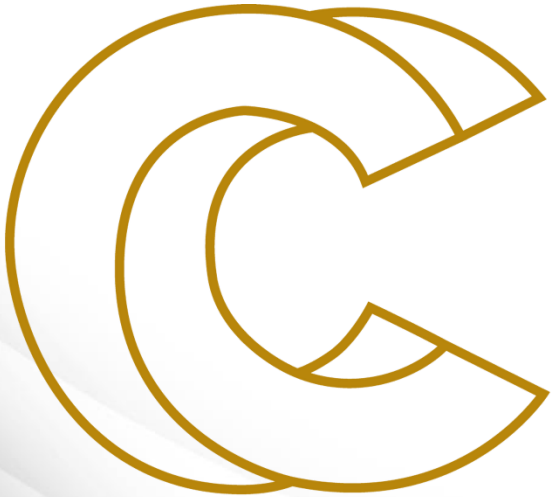


EURO 4SEE

# 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 4: SPECK Block Cipher



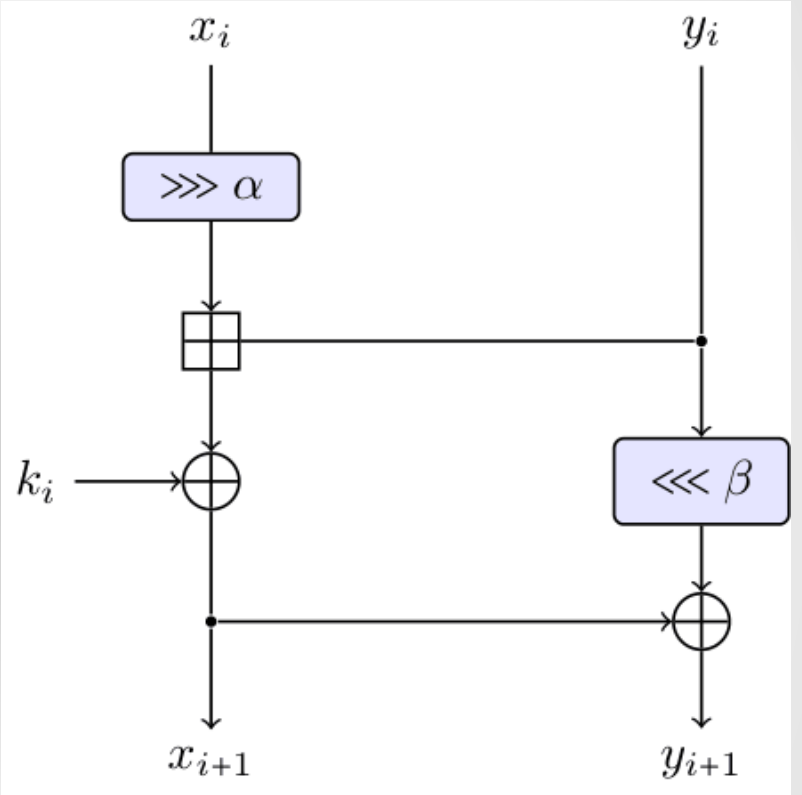
**SPECK Family of Block Ciphers**

- SPECK is a family of add-rotate-xor (ARX) lightweight block ciphers designed in 2013 by National Security Agency (NSA) of United States.
- SPECK supports seven key sizes: 64, 72, 96, 128, 144, 192, and 256 bits.
- Block size and number of rounds depend on the key size and possible variations are provided in the next slide.
- One round of SPECK is shown in the next slide and the key schedule of SPECK also uses this round function.

# Lesson 4: SPECK Block Cipher

## SPECK Family of Block Ciphers

| Block size | Key size | Rounds |
|---|---|---|
| 2x16 = 32 | 4×16 = 64 | 22 |
| 2x24 = 48 | 3×24 = 72 | 22 |
| 2x24 = 48 | 4×24 = 96 | 23 |
| 2x32 = 64 | 3×32 = 96 | 26 |
| 2x32 = 64 | 4×32 = 128 | 27 |
| 2x48 = 96 | 2×48 = 96 | 28 |
| 2x48 = 96 | 3×48 = 144 | 29 |
| 2x64 = 128 | 2×64 = 128 | 32 |
| 2x64 = 128 | 3×64 = 192 | 33 |
| 2x64 = 128 | 4×64 = 256 | 34 |




For the block word size of 16 bits ***alpha = 7*** and ***beta=2***.
For every other block word size ***alpha=8*** and ***beta=3***.

# Lesson 4: SPECK Block Cipher

## SPECK Family of Block Ciphers

- We represent ***k***-bit keyed SPECK with ***r*** rounds as ***SPECK-k-r***.
- In this work we optimized ***SPECK-64-22***, ***SPECK-72-22***, ***SPECK-96-26***, and ***SPECK-128-32*** using the CUDA programming language and our optimizations can easily be modified for other variants of SPECK.
- SPECK became an ISO/IEC RFID air interface standard in 2018 (ISO/IEC 29167-22:2018). This standard was reviewed in 2024 and confirmed.
- Note that the ISO standard contains ***SPECK-96-26***, ***SPECK-96-29***, ***SPECK-128-32***, and ***SPECK-256-34*** versions and without a proper warning of the security implications of using a short key, users may prefer short keys for performance and low hardware footprint.

# Next lecture

**TEA Family of Stream Ciphers**

- How TEA3 stream ciphers work
- How secure they are

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.