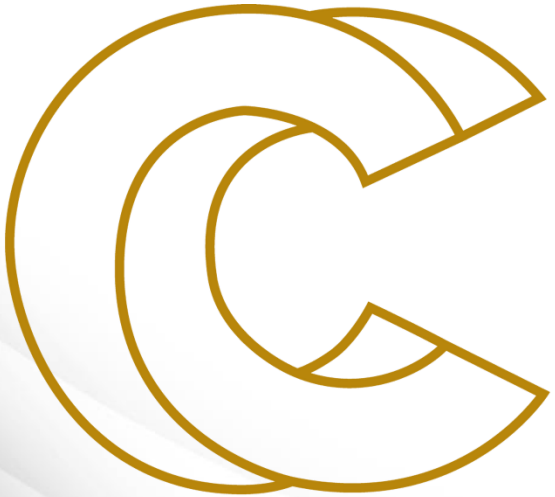


EURO 4SEE

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

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

ncc@ulakbim.gov.tr

# Lesson 5: TEA Stream Ciphers

## TEA Family of Stream Ciphers

- Terrestrial Trunked Radio (TETRA) is a European standard for trunked radio.
- It is globally used by military, police, emergency services, prisons, and government agencies.
- The cryptographic algorithms used in TETRA were kept secret for decades until it was shown how easy it is to reverse engineer in a recent work.
- Note that with millions of TETRA devices being deployed around the world, it was not hard for adversarial parties to obtain these cryptographic algorithms by reverse engineering or via stolen or leaked documents.
- But until the recent disclosure of these algorithms, academic community was not able to assess the security of these algorithms.
- It was shown that TETRA uses four very similar LFSR-based keystream generators called TEA1, TEA2, TEA3, and TEA4.

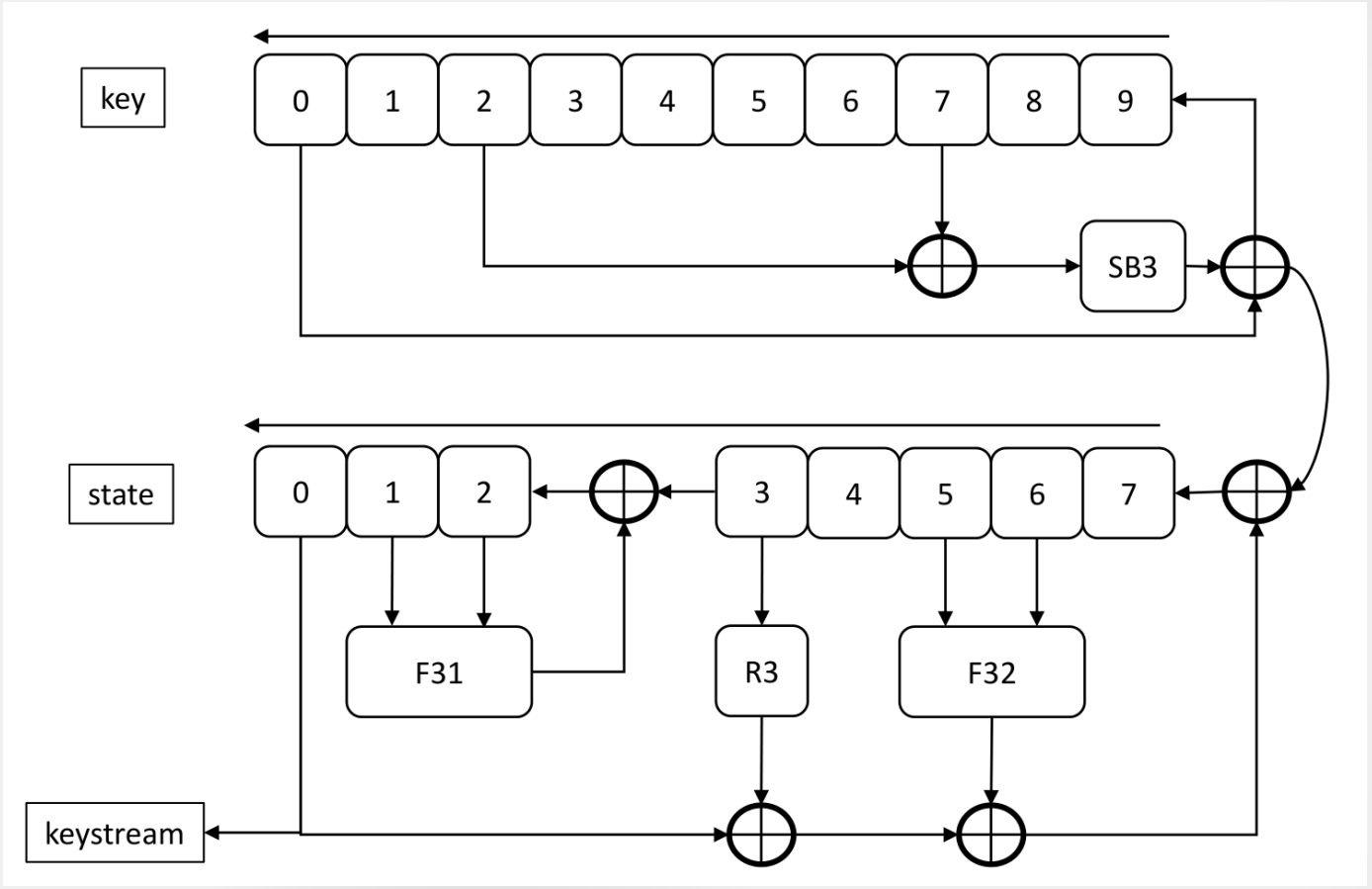
# Lesson 5: TEA Stream Ciphers

## TEA Family of Stream Ciphers

- They all consist of a key register and a state register which is initiated by an IV.
- Although all of these keystream generators use 80-bit secret keys, deliberately weakened TEA1 compresses the 80-bit key into 32 bits. Thus, it provides 32-bit security.
- The detailed structure of TEA4 is still unknown but since it was designed for commercial use and restricted export, it may have similar weaknesses of TEA1.
- TEA2 and TEA3 are almost identical in design. They have a 64-bit state register and 80-bit key register.
- Both registers perform byte-wise shifting, they have two F functions for non-linear filtering and a single R function for bit reordering.
- Both of them use a different 8x8 S-box.
- One main difference is that in TEA3 the S-box output is XORed with a key register byte before feeding back.
- In our GPU optimizations we focused on implementing TEA3 and our codes can be slightly modified to obtain the same results for TEA2.

# Lesson 5: TEA Stream Ciphers

## TEA3 Stream Cipher




In order to produce the first keystream byte, TEA3 is clocked 51 times and it is clocked 19 times for the subsequent keystream bytes.

# Next lecture

**GPU Implementation Techniques for Ciphers**

- Three implementation techniques for ciphers
- Their advantages and disadvantages

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.