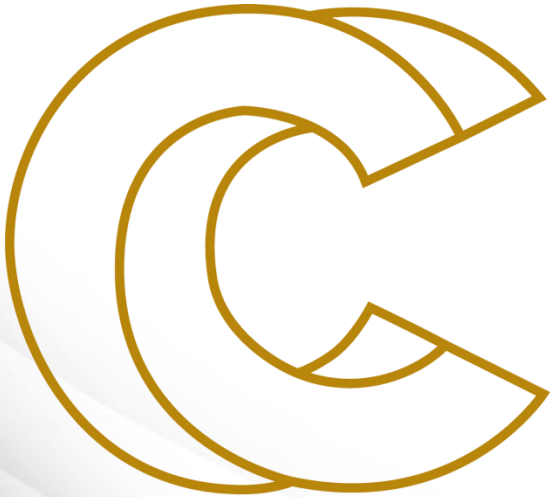

EURO 4SEE

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 10: Summary of GPU Performance of Ciphers

Summary of GPU Performance of Ciphers

Cipher	Key	Block	Rounds	RTX 2070 Super	RTX 4090
PRESENT-80	80	64	31	$2^{29.73}$ keys/s	$2^{32.90}$ keys/s
DES/3DES	56/168	64	16	$2^{30.78}$ keys/s	$2^{33.94}$ keys/s
AES-128	128	128	10	$2^{32.43}$ keys/s	$2^{34.64}$ keys/s
TEA3	80	-	-	$2^{32.54}$ keys/s	$2^{34.71}$ keys/s
KLEIN-64	64	64	12	$2^{33.19}$ keys/s	$2^{35.40}$ keys/s
KASUMI	128	64	8	$2^{32.72}$ keys/s	$2^{35.72}$ keys/s
SPECK-96-26	96	64	26	$2^{34.49}$ keys/s	$2^{36.72}$ keys/s

Lesson 10: Summary of GPU Performance of Ciphers

Summary of GPU Performance of Ciphers

Since a year has around $2^{24.91}$ seconds, in order to perform brute-force attack in a year, one needs around

1. **8** *RTX 4090 GPUs* to break ***SPECK-64-22***
2. **11** *RTX 4090 GPUs* to break ***KASUMI-64*** (GSM/GPRS)
3. **1575** *RTX 4090 GPUs* to break ***SPECK-72-22***
4. **1.36 million** *RTX 4090 GPUs* to break ***TEA3*** (TETRA)
5. **22 billion** *RTX 4090 GPUs* to break ***SPECK-96-26*** (ISO/IEC RFID standard)

Lesson 10: Summary of GPU Performance of Ciphers

Importance of Optimizations (KASUMI Example)

- [ACC+24] reported $2^{31.48}$ keys/s on an RTX 3090 GPU.
- [MBM25] reported $2^{35.59}$ keys/s on an AMD-Xilinx Alveo U250 FPGA.
- Although it is 16 times faster, that FPGA is 8 times more expensive than RTX 3090.
- Note that we achieved $2^{35.72}$ keys/s on an RTX 4090 GPU in [TL25], which is one fourth of the price of the FPGA used in [MBM25].

- [ACC+24] Gildas Avoine, Xavier Carpent, Tristan Claverie, Christophe Devine, and Diane Leblanc-Albarel. Time-memory trade-offs sound the death knell for GPRS and GSM. In Leonid Reyzin and Douglas Stebila, editors, Advances in Cryptology - CRYPTO 2024 - 44th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2024, Proceedings, Part IV, volume 14923 of Lecture Notes in Computer Science, pages 206–240. Springer, 2024.
- [MBM25] Konstantina Miteloudi, Lejla Batina, and Nele Mentens. A5/3 make or break: A massively parallel fpga architecture for exhaustive key search. IACR Transactions on Cryptographic Hardware and Embedded Systems, 2025(3):361–388, Jun. 2025.
- [TL25] Cihangir Tezcan and Gregor Leander. GPU assisted brute force cryptanalysis of GPRS, GSM, RFID, and TETRA. IACR Trans. Symmetric Cryptol., 2025(1):309–327, 2025.

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.