GPU-Assisted Brute-Force Cryptanalysis of KASUMI on Lower-Tier GPUs

Dániel Orsós
University of Szeged, Szeged, Hungary

This talk takes as its starting point the GPU-assisted brute-force cryptanalysis workflow demonstrated by Cihangir Tezcan and Gregor Leander and adapts the same core idea to the KASUMI block cipher as standardized for 3G/4G confidentiality and integrity [1]. The practical goal is to evaluate the KASUMI encryption mapping for a very large number of key candidates efficiently on graphics hardware.

We study two execution modes of the same CUDA implementation: REG, an early-reject (prefiltered) exhaustive search where most candidates are discarded after a partial computation, and TMTO (time–memory trade-off) table generation where every candidate produces an output that is written to memory. Here CUDA (Compute Unified Device Architecture) denotes NVIDIA's GPU programming model, and an S-box is a fixed substitution table that provides the dominant nonlinearity inside KASUMI's round functions.

The main contribution is an architecture-aware porting and re-parameterization of the baseline GPU kernels—originally tuned for a high-end device—to lower-tier Turing GPUs (GeForce RTX 2070 and GTX 1650 Ti) while keeping the cryptographic core invariant. This includes (i) feasible grid/block configurations under per-SM resource limits, (ii) shared-memory handling of S-boxes under reduced block sizes, and (iii) compiler-level guidance to avoid launch failures caused by excessive per-block resource usage.

Measured runtimes show large, reproducible performance gaps across the three GPUs and highlight the different bottlenecks of REG (compute-dominated due to early rejection) versus TMTO (memory-dominated due to mandatory global writes). Finally, a "dollarday" cost model is applied to translate runtimes into estimated monetary cost; under the tested workload, the higher-end GPU is not only faster but also more cost-effective per completed run, while renting GPUs is slightly more expensive than local execution under the chosen assumptions.

[1] C. Tezcan, G.Leander, GPU Assisted Brute Force Cryptanalysis of GPRS, GSM, RFID, and TETRA, *IACR Transactions on Symmetric Cryptology* (2025), 309–327.