

summary 2022

Open Script Labs Workshop

Bauhaus-Universität Weimar

Schwanseestraße 143

15. Juli
17–22 Uhr

16. Juli
14–17 Uhr

Professor*innen, Mitarbeitende und Student*innen des Fachbereichs Medieninformatik öffnen einen Abend und einen Nachmittag lang in der Schwanseestraße 143 ihre Arbeitsräume und Labore und präsentieren die neuesten Entwicklungen aus den Bereichen Digitale Medien, Computersysteme und Informationstechnologie.
www.uni-weimar.de/OLN

GEFÜHRTE TOUREN · GUIDED TOURS

Freitag, 15. Juli · Friday, 15 July

17 Uhr	Exklusive Alumni-Tour Anmeldung über alumni@uni-weimar.de
5 pm	Exclusive Alumni Tour Registration via alumni@uni-weimar.de
18 Uhr	Studentisch geführte Tour zu allen Projekten des Fachbereichs Medieninformatik
6 pm	Student-guided tour of all the projects of the Department of Computer Science

HUMAN-COMPUTER INTERACTION

Sally&Molly: Kinderbuch mit Echtzeit-Multiplayer-Mobile Augmented Reality.
Sally&Molly: A children's book with real-time multiplayer mobile augmented reality.

Teilnehmende · Participants	Gabriel De Ioannes Becker
Lehrende · Lecturers	Prof. Dr. Eva Hornecker
Raum · Room	2.40 – Beratungsraum

Das Buch »Sally&Molly« richtet sich an Kinder im Alter von fünf bis zehn Jahren. Dabei handelt es sich um eine Altsphase, in der Kinder von einer selbstbezogenen Weltanschauung zu sozialem Verständnis übergehen. Mit der mobilen AR bieten wir eine zweite Ebene und damit spielerische Aktivitäten zum Buch. Wir erforschen kooperative Echtzeit-Multiplayer-Mechaniken für Kinder mit mobiler AR. The book »Sally&Molly« is aimed at children aged five to ten. This is an age phase in which children move from a self-centred world view to social understanding. With mobile AR, we offer a second level and thus playful activities to the book. We explore cooperative real-time multiplayer mechanics for children with mobile AR.
www.sallymolly.com

Beyond Pink – Gender, Identity & Smartphones

Teilnehmende · Participants	Simisola Aremo, Sara Elhassan, Sophia Lick, Sophie Zaton, David Le
Lehrende · Lecturers	Prof. Dr. Eva Hornecker, Britta Schulte
Raum · Room	2.40 – Beratungsraum

Denken Sie über die Beziehung nach, die Sie zu Ihrem Smartphone haben. Stehen die Apps und integrierten Funktionen, die Sie nutzen oder die Personalisierung des Geräts in einer Beziehung zu Ihrer Geschlechtsidentität? Benutzen Sie Ihr Telefon aufgrund Ihrer Identität auf eine bestimmte Weise? Beeinflussen Ihre Identitäten, wofür und wie Sie Ihr Telefon nutzen? Dies sind nur einige der Fragen, mit denen wir uns in diesem Projekt beschäftigen und die wir zu beantworten versuchen. Die Praxis der Entwicklung digitaler Technologien wurde, wie viele andere Branchen auch, in der westlichen Welt lange Zeit von weißen Cis-Männern dominiert. Sprachassistenten, Textvorhersage und App-Design sind einige Beispiele für Smartphone-Funktionen, die stark von der männlichen Sicht beeinflusst wurden. In diesem Projekt diskutierte das Team aus HCI- und CS4DM-Studierenden feministische, queere und intersektionale HCI-Theorien sowie Designmethoden, die bei dem Versuch, die Verflechtungen des Smartphones mit dem Geschlecht und verschiedenen anderen Identitäten zu verstehen, nützlich sein können. Mit dem, was wir gelernt haben, hat jede*r von uns eine Forschungsstudie durchgeführt, um diesem Verständnis näher zu kommen, weil dies im Bereich der HCI das gerechte Design von Technologie fördern kann. Die Forschungsthemen umfassen die Bereiche Menstruation, Apps zur Finanzplanung, Dating-Apps und Sprachassistenten. Think about the relationship you have with your smartphone. Do the apps and built-in functions you use, or your personalization of it for example have any relationship with your gender identity? Do you use your phone in a certain way because of your identities? Do your identities influence what you use your phone for and how? These are just some of the questions we address and try to answer in this project. The practice of designing digital technologies, like many other industries, has been long dominated by white cis men in the western world. Voice assistants, predictive texting, and app design are a few examples of smartphone features that have been heavily influenced by male bias. In this project, our team of HCI and CS4DM students discussed Feminist, Queer, and Intersectional HCI theories as well as design methods that can be useful in our attempt to understand the intertwining connections the smartphone has with gender and various other identities. Using what we've learned, each of us conducted a research study to get closer to this understanding, because doing so in the field of HCI can encourage the equitable design of technology. Our research spans the topics of menstruation, financial literacy apps, dating apps, and voice assistants.

Daten mit anderen Sinnen wahrnehmen
Perceiving data with other senses

Teilnehmende · Participants	Julien Breunig
Lehrende · Lecturers	Prof. Dr. Eva Hornecker, Rosa van Koningsbruggen
Raum · Room	2.40 – Beratungsraum

Wenn wir mit Daten konfrontiert werden, geschieht dies fast immer in Form von Grafiken mit Diagrammen und Tabellen und vielen Zahlen. Dabei haben wir noch mehr Sinne, die wir nutzen, um Informationen in unserer Umgebung wahrzunehmen. Nicht alles lässt sich immer einfach in Zahlen ausdrücken bzw. die Zahlen lassen sich nicht immer einfach interpretieren. Wie wäre es stattdessen mit Vibration, mit Tönen oder mit Licht? Welche Eigenschaften schreiben wir diesen Modalitäten zu und für welche Daten sind sie als Darstellungsform gut geeignet? When we are confronted with data, it is almost always in the form of graphs with charts and tables and lots of numbers. Yet we have even more senses that we use to perceive information in our environment. Not everything can always be easily expressed in numbers or the numbers cannot always be easily interpreted. What about vibration, sound or light instead? What properties do we ascribe to these modalities and for which data are they well suited as a form of representation?

Developing mobile technology facilitating international students settling in Weimar

Teilnehmende · Participants	Tahmina Arab
Lehrende · Lecturers	Prof. Dr. Eva Hornecker
Raum · Room	2.40 – Beratungsraum

Bei diesem Projekt handelt es sich um eine englischsprachige Abschlussarbeit: The informational and social needs of international students that are met through technology when arriving in another country.

Future Landscape of Digital Ownership for Visual Art

Teilnehmende · Participants	Thi Thien Nhi Dam
Lehrende · Lecturers	Prof. Dr. Eva Hornecker, Britta Schulte
Raum · Room	2.40 – Beratungsraum

Bei diesem Projekt handelt es sich um eine englischsprachige Abschlussarbeit: Many blockchain-powered systems for digital ownership (you've probably heard about it under the term »NFT«), have been developed aiming for widespread usage. However, the approach still appears uncommon for both digital creators and consumers that accordingly raises the question: do current blockchain services meet users' actual needs? While the majority of research in this field has emphasized on technical implementation of such solutions, there is an extreme deficiency regarding users' viewpoints incorporated into the design and thus enlarging the barriers to mainstream adoption. Picking the domain of visual art, this project aims to adopt a user-centered design approach, shifting the focus of research from technical practice to actual user perspectives, to design a solution for ownership of digital artworks that facilitate potential users' needs and bring the technology closer to the mainstream audience. After investigating digital creators' needs and expectations, I designed a set of scenarios incorporating actual users' viewpoints to demonstrate a future landscape of producing, publishing, and consuming activities circulated in the digital art realm. The scenarios aim to confirm, and explore more users' viewpoints to define a preferable future of digital ownership for visual art.

SHUTTLEBUS CAMPUS – S143

Haltestelle Campus · Bus stop Campus
Ecke · Corner Bauhausstraße / Geschwister-Scholl-Straße

Haltestelle S143 · Bus stop S143
Parkplatz vor dem Drehkreuz · parking area at the turnstile

Freitag	17–22 Uhr	Freitag	5–10 pm
Samstag	12–20 Uhr	Saturday	12–8 pm
(30-Minuten-Takt)			(approx. every 30 minutes)

Professors, staff and students from the Department of Media Informatics will open their workrooms & laboratories for one evening and one afternoon at Schwanseestraße 143 and present the latest developments in the fields of digital media, computer systems and information technology.
www.uni-weimar.de/OLN

ÖFFNUNGSZEITEN · OPENING HOURS

Open Lab Night 2022
Freitag, 15. Juli, 17–22 Uhr
Mit Grillen, Getränken und Musik im Innenhof
Friday, 15 July, 5–10 pm
With barbecue, drinks and music in the courtyard

Open Labs 2022
Samstag, 16. Juli, 14–17 Uhr
Saturday, 16 July, 2–5 pm

Let's have fun – exploring playfulness in interaction design

Teilnehmende · Participants	Sreyoshi Dutta, Josephin Kröger, Urszula Kulon, Ekaterina Ladokhina, Irene López García, Faezeh Mansourkhaki, Isaiah Lenwick Mc Clean, Mufleha Ovais, Luca Schreiber
Lehrende · Lecturers	Prof. Dr. Eva Hornecker, Michaela Honauer
Raum · Room	2.40 – Beratungsraum

Spielen macht Spaß, jeder mag es. Aber was macht uns so enorme Freude am Spielen? Was bedeutet »spielen«? Was ist »Verspieltheit«? Können wir bessere Produkte entwerfen, wenn wir Interaktionskonzepte auf Aspekte der Verspieltheit stützen? Wir erforschen das Spielerische im Interaktionsdesign, indem wir bekannte Alltagsgegenstände neugestalten, neue spielerische Anwendungen schaffen und kleine Studien durchführen, um empirisch zu verstehen, was das Verspielte ausmacht. Parallel zur Entwicklung einer Ich-Perspektive auf das Thema befassen wir uns auch mit bestehender Literatur aus dem Bereich der Mensch-Computer-Interaktion, der Designforschung und anderen verwandten Bereichen. Wir schauen uns andere spielerische Beispiele an und suchen nach unseren eigenen Konzeptideen, die spielerische Interaktionen veranschaulichen. Neun Studierende aus verschiedenen Ländern und mit unterschiedlichen Hintergründen nehmen an diesem Projekt teil. Sie sind in drei verschiedenen Studiengängen an drei Fakultäten eingeschrieben. Der interdisziplinäre Austausch wird durch fünf verschiedene Projekte gekrönt. Playing is fun, everyone likes it. But what makes us enjoy playing? What means 'to play'? What is »playfulness«? Can we design better products if we base interaction concepts on aspects of playfulness? We explore playfulness in interaction design by re-designing well-known everyday objects, creating new playful applications, and conducting small studies to understand empirically what characterizes playfulness. In parallel to developing a first-person perspective on the topic, we likewise engage with existing literature in the field of Human-Computer Interaction, design research and other related areas. We look at other playful examples and search for our own concept ideas that exemplify playful interactions. Nine students from different countries and backgrounds participate in this project. They are enrolled in three different study programmes across three faculties. The interdisciplinary exchange is crowned by five different projects.

Rhyme Times (Josephin Kröger, Isaiah Lenwick Mc Clean)
Wartezeit an der Ampel musikalisch nutzen
Making musical use of waiting time at traffic lights

PR22 (Luca Schreiber)
PR22 ist ein Radio mit CD-Player, sowie Bluetooth- und AUX-Schnittstelle für Senior*innen. Es ist nach ergonomischen und emotionalen Bedürfnissen von älteren Menschen gestaltet und soll die spielerischen Aspekte des Musikhörens verstärken. PR22 is a radio with CD player, Bluetooth and AUX interface for senior citizens. It is designed to meet the ergonomic and emotional needs of older people and to enhance the playful aspects of listening to music.

Lucky Cookbook (Ekaterina Ladokhina, Urszula Kulon)
Mit dem Zufall spielerisch zur Mahlzeit
With the shuffle to the meal

Wall of Fun (Faezeh Mansourkhaki, Mufleha Ovais, Sreyoshi Dutta)
Interaktive Lichtinstallation für mehr Verspieltheit im öffentlichen Raum
Interactive light installation for more playfulness in public space

A remote meal together (Irene López García)
Digitales Platzdeckchen für mehr zwischenmenschliche Kommunikation
Digital placemat for more interpersonal playful communication

SYSTEME DER VIRTUELLEN REALITÄT
VIRTUAL REALITY AND VISUALIZATION RESEARCH

Demos im Virtual Reality Labor
Demonstrators in the Virtual Reality Lab

Teilnehmende · Participants	Karoline Brehm, Lucky Chandrarama, Krishna Choudoor, Aalok Gokhale, Viktor Hubert, Ankith Kodanda, Joshua König, David Krug, Anton Lammert, Jacob Lammert, Simon Meininger, Omar Nada, Margarita Osipova, Emil Reinert, Clemens Rettelbach, Vanessa Retz, Jonas Roquette, Eric Schlossberg, Pramooh Viriyathomrongul, Tony Zöppig Prof. Dr. Bernd Fröhlich, Dora Kiesel, Adrian Kreskowski, Sebastian Mühlhaus, Gareth Rendle, Ephraim Schott, Dr. Patrick Riehmann
Lehrende · Lecturers	
Raum · Room	1.10 – Virtual Reality Lab

Die Arbeitsgruppe Virtual Reality und Visualization Research gibt Einblicke in die Ergebnisse der Forschung und Lehre aus den vergangenen Semestern. Die Arbeitsgruppe beschäftigt sich mit den Themenfeldern Mehrbenutzerinteraktion in sozialer Virtual Reality, Informationsvisualisierung und Real-Time Rendering. Zur Open Lab Night laden die Studierenden und Mitarbeitenden dazu ein, an den vielseitigen Semester- und Forschungsprojekten im Virtual-Reality-Labor teilzuhaben. Unter anderem werden praktische Ergebnisse aus den studentischen Projekten »VR CreatiVE«, »Music Performances in VR« und »Non-Photorealistic Rendering for Virtual Reality Applications« ausgestellt. Diese können spielerisch mit aktuellen Head-Mounted-Displays wie der Oculus Quest 2 und am Desktop erprobt werden. Zudem werden Arbeiten aus der Forschung und Lehre der Arbeitsgruppe präsentiert. Insbesondere umfassen diese die laufenden Abschlussarbeiten der Bachelor- sowie Masterstudiengänge des Fachbereichs Medieninformatik. At the summary, the Virtual Reality and Visualization Research group provides insights into the results of research and teaching from the past semesters. The working group focuses on the topics of multi-user interaction in social virtual reality, information visualization and real-time rendering. At the Open Lab Night, the students and staff invite you to participate in the versatile semester and research projects in the Virtual Reality Lab. Among other things, practical results from the student projects »VR CreatiVE«, »Music Performances in VR« and »Non-Photorealistic Rendering for Virtual Reality Applications« will be on display. These can be playfully tested with current head-mounted displays such as the Oculus Quest 2 and on the desktop. In addition, current work from the research and teaching of the working group will be presented. These include the current final theses of the bachelor's and master's degree programmes of the Department of Computer Science.
www.uni-weimar.de/vr

GRAFISCHE DATENVERARBEITUNG
COMPUTER GRAPHICS

Bauhaus Gamesfabrik · Bauhaus Gaming Factory

Teilnehmende · Participants	Nico Brockmann, Jenny Döring, Peter Sebastian Dunn, Fionn Edward Erickson, Samuel Fientje, Tobias Bernhard Friedel, Niklas Häfner, Aaron Jordan Kammer, Jeremias Michael Kilian, Oskar Elias Babatunde Kraska Mc Kone, Victor Jose Mahecha Arango, Ozgesu Ozen, Jakob Béla Ruckel, Marie Trojan, Angelina Damm, Josefine Kira Engelhardt, Marvin Alex Elgentrebe, Ulrike Sophie Katschmann, Haoxing Li, Olga Molzan, Lisa-Marie Opitz, Anna Chiara Rudelt, Nora Marie Schulze, Anton Seiler, Adam Streicher, Lorenz Victor Weiland, Lisa Luise Zwintscher, Duc Tri Nguyen, Cesar Daher Prof. Charles Wüthrich, Prof. Wolfgang Kissel
Lehrende · Lecturers	Gianluca Pandolfo
Raum · Room	Erdgeschoss – Studierenden.Lounge · Ground Floor – Student.Lounge

In weniger als drei Monaten haben Studierende der Fakultäten Kunst & Gestaltung und Medien im interdisziplinären Projekt Indiegama Development Lab II individuelle Videospiele entwickelt. Wir freuen uns euch begrüßen zu dürfen und bieten euch die Gelegenheit alle Spiele der Studierenden zu spielen. In less than three months, students from the faculties of Art & Design and Media have developed individual video games in the interdisciplinary project Indiegama Development Lab II. We are happy to welcome you and offer you the opportunity to play all of the students' games.
bauhausgamesfabrik.it.ch.io

Open Labs 2022

summery 2022

Schwanseestraße 143

CONTENT MANAGEMENT UND WEB TECHNOLOGIEN
WEB TECHNOLOGY AND INFORMATION SYSTEMS

Im Dialog mit dem virtuellen Museum · In Dialog with the Virtual Museum

Teilnehmende · Participants	Ahsan Zubair, Mariam Korashi, Suryaprakash Kalvakolu
Lehrende · Lecturers	Prof. Dr. Benno Stein, Johannes Kiesel, Marcel Gohsen
Raum · Room	2.33 – MedSec- & WEBIS-Lab

Museen versuchen Besucher*innen ein interaktives und immersives Erlebnis zu bieten, um Informationen über ein bestimmtes Thema zu vermitteln. Audioguides können ein vertieftes Erlebnis bieten, sind aber in der Regel nicht interaktiv. Das Projekt zielt darauf ab, genau solche einen interaktiven Audioguide zu entwickeln, der es den Besucher*innen ermöglicht, Fragen zu stellen und so ihr Erlebnis auf ihre Interessen abzustimmen. Konkret konzipieren und entwickeln wir ein System für das Büro von Walter Gropius mit seiner bewegten Geschichte, seinem bahnbrechenden Design und seiner Bedeutung für den Bauhaus-Stil. Wir zeigen, wie Fakten und Beschreibungen in unserer »Wissensdatenbank« in Antworten auf verschiedene Fragen umgewandelt werden, die eine Besucher*in stellen könnte. Museums try to provide their visitors with an interactive and immersive experience to convey information about a particular topic. Audio guides can provide an in-depth experience but are typically not interactive. This project aims to develop an interactive audio guide that allows visitors to ask questions and thus customize their experience to their interests. Specifically, we are designing and developing a system for Walter Gropius's office, with its colorful history, groundbreaking design, and overall importance to the Bauhaus style. We show how facts and descriptions in our »knowledge base« are transformed into answers to various questions a visitor might ask.

Abenteuer in den digitalen Geisteswissenschaften
Adventures into the Digital Humanities

Teilnehmende · Participants	Jason Brockmeyer, Nazifa Kazimi
Lehrende · Lecturers	Prof. Dr. Benno Stein, Tim Gollub, Nikolay Kolyada
Raum · Room	2.33 – MedSec- & WEBIS-Lab

In Projekten der Digital Humanities (DH) geht es meist darum, einen Korpus unter Verwendung von Computertechnologien hinsichtlich einer Forschungsfrage auszuwerten. Technologisch setzt man dabei vor allem auf Klassifizierer, die die für die Fragestellung relevanten Konzepte im Korpus finden und auszeichnen sollen. Die Entwicklung spezifischer Klassifizierer, die mit hinreichend hoher Qualität arbeiten, ist jedoch sehr zeit- und ressourcenintensiv, und dadurch oftmals erst gegen Ende der Projektlaufzeit abgeschlossen. Im Forschungsprojekt »Adventures into the Digital Humanities« stellen wir uns als Informatiker daher die Frage, wie man DH Projekte gleich zu Beginn ihrer Laufzeit technologisch effektiv unterstützen kann. Welche Systeme und Strukturen sollten initial aufgesetzt werden? Wie kann schnell ein erster Prototyp entstehen? In der Auseinandersetzung mit verschiedenen Korpora und Fragestellungen entwickelten die Studenten Guidelines und Tools für ein Rapid Prototyping in DH Projekten. Digital Humanities (DH) projects usually involve the evaluation of a corpus with regard to a research question using computer technology. Technologically, the focus is on classifiers that are supposed to find and label the concepts in the corpus that are relevant to the research question. However, the development of specific classifiers that work with sufficiently high quality is very time- and resource-intensive, and thus often only completed towards the end of the project. In the research project »Adventures into the Digital Humanities«, we as computer scientists therefore ask ourselves how DH projects can be supported technologically effectively right at the beginning of their duration. Which systems and structures should be set up initially? How can a first prototype be created quickly? In dealing with various corpora and questions, the students developed guidelines and tools for rapid prototyping in DH projects.

SOFTWARE ENGINEERING

Ausgewählte Projekte der Professur Software Engineering
Selected Software Engineering Projects

Teilnehmende · Participants	Studierende des Studiengangs Digital Engineering
Lehrende · Lecturers	Prof. Dr. Jan Oliver Ringert
Raum · Room	2.35 – Software Engineering Lab

Wir präsentieren ausgewählte Projekte von Studierenden aus dem Master-Studiengang Digital Engineering. Eine Gruppe von Studierenden präsentiert die Ergebnisse eines Gruppenprojekts über autonome Fahrzeuge. Weiterhin werden Projekte präsentiert, die in der Vorlesung Software Engineering entstanden sind. We present selected software projects created by students of the Digital Engineering MSc programme. One group of students presents the results of a group project on autonomous vehicles. Other students present software projects they developed during the Software Engineering lecture.

COMPUTER VISION IN ENGINEERING

Auswirkungen von Kamerabewegungen auf die Bildauflösung
Effects of Camera Motion on Image Resolution

Teilnehmende · Participants	Nayana Satish Bhosale, Alina Schimko, Ganesh Kumar Uppirella
Lehrende · Lecturers	Christian Benz
Raum · Room	1.17 – Computer Vision Lab

Die Bedeutung von beweglichen Plattformen für die Bilderfassung – wie Mobiltelefone oder Drohnen – nimmt stetig zu. Die tatsächliche Bildauflösung, die eine sich bewegende Kamera erreicht, ist in der Regel jedoch schlechter als die theoretisch mögliche. Bewegungsunschärfe, Bildrauschen und ungeeignete Kameraeinstellungen können die Bildschärfe und damit die Fähigkeit, feine Strukturen aufzulösen, deutlich verringern. In diesem Projekt wird die praktische Auflösung mit Hilfe eines Siemenssterns abgeschätzt und mit der Kamerabewegung in Beziehung gesetzt. The relevance of moving platforms for image acquisition – such as mobile phones or drones – is steadily increasing. The practical image resolution achieved by a moving camera is, however, typically worse than the theoretically possible resolution. Effects of motion blur, out of focus, noise, and improper camera parameters can distinctly reduce image sharpness and, thereby, the capability of representing fine structures. In this project, the practical resolution will be estimated by means of a Siemens star and related to camera movement.

MEDIENSICHERHEIT
MEDIA SECURITY

Untersuchung »smarter« Türklingeln · Research into »smart« doorbells

Teilnehmende · Participants	Marcus Almert
Lehrende · Lecturers	Prof. Dr. Stefan Lucks, Nathalie Lang
Raum · Room	2.33 – MedSec- & WEBIS-Lab

Mit der steigenden Popularität des Internets der Dinge (Internet of Things, IoT) ergab sich die Möglichkeit, neue Funktionen in jedes Haus zu integrieren. Auch wenn dies zunächst aufregend und bequem klingt, müssen wir uns fragen: Wie sehr garantieren bestimmte IoT-Geräte Sicherheit und Privatsphäre? Wir haben mehrere »smarte« Türklingeln untersucht und dabei verschiedene Schwachstellen gefunden. Während einige dieser Schwachstellen nur ausschließlich bei einzelnen Klingeln auftraten, fanden wir auch größere Schwachstellen, die sich auf andere Türklingeln und sogar auf andere Geräte ausbreiteten. With the rising popularity of the Internet of Things (IoT) comes the opportunity to integrate new features into every home. While this may sound exciting and convenient at first, we have to ask: how much do certain IoT devices guarantee security and privacy? We have examined several »smart« doorbells and found several vulnerabilities. While some of these vulnerabilities are unique to certain doorbells, we also found larger vulnerabilities that spread to other doorbells and even to other devices.

Dancing with the Bears – Hash-basierte Signaturen
Dancing with the Bears – Hash-based signatures

Teilnehmende · Participants	Luigi Portwich, Marcus Almert, Vladimir Spassov
Lehrende · Lecturers	Prof. Dr. Stefan Lucks, Nathalie Lang
Raum · Room	2.33 – MedSec- & WEBIS-Lab

Verteilte Unterschriftsverfahren erlauben es, die Unterschriftsberechtigung an eine Gruppe von sogenannten Trustees zu delegieren. Typische Verfahren aus der Kryptographie benutzen arithmetik-basierte Verfahren (z.B. RSA). In diesem Projekt beschäftigen wir uns mit dem Dancing-Bear-Verfahren – der Realisierung eines verteilten Unterschriftsverfahrens basierend auf Hash-Funktionen. Ein Vorteil von hash-basierten Unterschriftsverfahren ist die post-quantum Sicherheit. Studierende implementieren Dancing Bear und werden es in einem nächsten Schritt evaluieren/benchmarken. Distributed signature procedures allow the possibility to delegate the signature to a group of so-called trustees. Typical procedures from cryptography use arithmetic-based procedures (e.g. RSA). In this project we deal with the Dancing Bear method, the realisation of a distributed signature method based on hash functions. One advantage of hash-based signature methods is post-quantum security. Students implement Dancing Bear and will evaluate/benchmark it in a next step.