Contents

About

In this booklet, you will find all the information concerning our upcoming open-seminar. Including the schedule, the abstracts and useful information on the organisation and the location.

Location

As is customary, we will hold our open-seminar in March. As a change compared to previous times, we will do it over two days: one day of presentations and one day in Weil der Stadt.

Weil der Stadt

Weil der Stadt is a town of about 19,000 inhabitants, located in Baden-Württemberg. It is about 30 km west of Stuttgart city centre, in the valley of the River Würm, and is often called the "Gate to the Black Forest".

The name Weil derives from the Latin word villa, an estate or manor. The suffix die Stadt (the town) was added to distinguish Weil from various nearby villages of the same name, such as Weil im Dorf and Weil im Schönbuch. The modern name is unusual in that it contains the dative article der rather than the nominative article die. This quirk arose because place names typically come after prepositions that govern the dative case in German, such as in or aus. The Roman origins of the town are immortalized in its coat of arms, which features the motto SPQR.

The village of Wile was first mentioned in 1075, and described as the property of the famous abbey of Hirsau. Weil der Stadt became a Free Imperial City in the 13th century, but had existed for centuries before as an important trading place.

The city was completely destroyed during the Thirty Years' War in 1648 but was subsequently rebuilt, and is still dominated by buildings from this period. The city's fortifications have survived largely intact, with city walls, gates, and several towers.

Weil der Stadt is best known as the birthplace of the astronomer Johannes Kepler (1571–1630), and it bears the unofficial title of Keplerstadt, or Kepler town. Another famous son is the Protestant reformer Johannes Brenz (1499–1570). Due to its surroundings and attractive cityscape, dominated by the church steeple of St. Peter and Paul, Weil der Stadt is a popular destination for excursions in the Stuttgart region.

Organisation

The open-seminar will spread over 2 days: one day of presentation at the institute and one day in Weil der Stadt. Each talk will be 20 minutes, followed by another 20 minutes of questions and/or discussions (with the exception of the first presentation). The schedule is available below, as well as the abstracts.

As it will be a long day of presentations, so please stick to **20 minutes presentations**.

Social Event

On the second day, we will go for a hike in Weil der Stadt. The hike is called Johannes-Kepler-Planetenweg, as it goes through several points of interests, which are named after our solar system's planets. The complete Planetenweg is however around 24km as a round trip, so we will only go through slightly less than half of it and then take a more scenic route on the way back to Weil der Stadt for lunch.

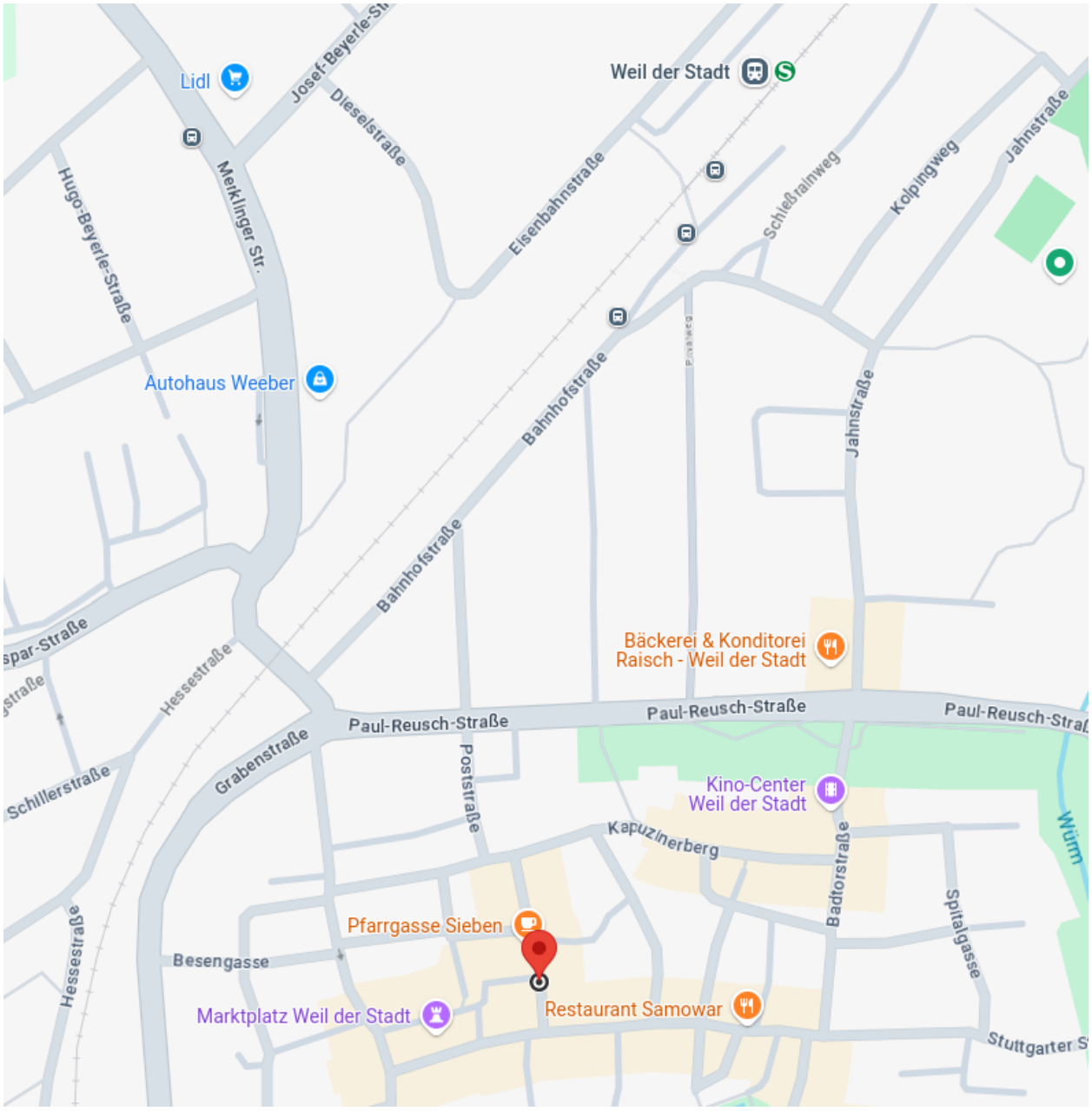
Here is a link to the description of the hike: Planetenweg.

We will have lunch at the Russian restaurant Samowar.

Travel

The first day will be in our seminar room, which you all know. On the second day, we will meet in Weil der Stadt which is reachable by S-Bahn (S6). Please be there on time on both days.

Below is a map of Weil der Stadt. The red pin is where we meet. Directly above, you can see the S-Bahn station. The meeting point is the sun (Sonne), which you can find on the previous link's PDF (downloadable at the bottom of the page).


Lidl
Josef-Beyerle-Straße
Dieselstraße
Weil der Stadt
Hugo-Beyerle-Straße
Merklinger Str.
Eisenbahnstraße
Schießrainweg
Kolpingweg
Jahnstraße
Autohaus Weeber
Bahnhofstraße
Jahnstraße
Bahnhofstraße
Bäckerei & Konditorei
Raisch - Weil der Stadt
Hessestraße
Paul-Reusch-Straße
Paul-Reusch-Straße
Paul-Reusch-Straße
Grabenstraße
Poststraße
Kino-Center
Weil der Stadt
Schillerstraße
Kapuzinerberg
Würm
Badtorstraße
Spitalgasse
Pfarrgasse Sieben
Besengasse
Hessestraße
Marktplatz Weil der Stadt
Restaurant Samowar
Stuttgarter

Timetable

Tuesday, 11th of March

08:45–09:00	Orga.	**Maël Gay**	Opening Session
09:00–10:00	Talk	**Devanshi Upadhyaya**	Secure Cryptographic Hardware: Assessing Logic-Locking and Fault Attack Vulnerabilities
10:00–10:40	Talk	**Tarick Welling**	Side Channel Security of Pointwise Multiplication in an FPGA Implementation of Crystals-kyber
10:40–11:20	Talk	**Li-Wei Chen**	PINI to memristive PINI: Leveraging the in-Memory Computing
11:20–12:00	Talk	**Felix Bayhurst**	Synthesis for Mixed-Mode Memristive Circuits based on Boolean Decomposition
12:00–13:00	**Lunch Break**		
13:00–13:40	Talk	**Nourhan Elhamawy**	System-Level Test for Multi-Time Frame Faults
13:40–14:20	Talk	**Denis Schwachhofer**	Comparison of Multiple Methods for System-Level Test Program Generation Targeting Non-functional Properties
14:20:–15:00	Talk	**Anand Venkatachalam**	Automated Test Equipment Drift Characterization Based on Gauge Repeatability and Reproducibility
15:00–15:40	Talk	**Karthik Pandaram**	ML-based Detection of Marginal Defects
15:40–16:00	**Afternoon break**		
16:00–16:40	Talk	**Roshwin Sengupta**	Low-Power Continuous Wavelet Transform Employing Stochastic Computing
16:40–17:20	Talk	**Biswash Ghimire**	Neutral-Atom Architecture and the Qubit Mapping Problem
17:20–17:30	Orga.	**Maël Gay**	Closing Session

Wednesday, 12th of March

09:00–09:00	**Meet in Weil der Stadt (Sun/Sonne)**
09:00–12:00	**Planetenweg Hike**
12:00–13:00	**Lunch at restaurant Samowar**
13:00–16:00	**Free Time in Weil der Stadt**

List of Abstracts

Tuesday, 11th of March

Secure Cryptographic Hardware: Assessing Logic-Locking and Fault Attack Vulnerabilities

Devanshi Upadhyaya

Safeguarding hardware implementations of cryptographic primitives from physical attacks and supply-chain threats continues to present a significant challenge. This work examines the vulnerabilities of cryptographic hardware to fault attacks and raises essential questions regarding the "secure composability" of various countermeasures, specifically focusing on logic locking—a widely adopted design-for-trust technique aimed at protecting hardware against intellectual property theft and overproduction.

Side Channel Security of Pointwise Multiplication in an FPGA Implementation of Crystals-kyber

Tarick Welling

Quantum Computers are expected to be able to solve hard problems such as prime number factorization using Shor's algorithm in the coming decades. The adoption of Quantum Computing safe cryptographic primitives has progressed to the point that several candidates from the NIST Post-Quantum Cryptography standardization project have been adopted. We know that this subset of primitives will be deployed in real-world systems. As such the need for understanding in the realm of Side Channel Attacks on these primitives is increasing. A particular flaw of physical devices is the data dependent power consumption.

In this work we focus on a hardware implementation of crystals-Kyber KEM (a module learning with errors lattice based Key Exchange Mechanism) and attack the pointwise polynomial multiplication during decryption. We employ an unprofiled Correlation Power Analysis using the pearson correlation.

PINI to memristive PINI: Leveraging the in-Memory Computing

Li-Wei Chen

Probe-isolating Non-interference(PINI) is a secure notion that a secure gadget is composable and their combination remains secure. The basic idea is that information accessed by one probe cannot review more than one share of the data. We extend this secure notion into the memristor domain while considering the memristor's feature. In this work, we protect the memristive cryptographic circuit using DOMSbox and demonstrate that our memristive DOMSbox is mPINI secure.

Synthesis for Mixed-Mode Memristive Circuits based on Boolean Decomposition

Felix Bayhurst

Different modes of operation can be combined on the same memristive cells, compensating for some of their individual disadvantages. Using conventional synthesis tools to do this does not lead to satisfactory results, as they struggle with the specific nature of the mixed-mode operations. We introduce a specialized Boolean decomposition approach that is able to create a graph-based representation of mixed-mode operations sufficiently quickly to be utilized in a scalable synthesis approach.

System-Level Test for Multi-Time Frame Faults

Nourhan Elhamawy

In an attempt to comprehend what System-Level Test detects which can not be detected by other structural & functional tests, the Multi-Time Frame faults seem to be a possible candidate for SLT-unique fails. Because the activation conditions require more than two clock cycles, we show tat some SLT workload is able to detect these faults in some cases.

Comparison of Multiple Methods for System-Level Test Program Generation Targeting Non-functional Properties

Denis Schwachhofer

System-Level Test (SLT) is crucial for evaluating integrated circuits as it can detect defects that traditional testing misses. Nowadays, test engineers manually compose test suites using off-the-shelf software. This process, however, is an arduous task and offers only limited control over non-functional properties. As such, it is of interest to research methods to automatically generate SLT programs. This work compares three methods for test program generation for SLT, specifically targeting non-functional properties, namely fuzzing, genetic programming, and Large Language Models (LLMs).

Automated Test Equipment Drift Characterization Based on Gauge Repeatability and Reproducibility

Anand Venkatachalam

Management of the measurement drift in Auto-mated Test Equipment (ATE) is essential for maintaining good measurement quality while minimizing test interruptions and keeping test costs in check. For the first time, we propose a method to characterize measurement drift that considers the data from both Device Under Test (DUT) and ATE. Proposed approach for ATE drift analysis leverages Gauge Repeatability and Reproducibility (GRR) as an observable. We present the first experimental results on a CAN Transceiver device that confirm that the relationship between GRR and ATE inaccuracies modelled by a-posteriori modifications of measured data, is linear for a broad range of different types of tests. We also discuss further potentials of applying the experimental findings to fine tune the process of ATE calibration and enhance yield analysis wherein a distinction is made out between process variation and measurement inaccuracy due to wearing calibration.

ML-based Detection of Marginal Defects

Karthik Pandaram

Marginal defects, such as high-resistance shorts or low-resistance opens, can be difficult to detect using conventional pass-fail testing methods. This is because their effects are often nearly indistinguishable from normal variations. However, identifying these defects is crucial for circuits that require high quality and for addressing concerns about early-life failures. In our research, we propose an alternative detection approach that involves evaluating multiple parametric responses of a circuit against a machine learning (ML) model.

Low-Power Continuous Wavelet Transform Employing Stochastic Computing

Roshwin Sengupta

The continuous wavelet transform (CWT) is essential for analyzing non-stationary signals in edge computing, but traditional implementations are limited by high power demands, particularly in resource-constrained environments. Stochastic computing (SC), which leverages probabilistic bit-streams and compact arithmetic units, provides a promising alternative for ultra-low-power CWT designs. However, such circuits are vulnerable to transient faults and involve careful power-reliability trade-offs. We comprehensively analyzed our design, which features a Sobol-based pseudo-random number source and accumulative parallel counter-based addition. In a fault-free environment, this design achieves an 84% power reduction over non-SC CWTs and a 37% reduction over other SC designs. It also achieves up to 64% area savings and reduces latency by 8×. Under a 30% fault rate, our design improves RMSE by 74% over binary CWTs and 32% over other SC implementations.

Neutral-Atom Architecture and the Qubit Mapping Problem

Biswash Ghimire

One of the major problems in today's noisy intermediate-scale quantum (NISQ) computers is the limited connectivity among available qubits. In circuit-based quantum computation, quantum programs in the form of quantum circuits assume all-to-all connectivity among qubits. A consequence of this discrepancy is that in general it is not possible to directly execute an arbitrary quantum circuit on NISQ computers. This is the so-called "qubit mapping problem." The standard solutions for sidestepping this problem involve dynamic mutation of the mapping between the circuit qubits and the physical qubits during the execution of the circuit.

This presentation is on the qubit mapping problem in the context of NISQ computers based on the neutral-atom architecture. The architecture offers unique features such as a large number of physical qubits, native multi-qubit gates, and physical displacements of qubits. The standard architecture-agnostic algorithms do not take into account these features for qubit mapping and thus produce inefficient solutions. We will discuss the ongoing efforts in incorporating architecture-aware features into the algorithms for the qubit-mapping problem.