universität freiburg

CS
INSTITUT FÜR
INFORMATIK

CoNe
Freiburg

Theses and Projects at CoNe

29.10.2025

Version 29.10.2025
Winter Semester 2025/2026

Technische Fakultät
Christian Schindelhauer

Projects and Theses

General Remarks

Your Project

Localization

Computational Complexity

Peer-to-Peer Networks

Telocate

Axel Sikora

MIMO and Near-Field

Ray Tracing based Cryptography

Cryptography

General Remarks

What, where, how?

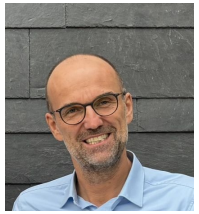
Our Group
Who, what, where?

- **People**
  - Prof. Dr. Christian Schindelhauer
  - Sneha Mohanty
  - Saptadi Nugroho
  - Peter Krämer
  - Dr. Johannes Wendeberg (Telocate)
  - Dr. Fabian Höflinger (Telocate)
  - Dr. Joan Bordoy (Telocate)
- **Partners**
  - Telocate
  - Prof. Dr. Axel Sikora
  - Prof. Dr. Stefan Rupitsch









General Remarks

What is a project?
What is a thesis?

- **Study programs at the Faculty**
  - Computer Science, Embedded Systems Engineering, (IMTEK, SSE)
  - Bachelor, Master, (PhD, PostDoc)
- **Project**
  - Bachelor project (6 ECTS)
  - Master project (18 ECTS)
- **Theses**
  - Bachelor Thesis (15 ECTS)
  - Master Thesis (30 ECTS)

- **Projects**
  - are practical and should train for your future work as an engineer/IT specialist
  - help us to perform research
  - can be the warm-up phase for a thesis
- **Theses**
  - is the plural of thesis
  - is an academic individual work of the student
    - i.e. could lead to a scientific publication

Types
What kinds of projects/theses exist?

Theory

- Mathematical treatment of a topic
  - i.e. Theorem, Lemma, Proof

Practical Work

- Design, Implementation, Set-up, Testing
- of programs or embedded systems

Experimental Work

- Design of an experimental buildup
- Documentation of the setup, experiments and surrounding
- Analysis of the experiment and conclusion
  - may involve programming, building a system, etc.

Lemma 7. *The expected potential in round $t+1$ is at most $\left(r^2+(1-r)^2\left(1-\frac{1}{n}\right)\right)$ times the potential in round t. Formally: $\mathbb{E}\left[\Phi_{t+1}|\Phi_t=\phi\right] \leq \left(r^2+(1-r)^2\left(1-\frac{1}{n}\right)\right)\phi$.*

Proof. The proof is similar to the proof in [5]. The key difference is the parameter r. For ease of notation, the time indices are dropped. Given all $v_{i,j}$ and all calling assignments $f(i)=k$ at time t the potential in the next round can be computed as:

$$\Phi_{t+1} = \sum_{i,j}\left(rv_{i,j} + \sum_{k:f(k)=i}(1-r)\,v_{k,j} - \frac{rw_i + \sum_{k:f(k)=i}(1-r)\,w_k}{n}\right)^2 \tag{17}$$

$$= \sum_{i,j}\left(\underbrace{r\left(v_{i,j}-\frac{w_i}{n}\right)}_{a} + \underbrace{\sum_{k:f(k)=i}(1-r)\left(v_{k,j}-\frac{w_k}{n}\right)}_{b}\right]\right)^2 \tag{18}$$

$$= \underbrace{\sum_{i,j} r^2\left(v_{i,j}-\frac{w_i}{n}\right)^2}_{a^2} + \underbrace{\sum_{i,j} 2r\left(v_{i,j}-\frac{w_i}{n}\right)\sum_{k:f(k)=i}(1-r)\left(v_{k,j}-\frac{w_k}{n}\right)}_{2ab} \tag{19}$$

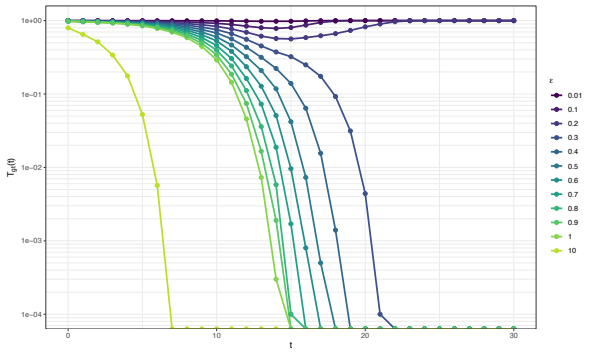


Figure 15: Tail weight $T_{gt}(t)$ of 10000 nodes aggregating the average using *Random-Call-Pull*. The inputs to the nodes are constant and uniformly distributed from the interval $[0, 100]$.

Design and Implementation of a Simulation Environment for Peer-to-Peer based Data Aggregation of Time-Series Data
Alexander Weinmann June 29, 2021

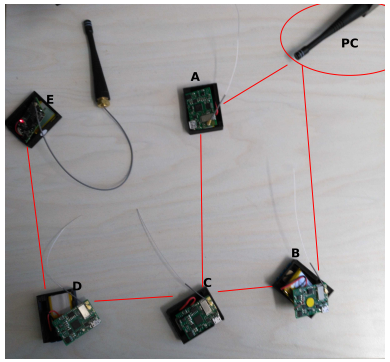


Figure 13: Experiment with ignore lists for each node

GasLok Network Protocol
Philip Klein 2020

Timeline of a Project/Thesis

Preparing

- contact the contact person
- work out the specifics of the task
- get the literature
- get the material

Starting

- **Register** with the examination office
- **Kickoff presentation** at the Oberseminar
  - contact Sneha Mohanty
  - with desired date, title, abstract

Working

- go to **meetings**
  - especially if you think there is nothing to report
- stay in **contact** with your contact person
- report difficulties, new insights, successes
- Start writing down your results early

Finishing

- **deadlines of theses are strict**
  - except you break your arm or leg
  - then apply for an extension at the examination office
- projects have a flexible deadline
- **Submission**
  - your **thesis** to the **examination office**
  - project report to your contact and to the chair (me)
    - via NextCloud, E-Mail, paper
- **final presentation** in the Oberseminar
  - contact Sneha Mohanty for scheduling

Your Project

Everything you have ever dreamt of

Many Industrial Projects and Theses are Scams

- Famous, prestigious companies are **scamming students**
- **Promise thesis**
  - *„tHe OnLy tHiNg yOu nEeD iS tO fInD a sUpErVisiNg pRoFeSSor“*
  - offer some money
- **BUT**
  - finding a supervisor is **their job**
  - offered theses are often **not academic**
  - offered money is way below your pay grade
  - They want hard work for cheap money

- **If you find a supervisor and start such a thesis**
  - **Plus**
    - Money and a thesis
    - contact to company
  - **Minuses**
    - you have two bosses
    - you cannot publish your results NDA
    - worse grades, less money
    - finding a job is not a problem
    - you are wasting your only chance to get into academic research

The good industrial theses and Pitch your idea.

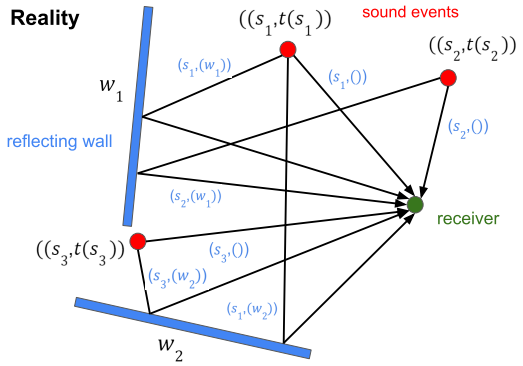
- The **good** industrial theses
  - the supervisor is in the field, e.g. computer scientist
  - supervisor has a publication record
  - contacts to universities have been established
  - they are interested in publishing the results
- **Good industrial projects**
  - projects work much better than theses with industry
  - but, they do not know how grading works…
- **or just going YOUR WAY**
- **You have an original idea**
  - tell us about it
  - show us that it has academic potential
  - show us the relation to our research
    - or at least the name of the chair
- You work out the fine print
  - own literature research
  - own risk
  - but also your own chance of doing your thing

Localization

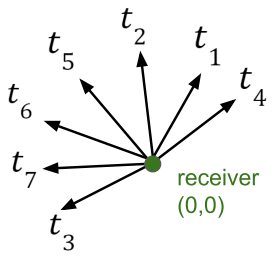
ILDARS, Self-Calibration
Signal Processing

ILDARS
Indoor Localization based on Directed and Reflected Signals

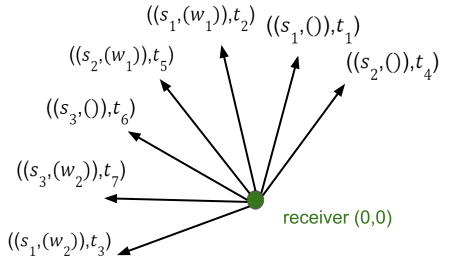
- A **silent bat** hears some other bats
  - can detect the **direction** and the **time** of a sound signal
  - can be **directed or reflected** signal
- **Question**:
  - What can a silent bat locate?
  - ILDARS problem
- **Oracle version:**
  - The names of the reflecting walls are given
    - e.g. in a characteristic table
- **General version:**
  - Nothing is known
    - **Use Occam's razor for explanation of the world**
- Literature
  - Mohanty, S., What can a Silent Bat Locate?, draft, 2023



ILDARS Problem



Oracle ILDARS problem



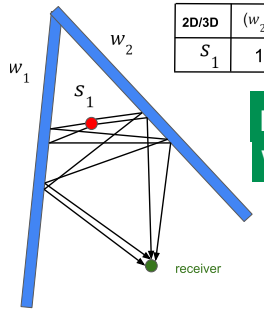
Characteristic Table

Line of sight

2D	()	(w_1)	(w_2)
s_1	(d_1,t_1)	(d_2,t_2)	(d_3,t_3)
s_2	(d_4,t_4)	(d_5,t_5)	$\emptyset$
s_3	(d_6,t_6)	$\emptyset$	(d_7,t_7)

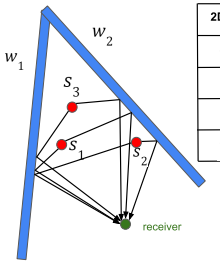
Theoretical ILDARS

- **Task**:
  - Assuming perfect precision input
  - Can we determine the position of the signals for this input?
  - Can we calculate the walls?
- **Literature**
  - Mohanty, S., What can a Silent Bat Locate?, draft, 2023
  - Marcel Schuhmacher, Theoretical Analysis of the Two-Dimensional Indoor Localization Problem based on TDOA and Direction Vectors for one Source and two Reflecting Lines, Bachelor Thesis, 2025
    - solved the case of two walls in 2D
- **Projects**
  - many senders, two walls, in 2D
  - one sender, two walls in 3D
  - one sender, three walls in 2D
  - which reflections scenarios are possible?
- **Contact**
  - Christian Schindelhauer, Sneha Mohanty



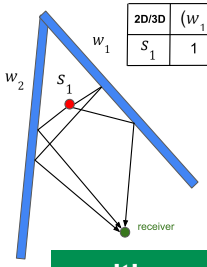
2D/3D	(w_2)	(w_1,w_2)	(w_2,w_1)	(w_1,w_2,w_1)
s_1	1	1	1	1

positions can be determined
walls can be determined



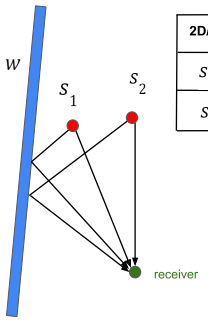
2D/3D	(w_1)	(w_2)
s_1	1	1
s_2	1	1
⋮	⋮	⋮
s_n	1	1

walls not computable



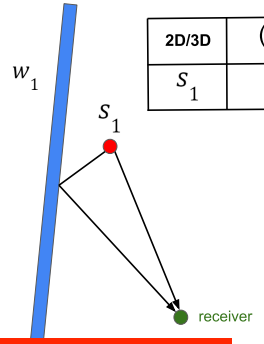
2D/3D	(w_1)	(w_2)	(w_1,w_2)
s_1	1	1	1

positions can be determined
walls can be determined



2D/3D	()	(w)
s_1	1	1
s_2	1	1

positions can be determined
walls can be determined



2D/3D	()	(w_1)
s_1	1	1

walls not computable

position not computable

Silent Bat in „Normal“ Architecture

- **In the silent bat approach we have assumed walls in general position**
- **Question**
  - Can we transfer the results to parallel and rectangular mirrors?
  - How about new shapes (planes, spheres, cylinders)
- **Task**
  - Find algorithms to detect such walls and perform localization
- **Contact**
  - Christian Schindelhauer
  - Sneha Mohanty

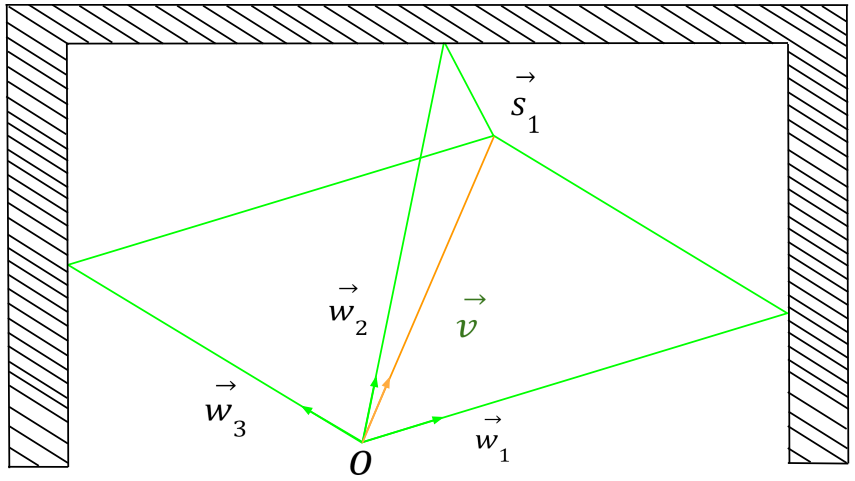


Fig. 1. Receiver device at position o receives one direct and multiple reflected signals from sound source s_1

https://www.cgtrader.com/free-3d-models/interior/living-room/living-room-design-001

Signal Processing for ILDARS Machine Learning/Fingerprinting

- **Based on several incoming signals**
  - predict pairing and order of reflection
  - differentiate and detect reflected and LOS signal
  - compare ILDARS, Fingerprinting and ML
- **Literature**
  - Gabbrielli, 3-D Angle of Arrival Ultrasonic Indoor Localization System with Chirp Spread Spectrum Multi-User Identification, PhD Thesis, 2023
- **Contact**
  - Christian Schindelhauer, Sneha Mohanty

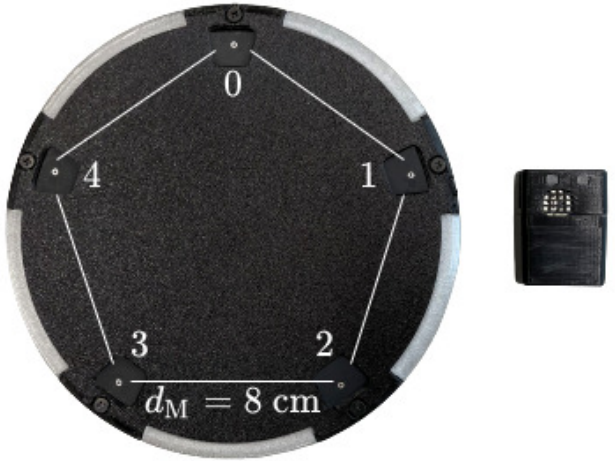


Fig. 2. The AoA ultrasonic receiver composed of 5 microphone placed on a pentagon of length $d_M = 8$ cm (on the left) and the ultrasonic speaker tag (on the right).

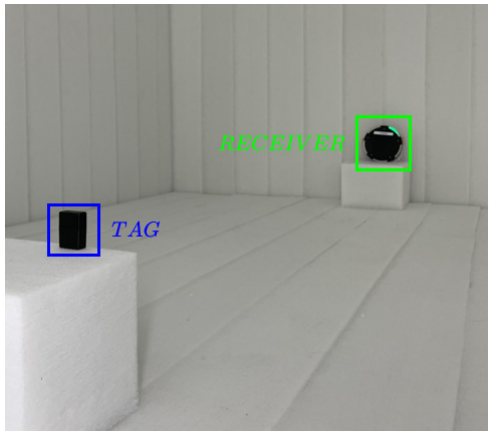
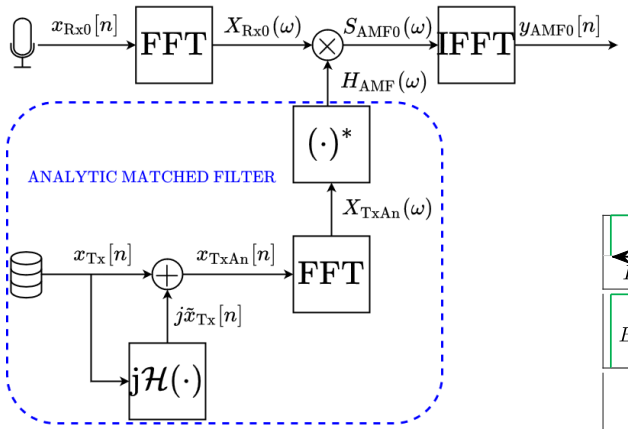


Fig. 3. Test setup in the ultrasonic anechoic chamber. The receiver and tag are place at 1 m distance, facing each other.



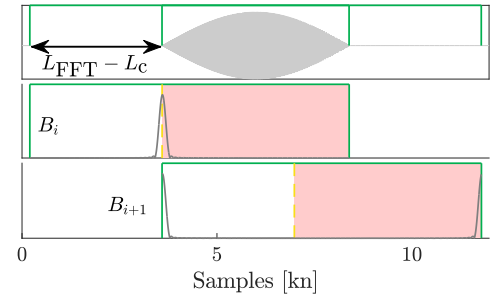


Fig. 8. Peak search limit case. *Top plot*: Both blocks entirely include the chirp stored in the ring buffer. *Middle and bottom plot*: The chirp is included in both B_i and B_{i+1}, however only the half compressed pulse is present in the peak search region.

ILDARS Simulation for Complex Scenarios

- **Task**
  - **Multiple Reflections** (recursive Half-Circle-Lemma)
  - **Complicated Scenarios**
  - **Producing Input triples** (ongoing)
  - **Integrate the System**
- **Literature**
  - Mohanty, Müller, S, Simulation of a first prototypical 3D solution for Indoor Localization based on Directed and Reflected Signals, Poster IPIN, 2023
- **Contact**:
  - Christian Schindelhauer, Sneha Mohanty

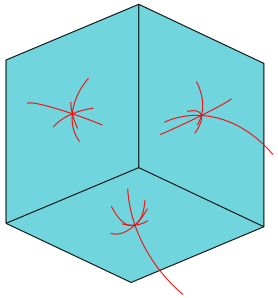


Fig. 3. Circular Segments from three different walls

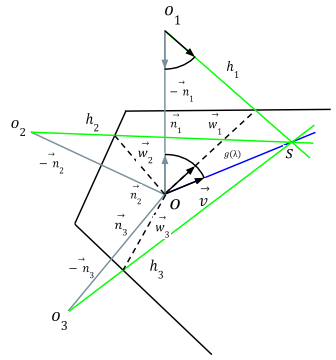


Fig. 7. Closest Lines extended

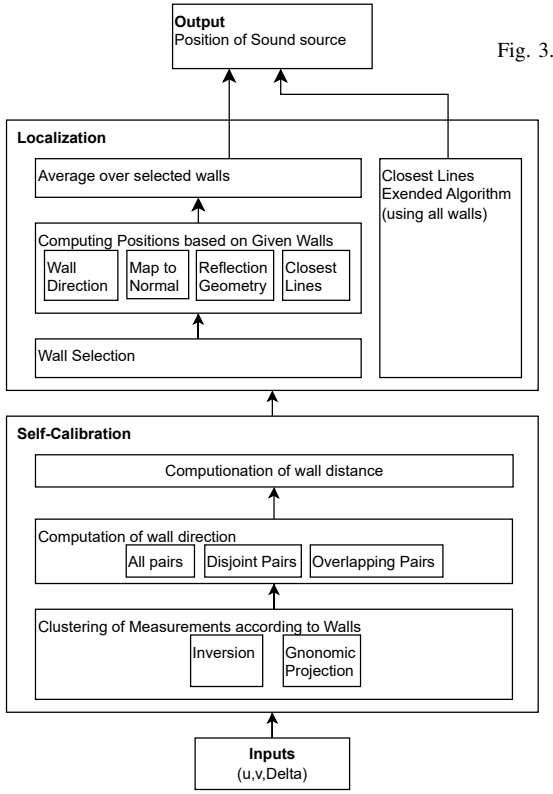
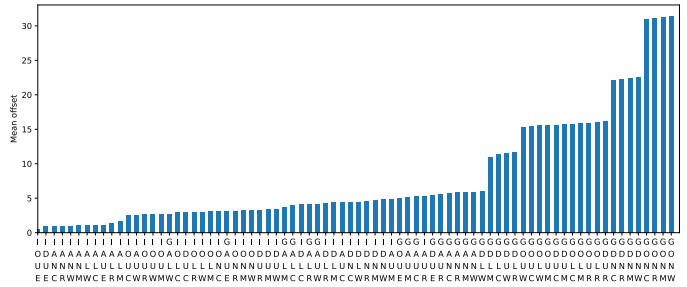
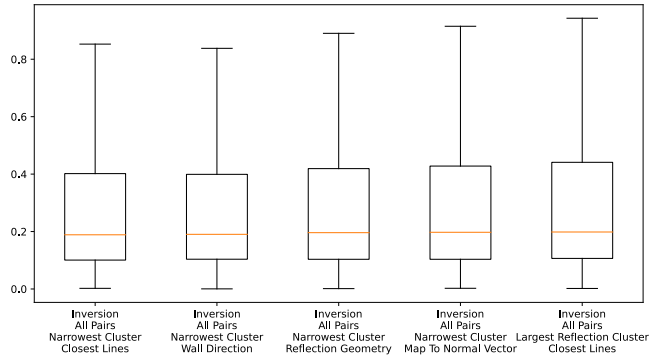


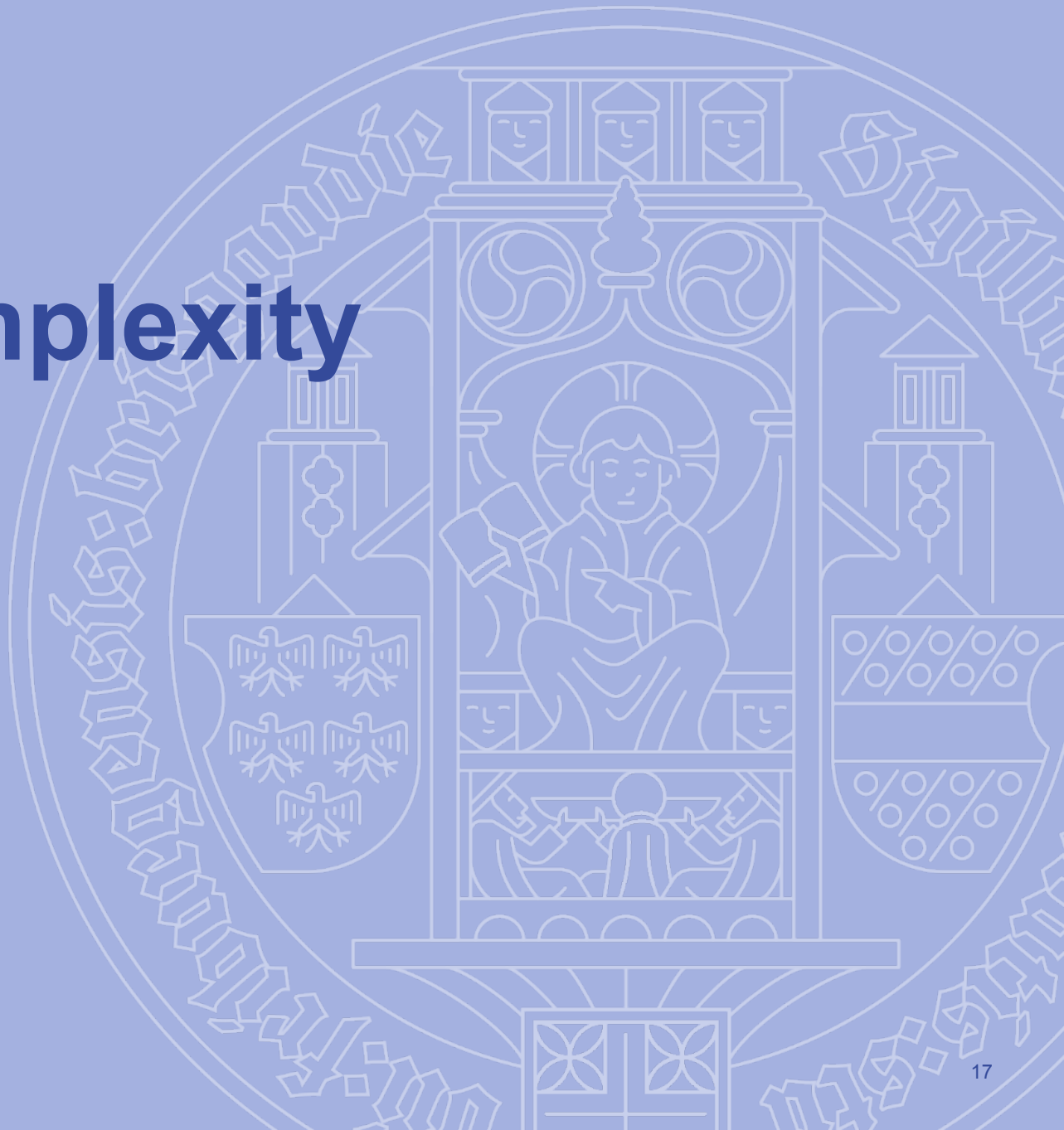
Fig. 2. Design of the ILDARS system





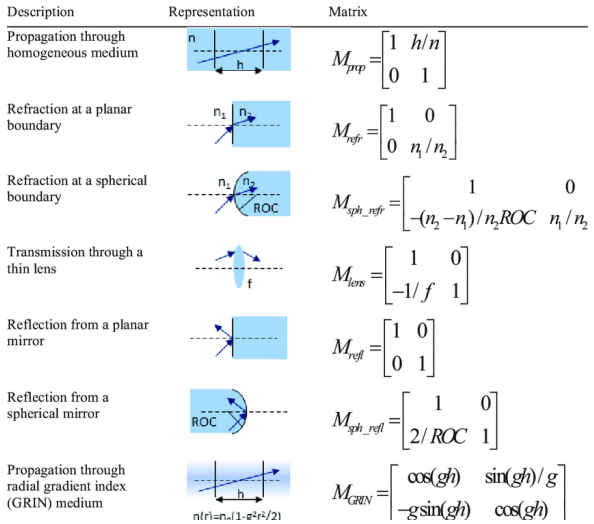
Computational Complexity

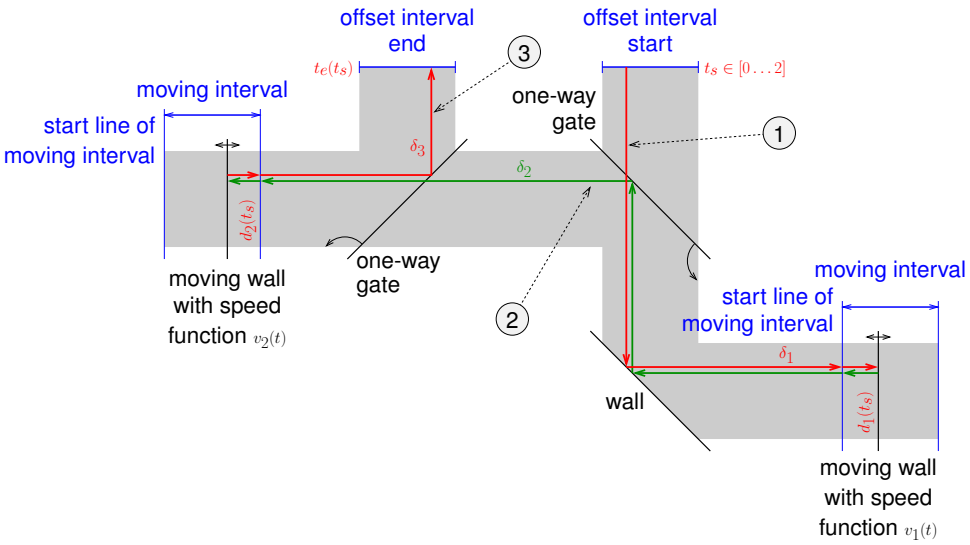
Proving the hardness



Computational Complexity of Ray tracing and Illumination Dist-NP

- **Theoretical Tasks**
  - Prove that 2-D Ray-Tracing in the ABCD model is not computable with constant probability
  - Prove that Reif's 3D Ray-Tracing problem is not computable with constant probability
  - Prove DistNP-hardness for
    - the linear bounded Reif 3D illumination problem
    - the linear bounded 2D ABCD-model illumination problem
- **Simulation**
  - Build a simulator for the 2D Pinball problem
- **Literature**
  - Adejoh, Jakoby, Mohanty, S., „Complexity Bounds for Illumination and Ray Tracing in 2D“, draft, 2023
  - Adejoh, R., Jakoby, A., Mohanty, S. and Schindelhauer, C., 2025. How Pinball Wizards Simulate a Turing Machine. arXiv preprint arXiv:2510.02560.
  - John H. Reif, J. Doug Tygar, and A. Yoshida. Computability and complexity of ray tracing. Discrete & Computational Geometry, 11:265–288, 1994.

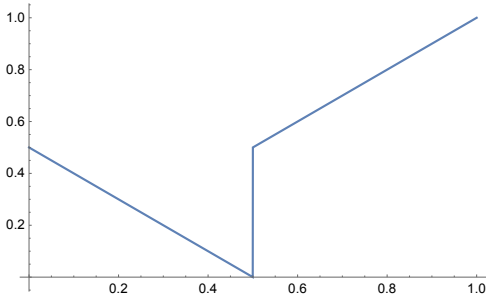


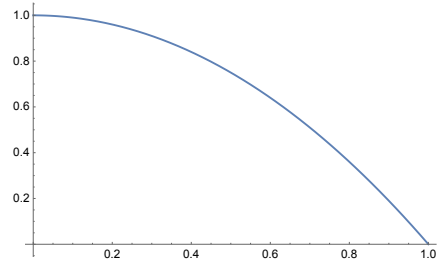


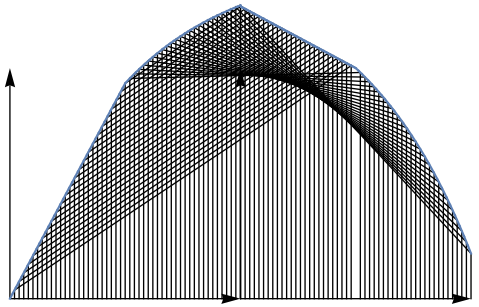
https://www.researchgate.net/figure/ABCD-matrices-of-some-optical-elements-18_tbl1_365741941

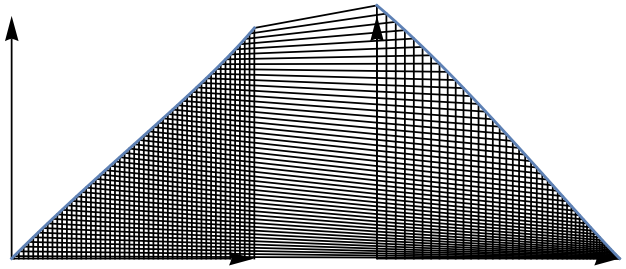
Computational Power of Mirrors

- **Mirrors are computational tools**
  - Input/output Direction, offset, time
  - What is the computational power
- **SimTasks**
  - Create mirrors performing given operations
  - Prove that it is hard to compute when a signal of a point has arrived at a target
  - Design mirror system that compute complex tasks or fulfill other properties
    - e.g. an aerodynamic car mirror using multiple reflections
- **Literature**
  - Serge Tabachnikov. Geometry and billiards, Volume 30. American Mathematical Soc., 2005.
- **Contact**
  - Christian Schindelhauer



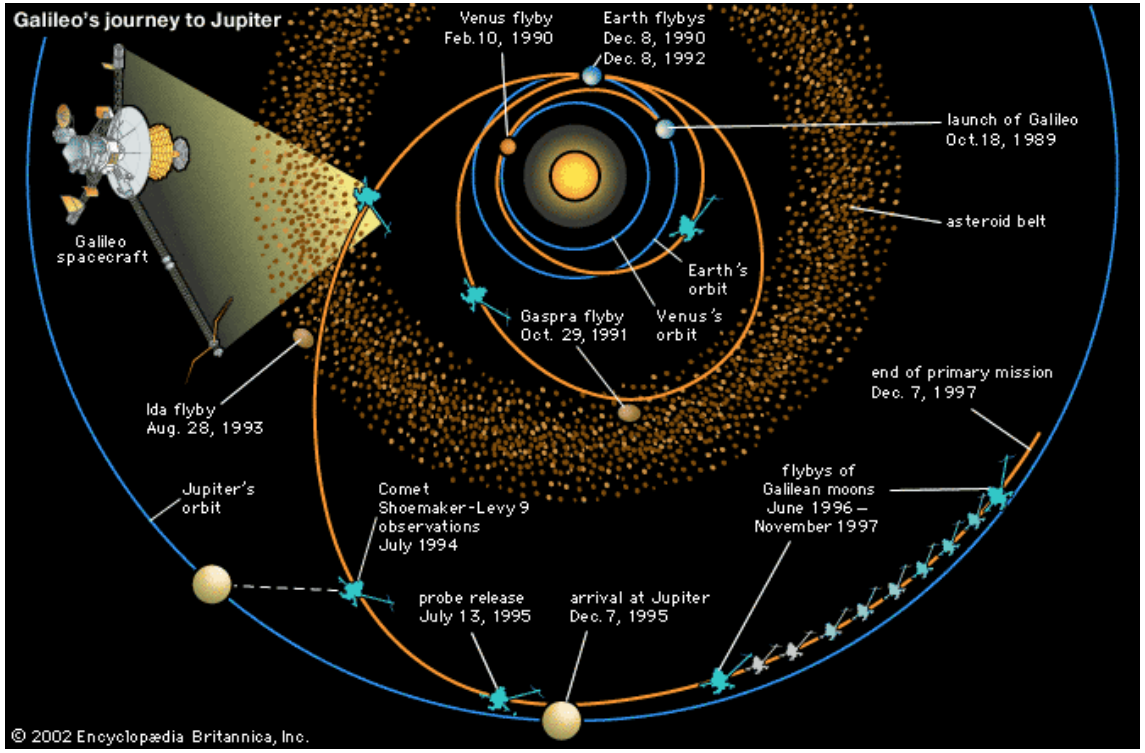






Computational Complexity of Gravity Assist

- **Problem**
  - given moving planets in space
  - compute the fastest rocket path to reach a target
- **Theory**
  - Show that Gravity-Assist with „normal stellar objects“ is NP-hard (ongoing)
  - Is it hard to solve Gravity-Assist for randomly moving objects?
- **Simulation**
  - How well can we approximate Gravity-Assist on the long run



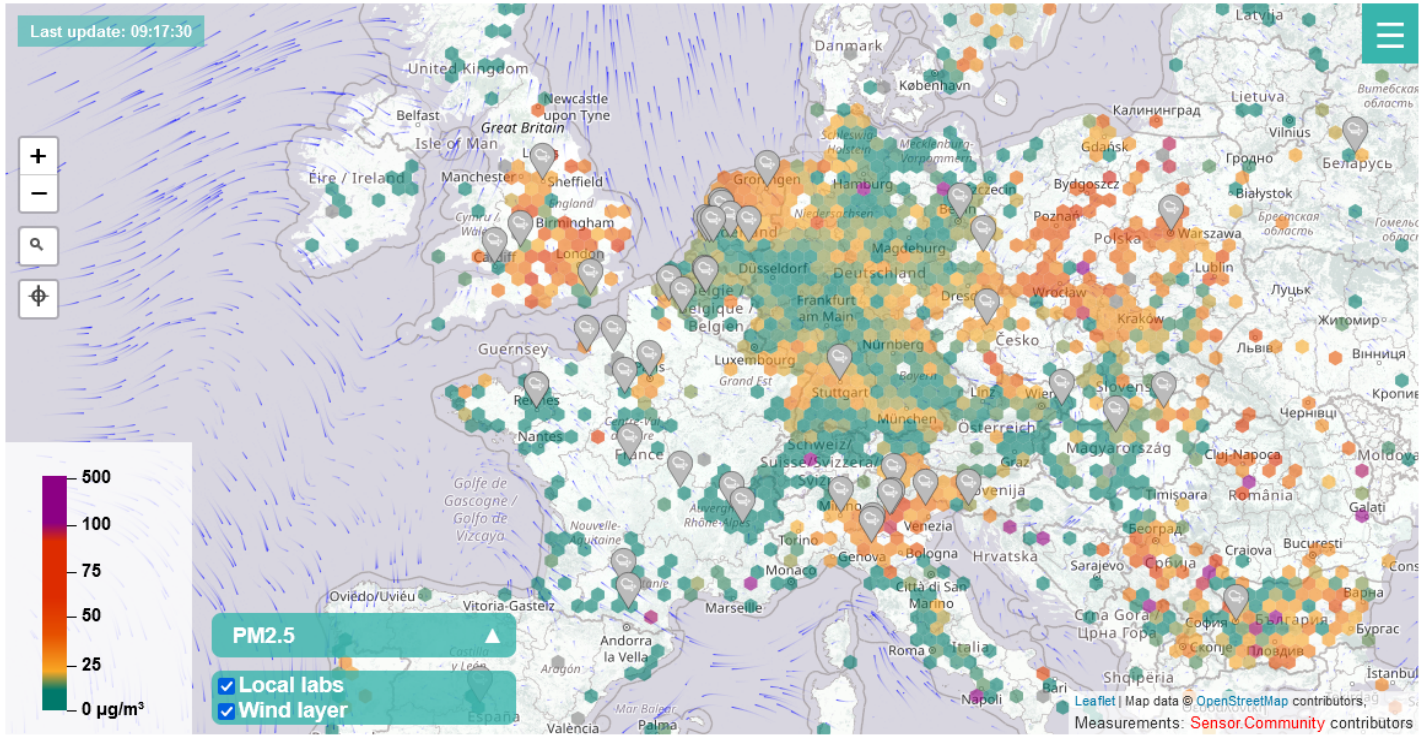
https://kids.britannica.com/kids/assembly/view/74053

Peer-to-Peer Networks

Everybody is equal

Data Aggregation in Peer to Peer Network

- Consider
  - Sensors and data from sensor.community
- **Experimental and Simulation Tasks**
  - Build P2P-sensor data network Compute/ Simulate the asynchronous rumor spreading (ongoing)
  - Providing Aggregation Function (Min, Max, Average, Sum, Count)
  - Providing Encryption
- **Contact**
  - Christian Schindelhauer
  - Saptadi Nugroho (saptadinugroho at gmail.com)

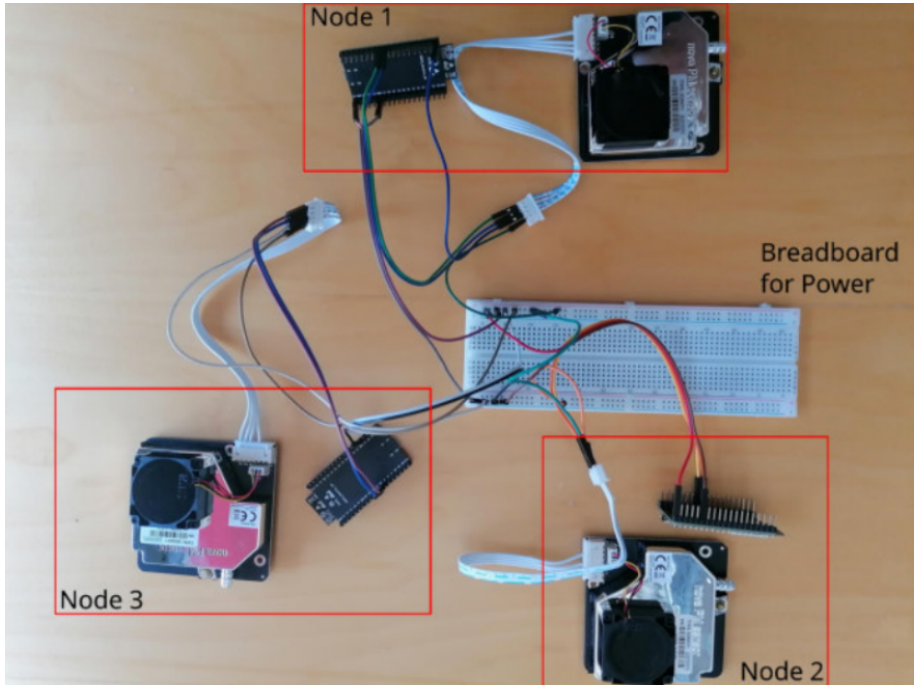


Source picture: https://sensor.community/en/

Smart sensor agents can communicate with each other in a communication network to exchange data. Each sensor agent produces measurement data. In this project we will try to simulate asynchronous data aggregation using data from sensor.community.

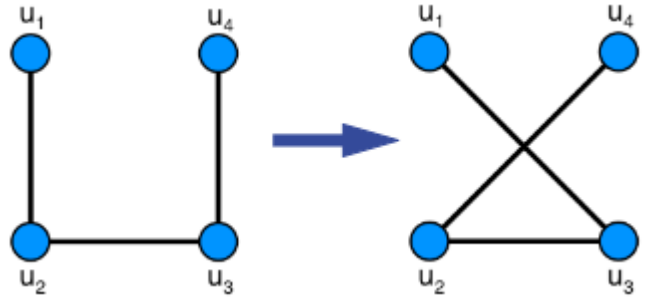
Peer-to-Peer Embedded Systems

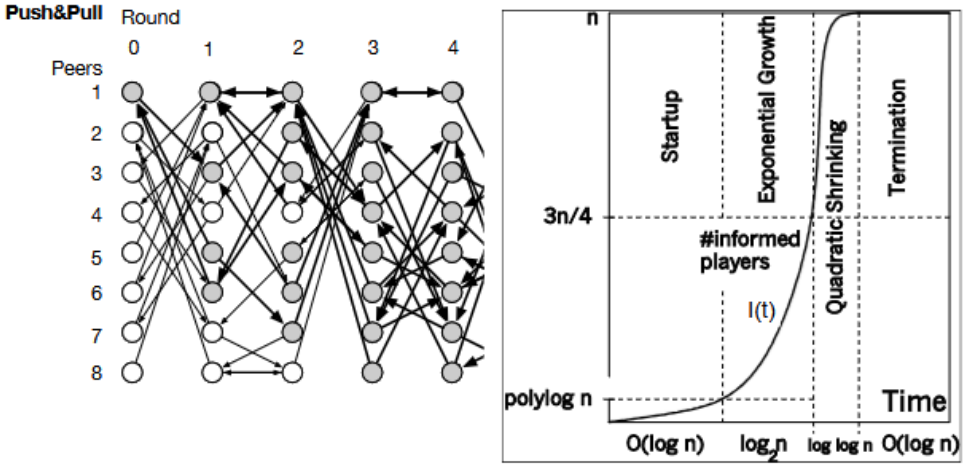
- Internet of Things devices exchange data without relying on a server or super node.
- **Tasks**
  - Establish the Peer-to-Peer hardware communication
  - Implement the cryptography to have secure communication between devices
- **Ongoing Work**
  - Utilizing ESP32 to establish P2P Network communication
- **Literature**
  - A. Nugraha Tama, H. Kusuma Wardana and S. Nugroho, "Gossip Algorithm Implementation for Network Protocol," 2018 International Seminar on Application for Technology of Information and Communication, Semarang, Indonesia, 2018, pp. 299-303, https://doi.org/10.1109/ISEMANTIC.2018.8549774
  - R. Karp, C. Schindelhauer, S. Shenker and B. Vocking, "Randomized rumor spreading," Proceedings 41st Annual Symposium on Foundations of Computer Science, Redondo Beach, CA, USA, 2000, pp. 565-574, doi: 10.1109/SFCS.2000.892324.
- **Supervisors**
  - Christian Schindelhauer, Saptadi Nugroho, Sneha Mohanty



Rumor Spreading and Graph Transformation

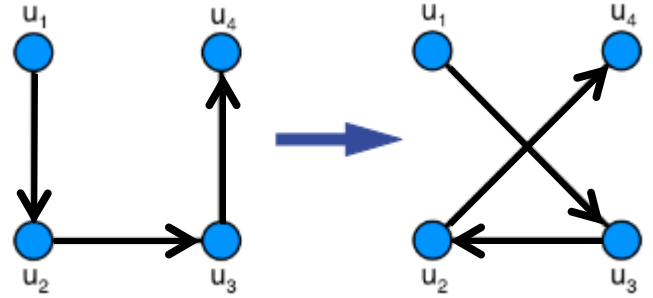
- **Tasks (theory/simulations)**
  - Combine Rumor Spreading (PushSum, PullSum, Push-PullSum) with Random Graph Transformations
  - Distributed Connectivity Tester
- **Literature**
  - Lecture P2P-Networks, S., Sommer 2023
  - George Giakkoupis. 2022. Expanders via local edge flips in quasilinear time. In Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2022). Association for Computing Machinery, New York, NY, USA, 64–76.
  - Giakkoupis, G., Sauerwald, T., Stauffer, A. (2014). Randomized Rumor Spreading in Dynamic Graphs. In: Esparza, J., Fraigniaud, P., Husfeldt, T., Koutsoupias, E. (eds) Automata, Languages, and Programming. ICALP 2014. Lecture Notes in Computer Science, vol 8573. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-43951-7_42
- **Supervisors**
  - Christian Schindelhauer
  - Saptadi Nugroho (saptadinugroho at gmail.com)

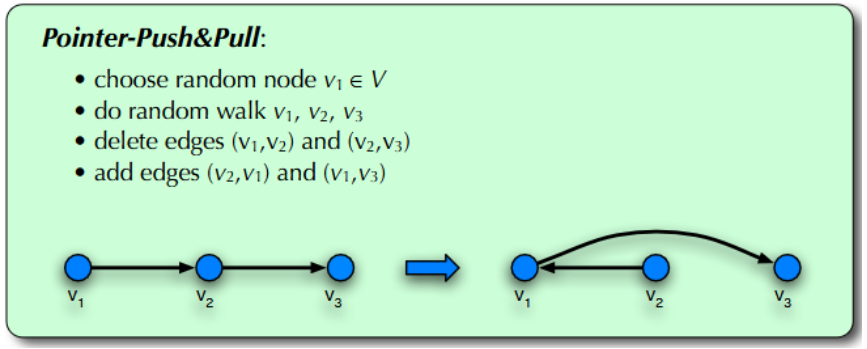


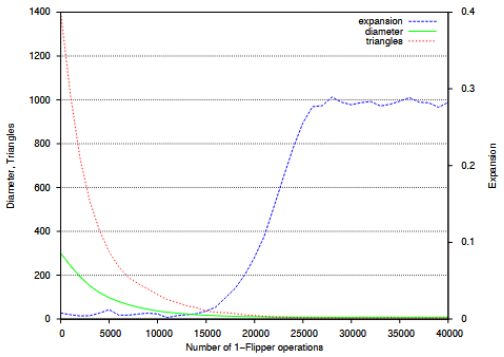


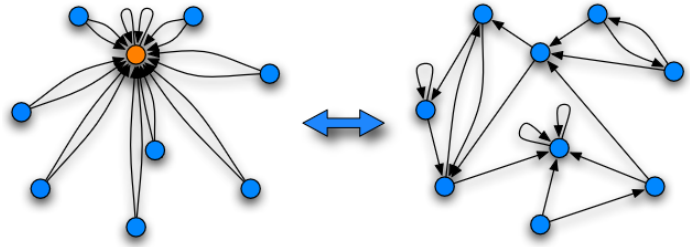
Random Directed Network Operations and Expanders

- **Questions**
  - Does Pointer-Push&Pull converge in time O(n log n)
  - Does directed Flipper converge fast?
- **Literature**
  - Csóka, E., & Grabowski, Ł. (2022). On directed analogues of expander and hyperfinite graph sequences. Combinatorics, Probability and Computing, 31(2), 184-197
  - George Giakkoupis. 2022. Expanders via local edge flips in quasilinear time. In Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2022). Association for Computing Machinery, New York, NY, USA, 64–76.
  - S. Nugroho and C. Schindelhauer, "DiFlip: Directed Flip-Chain Operation for Regular Directed Graph," 2024 International Symposium on Parallel Computing and Distributed Systems (PCDS), Singapore, Singapore, 2024, pp. 1-6, doi: 10.1109/PCDS61776.2024.10743739.
- **Supervisors**
  - Christian Schindelhauer
  - Saptadi Nugroho (saptadinugroho at gmail.com)



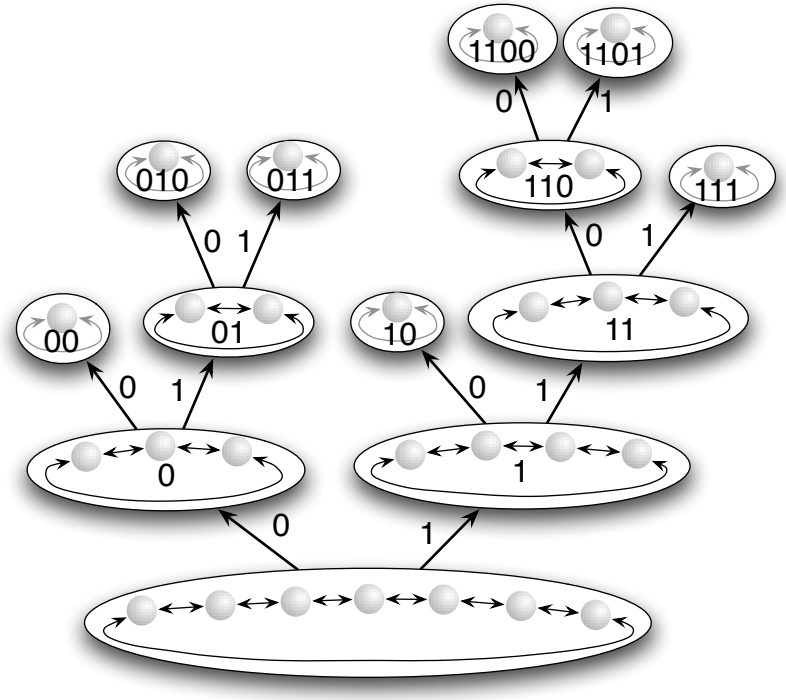


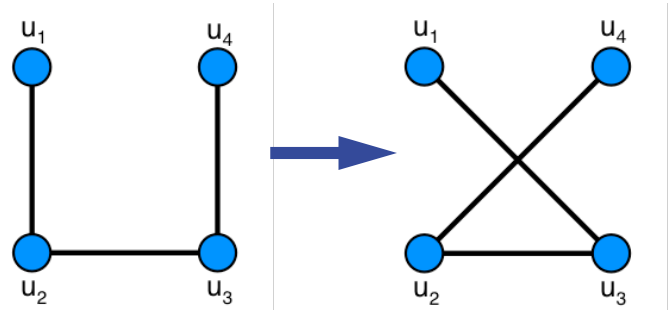




Self-Stabilization Flipping P2P

- **Task (Theory or Simulations)**
  - Self-Stabilizing SkipNet/3-Nuts (ongoing)/Kademlia
  - using Random Flip operations
- **Supervisors**
  - Christian Schindelhauer (schindel at informatik.uni-freiburg.de)
  - Saptadi Nugroho (saptadinugroho at gmail.com)





Expanders via Local Edge Flips in Quasilinear Time

George Giakkoupis
Inria, Univ Rennes, CNRS, IRISA
Rennes, France
george.giakkoupis@inria.fr

ABSTRACT

Mahlmann and Schindelhaue (2005) proposed the following simple process, called *flip-chain*, for transforming any given connected d-regular graph into a d-regular expander: In each step, a random 3-path $abcd$ is selected, and edges ab and cd are replaced by two new edges ac and bd, provided that ac and bd do not exist already. A motivation for the study of the flip-chain arises in the design of overlay networks, where it is common practice that adjacent nodes periodically exchange random neighbors, to maintain good connectivity properties. It is known that the flip-chain converges to the uniform distribution over connected d-regular graphs, and it is conjectured that an expander graph is obtained after $O(nd \log n)$ steps, w.h.p., where n is the number of vertices. However, the best known upper bound on the number of steps is $O(n^2 d^2 \sqrt{\log n})$, and the best bound on the mixing time of the chain is $O(n^{16} d^{36} \log n)$.

We provide a new analysis of a natural flip-chain instantiation, which shows that starting from any connected d-regular graph, for $d = \Omega(\log^2 n)$, an expander is obtained after $O(nd \log^2 n)$ steps, w.h.p. This result is tight within logarithmic factors, and almost matches the conjectured bound. Moreover, it justifies the use of edge flip operations in practice: for any d-regular graph with $d = \text{poly}(\log n)$, an expander is reached after each vertex participates in at most $\text{poly}(\log n)$ operations, w.h.p. Our analysis is arguably more elementary than previous approaches. It uses the novel notion of the *strain* of a cut, a value that depends both on the crossing edges and their adjacent edges. By keeping track of the cut strains, we form a recursive argument that bounds the time before all sets of a given size have large expansion, after all smaller sets have already attained large expansion.

ACM Reference Format:
George Giakkoupis. 2022. Expanders via Local Edge Flips in Quasilinear Time. In *Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing (STOC '22), June 20–24, 2022, Rome, Italy.* ACM, New York, NY, USA, 13 pages. https://doi.org/10.1145/3519935.3520022

1 INTRODUCTION

In [24], Mahlmann and Schindelhaue proposed a very simple and elegant process to transform any given connected d-regular graph into a d-regular expander.[1] This process consists of a sequence of *flip operations*. A flip operation on graph $G = (V, E)$ chooses a 3-path $abcd$ of G u.a.r., and if neither of the edges ac and bd exist already, then edges ab and cd are removed, and are replaced by edges ac and bd; otherwise, the operation does not modify the graph.

A flip operation does not change the degrees of vertices, and does not disconnect a connected graph. Moreover, it is a very *local* operation, as it affects only four vertices, at distance at most three apart. This is minimal, in the sense that no edge switching operation involving fewer than four vertices preserves the degrees, and the only shallower subgraph than a 3-path is the 3-star, for which there are no degree-preserving operations [6].

The Markov chain $(G_t = (V, E_t))_{t \in \mathbb{N}_0}$ induced by a sequence of flip operations is called a *flip-chain*, and it converges to the uniform distribution over all connected d-regular graphs on V, if the initial graph $G_0 = (V, E_0)$ is connected and d-regular [24]. Moreover, based on experimental evidence, it has been conjectured that $t = O(nd \log n)$ operations suffice to ensure that graph G_t is an expander w.h.p. [23, 24].

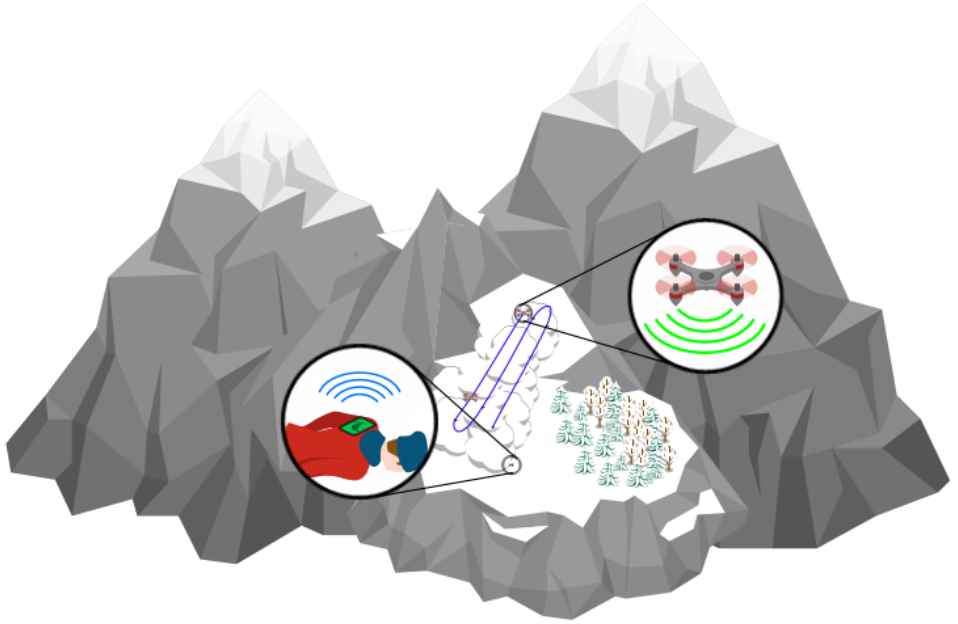
A motivation for the study of flip-chains arises in the design of

Telocate

Professional Localization

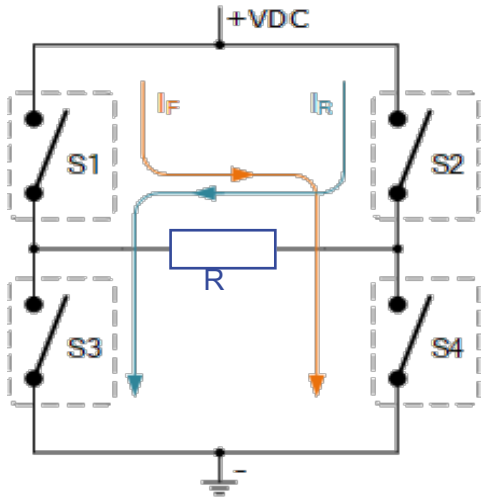
avaRES

- **Accelerate and make safer the detection and localization of missing or buried persons, especially in winter, by means of an autonomously flying search-radar system**
- Goal:
  - Locate a linear transponder using an I/Q Doppler radar attached to a drone
  - Estimate drone absolute localization and attitude estimation using GNSS and IMU data
  - Data fusion, estimation of optimal rescue trajectory
- Contact:
  - Joan Bordoy bordoy at informatik.uni-freiburg.de
  - Johannes Wendeberg



Bidirectional PWM Control Scheme

- **Development of an Embedded System for Generating a Bidirectional PWM Current to Control the Heating Process of a Resistive Heating Element**
- Goal:
  - System based on H-bridge topology to generate bidirectional heating current for preventing platinum migration in a thin-film heating element
  - Adequate control scheme through soft- or hardware to avoid shoot-through when switching the current direction
  - Simultaneous heating of the element and sensorless temperature estimation to enable real-time temperature control
  - Design and evaluation of soft- and hardware components
- Contact:
  - Joan Bordoy bordoy at informatik.uni-freiburg.de
  - Johannes Wendeberg



https://www.electronics-tutorials.ws/io/h-bridge-circuit.html

FOOTPRINT

- **Collection of materials, machines and traffic flows for the calculation of the CO2 footprint of road construction site**
- Goal
  - Estimate and reduce CO2 footprint of road construction sites
  - Ultra-wideband (UWB) localization, inertial measurement units (IMUs) and GPS to detect machine usage
  - Light Detection and Ranging (LiDAR) to detect traffic
  - Analyze data, fuse sensors, detect inefficiencies
- Contact:
  - Joan Bordoy bordoy at informatik.uni-freiburg.de
  - Johannes Wendeberg

FreiburgResist

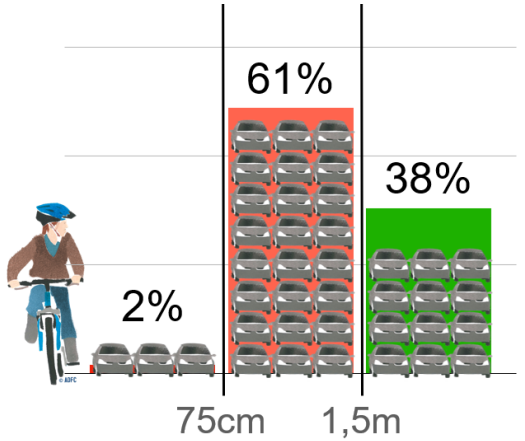
- **A system for enhancing municipal resilience at large-scale events.**
- Goal:
  - Estimate location and movement of crowds
  - Privacy and data security are crucial
  - Paxcounters in the city, data anonymized and sent to gateway
  - Analyze validity of recorded data, data forwarding and storage, bloom filter flow/volume, forecasting
- Contact:
  - Joan Bordoy

    bordoy at informatik.uni-freiburg.de
  - Johannes Wendeberg

Patrick Seeger/Stadt Freiburg

Bicycle Overtaking Distance Estimation

- **Distance and risk detection between bicycles and cars to reduce collisions and near-misses using a time-of-flight camera.**
- Goal:
  - Detect bicycles and vehicles
  - Estimate range and relative speed
  - Classify risk
- Contact:
  - Joan Bordoy <bordoy at informatik.uni-freiburg.de>
  - Johannes Wendeberg

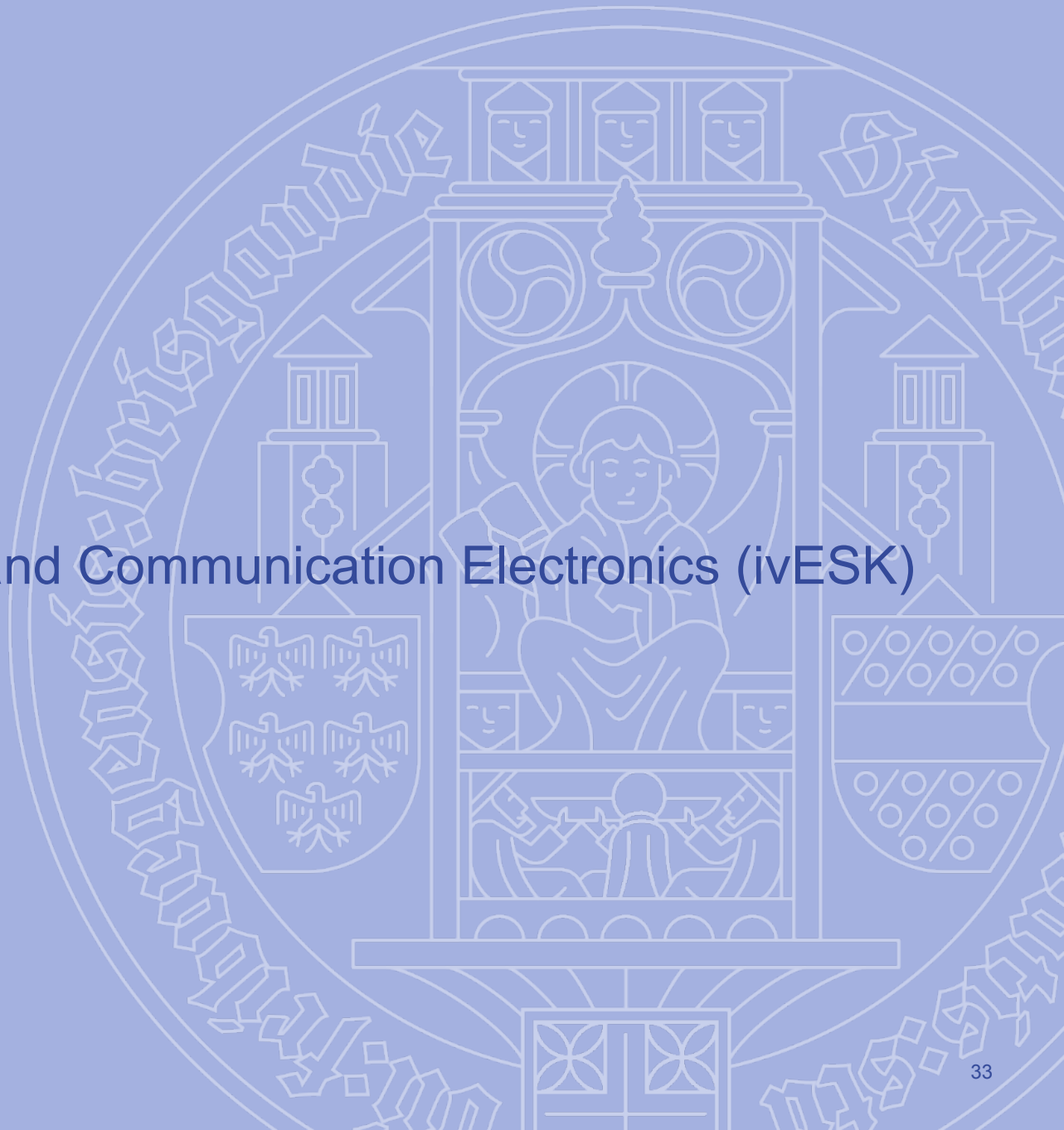


https://dachau.adfc.de/artikel/abstandsmessungen-mit-dem-openbikesensor

https://en.wikipedia.org/wiki/Time-of-flight_camera

Axel Sikora

Institute of Reliable Embedded Systems and Communication Electronics (ivESK)



CANsec demonstrator
for layer 2 protected CAN-based

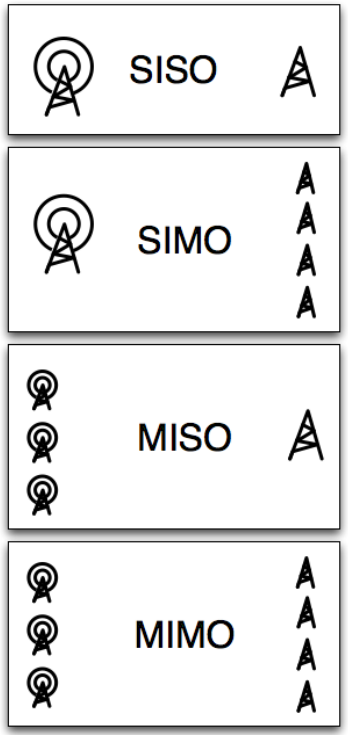
- **ivESK research focus**
  - Projects on **Controller-Area-Network (CAN)**-based communication and cybersecurity in connected, automated vehicles.
- **Key challenges and solutions**
  - Traditional CAN networks are reliable but lack built-in security.
  - With the rise of attacks, CANsec, inspired by Ethernet MACsec (IEEE 802.1AE), is proposed to ensure
    - integrity,
    - authenticity, and
    - confidentiality.
- **Tasks**
  - **Implement and test CANsec on real CAN XL hardware** to assess performance.
  - **Develop a demonstrator** as a reference for future standards and secure-by-design automotive networks.
- **Contact**
  - Institute of Reliable Embedded Systems and Communication Electronics (ivESK), Offenburg University of Applied Sciences
    - https://ivesk.hs-offenburg.de/en/article/prof-dr-axel-sikora-assoziierter-hochschullehrer
  - Prof. Dr.-Ing. Ing. Axel Sikora
    - axel(dot)sikora(at)hs(dash)offenburg(dot).de

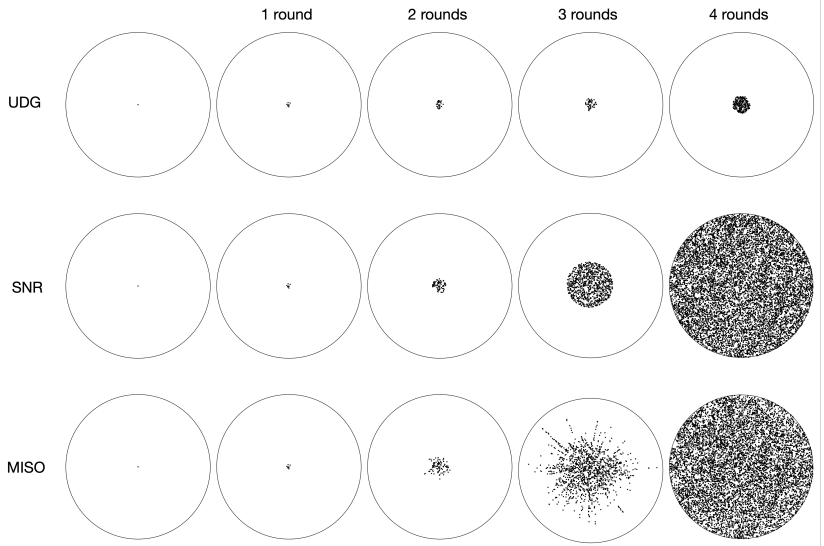
MIMO and Near-Field

Understanding the physical foundations of communication

MIMO

- **Tasks (theoretically/practical)**
  - Is there a MIMO-Multicast with Multiplexing Gain
  - Parallel broadcast in 3D
  - Concurrent Multicast with multiplexing gain/diversity gain tradeoff
- **Literature**
  - S., C., Oak, A. and Janson, T., 2019, September. Collaborative Broadcast in O(log log n) Rounds. In International Symposium on Algorithms and Experiments for Sensor Systems, Wireless Networks and Distributed Robotics (pp. 119-136). Cham: Springer International Publishing.
  - S., Lecture Algorithms for Wireless Communication, 2022
  - Thomas Janson, Energy-Efficient Collaborative Beamforming in Wireless Ad Hoc Networks, 2015
  - Tim Mugele, Simulation and Analysis of Different Variants of a Collaborative Broadcast Algorithm Regarding Different Path-Loss-Models, Bachelor Thesis, 2020
- **Supervisor:**
  - Christian Schindelhauer & Peter Krämer

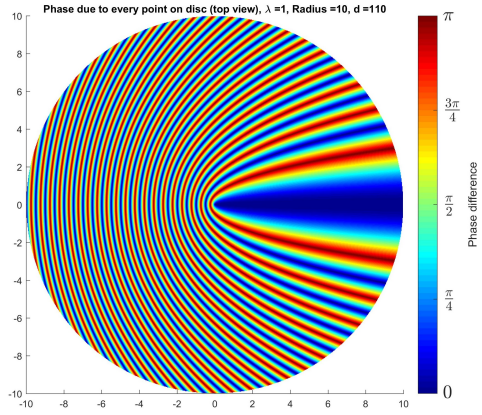




- MIMO capacity (with waterfilling)

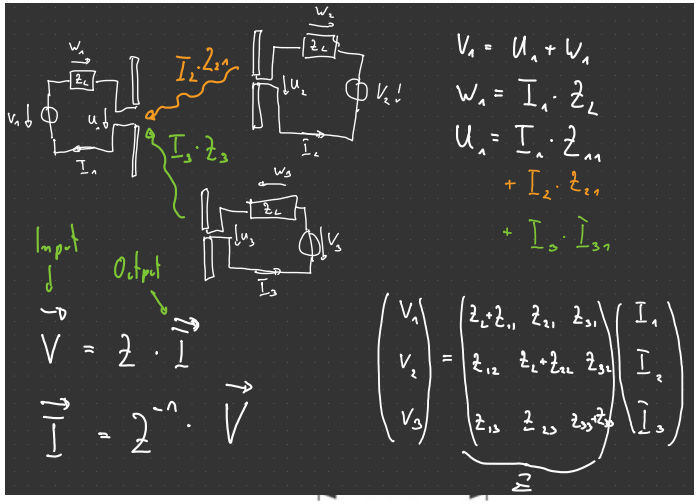
$$C = \sum_{i=1}^{n_{\min}} \log_2 \left(1 + \frac{P_i \lambda_i^2}{N_0} \right)$$

- with $P_i = \left[\mu - \frac{N_0}{\lambda_i^2} \right]^+$



Near-Field Antenna Fields.

- **Questions**
  - Test of the validity of near-field models
    - Zuhrt, Balanis, Hertz Model
    - Eigenvalues, Eigenmodes
  - Do Near-Field models scale?
- **Tasks**
  - Simulation of large antenna fields in the Near-Field
  - Finding worst case position for near-field communication
  - General Near-Field-Simulator
- **Literature**
  - Krämer, P. and Schindelhauer, C., 2024, September. Critical near-field impedance matrices. In 2024 International Symposium ELMAR (pp. 81-84). IEEE
  - Bundy, M. „A General Model of the Mutual Impedance between Hertzian Dipoles“, Bachelorarbeit, Uni Freiburg, 2025
- **Supervisor**:
  - Christian Schindelhauer & Peter Krämer



Zuhrt's Model

$$Z_{nm} = R_{nm} + iX_{nm}$$

$$A = k_0\sqrt{a^2+b^2}+b \qquad \bar{A} = k_0\sqrt{a^2+b^2}-b$$

$$B = k_0\sqrt{a^2+(b-l)^2}+(b-l) \qquad \bar{B} = k_0\sqrt{a^2+(b-l)^2}-(b-l)$$

$$C = k_0\sqrt{a^2+(b+l)^2}+(b+l) \qquad \bar{C} = k_0\sqrt{a^2+(b+l)^2}-(b+l)$$

$$\frac{8\pi R_{nm}}{Z_0} = -\cos(k_0 b)\left[-2\mathrm{Ci}(A)-2\mathrm{Ci}(A')+\mathrm{Ci}(B)+\mathrm{Ci}(B')+\mathrm{Ci}(C)+\mathrm{Ci}(C')\right]+$$
$$+\sin(k_0 b)\left[2\mathrm{Si}(A)-2\mathrm{Si}(A')-\mathrm{Si}(B)+\mathrm{Si}(B')-\mathrm{Si}(C)+\mathrm{Si}(C')\right]$$

$$\frac{8\pi X_{nm}}{Z_0} = -\cos(k_0 b)\left[2\mathrm{Si}(A)+2\mathrm{Si}(A')-\mathrm{Si}(B)-\mathrm{Si}(B')-\mathrm{Si}(C)-\mathrm{Si}(C')\right]+$$
$$+\sin(k_0 b)\left[2\mathrm{Ci}(A)-2\mathrm{Ci}(A')-\mathrm{Ci}(B)+\mathrm{Ci}(B')-\mathrm{Ci}(C)+\mathrm{Ci}(C')\right]$$

Hertz's Model

$$Z_{nm} = \frac{3}{2}R_{nn}\left[\left(\frac{sinx}{x}+\frac{cosx}{x^2}-\frac{sinx}{x^3}\right)+j\left(\frac{cosx}{x}-\frac{sinx}{x^2}-\frac{cosx}{x^3}\right)\right]$$

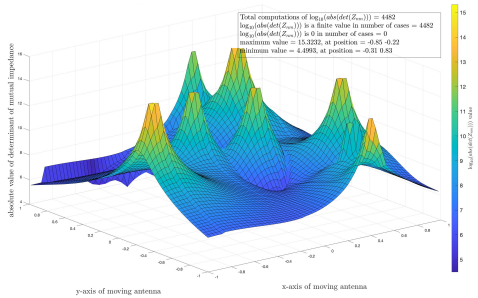
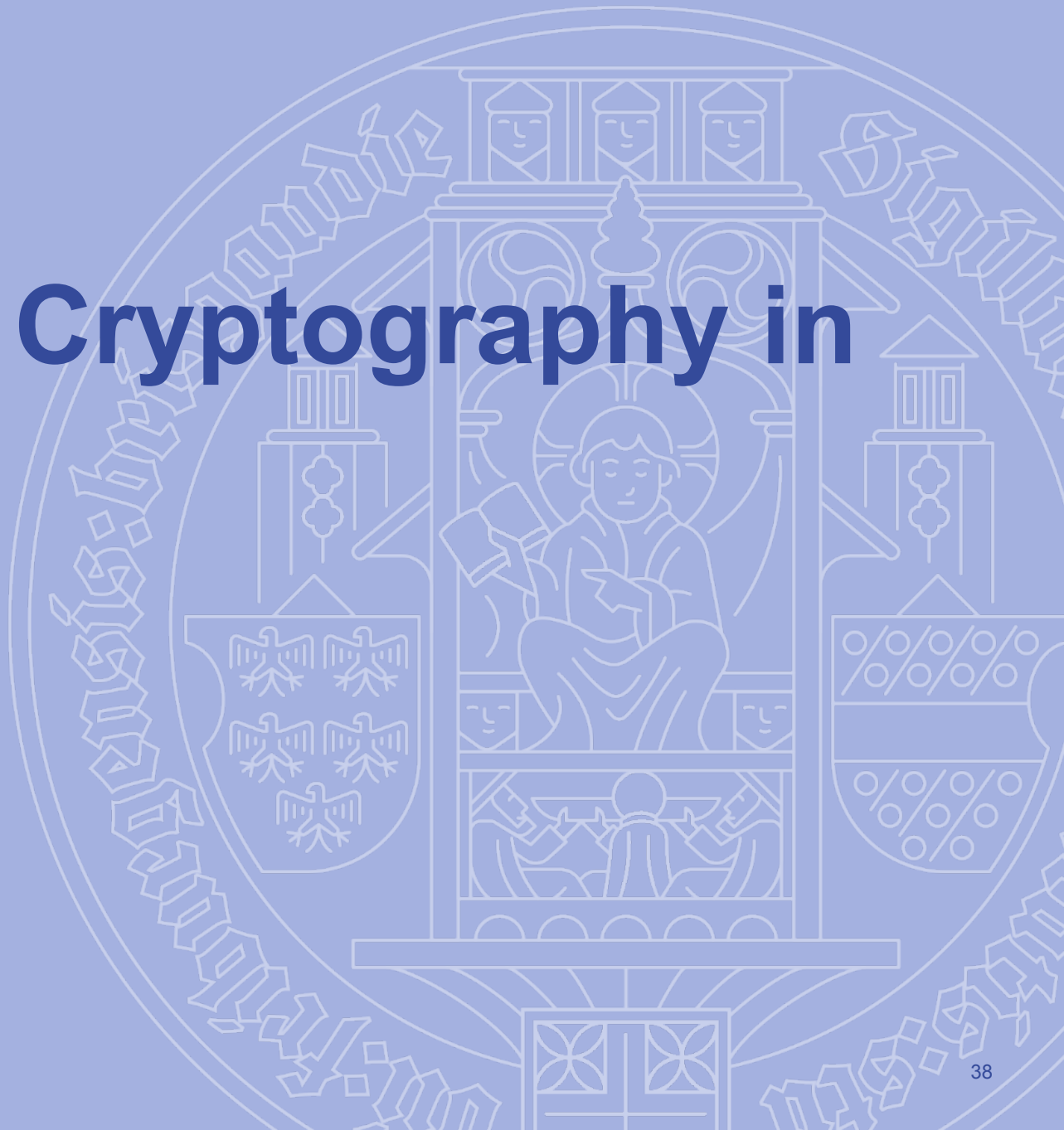


Figure 20: 3D surface plot of the computations of the logarithm of the absolute value of the $|Z_{nm}|$ is plotted against all the possible positions with respect to the 8 fixed dipoles in all of the instances.

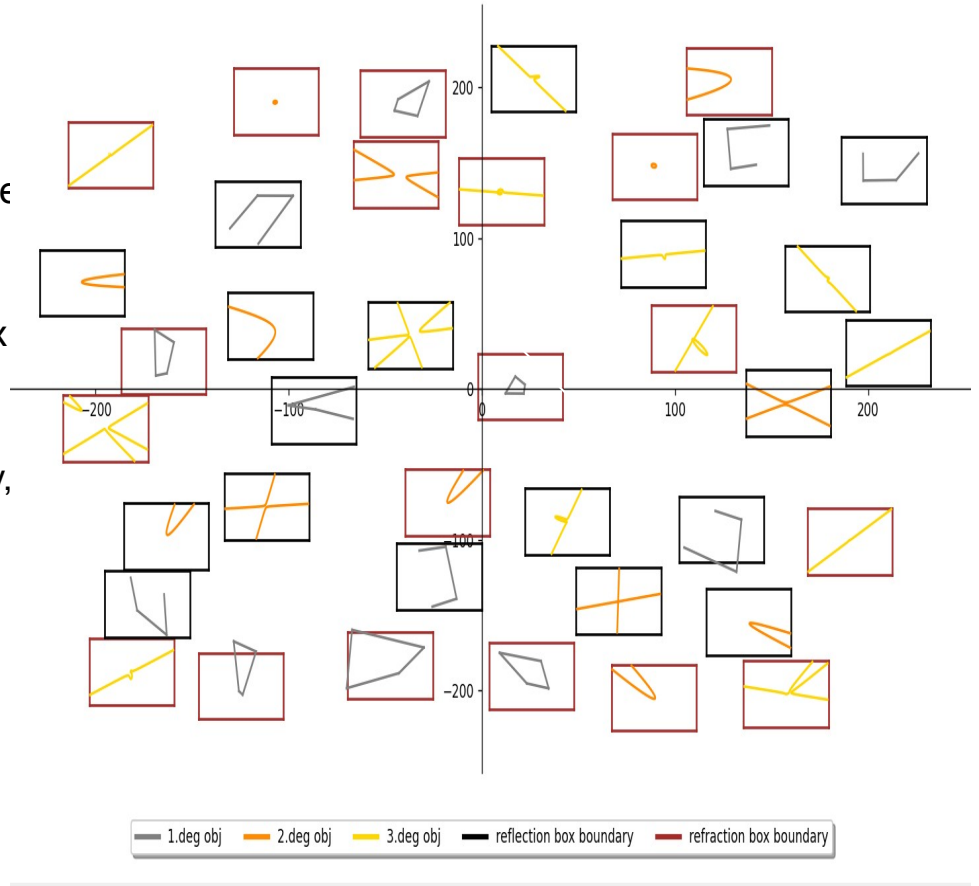
Ray Tracing based Cryptography in 2D/3D

Sneha Mohanty

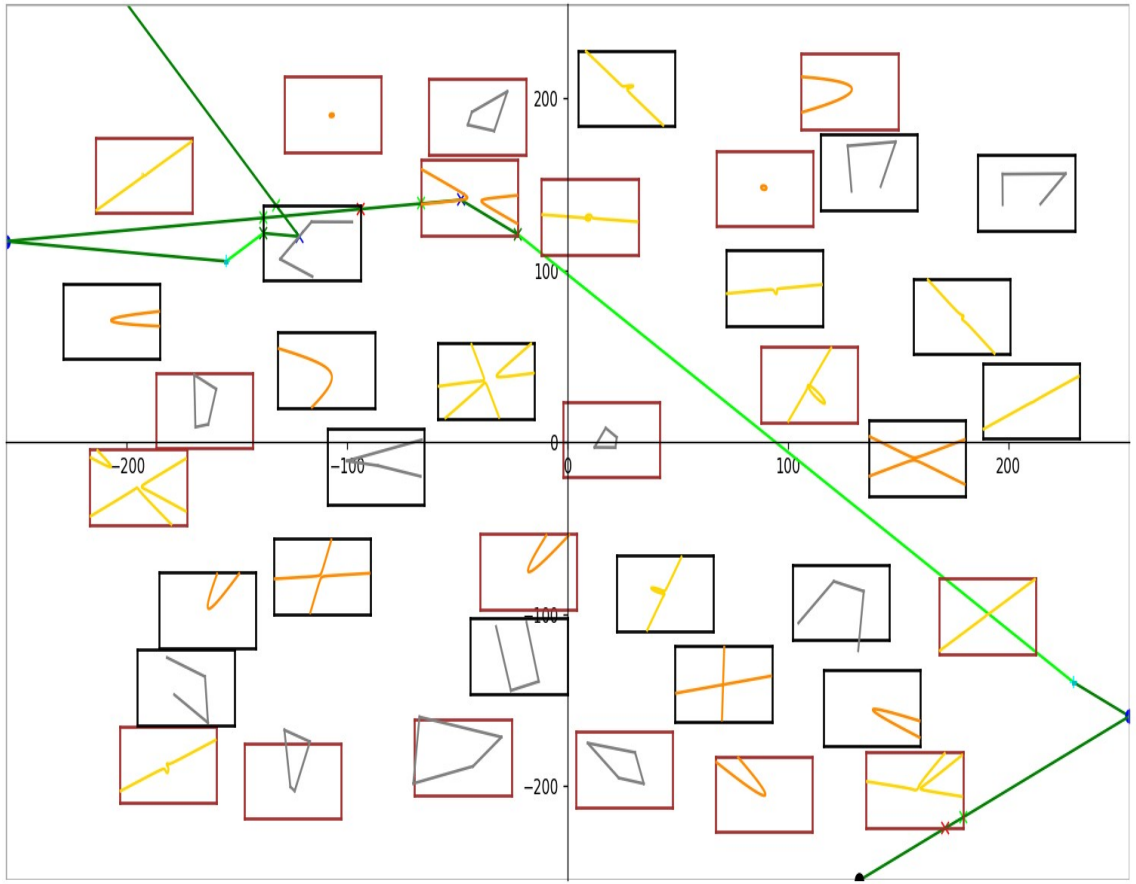


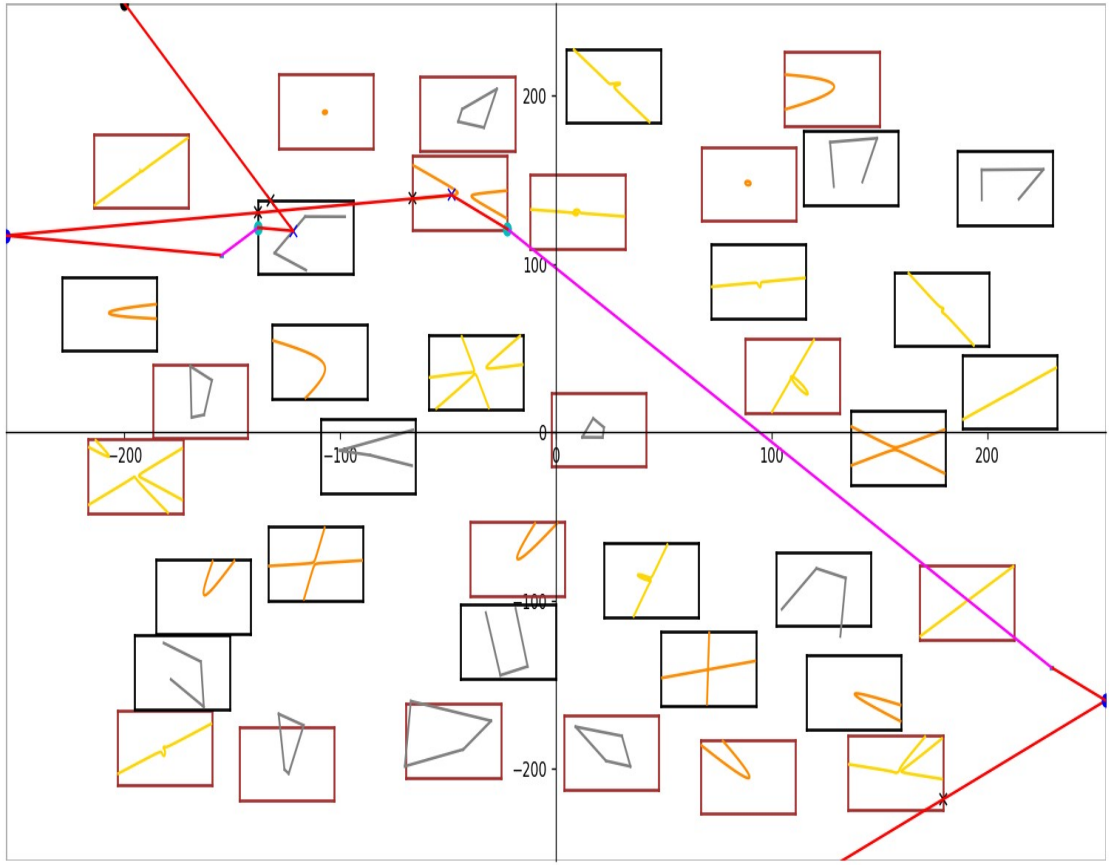
Key Components and Processes

- **Novel symmetric key cryptographic system.**
  - Global Bounding box in 2D/3D cartesian coordinate system (in x,y and z axe
  - Several Local bounding boxes
  - At most one polynomial of 1st, 2nd or 3rd degree within Local bounding box
- **During encryption,**
  - the light ray vector starts at the boundary of the Global bounding box at (x,y,
  - alternating interaction between polynomials and boolean gate (XOR).
  - The light ray vector then exits at (x,y, dx,dy).
  - This is stored as the Ciphertext of the cryptographic scheme.
- **During decryption,**
  - the light ray retraces its way back,
  - from the final exit point to the initial Plaintext.
  - This marks the end of decryption.

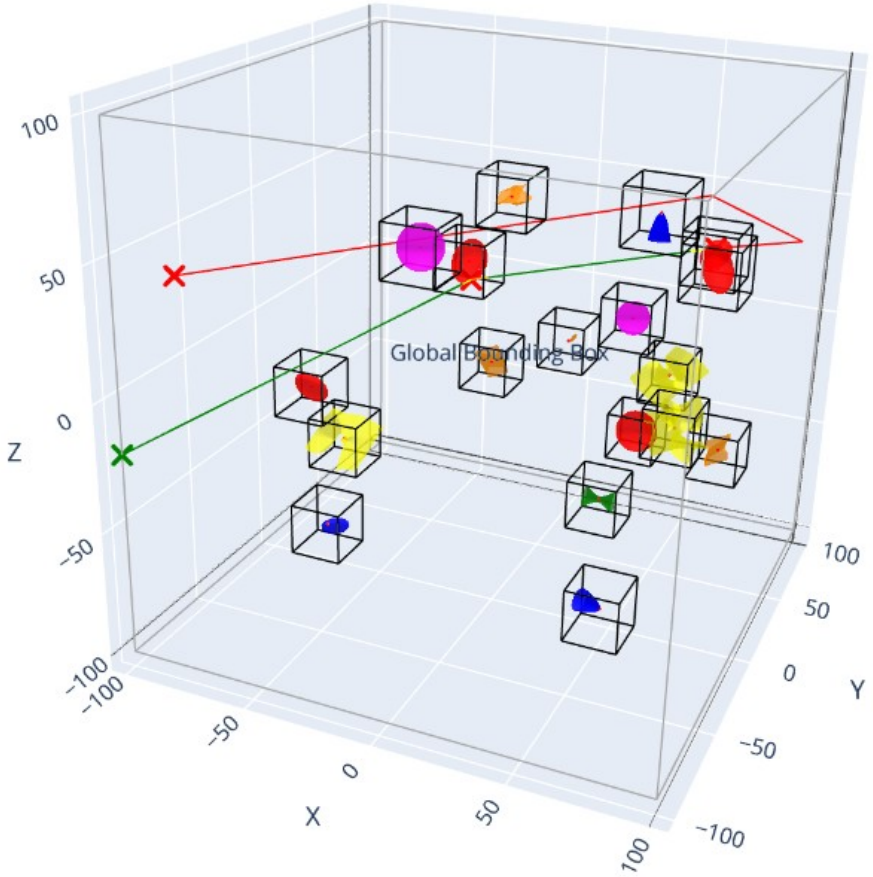


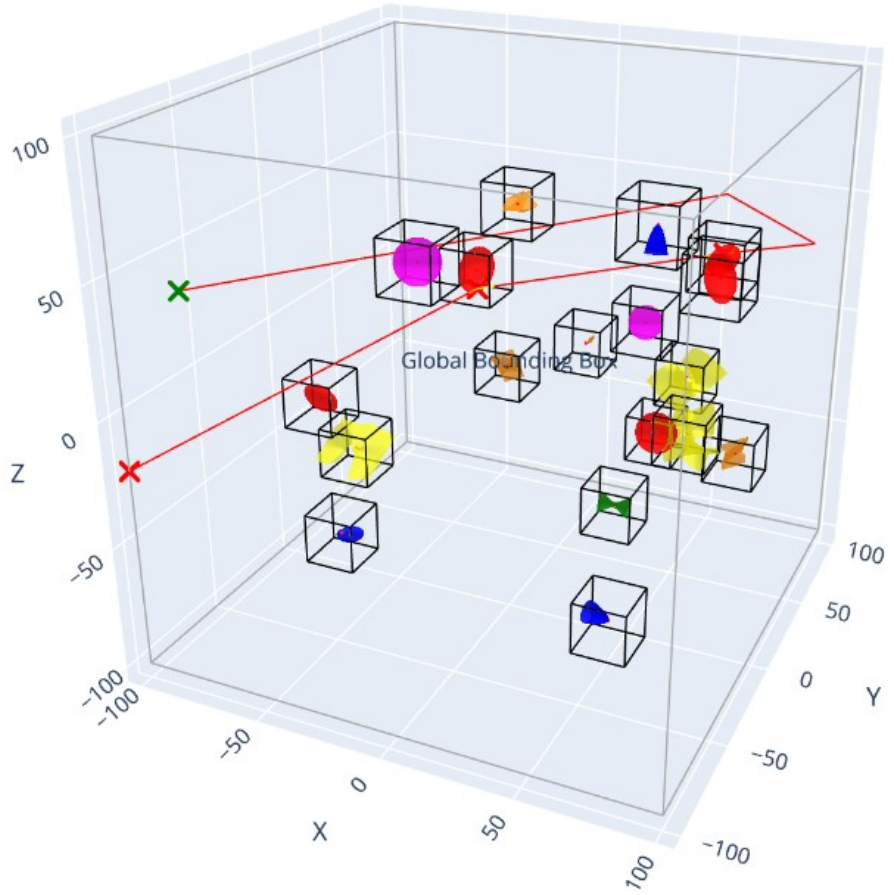
Sample Encryption-Decryption in 2D





Sample Encryption-Decryption in 3D





Open Questions

- **Mathematical (Theory based) :**
  1. A mathematically rigorous **comparison** between our proposed cryptosystem with other **established Symmetric Key Crypto** systems in the industry,
     - such as AES and ChaCha (or rather, other analog cryptographic systems)
     - what additional aspects are fulfilled by us, that were lacking in these or exactly 'what' we have achieved with our novel cryptosystem
  2. the **reduction** of our construction to a **pre-established hardness assumption**
  3. what is the **efficiency** of our cryptosystem as far as encryption and decryption are concerned ?
     - Does it lead to too much computational overhead, vis-a-vis the other standard SKE systems?
     - in that case, is it impractical to use our crypto system in the industry due to the huge overhead?
- **Simulation :**
  1. **Precision handling** in 3D (some buffer bits)
  2. Adding **refraction** to the codebase in 3D

Cryptography

Mental Card Games and Peer-to-Peer

Tasks: Mental Card Games

- **Vision:**
  - **Implement the most efficient Mental Card Game**
  - **on a Smartphone**
- **Tasks**
  - **How to start a Mental Card Game**
    - Finding tables, sharing keys
  - The **Software Architecture** of a Mental Card Game build on mobile Devices
    - Money, Rule Breaking
  - **Game Description Languages**
    - automatic visualization of rules
    - interpretation of GDL
  - Mental Card Games based on **other crypto systems**
    - Paillier, RSA,
    - Lattice Codes (implementation only),
    - Vernam, Quantum Communication
    - Private Computation and Commitments
  - **Communication Layer of Mental Card Games**
    - How to build a Reliable Forum system
    - Reaktionstest (Lightning Reaction Extreme)
  - **Phone-to-phone communication** in Rust for Mental Card Games
    - P2P (ongoing)
    - Bluetooth, NFC
    - WiFi Direct
    - QR Codes (ongoing)
  - **Supervisor**:
    - Christian Schindelhauer

Theses and Projects at CoNe
Thanks for your Attention

Christian Schindelhauer
Rechnernetze und Telematik
Institut für Informatik
Technische Fakultät
schindel(at)tf.uni-freiburg.de

Sneha Mohanty
Rechnernetze und Telematik
Institut für Informatik
Technische Fakultät
mohanty(at)informatik.uni-freiburg.de