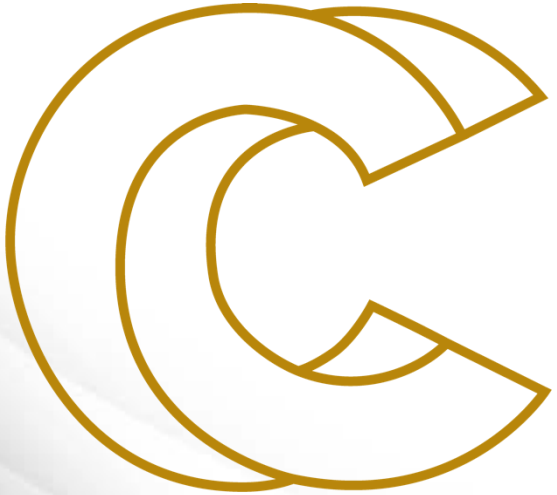
TÜBİTAK



# EURO$^2$

## GPU Optimization of Advanced Encryption Standard

Cihangir Tezcan, PhD
Graduate School of Informatics, METU, Ankara

# Meet the Instructor

- **EDUCATION**
  - B.Sc. Mathematics METU (2003 - 2007)
  - M.Sc. Cryptography METU (2007 – 2009)
  - Ph.D. Cryptography METU (2009 – 2014)

- **PROFESSIONAL**
  - Associate Professor, Cyber Security (Informatics Institute) METU (2022 - … )
  - Head of Department of Cyber Security, METU (2020 - … )
  - Director of Cyber Security Research Center, METU (2020 - … )
  - Assistant Professor, Cyber Security (Informatics Institute) METU (2019 - 2022)
  - Researcher, Ruhr-Universitaet Bochum (2017 – 2018)
  - Research Assistant, Ecole Polytechnique Federale De Lausanne (2010 - 2011)

# Meet the Instructor

- Teaching
  - CSEC501 **CYBER SYSTEMS AND INFORMATION SECURITY**
  - CSEC502 **NETWORK SECURITY**
  - CSEC504 **PENETRATION TESTING AND VULNERABILITY ANALYSIS**
  - CSEC507 **APPLIED CRYPTOLOGY**
  - CSEC508 **APPLIED CRYPTANALYSIS**
  - CSEC510 **OPERATING SYSTEMS SECURITY**
  - CSEC513 **LIGHTWEIGHT CRYPTOGRAPHY FOR THE INTERNET OF THINGS**
  - CSEC519 **BLOCKCHAIN AND CRYPTOCURRENCY TECHNOLOGIES**

# Preknowledge/Prerequisite(s)

- General understanding of cryptography concepts and principles
- Basic programming skills in C and CUDA
- Codes are also available at https://www.github.com/cihangirtezcan/CUDA_AES

# What you will learn?

- Fundamental Concepts in Symmetric Cryptography
- Implementation of Cryptographic Algorithms
- Performance Optimization of Block Ciphers on GPUs

# Course Outline

**PART I: Block Ciphers**

- Introduction to Block Ciphers
- Advanced Encryption Standard (AES)
- Mode of Operations for Block Ciphers

# Course Outline

**PART II: CUDA Optimization of AES**

- Reference C and CUDA Implementation of AES
- CUDA Optimization of AES
- Encryption Performance of AES on GPUs

# What this course is

- This course provides fundamentals of block ciphers and mode of operations for block ciphers. As an example, we focus on Advanced Encryption Standard (AES). AES block cipher is responsible for the most of the world‘s encryption.
- This course also teaches how to implement cryptographic algorithms like AES in C and CUDA.
- Finally, this course teaches how to optimize AES on GPUs to obtain record-breaking performance.

# Set Up/Configure/Install …..

EURO$^2$

- You need to install CUDA SDK to run the CUDA codes provided in the course
- You need an NVIDIA GPU to run the CUDA codes

# Thanks

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101101903. The JU receives support from the Digital Europe Programme and Germany, Bulgaria, Austria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Italy, Lithuania, Latvia, Poland, Portugal, Romania, Slovenia, Spain, Sweden, France, Netherlands, Belgium, Luxembourg, Slovakia, Norway, Türkiye, Republic of North Macedonia, Iceland, Montenegro, Serbia