehr Sameni, Paolo Favaro

**Financial support:** Swiss National Science Foundation Project No. 188690

## 6.4 Ph.D. Theses

- Simon Jenni, “Learning Generalizable Visual Patterns Without Human Supervision”, June 2021.

## 6.5 Master's Theses

- Anthony Gillioz, “Adversarial Data-Augmentation”, August 2020.

- Benjamin Fankhauser, “Hyperparameter optimization for gradient descent with momentum An introduction to hyper gradients in deep neural networks Master Thesis”, August 2020.

- Zhao Xueqi, “Multi-scale Momentum Contrast for Self-supervised Image Classification”, December 2020.

- Ramona Beck, “A Study on the Inversion of Generative Adversarial Networks”, March 2021.

- Jonathan Peclat, “Localization of an Autonomous Vehicle Using Visual-Inertial SLAM and GNSS”, March 2021.

- Maurice Rupp, “PolitBERT - Deepfake Detection of American Politicians using Natural Language Processing”, April 2021.

- Stefan Jonas, “CNN Spike Detector Detection of Spikes in Intracranial EEG using Convolutional Neural Networks”, April 2021.

## 6.6 Bachelor's Theses

- Adrian Walter Schmucker, “Learning to generate topographic maps from satellite images with conditional generative adversarial networks”, July 2020.

- Eric Lagger, “Examination of Unsupervised Representation Learning by Predicting Image Rotations”, September 2020.

## 6.7 Memberships

**Paolo Favaro**

- Member of IEEE

- Member of ELLIS

## 6.8 Further Activities

### Evaluation Committes

#### Paolo Favaro

- SNF Ambizione Committee 2021
- University of Saarland 2021
- Finland Center of Excellence 2021
- Technion, IIT, Israel 2020

### Invited Talks

#### Paolo Favaro

- “Deep Lerninag, Overview and Insight”, Center for Space and Habitability/WP, UniBe, June 2021.
- “KOALA: A Kalman Optimization Algorithm with Loss Adaptivity”, University of Oxford, September 2021
- “Unsup3D: Unsupervised 3D Learning in the Wild”, ACCV 2021.
- “Perspectives on Unsupervised Representation Learning”, Workshop at ECCV 2020.

### Online Seminars Given by External Speakers

- David Ginsbourger, “Modeling and optimizing set functions via RKHS embeddings”, February 25, 2021.
- Emiel Hoogeboom, “Distributions and Geometry”, March 26, 2021
- Shuai Zhang, “Uncovering the Intrinsic Structures: Representation Learning and Its Applications”, April 30, 2021.
- Jonas Peters, “Causality and Distribution Generalization”, May 27, 2021.
- Yang Song, “Generative Modeling by Estimating Gradients of the Data Distribution”, June 24, 2021.
- Vincent Sitzmann, “Light Field Networks”, July 22, 2021.

## Conference Program Committees

### Paolo Favaro

- CVPR 2021
- BMVC 2021
- BMVC 2020
- GCPR 2020

## Journal Committees

### Paolo Favaro

- Associate Editor for IEEE Transactions on Pattern Analysis and Machine Intelligence

### Abdelhak Lemkhenter

- ICCV 2021

### Sepehr Sameni

- ICCV 2021

# Refereed Conference Proceedings

- S. Jenni and P. Favaro, “Self-Supervised Multi-View Synchronization Learning for 3D Pose Estimation”, Asian Conference on Computer Vision (ACCV), 2020.
- J. P. Vizcaino, Z. Wang, P. Symvoulidis, P. Favaro, B. Guner-Ataman, E. S. Boyden, and T. Lasse, “Real-Time Light Field 3D Microscopy via Sparsity-Driven Learned Deconvolution”, International Conference on Computational Photography (ICCP), 2021.
- T. Watanabe and P. Favaro, “A Unified Generative Adversarial Network Training via Self-Labeling and Self-Attention”, International Conference on Machine Learning (ICML), 2021.

- J. P. Vizcaíno, F. Saltarin, Y. Belyaev, R. Lyck, T. Lasser, and P. Favaro, “Learning to Reconstruct Confocal Microscopy Stacks from Single Light Field Images”, IEEE Transactions on Computational Imaging, 2021.
- A. Tejankar, S. A. Koohpayegani, V. Pillai, P. Favaro, H. Pirsiavash, “ISD: Self-Supervised Learning by Iterative Similarity Distillation”, in International Conference on Computer Vision (ICCV), 2021.

## Technical Reports

- A. Wälchli and P. Favaro, “Optical Flow Dataset Synthesis from Unpaired Images”, arXiv:2104.02615, Technical Report 2020.
- A. Davtyan, S. Sameni, L. Cerkezi, G. Mieshvilli, A. Bielski, “KOALA: A Kalman Optimization Algorithm with Loss Adaptivity”, under review, 2021.
- A. Lemkhenter, A. Bielski, A. E. Sari, P. Favaro, “Generative Adversarial Learning via Kernel Density Discrimination”, under review. 2021.
- A. Bielski, P. Favaro, “Unsupervised Learning of Object Segmentation From Perturbed Generative Models”, under review. 2021.
- Z. Zhang, P. Favaro, J. Li and Y. Tian, “Single Image Super-Resolution by Learning to Zoom in”, Technical Report.
- L. Fiorillo, P. Favaro, F. D. Faraci, “DeepSleepNet-Lite: A Simplified Automatic Sleep Stage Scoring Model with Uncertainty Estimates”, arXiv:2108.10600, Technical Report 2021.
- R. Fantinel, A. Cenedese, P. Favaro, “Learning to Detect Faults by Generating Them”, Technical Report.

# 7 Cryptology and Data Security Group

## 7.1 Personnel

| | |
|---|---|
| **Head:** | Prof. Dr. Christian Cachin<br>Tel.: +41 31 684 8560<br>email: cachin@inf.unibe.ch |
| **Office Manager:** | Bettina Choffat<br>Tel.: +41 31 684 8426<br>email: bettina.choffat@inf.unibe.ch |
| **Scientific Staff:** | Orestis Alpos<br>email: orestis.alpos@inf.unibe.ch |
| | Ignacio Amores Sesar<br>email: ignacio.amores@inf.unibe.ch |
| | Nathalie Steinhauer<br>email: nathalie.steinhauer@inf.unibe.ch<br>(From April 2021) |
| | Jovana Mićić<br>email: jovana.micic@inf.unibe.ch |
| | Dr. Giorgia Marson<br>email: giorgia.marson@inf.unibe.ch<br>(Until April 2021) |
| | Anna Parker<br>email: anna.parker@inf.unibe.ch<br>(Until August 2020) |
| | Alex Pellegrini<br>email: alex.pellegrini@inf.unibe.ch<br>(Until September 2020) |
| | Noah Schmid<br>email: noah.schmid@inf.unibe.ch<br>(From July 2021) |
| | Luca Zanolini<br>email: luca.zanolini@inf.unibe.ch |

## 7.2 Overview

The Cryptology and Data Security Group broadly investigates security and privacy in a digital world. Concrete topics include cryptographic protocols, distributed consistency, consensus, and cloud-computing security, with applications to blockchains, distributed ledger technology, cryptocurrencies, and their economics.

Security and privacy are at stake in the information society, threatened by the enormous developments in networks, cloud, and mobile. Information technology has already revolutionized many aspects today's life. Finding a balance between the practical convenience of being ”always online”, current business practices, the changing demands of society, and the privacy and security concerns of individual people represents one of the great open questions of our time. Cryptography and data security provide techniques to answer this question.

## 7.3 Research Projects

### Advanced Consensus Protocols

Protocols for reaching agreement among the nodes in a distributed network have received renewed interest in recent years due to their relevance for blockchain systems. In principle, every transaction executed on a blockchain requires a consensus decision from the participating nodes. Platforms like Bitcoin, Ethereum, Ripple, and many others have relaxed key assumptions made in earlier models and operate agreement protocols over the Internet today.

Although research on distributed consensus has been a central and well-investigated problem in distributed computing, the resurging interest from practice has brought up new questions. At the same time, many blockchain consensus algorithms operating today lack formal analysis. Our research addresses *advanced consensus protocols* on a fundamental level and aims at extending the understanding of protocols for distributing trust.

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

## Security Analysis of Ripple Consensus

The Ripple network is one of the most prominent blockchain platforms and its native XRP token currently has one of the highest cryptocurrency market capitalizations. The Ripple consensus protocol powers this network and is generally considered to a Byzantine fault-tolerant agreement protocol, which can reach consensus in the presence of faulty or malicious nodes. In contrast to traditional Byzantine agreement protocols, there is no global knowledge of all participating nodes in Ripple consensus; instead, each node declares a list of other nodes that it trusts and from which it considers votes.

Previous work has brought up concerns about the liveness and safety of the consensus protocol under the general assumptions stated initially by Ripple, and there is currently no appropriate understanding of its workings and its properties in the literature. This project closes this gap and makes two contributions. It first provides a detailed, abstract description of the protocol, which has been derived from the source code. Second, the work points out that the abstract protocol may violate safety and liveness in several simple executions under relatively benign network assumptions

**Research staff:** Ignacio Amores-Sesar, Christian Cachin, Jovana Mićić

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

## Generalized Byzantine Quorums Made Practical

Existing Byzantine fault-tolerant (BFT) consensus protocols address only *threshold failures*, where the participating nodes fail independently of each other, each one fails equally likely, and the protocol's guarantees follow from a simple bound on the *number* of faulty nodes. With the widespread deployment of Byzantine consensus in blockchains and distributed ledgers today, however, more sophisticated trust assumptions are needed.

This work has developed the first implementation of BFT consensus with generalized quorums. It starts from a number of generalized trust structures motivated by practice and explores methods to specify and implement them efficiently. In particular, it expresses the trust assumption by a monotone Boolean formula (MBF) with threshold operators and by a monotone span program (MSP), a linear-algebraic model for computation. An implementation of HotStuff BFT consensus using these quorum systems has been developed and was compared to the existing threshold model. Benchmarks with HotStuff running on up to 40 replicas demonstrate that the MBF specification incurs no significant slowdown, whereas the MSP expression affects latency and throughput noticeably due to the involved computations.

**Research staff:** Orestis Alpos, Christian Cachin

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

## Consensus with Asymmetric Quorums

*Byzantine quorum systems* provide a widely used abstraction for realizing consensus in a distributed system prone to Byzantine faults, in which every process has the same failure assumption. Motivated by the requirements of more flexible trust models in the context of blockchain consensus, Cachin and Tackmann (OPODIS 2019) introduced *asymmetric quorum systems* as a generalization of Byzantine quorum systems, where every process is free to choose which other processes to trust and which not; this results in a subjective, *asymmetric* trust assumption. Consensus is arguably one of the most important notions in distributed computing and also relevant for practical systems.
This work shows how to realize consensus protocols with asymmetric trust. A first protocol works in partially synchronous systems; it generalizes the consensus algorithm underlying PBFT and uses digital signatures. A second protocol is asynchronous, uses no cryptographic signatures, and achieves optimal resilience. Randomization is provided through a common coin primitive with asymmetric trust.

**Research staff:** Christian Cachin, Luca Zanolini

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

## The Synchronization Power of Token Smart Contracts

Modern blockchains support a variety of distributed applications beyond cryptocurrencies, including *smart contracts*, which let users execute arbitrary co de in a distributed and decentralized fashion. Regardless of their intended application, blockchain platforms implicitly assume consensus for the correct execution of a smart contract, thus requiring that al l transactions are totally ordered. It was only recently recognized that consensus is not necessary to prevent doubl e-spending in a cryptocurrency, contrary to common belief. This result suggests that current implementations may be sacrificing efficiency and scalability because they synchronize transactions much more tightly than act ually needed.

In this work we study the synchronization requirements of Ethereum's ERC20 token contract, one of the most widely adopted smart contacts. Namely, we model a smart-contract token as a concurrent object and analyze its consensus number as a measure of synchronization power. We show that the richer set of methods supported by ERC20 tokens, compared to standard cryptocurrencies, results in strictly stronger synchronization requirements. More surprisingly, the synchronization power of ERC20 tokens depends on the object's state and can thus be modified by method invocations. To prove this result, we develop a dedicated framework to express how the object's state affects the needed synchronization level.

Our findings indicate that ERC20 tokens, as well as other token standards, are more powerful and versatile than plain cryptocurrencies, and are subject to *dynamic* requirements. Developing specific synchronization protocols that exploit these dynamic requirements will pave the way towards more robust and scalable blockchain platforms.

**Research staff:** Orestis Alpos, Christian Cachin, Giorgia Azzurra Marson, Luca Zanolini

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

## Generalizing Blockchain Consensus

Despite the tremendous interest in cryptocurrencies like Bitcoin and Ethereum today, many aspects of the underlying consensus protocols are poorly understood. Therefore, the search for protocols that improve either throughput or security (or both) continues. Bitcoin always selects the longest chain (i.e., the one with most work). Forks may occur when two miners extend the same block simultaneously, and the frequency of forks depends on how fast blocks are propagated in the network. In the GHOST protocol, used by Ethereum, all blocks involved in the fork contribute to the security. However, the greedy chain selection rule of GHOST does not

consider the full information available in the block tree, which has led to some concerns about its security.
This work introduces a new family of protocols, called Medium, which takes the structure of the whole block tree into account, by weighting blocks differently according to their depths. Bitcoin and GHOST result as special cases. This protocol leads to new insights about the security of Bitcoin and GHOST and paves the way for developing network- and application-specific protocols, in which the influence of forks on the chain-selection process can be controlled. It is shown that almost all protocols in this family achieve strictly greater throughput than Bitcoin (at the same security level) and resist attacks that can be mounted against GHOST.

**Research staff:** Ignacio Amores-Sesar, Christian Cachin, Anna Parker

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

## Composition of Byzantine Quorum Systems

Trust is the basis of any distributed, fault-tolerant, or secure system. A *trust assumption* specifies the failures that a system, such as a blockchain network, can tolerate and determines the conditions under which it operates correctly. In systems subject to Byzantine faults, the trust assumption is usually specified through sets of processes that may fail together. Trust has traditionally been *symmetric*, such that all processes in the system adhere to the same, global assumption about potential faults. Recently, *asymmetric* trust models have also been considered, especially in the context of blockchains, where every participant is free to choose who to trust. In both cases, it has been an open question how to compose trust assumptions. Consider two or more systems, run by different and possibly disjoint sets of participants, with different assumptions about faults: how can they work together? This work has answered this question for the first time and offered composition rules for symmetric and for asymmetric quorum systems. These rules are static and do not require interaction or agreement on the new trust assumption among the participants. Moreover, they ensure that if the original systems allow for running a particular protocol (guaranteeing consistency and availability), then so will the joint system. At the same time, the composed system tolerates as many faults as possible, subject to the underlying consistency and availability properties.

Reaching consensus with asymmetric trust in the model of personal Byzantine quorum systems (Losa *et al.*, DISC 2019) was shown to be impossible, if the trust assumptions of the processes diverge from each other. With asymmetric quorum systems, and by applying our composition rule, we show how consensus is actually possible, even with the combination of disjoint sets of processes.

**Research staff:** Orestis Alpos, Christian Cachin, Luca Zanolini

**Financial support:** Swiss National Science Foundation (SNSF), grant agreement Nr. 200021_188443.

### Distributed Cryptography

The design of threshold cryptosystems and proactively secure protocols has received renewed attention in recent years thanks to the rise of cloud services, blockchain, and cryptocurrency technologies. The current focus is on solutions that work in real-world environments, in particular over realistic *asynchronous* networks. However, many of the works in the area of threshold cryptography assume synchronous networks with broadcast, thereby enabling solutions that can withstand up to half of the parties being corrupted. This is in contrast to the asynchronous setting, where one can only tolerate up to a third of the parties being corrupted. Our goal in this work is to develop protocols that work in a realistic asynchronous setting while at the same time enjoy some of the better resilience properties of synchronous schemes with broadcast.

**Research staff:** Christian Cachin, Noah Schmid, Nathalie Steinhauer

**Financial support:** Interchain Foundation, 6340 Baar, Switzerland.

## 7.4 Master's Theses

- Arbër Kuçi, “Provably Robust Proof-of-Stake Protocols”, March 2021.
- Aleksandar Lazic, “The Library of Distributed Protocols”, Jaunary 2021.

## 7.5 Bachelor's Theses

- Jérémie De Faveri, “Implementation of an Asset Transfer System based on Parallel Blockchain Instances”, August 2021.
- Lukas Schacher, “Encrypting into the Future”, August 2021.
- Marius Asadauskas, “PoET: An Eco-Friendly Alternative to PoW”, July 2021.
- Noah Schmid, “Secure Causal Atomic Broadcast”, July 2021.
- Michael Senn, “Implementing RSA Signatures on the Internet Computer”, May 2021.
- Michael Brunner, “Analysis of the Tangle”, January 2021.
- Luca Althaus, “Blockchain and BlockDAG Protocols”, December 2020.
- Annina Helmy, “Using Polynomial Systems to Decode Binary Linear Codes”, September 2020.

## 7.6 Further Activities

### Invited Talks

**Christian Cachin**

- “The synchronization power of token smart contracts.” Facebook Novi Systems Research Seminar, Virtual, Aug. 2021.
- “Asymmetric distributed trust.” **Keynote talk**, 22nd International Conference on Distributed Computing and Networking (ICDCN), Virtual Event, Jan. 2021.
- “Trust and security in consensus protocols.” DLT Banking Virtual Conference, Sapienza University of Rome, (`https://bankingconference.eu/`, Virtual Event, Dec. 2020.

### Editorial Boards

**Christian Cachin**

- Associate editor for Distributed Computing, 2015–, Springer.

## Societies and Steering Committees

### Christian Cachin

- Member of Steering Committee for ACM Conference on Advances in Financial Technologies (AFT), 2019–.
- Member of Steering Committee for ACM Symposium on Principles of Distributed Computing (PODC), 2019–2022.

## Conference Organization

### Christian Cachin

- **Program Co-Chair** of Theory and Practice of Blockchains Workshop (TPBC), online weekly seminars, 2021.

## Conference Program Committees

### Christian Cachin

- Member of Program Committee for 43rd IEEE Symposium on Security and Privacy (IEEE S&P) 2022, San Jose, USA.
- Member of Program Committee for 3rd ACM Conference on Advances in Financial Technologies (AFT), 2021, virtual.
- Member of Program Committee for 41st IEEE International Conference on Distributed Computing Systems (ICDCS), 2021.
- **Program Co-Chair** of Theory and Practice of Blockchains Workshop (TPBC), online weekly seminars, 2021.
- Member of Program Committee for Financial Cryptography and Data Security (FC'21), 2021, virtual.

### Giorgia Marson

- Member of Program Committee for Asiacrypt 2021 Conference, Online event.
- Member of Program Committee for CFail, the Conference for Failed Approaches and Insightful Losses in Cryptology, 2021, virtual.
- Member of Program Committee for CT-RSA 2022, Cryptographers Track at RSA Conference, 2022.

## 7.7 Publications

## Conference Papers

- O. Alpos, C. Cachin, G. A. Marson, and L. Zanolini, “On the synchronization power of token smart contracts,” in *Proc. ICDCS*, IEEE, 2021 (to appear).
- C. Cachin, “Asymmetric distributed trust,” in *Proc. ICDCN*, ACM, 2021.
- I. Amores-Sesar, C. Cachin, and J. Mićić, “Security analysis of Ripple consensus,” in *Proc. 24th International Conference on Principles of Distributed Systems (OPODIS)* (Q. Bramas, R. Oshman, and P. Romano, eds.), vol. 184 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pp. 10:1–10:16, Schloss Dagstuhl–Leibniz-Zentrum für Informatik, 2021.
- C. Müller, M. Brandenburger, C. Cachin, P. Felber, C. Göttel, and V. Schiavoni, “Tz4fabric: Executing smart contracts with ARM trustzone (Practical experience report),” in *Proc. 39th Symposium on Reliable Distributed Systems (SRDS)*, pp. 21–30, Oct. 2020.
- O. Alpos and C. Cachin, “Consensus beyond thresholds: Generalized Byzantine quorums made live,” in *Proc. 39th Symposium on Reliable Distributed Systems (SRDS)*, pp. 21–30, Oct. 2020.

## Proceedings, Books and Book Chapters

## Preprints and Other Publications

- I. Amores-Sesar and C. Cachin, “Generalizing weighted trees: A bridge from Bitcoin to GHOST.” e-print, arXiv:2108.13502 [cs.DC], 2021.
- O. Alpos, C. Cachin, and L. Zanolini, “How to trust strangers: Composition of byzantine quorum systems.” e-print, arXiv:2107.11331 [cs.DC], 2021.
- O. Alpos, C. Cachin, G. A. Marson, and L. Zanolini, “On the synchronization power of token smart contracts.” e-print, arXiv:2101.05543 [cs.DC], 2021.

- C. Cachin and L. Zanolini, "From symmetric to asymmetric asynchronous Byzantine consensus." e-print, arXiv:2005.08795v2 [cs.DC], 2020.

# 8 Logic and Theory Group

## 8.1 Personnel

| | | |
|---|---|---|
| **Head:** | Prof. Dr. T. Studer | Tel.: +41 (0)31 631 39 84<br>email:<br>thomas.studer@inf.unibe.ch |
| | Prof. Dr. T. Strahm | Tel.: +41 (0)31 631 49 98<br>email:<br>thomas.strahm@inf.unibe.ch<br>(until 26.04.2021) |
| **Office Manager:** | B. Choffat | Tel.: +41 (0)31 631 84 26<br>email:<br>bettina.choffat@inf.unibe.ch |
| **Scientific Staff:** | E. Lehmann* | Tel.: +41 (0)31 511 76 09<br>email:<br>eveline.lehmann@inf.unibe.ch<br>(until 31.01.2021) |
| | M. Bärtschi* | Tel.: +41 (0)31 511 76 16<br>email:<br>michael.baertschi@inf.unibe.ch<br>(external PhD student)<br>(until 26.04.2021) |
| | A. Rohani* | Tel.: +41 (0)31 511 76 09<br>email:<br>atefeh.rohani@inf.unibe.ch |
| | M. Baur* | Tel.: +41 (0)31 511 76 32<br>email:<br>michael.baur@inf.unibe.ch |
| | L. Zenger*. | Tel.: +41 (0)31 511 76 09<br>email:<br>lukas.zenger@inf.unibe.ch<br>(since 01.03.2021) |
| **Emeriti:** | Prof. Dr. G. Jäger | email:<br>gerhard.jaeger@inf.unibe.ch |

* with financial support from a third party

## 8.2 Overview

The LTG research group (logic and theory group) focuses on theoretical computer science and mathematical logic, especially proof theory, computational logics and theory of computation. We have been dealing for many years with formal methods, analysis of deductions, general computations and, in particular, applications of mathematical logic to computer science. During the previous year the main subject areas have been the following:

**Computational Logic:** Logical formalisms are perfectly suited to the specification of complex systems, the representation of knowledge and information, the description of processes (e.g. in distributed multi-agent systems) and for providing formal proofs of important system properties such as, for example, correctness and fairness. The research group has long been interested in the deductive, procedural and dynamic aspects of the corresponding formalisms and in the design of modern deductive systems. New approaches are being developed for information update purposes. In addition, the way in which simple, logical formalisms can be extended to become genuine multi-user systems taking into account the dynamic aspects of ontologies in the data mining context and in connection with the semantic web is being investigated.

**Proof Theory:** This research topic focuses on the development and analysis of formal systems of first and second order arithmetic, set theory and of what are known as logical frameworks (type and set theoretical, explicit, constructive, extensional, intentional). Our interests range from feasible subsystems of arithmetic to highly impredicative set and type theories and deals with the interplay between constructive, recursive and operational approaches. In addition, abstract computations and computable knowledge are being investigated.

## 8.3 Research Projects

### Modalities in Substructural Logics: Theory, Methods and Applications

Modal logics are a family of formal systems based on classical logic which aim at improving the expressive power of the classical calculus allowing to reason about “modes of truth”. The aim of the present proposal is to put forward a systematic study of substructural modal logics, understood as those modal logics in which the modal operators are based upon the general ground of substructural logics, weaker deductive systems than classical logic. Our aim is also to explore the applications of substructural modal logics outside the bounds of mathematical logic and, in particular, in the areas of knowledge representation; legal reasoning; data privacy and security; logical analysis of natural language.

**Research staff:** All members of the research group

**Financial support:** Horizon 2020, MSCA-RISE

## Explicit Reasons

This project is concerned with reasons why one believes something, reasons why one knows something, and reasons why one ought to do something. We develop formal languages in which reasons can be represented explicitly and investigate the logical properties of explicit reasons. To achieve this, we rely on the framework of justification logic. In particular, we present non-normal deontic logics with justifications. Further, we develop a semiring framework for justifications, and we engineer a possible world semantics for justifications that supports additional structure like graded justifications or probability distributions on justifications. Moreover, we add justifications and belief dynamics to Artemov's new foundations for epistemic logic.

**Research staff:** M. Baur, A. Rohani, T. Studer

**Financial support:** Swiss National Science Foundation (No. 184625)

## Proof and Model Theory of Intuitionistic Temporal Logic

Intuitionistic logic enjoys a myriad of interpretations based on computation, information or topology, making it a natural framework to reason about dynamic processes in which these phenomena play a crucial role. Yet there is a large gap to be filled regarding our understanding of the computational behaviour of intuitionistic temporal logics. The aim of this project is to cement our understanding of intuitionistic temporal logics by developing their model theory based on dynamic topological systems, and their proof theory based on prominent paradigms such as Gentzen-style calculi as well as cyclic proofs.

**Research staff:** L. Zenger, T. Studer

**Financial support:** Swiss National Science Foundation (No. 196176)

## 8.4 Ph.D. Theses

- E. Lehmann: Subset semantics for justifications
- M. Bärtschi: $\mathrm{ATR}_0$ and some related theories

## 8.5 Bachelor's Theses

- J. Zuber: Proof of Gödel's Incompleteness Theorem based on Computability Theory
- D. Jaha: Partitionierung als Unterstützung für Big Data in PostgreSQL
- B. Kürekci: Einführung in den Lambda Kalkül und der Beweis des Church–Rosser Theorems

## 8.6 Further Activities

### Editorial Boards

**Gerhard Jäger**

- Member of the Editorial Board of Archive for Mathematical Logic
- Member of the Editorial Board of Logica Universalis

**Thomas Strahm**

- Member of the Consulting Board of Dialectica
- Member of the Editorial Board of Journal of Symbolic Logic

**Thomas Studer**

- Member of the Editorial Board of Springer book series on Progress in Computer Science and Applied Logic

## Invited Talks

### Thomas Studer

- A modal logic formalization of controlled query evaluation, Logic and Applications, Dubrovnik, September, 2020
- The impact of logic on science and technology, World Philosophy Day, Egypt-Japan University for Science and Technology, Alexandria, November, 2020
- On the proof theory of modal logics with fixed points, St. Petersburg Days of Logic and Computability, St. Petersburg, May 2021

### Gerhard Jäger

- Strict $\Pi^1_1$-reflection: A proof-theoretic perspective, Logical Perspectives 2021, Moscow, June 2021.
- Remembering Thomas Strahm, Higher Proof Theory after Gödel, Celebrating 90 Years of Gödel's Incompleteness Theorems, Tübingen, July 2021.

## Technical and Research Committees

### Gerhard Jäger

- Member of the Scientific Council of the European Association for Computer Science Logic

### Thomas Strahm

- Board Member of the Swiss Society for Logic and Philosophy of Science

### Thomas Studer

- Swiss Delegate to the International Federation for Information Processing Technical Committee 1 (Foundations of Computer Science)
- Swiss Delegate to the International Union of History and Philosophy of Science and Technology

- Presidium Member of the Platform Mathematics, Astronomy and Physics of the Swiss Academy of Sciences
- Board member of the Swiss Society for Logic and Philosophy of Science
- Member of the Jury for Bernays Award
- Member of the Jury for Priz Schläfli
- Member of the Committee for the Promotion of Young Talents (Kommission Nachwuchsförderung) of ScNat
- Member of the Kantonale Maturitätskommission, Hauptexperte Informatik

## Organized Events

### Thomas Studer

- Logic and Application, Inter University Centre Dubrovnik and online, 21-25 September 2020

## Project and Person Reviewing Activities

### Thomas Studer

- Tsinghua University, Beijing, China

## PhD Committee Memberships

### Thomas Studer

- *Reasoning with defeasible reasons*, Stipe Pandzic, University of Groningen
- *Cryptoanalysis upon RSA and its variants via continuous midpoint subdivision analysis and lattices*, Wan Nur Aqlili Binti Wan Mohd Ruzai, Universiti Putra Malaysia

## 8.7 Publications

- Michael Bärtschi, $\mathrm{ATR}_0$ and some related theories. Dissertation, Universität Bern, Philosophisch-naturwissenschaftliche Fakultät, 2021
- Michael Bärtschi und Gerhard Jäger, Some set-theoretic reduction principles, to appear in: T. Piecha, K. Wehmeier (eds.), Peter Schroeder-Heister on Proof-Theoretic Semantics, Outstanding Contributions to Logic.
- Kai Brünnler, Dandolo Flumini, and Thomas Studer, A Logic of Blockchain Updates, Journal of Logic and Computation, 30(8):1469-1485, 2020
- Gerhard Jäger, Stage comparison, fixed points, and least fixed points in Kripke- Platek environments, submitted.
- Gerhard Jäger, Simplified cut elimination for Kripke-Platek set theory, to appear in: F. Ferreira, R. Kahle, G. Sommaruga (eds), Axiomatic Thinking, Springer.
- Gerhard Jäger, Identity, equality, and extensionality in explicit mathematics, to appear in: D.S. Bridges, H. Ishihara, M. Rathjen, H. Schwichtenberg (eds.), Handbook of Bishop Constructive Mathematics.
- Gerhard Jäger. Short note: least fixed points versus least closed points, Archive for Mathematical Logic, 2021
- Eveline Lehmann, Subset Semantics for Justifications. Dissertation, Universität Bern, Philosophisch-naturwissenschaftliche Fakultät, 2020
- Atefeh Rohani und Thomas Studer, Explicit non-normal modal logic, to appear in: WoLLIC 2021 27th Workshop on Logic, Language, Information and Computation
- Nenad Savić, Non-classical Reasoning and Justifications. Dissertation, Universität Bern, Philosophisch-naturwissenschaftliche Fakultät, 2020
- Thomas Studer, A conflict tolerant logic of explicit evidence, Logical Investigations, 27(1):124-144, 2021

# 9 Pattern Recognition Group

## 9.1 Personnel

| | | |
|---|---|---|
| **Head:** | PD Dr. Kaspar Riesen<br>email: kaspar.riesen@inf.unibe.ch | Tel.: +41 79 688 7719 |
| **Office Manager:** | Bettina Choffat<br>email: bettina.choffat@inf.unibe.ch | Tel.: +41 31 631 8426 |
| **Scientific Staff:** | Mathias Fuchs<br>email: mathias.fuchs@inf.unibe.ch | |
| | Anthony Gillioz<br>email: anthony.gillioz@inf.unibe.ch | |

## 9.2 Overview

The Pattern Recognition Group has been established in 2020 by Kaspar Riesen at the University of Bern. We broadly investigate algorithms and complex data structures in the field of pattern recognition and data science. In particular, the group has a strong expertise in graph based representation in intelligent information processing.

Due to fast developments in both storage media and data acquisition, we observe rapidly increasing amounts of data available in diverse areas in both science and industry. Simultaneously, we observe that in many applications the underlying data is inherently complex, making graphs the most useful and adequate data structure available to date. These two developments evoke the need for ongoing research of robust and efficient methods that assist humans in understanding and handling their pools of big sets of complex data.

The group's research is devoted to the development of novel graph based algorithms for pattern recognition and data science that actually provide feasible and robust solutions for this need.

# 9.3 Research Projects

## Novel State-of-the-Art Graph Matching Algorithms

A large amount of graph based methods for pattern recognition and related fields have been proposed. One of these methods is *graph edit distance* – a powerful and flexible graph dissimilarity measure and actually one of the main subjects of this project. Regarding graph edit distance (or more generally graph matching) we observe two substantial gaps in research that we aim to research and bridge. Formally, within the present project we research…

1. … encodings of matching information in a novel data structure to formalize the stable cores of specific classes by means of graphs. The rationale of this matching-graph representation is that it can be beneficial to focus on stable/important parts of graphs during algorithmic comparisons (rather than on complete graphs).

2. … hierarchical graph representations in conjunction with linear time graph embedding. This procedure is motivated by the fact that hierarchical representations (including fast and expressive graph embeddings) can be exploited in *filter-and-verify* strategies in order to substantially speed up and improve the matching processes.

By verifying both hypotheses we plan to make significant advances in the field of structural pattern recognition and establishing novel paradigms that go beyond the current understanding. In particular, the overall objective is the development and research of novel, robust graph edit distance methods that outperform the current state-of-the-art in graph matching on existing and novel data sets stemming from different real world scenarios. Hence, the proposed project involves both research on fundamental algorithms and solving concrete problems in applications.

**Financial support:** Swiss National Science Foundation Project No. 188496

**Research staff:** M. Fuchs, A. Gillioz, K. Riesen

# 9.4 Further Activities

## Editorial Boards

**Kaspar Riesen**

- Associate editor for Pattern Recognition, 2015–, Elsevier.

### Conference Program Committees

#### Kaspar Riesen

- Member of Program Committee for 16th International Conference on Document Analysis and Recognition ICDAR 2021

### Invited Talks

#### Mathias Fuchs

- Graph Embedding in Vector Spaces Using Matching-Graphs, SISAP (Dortmund), September 2021
- Iterative Creation of Matching-Graphs – Finding Relevant Substructures in Graph Sets, CIARP (Porto), May 2021
- Matching of Matching-Graphs - A Novel Approach for Graph Classification. ICPR (Milano), January 2021

#### Kaspar Riesen

- A Novel Data Set for Information Retrieval on the Basis of Subgraph Matching. S+SSPR (Venice), January 2021

## 9.5 Publications

## Journal Publications

- Michael Stauffer, Andreas Fischer, Kaspar Riesen: Filters for graph-based keyword spotting in historical handwritten documents. Pattern Recognit. Lett. 134: 125-134 (2020)
- Kaspar Riesen, Miquel Ferrer, Horst Bunke: Approximate Graph Edit Distance in Quadratic Time. IEEE/ACM Trans. Comput. Biology Bioinform. 17(2): 483-494 (2020)

## Refereed Conferences

- Mathias Fuchs, Kaspar Riesen: Graph Embedding in Vector Spaces Using Matching-Graphs. Accepted for Publication in Similarity Search and Applications, SISAP 2021
- Mathias Fuchs, Kaspar Riesen: Iterative Creation of Matching-Graphs – Finding Relevant Substructures in Graph Sets. Accepted for Publication in 25th Iberoamerican Congress on Pattern Recognition, CIARP 2021
- Mathias Fuchs, Kaspar Riesen: Matching of Matching-Graphs - A Novel Approach for Graph Classification. ICPR 2020: 6570-6576
- Kaspar Riesen, Hans Friedrich Witschel, Loris Grether: A Novel Data Set for Information Retrieval on the Basis of Subgraph Matching. S+SSPR 2020: 205-215
- Hans Friedrich Witschel, Kaspar Riesen, Loris Grether: KvGR: A Graph-Based Interface for Explorative Sequential Question Answering on Heterogeneous Information Sources. ECIR (1) 2020: 760-773

## Proceedings, Books and Book Chapters

- Kaspar Riesen: Java in 14 Wochen: Ein Lehrbuch für Studierende der Wirtschaftsinformatik (Springer), 2020

# 10 Research Center for Digital Sustainability Group

## 10.1 Personnel

| | | |
|---|---|---|
| **Head:** | PD Dr. M. Stürmer* | Tel.: +41 31 684 3809<br>email: matthias.stuermer@inf.unibe.ch |
| **Office Manager:** | N. Brugger* | Tel.: +41 31 684 4771<br>email: nathalie.brugger@inf.unibe.ch |
| **Scientific Staff:** | J. Niklaus* | email: joel.niklaus@inf.unibe.ch |
| | T. Welz* | Tel.: +41 31 511 7620<br>email: tobias.welz@inf.unibe.ch |
| **Developers:** | P. Brunner* | email: patrick.brunner@inf.unibe.ch |
| | S. Brunner* | email: sabine.brunner@inf.unibe.ch<br>(until December 2020) |
| | M. Buchholz* | email: marco.buchholz@inf.unibe.ch |
| | Y. Dällenbach* | email: yannik.daellenbach@inf.unibe.ch |
| | R. Gruber* | email: roman.gruber@inf.unibe.ch |
| | S. Kafader* | email: simon.kafader@inf.unibe.ch<br>(until Mai 2021) |
| | O. Meier* | email: oscar.meier@inf.unibe.ch |
| | A. Nardo* | email: alejandro.nardo@inf.unibe.ch |
| | M. Piu* | email: maurizio.piu@inf.unibe.ch |
| | A. Schürmann* | email: alec.schuermann@inf.unibe.ch |
| | D. Schweizer* | email: dominic.schweizer@inf.unibe.ch |
| | K. Stauffer* | email: kerrie.stauffer@inf.unibe.ch |
| | L. Stürmer* | email: lionel.stuermer@inf.unibe.ch |
| | N. Thalheim* | email: noe.thalheim@inf.unibe.ch |
| | R. Widmer* | email: roland.widmer@inf.unibe.ch |
| **Other Staff:** | M. Behn* | email: marcel.behn@inf.unibe.ch<br>(until December 2020) |
| | L. Biehl* | email: lara.biehl@inf.unibe.ch |
| | M. Fanger* | email: maria.fanger@inf.unibe.ch |
| | F. Giardina* | email: francesca.giardina@inf.unibe.ch<br>(until December 2020) |
| | Dr. B. Hitz-Gamper* | Tel.: +41 31 684 4712<br>email: benedikt.hitz@inf.unibe.ch |
| | A. Jörg* | email: adrian.joerg@inf.unibe.ch |

| | |
|---|---|
| R. Kehl-Sanchez* | email: rebeca.kehl@inf.unibe.ch |
| T. Lüthi* | email: thomas.luethi@inf.unibe.ch |
| G. Metzger* | email: gerry.metzger@inf.unibe.ch |
| Dr. J. Nussbaumer* | Tel.: +41 31 684 3401<br>email: jasmin.nussbaumer@inf.unibe.ch |
| K. Plüss* | email: kristelle.pluess@inf.unibe.ch |
| N. Sinz* | Tel.: +41 31 511 7633<br>email: nathalie.sinz@inf.unibe.ch |
| FH Prof. Dr. R. Standtke* | email: ronny.standtke@inf.unibe.ch |
| S. Weilenmann* | Tel.: +41 31 684 3879<br>email: stefanie.weilenmann@inf.unibe.ch |

*with financial support from a third party

## 10.2 Overview

The Research Center for Digital Sustainability can look back on another eventful year: The Research Center's courses could be further elaborated and are established as steady courses in the INF-curriculum.

In late 2020 the Federal Department of Foreign Affairs commissioned the Research Centre to conduct a study on Environmental Big Data and the possible pitfalls of Open Data. The study led to very interesting insights on the emerging topic of "Data Colonialism" and eventually a conference with international experts on this topic could be held.

In spring 2021 the triennial "Open Source Software Studie Schweiz" could be published with the support of CH Open and swissICT. The study investigates the application and use of Open Source Software in Switzerland. Furthermore, two projects that have been in development for a long time could be published: One is the revised platform "OSS Directory", Switzerland's largest Open Source directory. The other project is the first release of the app "UniBE Mobile" which the Research Center developed on behalf of the University of Bern. The app is going to be further developed in the following months to include the functions of "Ilias" and the contents of "Unisport".

As far as research projects are concerned, the project NRP73 on sustainable public procurement was successfully completed in June 2021. The project NRP77 on "Open Justice vs Privacy" is in full swing, our PhD student could make valuable progress within this research area.

The biggest news of them all is that PD Dr. Matthias Stürmer was called upon to take the chair in the Institute of Public Sector Transformation in the Economics Department at the Bern University of Applied Sciences (BFH). Starting July 1st, Matthias Stürmer is head of this Institute consisting of five workgroups but remains a lecturer at the University for the lecture “Digital Sustainability” and the “Open Source” lecture and exercise. The Research Center will, coming January 2022, also transfer to the BHF and leave the University of Bern.

We are looking forward to taking up new activities at the BFH but are also looking back with gratefulness on our last seven years at the University of Bern.

## 10.3 Research Projects

### NFP73 - Sustainable Public Procurement

In Switzerland, over 40 billion Swiss francs are spent annually on public procurement at the federal, cantonal and municipal levels. Based on existing bidding data and taking into consideration various sustainability indicators, effective criteria to foster sustainable procurement are developed. So far, procurement offices can already define ecological and social guidelines by means of suitable criteria. In accordance with new international and national procurement law and international agreements, sustainability criteria are to be taken into account to an even greater extent. Within the framework of this research project sustainability criteria for public tenders are developed that base on previous procurement and performance indicators from the sustainability reports of companies. The result will be an inventory of procurement-specific suitability and approval criteria, checked and tested in procurement practice. The aim of the research project is to initially determine the status quo of Swiss procurement regarding sustainability criteria. For this purpose, over 50,000 computerised procurement tenders will be evaluated. The project thus contributes towards sustainable development in general and a sustainable economy in Switzerland in particular.

**Research staff:** T. Welz, M. Stürmer.

**Financial support:** National Research Project NRP 73 Sustainable Economy, SNSF project No. 407340-172351

### NFP77 - Open Justice vs. Privacy

Justice should be open and transparent to ensure the public understanding of court decisions. On the other hand, each person should have the right to privacy and in particular the right to be forgotten. With this work we try to find a balance in this antagonism. The literature for anonymization of unstructured text documents is thin and for court decisions virtually non-existent. We plan to implement an end-to-end system for anonymization and re-identification of Swiss court decisions. This system will serve as a proof of concept that both the re-identification of a large part of manually anonymized court decisions is possible and that re-identification can be made significantly harder with the automated anonymization of our system. Our system will relieve legal experts of the burdensome task of manually anonymizing court decisions. Additionally, we hope to advance the knowledge in the field of text anonymization in general which will also serve many other fields.

**Research staff:** J. Niklaus, M. Stürmer.

**Financial support:** National Research Project NRP 77 Digital Transformation, SNSF project No. 407740-187477

## 10.4 Further Activities

### Memberships

**Joel Niklaus**

- Member of SwissNLP

**Matthias Stürmer**

- President of the Digital Impact Network
- Vice President of CH Open
- Board Member of Opendata.ch
- Member of Smart Capital Region
- Managing Director of Parldigi (Parlamentarische Gruppe Digitale Nachhaltigkeit)

### Tobias Welz

- Member of Sustainable Europe Research Institute (SERI), German Chapter, 2010-.
- Member of European Roundtable for Sustainable Consumption and Production (ERSCP), 2020-.

## Conference and workshop organization

### Matthias Stürmer

- IT-Beschaffungskonferenz 2020, conference on IT procurement, Bern, Switzerland, August 31, 2020
- DINAcon 2020, conference on digital sustainability, Bern, Switzerland, October 23, 2020

## Invited Talks

### Joel Niklaus

- Poster Presentation ”ESRA: An end-to-end system for re-identification and anonymization of Swiss court decisions”, Advanced Language Processing winter school (ALPS), January 2021
- Poster Presentation ”ESRA: An end-to-end system for re-identification and anonymization of Swiss court decisions”, Bern Data Science Day, April 2021
- ESRA: An End-to-End System for Re-Identificationand Anonymization of Swiss Court Decisions, Doctoral Consortium International Conference for Artificial Intelligence and Law (ICAIL),Sao Paolo, online, June 2021

### Matthias Stürmer

- Digitale Transformation und ihre Herausforderungen/Open Government Data (OGD) in der Schweiz/IT-Beschaffungen und Hersteller-Abhängigkeiten/Datenkolonialismus und digitale Nachhaltigkeit” 10 December 2020 module 4 “Digitale Transformation der Verwaltung und staatliche Kommunikation” of the KPM Executive Master of Public Administration (EMPA), virtual teaching

- Data Colonialism and Digital Sustainability: Problems and Solutions to Current Trends in Digitalization" 12 December 2020 virtual presentation at the The Global Dialogue Security Summit (India)
- 2030 nachhaltig digital: Welche Digitalstrategie braucht ein Kanton?" 13 January 2021 virtual presentation for the group "Parlamentarische Gruppe digitaler Wandel Kantonsrat Luzern"
- Parolenfassung EVP BL zum E-ID-Gesetz" 22 January 2021 virtual presentation at the Parteiversammlung EVP Kanton Baselland
- Open Source Entwicklung: Kür, Pflicht oder Bürde für die Verwaltung?" 17 February 2021 virtual presentation at conference of "Digitaler Staat" (Germany)
- "Learnings aus 15 Jahren Open Source Aktivismus" 26 February 2021 virtual presentation at Winterkongress 2021 of the association Digitale Gesellschaft
- Digital Sustainability: A Societal Concept for our Digital Future" 9 March 2021 virtual presentation at ethix Tech + Society Breakfast
- "Digitale Nachhaltigkeit vs. nachhaltige Digitalisierung? Nein, es braucht beides!" 23 March 2021 within the Semesterprogramm BENE of the association "Nachhaltige Entwicklung an den Berner Hochschulen"
- "Open Data und interaktive Datenvisualisierungen" 26 March 2021 virtual presentation at the University of Bern CAS Forschungsmanagement
- "Open Justice versus Privacy" 19 April 2021 virtual presentation about the National Research Programme 77 project at the "20. Magglinger Rechtsinformatikseminar"
- Open Education Server: Aktueller Stand und Ausblick" 24 April 2021 at the Open Education Day 2021
- Insights on Open Source and Inner Source" 25 May 2021 virtual presentation at Open Source @ Siemens
- Security implications of digitalization: The dangers of data colonialism and the way towards sustainable and sovereign management of environmental data" 26 May 2021 virtual presentation at the Online Conference on Data Colonialism of University of Bern

- “Digitale Nachhaltigkeit vs. nachhaltige Digitalisierung? Nein, es braucht beides!” 8 June 2021 within the University of Bern CAS Nachhaltige Entwicklung, module “Digitalisierung –Chancen und Risiken für eine nachhaltige Gesellschaftsentwicklung”
- Digitale Nachhaltigkeit vs. nachhaltige Digitalisierung? Es braucht beides!” 11 June 2021 virtual presentation at the Smart City Standards Forum (Germany)
- Künstliche Intelligenz und Möglichkeiten der Datennutzung und –auswertung” 15 June 2021 virtual presentation at the “Fachtagung Digitalisierung” of the Bundesamt für Lebensmittelsicherheit und Veterinärwesen (BLV)
- Status Quo Open Source in der Schweiz: Highlights der Open Source Studie 2021” 24 June 2021 virtual presentation the DBI event on open source databases

**Tobias Welz**

- “Facts und Trends bei nachhaltigen ICT-Hardware Beschaffungen.” IT-Beschaffungskonferenz 2020, Bern, Switzerland, August 2020
- ”Nachhaltigkeit in der öffentlichen Beschaffung” simap – Tag der Kompetenzzentren 2020, Bern, Switzerland, September 2020
- ”Messbarkeit von Nachhaltigkeit am Beispiel Strassenfahrzeuge”. BKB Tagung – nachhaltige öffentliche Beschaffung 2021, Bern, Switzerland, March 2021

## 10.5 Publications

**Disclaimer:** The publication list only includes publications published during the academic year, but does not include submitted and not yet published papers.

### Conference Papers

- Stucki, M., Jattke, M., Berr, M., Desing, H., Green, A., Hellweg, S., Laurenti, R., Meglin, R., Muir, K., Pedolin, D., Shinde, R., Welz, T., Keller, R. (2021). *How life cycle–based science and practice support the transition towards a sustainable economy* Int J Life Cycle Assess 26, 1062–1069, April 2021

## Journal Papers

## Other Publications

- Seele, P., de Rossa, F., Stürmer, M., Knebel, S., David, C., Welz, T. (2021). *Nachhaltige Öffentliche Beschaffung, Ergebnisbericht des SNF NFP 73 Forschungsprojekts.* July 2021

# 11 Software Composition Group

## 11.1 Personnel

| | | | |
|---|---|---|---|
| **Head:** | Prof. Dr. O. Nierstrasz | Tel: | +41 31 631 46 18 |
| | | email: | oscar.nierstrasz@inf.unibe.ch |
| **Office Managers:** | B. Choffat | Tel: | +41 31 631 46 92 |
| | | email: | bettina.choffat@inf.unibe.ch |
| **Scientific Staff:** | Dr. A. Bergel | Tel: | +41 31 511 7637 |
| | (Feb-Jul. 2021) | email: | abergel@dcc.uchile.cl |
| | O. Flückiger* | Tel: | +41 31 511 7638 |
| | | email: | o@o1o.ch |
| | P. Gadient | Tel: | +41 31 511 7644 |
| | | email: | pascal.gadient@inf.unibe.ch |
| | Dr. M. Ghafari | Tel: | +41 31 511 7637 |
| | (to Sept. 2020) | email: | mohammad.ghafari@inf.unibe.ch |
| | M. Hazhirpasand* | Tel: | +41 31 511 7644 |
| | | email: | mohammadreza.hazhirpasand@inf.unibe.ch |
| | M. Leuenberger | Tel: | +41 31 511 7636 |
| | (to Feb. 2021) | email: | manuel.leuenberger@inf.unibe.ch |
| | N. Patkar* | Tel: | +41 31 511 7644 |
| | | email: | nitish.patkar@inf.unibe.ch |
| | P. Rani* | Tel: | +41 31 511 7639 |
| | | email: | pooja.rani@inf.unibe.ch |
| | Dr. N. Stulova | Tel: | +41 31 511 7637 |
| | | email: | nataliia.stulova@inf.unibe.ch |

*with financial support from a third party

## 11.2 Overview

Software systems that are used in practice must evolve over time to maintain their relevance, yet as systems evolve, they become more complex and harder to evolve. The Software Composition Group carries out research into tools, techniques and programming language mechanisms to enable the graceful evolution of complex software systems.

## 11.3 Research Projects

### Agile Software Assistance

**Research staff:** All members of the research group.
**Duration:** Feb 1, 2019 – Apr. 30, 2022
**Financial support:** SNSF project #200020-181973

- **Software maintenance tool support.** About 5%-20% of the source code in software systems are usually duplicated (cloned), leading to decoupled bugs and increased maintenance costs among other issues. However, most research efforts to date have focused on detecting duplication rather than explaining the reasons behind it. We have developed a prototype of a tool that produces a set of connected multi-view visualizations at different abstraction levels for inspecting software duplication and the patterns behind it.

- **Speculative software analysis.** Code comments are important artifacts in software systems, and play a paramount role in many software engineering (SE) tasks related to maintenance and program comprehension. However, while it is widely accepted that high quality matters in code comments just as it matters in source code, defining and assessing comment quality in practice is still an open problem. To obtain a clear picture the state of the art in comment quality assessment techniques and approaches, we have conducted a systematic literature review on comment quality evaluation practices, focusing on the scientific publications in software engineering in the past 10 years. This work allowed us to complement the existing body of research with the new data, and identify research gaps and industry needs more precisely. We have also analyzed current industry comment writing practices and their adoption by practitioners from several perspectives. To gain insight into actual commenting practices we have studied the adherence of comments to comment writing guidelines. We have produced a taxonomy of guidelines based on the data that was extracted from open-source software projects for several popular programming languages, allowing us to gain insight which writing guidelines are followed less strictly, indicating issues with them. Additionally, we have studied tool support for verifying comments against the taxonomy of guidelines using a dataset of open-source projects and a number of linters and style checkers actively used in those projects. We have produced a mapping between comment writing rules that are specified in the guidelines and that are actually checked by specialized tools (like style checkers and code linters), making it easier to identify focus points for tool improvement.

- **Executable domain models.** To facilitate non-technical stakeholder participation in software engineering (SE) activities, such as requirements engineering (RE) and software modeling, an appropriate methodology and corresponding tools must be developed. We studied 112 RE tools published at top SE venues to characterize their limitations and to reflect on the rigor (*i.e.*, how extensive the evaluations were) and relevance (*i.e.*, accessibility of the tools). Furthermore, we analyzed the main topics and sub-research topics the selected 112 tools cover to study evolution over the years 2015-2019. One of the ways to enable non-technical stakeholders to specify and verify application behavior is to use behavior-driven development (BDD) tools. We studied existing BDD tools to characterize their limitations and subsequently proposed an approach and prototype implementation to improve the interaction capabilities for non-technical stakeholders within an IDE. We also studied a plethora of RE artifacts to characterize their properties. Subsequently, we proposed a prototype implementation to model a selection of software-related artifacts within an IDE and use them to compose live executable documentation. Finally, we are working on characterizing the properties of scenario specifications and test cases from a large-scale survey of open-source BDD projects hosted on GitHub, further complimented with a practitioner survey.

- **Domain-specific software quality.** We continued the *Security Code Smells* journey from mobile apps to web APIs, *i.e.*, we performed an empirical study on the prevalence of smells in app servers of Android mobile apps. We found that the majority of apps suffers from three different kinds of security smells, and that misconfigurations are very common. We conclude that app server security smells are omnipresent and they indicate poor app server maintenance. Fortunately, many of our identified smells could be mitigated with appropriate protection, *e.g.*, by using more intelligent String classes. However, the String classes in existing programming languages usually do not provide such functionality and only provide rather basic methods for manipulation. Therefore, we are currently investigating the security gains that we can achieve by extending the existing String class in the Java SDK. With such a modernized String implementation we can precisely track the spread of information and ensure that the information only leaks when it is safe. All existing Java applications that run on a particular Java VM remain compatible with our custom Java VM and do not require any changes in the code nor a recompilation. We are currently experimenting with a prototype and preparing an upcoming empirical study.

We analyzed crypto-related vulnerability reports on the HackerOne platform to understand what types of crypto flaws exist in practice. We extracted eight themes in the reports and suggested the proper mitigation strategies.

We surveyed the top 1% of crypto responders on Stack Overflow. The participants were asked to provide us with why inexperienced developers fail using cryptography correctly, and what resources might help such developers or crypto designers.

We analyzed 500 posts from 20 crypto libraries on Stack Overflow. We found various problematic areas that are shared among the crypto libraries, such as sign/verification, working with modes of encryption, IV, and salt.

We proposed a wrapper for the .NET crypto runtime in order to ease the process of using cryptography for .NET developers. Furthermore, the wrapper is able to conduct the misuse detection analysis on applications in which the source code is not available.

We conducted careful scrutiny of the .NET and Java crypto libraries to understand what APIs are more complex than others. Next, we checked the associated questions to these APIs on Stack Overflow to observe developer confusion with such APIs. In our preliminary study, we realized that when an API has many arguments, there exist a considerable number of questions on Stack Overflow.

For further details, please consult:
`http://scg.unibe.ch/asa3`

## 11.4 Master's Theses

- Patrick Frischknecht. Detection of cybersquatted domains. Masters thesis, University of Bern, July 2021. URL: `http://scg.unibe.ch/archive/masters/Fris21a.pdf`.

- Robert Niemiec. Modeling requirements artifacts in an IDE. Masters thesis, University of Bern, September 2020. URL: http://scg.unibe.ch/archive/masters/Niem20a.pdf.

- Jonas Richner. Interactive visualizations for software duplication. Masters thesis, University of Bern, January 2021. URL: http://scg.unibe.ch/archive/masters/Rich21a.pdf.

- Andreas Wälchli. A sampling profiler for a JIT compiler. Masters thesis, University of Bern, September 2020. URL: http://scg.unibe.ch/archive/masters/Wael20a.pdf.

## 11.5 Bachelor's Theses and Computer Science Projects

- Rafael Burkhalter. Finding and mitigating cross-site scripting attack vectors — testing different web application security scanners. Bachelor's thesis, University of Bern, April 2021. URL: http://scg.unibe.ch/archive/projects/Burk21a.pdf.

- Michael Dooley. Tool support for commenting conventions. Bachelor's thesis, University of Bern, July 2021. URL: http://scg.unibe.ch/archive/projects/Dool21a.pdf.

- Lino Hess. Generating automatically class comments in Pharo. Bachelor's thesis, University of Bern, July 2021. URL: http://scg.unibe.ch/archive/projects/Hess21a.pdf.

- Dean Klopsch. Biomimicry-based algorithms and their lack of generalization. Bachelor's thesis, University of Bern, February 2021. URL: http://scg.unibe.ch/archive/projects/Klop21a.pdf.

## 11.6 Awards

- Joint Computer Science Alumni Association Award for Pascal Gerig's MSc thesis, Investigating Phishing on Demand

## 11.7 Further Activities

### Invited Talks

**Oscar Nierstrasz**

- Keynote Speaker (remote) at ASE 2020 Doctoral Symposium (35th IEEE/ACM International Conference on Automated Software Engineering — Melbourne, Australia, Sept. 21, 2020)

### Editorial Boards and Steering Committees

**Oscar Nierstrasz**

- AITO — Association Internationale pour les Technologies Objets (Member)
- CHOOSE — Swiss Group for Object-Oriented Systems and Environments (Board member)
- Elsevier Science of Computer Programming (Advisory Board Member, Software Section)
- JOT — Journal of Object Technology (Steering Committee Member)

### Program Committees

**Oscar Nierstrasz**

- PC Member of ICSME 2021 (37th International Conference on Software Maintenance and Evolution — Luxembourg City, Sept. 27 - Oct. 1, 2021)

### Reviewing Activities

**Oscar Nierstrasz**

- Deutsche Forschungsgemeinschaft
- Science of Computer Programming
- Information and Software Technology
- The Journal of Systems & Software

- Software Quality Journal
- Transactions on Software Engineering and Methodology

**Pascal Gadient**

- ICSME 2021

**Pooja Rani**

- TOSEM 2021

## 11.8 Publications

### Journal Papers

- Pooja Rani, Sebastiano Panichella, Manuel Leuenberger, Andrea Di Sorbo, and Oscar Nierstrasz. How to identify class comment types? A multi-language approach for class comment classification. *Journal of Systems and Software*, 181:111047, 2021. URL: https://www.sciencedirect.com/science/article/pii/S0164121221001448, doi:https://doi.org/10.1016/j.jss.2021.111047.
- Pooja Rani, Sebastiano Panichella, Manuel Leuenberger, Mohammad Ghafari, and Oscar Nierstrasz. What do class comments tell us? An investigation of comment evolution and practices in Pharo Smalltalk. *arXiv preprint arXiv:2005.11583*, 2020. To be Published in Empirical Software Engineering.

### Conference Papers

- Mathias Birrer, Pooja Rani, Sebastiano Panichella, and Oscar Nierstrasz. Makar: A framework for multi-source studies based on unstructured data. In *2021 IEEE International Conference on Software Analysis, Evolution and Reengineering (SANER)*, pages 577–581, 2021. URL: http://scg.unibe.ch/archive/papers/Rani21c.pdf, doi:10.1109/SANER50967.2021.00069.
- Mohammadreza Hazhirpasand, Arash Ale Ebrahim, and Oscar Nierstrasz. Stopping DNS rebinding attacks in the browser. In *Proceedings of the 7th International Conference on Information Systems Security and Privacy - ICISSP*, 2021. URL: http://scg.unibe.ch/archive/papers/Hazh21a.pdf, doi:10.5220/0010310705960603.

- Mohammadreza Hazhirpasand, Mohammad Ghafari, and Oscar Nierstrasz. Java cryptography uses in the wild. In *Proceedings of the 14th ACM / IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, 2020. URL: `http://scg.unibe.ch/archive/papers/Hazh20c.pdf`, `doi:10.1145/3382494.3422166`.

- Nitish Patkar. Moldable requirements. In *Benevol'20*, 2020. URL: `http://scg.unibe.ch/archive/papers/Patk20c.pdf`.

- Pooja Rani. Speculative analysis for quality assessment of code comments. In *2021 IEEE/ACM 43rd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion)*, pages 299–303, 2021. URL: `http://scg.unibe.ch/archive/papers/Rani21a.pdf`, `arXiv:2102.09605`, `doi:10.1109/ICSE-Companion52605.2021.00132`.

- Nataliia Stulova, Arianna Blasi, Alessandra Gorla, and Oscar Nierstrasz. Towards detecting inconsistent comments in java source code automatically. In *2020 IEEE 20th International Working Conference on Source Code Analysis and Manipulation (SCAM)*, pages 65–69. IEEE, 2020. URL: `http://scg.unibe.ch/archive/papers/Stul20b-InconsistentComments.pdf`, `doi:10.1109/SCAM51674.2020.00012`.

# 12 Administration

**University:**

| | |
|---|---|
| T. Braun: | Member of the Committee for Computing Services (Kommission für Informatikdienste)<br>Member of Committee for Wyss Academy |
| T. Studer: | Member of *Kantonale Maturitätskommission* |

**Faculty:**

| | |
|---|---|
| D. Bommes: | Joint Master in Computer Science of the Universities of Bern, Fribourg and Neuchâtel: Member of the Branch Committee |
| T. Braun: | Member Faculty Strategy Committee |
| C. Cachin: | Joint Master in Computer Science of the Universities of Bern, Fribourg and Neuchâtel: Member of the Branch Committee |
| P. Favaro: | Member of the Board of Studies<br>Faculty delegate (until December 2020) |
| O. Nierstrasz: | Member Digitalization Strategy Working Group<br>Deputy Faculty delegate (until December 2020)<br>Faculty contact person for digitalization |
| T. Studer: | Member of the Strategy Board<br>Representative of high Mittelbau in faculty meetings |

**Institute:**

| | |
|---|---|
| D. Bommes: | Director of Studies |
| T. Braun: | Managing Director of INF (until 18.05.21) |
| C. Cachin: | Deputy Director of Studies<br>Member of Library Committee on behalf of INF<br>Representative to CUSO Doctoral School in Computer Science |
| P. Favaro: | Managing Director of INF (as of 19.05.21) |
| O. Nierstrasz: | Deputy Director of INF (as of 19.05.21)<br>Member of Hauskommission Engehalde |
| T. Studer: | Member of Hauskommission Exakte Wissenschaften |