

CRYPTOGRAPHIC SOLUTIONS FOR PRIVACY ENHANCING TECHNOLOGIES

SUMMER SCHOOL 28 AUGUST - 01 SEPTEMBER 2023

Homomorphic encryption (HE) is one of the most powerful privacy enhancing technologies to ensure data privacy while deriving value from data, which has been growing at an unprecedented speed. Lattice-based cryptographic schemes, with their superior security, scalability and functionality properties, stand the most promising family of HE algorithms to achieve data capitalization in a privacy-preserving way.

enCRYPTON consortium (<https://www.encrypt-on.com/>) organizes a summer school for early stage researchers to learn not only the theoretical foundations of lattice-based HE but also its applications in machine learning. The implementation challenges of HE will also be covered in the summer school by internationally renowned scientists. In the last day of the summer school, there will be a hackathon, where students can work on homomorphic application project.

The summer school will take place on August 28 - September 1 in Sabancı University campus, Istanbul. There is on-campus accommodation available for students.

Please send all your inquiries to Erkay Savaş (erkays@sabanciuniv.edu) or Tuğçe Akkaş (tugce.akkas@sabanciuniv.edu)

TOPICS

✓ Day 1 | 28.08.2023

Mathematical Background

✓ Day 2 | 29.08.2023

Lattice Based Cryptography and Homomorphic Encryption Schemes - I

✓ Day 3 | 30.08.2023

Lattice Based Cryptography and Homomorphic Encryption Schemes - II

✓ Day 4 | 31.08.2023

Software libraries and Implementation Issues

✓ Day 5 | 01.09.2023

Privacy-Preserving Machine Learning/Data Mining

REGISTER
NOW!



INSTRUCTORS

AHMAD AL BADAWI
AHMET CAN MERT
ARSALAN JAVEED

BENEDIKT GIERLICHS
DIMITAR JETCHEV
ERCHAN APTOULA

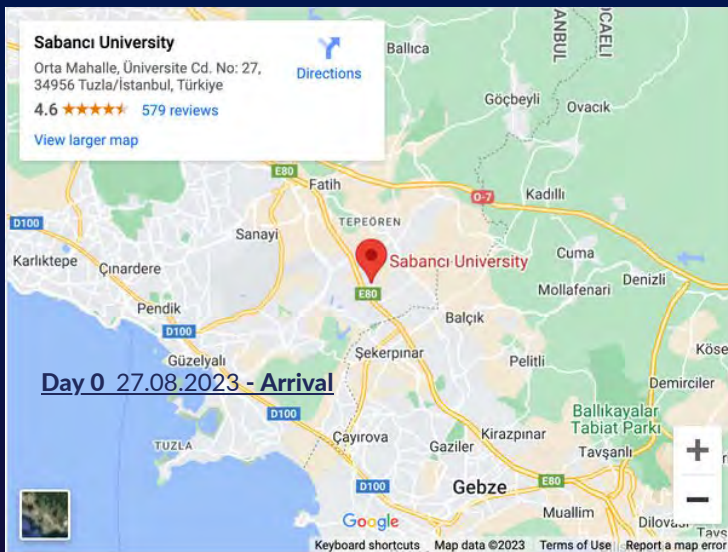
ERDİNÇ ÖZTÜRK
ERKAY SAVAŞ
FERRUH ÖZBUDAK

TOLUN TOSUN
YÜCEL SAYGIN
WOUTER CASTRYCK

CRYPTOGRAPHIC SOLUTIONS FOR PRIVACY ENHANCING TECHNOLOGIES

SUMMER SCHOOL 28 AUGUST - 01 SEPTEMBER 2023

DATES & TOPICS



Day 0 27.08.2023 - Arrival

Day 2 29.08.2023

Lattice Based Cryptography and Homomorphic Encryption Schemes - I

Before Noon
09:00 - 11:45
Lattices and Hard Problems over Lattices - I
Lattices and Hard Problems over Lattices - II
Coffee Break
Lattices and Hard Problems over Lattices - III
Lunch

After Noon
13:00 -19:30
Introduction to Homomorphic Encryption - I
Introduction to Homomorphic Encryption - II
Coffee Break
The BFV Scheme - I
The BFV Scheme - II
Social Activities

Day 4 31.08.2023

Software libraries and Implementation Issues

Before Noon
09:00 - 11:45
General Introduction to a Homomorphic Encryption Library - I
General Introduction to a Homomorphic Encryption Library - II
Coffee Break
Applied Study - Developing a Simple Homomorphic Application
Lunch

After Noon
13:00 -19:30
Implementation Issues I: Hardware Acceleration
Implementation Issues II: Hardware Acceleration
Coffee Break
Implementation Issues III: A Side-Channel Attack Overview
Implementation Issues IV: Side-Channel Protection for Lattice-Based Cryptography
Social Activities

Day 1 28.08.2023

Mathematical Background

Before Noon
09:00 - 11:45
Modular and Finite Field Arithmetic - I
Modular and Finite Field Arithmetic - II
Coffee Break
Modular and Finite Field Arithmetic - III
Lunch

After Noon
13:00 -19:30
Cyclotomic Polynomials and Polynomial Rings
Arithmetic in Polynomial Rings
Coffee Break
Number Theoretic Transform (NTT)
Polynomial Multiplication with NTT
Social Activities

Day 3 30.08.2023

Lattice Based Cryptography and Homomorphic Encryption Schemes - II

Before Noon
09:00 - 11:45
The CKKS Scheme - I
The CKKS Scheme - II
Coffee Break
The TFHE Scheme
Lunch

After Noon
13:00 -19:30
Social Activity (Excursion in Istanbul)

Day 5 01.09.2023

Privacy-Preserving Machine Learning/Data Mining

Before Noon
09:00 - 11:45
A Brief Introduction to Machine Learning: Basics (SVM, Tree-Based Techniques (Decision tree, Random Forest, XGBoost)
Privacy-Preserving Machine Learning with HE
Coffee Break
Privacy-Preserving Machine Learning and Data Mining
Lunch

After Noon
13:00 -19:30
A project/hackathon: Project definition
Design & Implementation
Closing