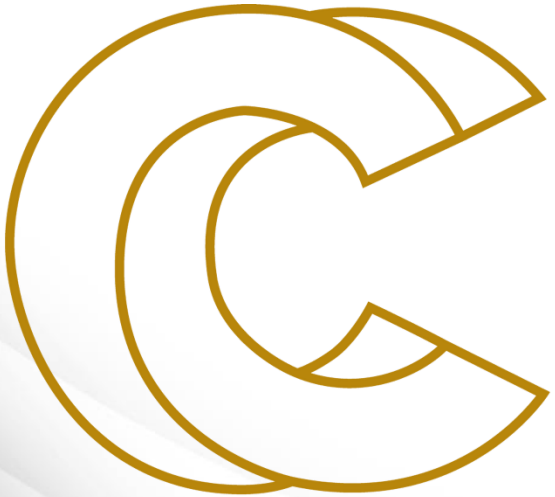

EURO 4SEE

GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA

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

ncc@ulakbim.gov.tr

Welcome to the Course

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)
- *Teaching Assistant*, Ecole Polytechnique Federale De Lausanne (2010 - 2011)

Welcome to the Course

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**
- EE442 **OPERATING SYSTEMS**

Preknowledge/Prerequisite(s)

- General understanding of cryptography concepts and principles
- Basic programming skills in C and CUDA

- Codes are available at https://artifacts.iacr.org/fse/2025/a7/ or alternatively at GitHub
  - https://www.github.com/cihangirtezcan/CUDA_KASUMI
  - https://www.github.com/cihangirtezcan/CUDA_SPECK
  - https://www.github.com/cihangirtezcan/CUDA_TEA3

- Related paper is available at https://tosc.iacr.org/index.php/ToSC/article/view/12078

Tezcan, C., & Leander, G. (2025). *GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA*. IACR Transactions on Symmetric Cryptology, 2025(1), 309-327. https://doi.org/10.46586/tosc.v2025.i1.309-327

Course Overview

What you will learn?

- Fundamental Concepts in Symmetric Cryptography
- Implementation and optimization of Cryptographic Algorithms on GPUs
- Brute-Force Cryptanalysis of Ciphers

What this course is

- This course provides fundamentals of block and stream ciphers.
- As an example, we focus on KASUMI, TEA3, and SPECK ciphers which are used in GSM/GPRS, TETRA, and RFID communications, respectively.
- This course also teaches how to implement and optimize cryptographic algorithms in CUDA.
- Finally, this course teaches how to perform GPU assisted brute-force attacks on ciphers.

Course Overview

PART I: Block and Stream Ciphers

1. Introduction to Block Ciphers
2. Introduction to Stream Ciphers
3. KASUMI Block Cipher
4. SPECK Block Cipher
5. TEA Stream Ciphers

Course Overview

PART II: CUDA Optimizations of KASUMI, SPECK, and TEA3

1. GPU Implementation Techniques for Ciphers
2. CUDA Optimization of KASUMI
3. CUDA Optimization of SPECK
4. CUDA Optimization of TEA3
5. Summary of GPU Performance of Ciphers

What this course isn’t

- Although this course is about the weaknesses of the GSM/GPRS, TETRA, and RFID communications, it explains how to break underlying cryptographic algorithms.
- It is not about capturing a real-world communication and decrypting it, which is illegal.

Introduction and Set Up/Configure/Install .....

- 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
- You need a compatible compiler to compile CUDA codes

EURO 4SEE

Thanks!

Co-funded by
the European Union

EuroHPC
Joint Undertaking

This project has received funding from the European High-Performance Computing Joint Undertaking (JU) under grant agreement No 101191697. The JU receives support from the Digital Europe Programme and Germany, Türkiye, Republic of North Macedonia, Montenegro, Serbia, Bosnia and Herzegovina.