UNIVERSITÄT HOHENHEIM | Computational Science Hub

Jun.-Prof. Dr. Christian Krupitzer · Coordinator · christian.krupitzer@uni-hohenheim.de

Registration now open for the

CSH Winter School 2025 Practical Introduction to Homomorphic Cryptography

with Thomas Prantl
Feb 24 – Feb 28, 2025
Hohenheim

Overview

Homomorphic cryptography is a form of encryption that allows computations to be performed directly on encrypted data without decrypting it, producing encrypted results that can later be decrypted to reveal the correct outcome. This property is particularly valuable when sensitive data must remain private, such as secure data processing in cloud computing, privacy-preserving machine learning, or secure voting systems. For example, healthcare providers can analyze encrypted patient data for research purposes without accessing the original sensitive information, ensuring both privacy and utility.

Join us in the CSH Winter School 2025! The aim of the module is that:

1. Participants can explain the necessary mathematical basics, such as groups, rings, and homomorphism.
2. Participants should have a basic understanding and overview of existing homomorphic cryptosystems. To this end, participants should be able to explain which operations can be realized homomorphically by the various cryptosystems.
3. Participants should have learned the basics for using the CKKS cryptosystem in practice. This includes being able to name the sources of error in the cryptosystem and being able to explain how the following functions can be realized homomorphically: Division, root, exponential function, maximum, minimum.
4. Participants should have gained practical experience working with the OpenFHE library.

All components will be supplemented by practical exercises, focusing on various applications of sentiment analysis. Participants are not required to have prior knowledge of cryptography or IT security.

Jun.-Prof. Dr. Christian Krupitzer · Coordinator · christian.krupitzer@uni-hohenheim.de

Planned schedule

University Hohenheim, 70599 Stuttgart.

Async online course (upfront the Winter school): Jan 15 - Feb 21, 2025:	
	Introduction into Programming with C++
Setup (via Zoom): February 17, 2024, 15h00 - 17h00:	
15h00 - 17h00	Check your technical setup.
Day 1 (in presence): February 24, 2024, 9h00 - 17h00:	
9h00 - 12h00	Lecture: Introduction and mathematical foundations
12h00 - 13h00	Lunch Break
13h00 - 17h00	Exercise: Mathematical foundations
Day 2 (in presence): February 25, 2024, 9h00 - 17h00:	
9h00 - 12h00	Lecture: CKKS - Basics (1/2)
12h00 - 13h00	Lunch Break
13h00 - 17h00	Exercise: CKKS - Basics
Day 3 (in presence): February 26, 2024, 9h00 - 17h00:	
9h00 - 12h00	Lecture: CKKS - Basics (2/2) and extensions (1/2)
12h00 - 13h00	Lunch Break
13h00 - 17h00	Exercise: CKKS - Basics and extensions
Day 4 (in presence): February 27, 2024, 9h00 - 17h00:	
9h00 - 12h00	Lecture: CKKS - Extensions (2/2)
12h00 - 13h00	Lunch Break
13h00 - 17h00	Exercise: CKKS extensions
Day 5 (in presence): February 28, 2024, 9h00 - 17h30:	
9h00 - 10h30	Lecture: CKKS - Data science applications
10h30 - 11h00	Lunch Break
16h00 - 17h30	**Final Examination**

Jun.-Prof. Dr. Christian Krupitzer · Coordinator · christian.krupitzer@uni-hohenheim.de

Target Audience

The course mainly aims at Master and PhD-students interested in understanding and applying homomorphic cryptography. No prior knowledge is required. However, basic knowledge in math and statistics (e.g., in linear regression) and experiences in programming might be helpful. **3 ECTS points can be earned if participants take the final examination on the last day. By attending solely, participants can earn a certificate of participation.**

Fees, Devices and Credits

Interested participants can register through weiterbildung.uni-hohenheim.de for the workshop until **February 15, 2025**.

For external participants, the following tuition fee structure applies:

Group	Prices in EUR
Students	100.00
PhD students / Staff Members	150.00
PostDocs	200.00
Professors	300.00

The outstanding fees must be wired as indicated in the payment instructions. An email with detailed payment instructions will be sent to participants after registration and before the workshop. Registration is binding. Fees transferred are non-refundable.

Participants should bring their own laptop (incl. charger) with a working Linux, Mac, or Windows/WLS installation. The required tools and libraries will be installed in the Zoom session upfront the workshop week.

After the Winter School, participants will receive a certificate for the number of hours attended.

Contact

For any further information, please contact

University of Hohenheim
Jun.-Prof. Dr. Christian Krupitzer
Computational Science Hub (CSH)
E-Mail: christian.krupitzer@uni-hohenheim.de