FPGA-Based Massively Parallel Architecture for Exhaustive Key Search of A5/3

Konstantina Miteloudi[1] Lejla Batina[1] Nele Mentens[2,3]

[1]DiS Group, Radboud University, Nijmegen, The Netherlands [2]imec-COSIC - ES&S, ESAT, KU Leuven, Belgium [3]LIACS, Leiden University, The Netherlands

Motivation

- A5/3 algorithm is used in 2G (GSM) and 3G (UTMS) mobile networks.
- Key size of A5/3 is 128 bits. For compatibility reasons with an older version of A5/1, the effective key size is 64 bits. This makes A5/3 theoretically vulnerable to brute-force attacks.
- If we do a brute-force attack, how fast can we recover the key depending on the available computing power we have?
- In this work we present:
  - a massively parallel FPGA-based architecture for exhaustive key search in order to determine the feasibility of a brute-force attack on A5/3 and
  - a coarse evaluation of the trade-off between time and cost for this attack.

The Idea

- The standard A5/3 algorithm is based on five (5) blocks of the KASUMI block cipher and produces a 228-bit ciphertext.
- The basic idea in our approach is that from the 228 bits of the ciphertext only the first 64 bits need to match in order to have a key candidate.

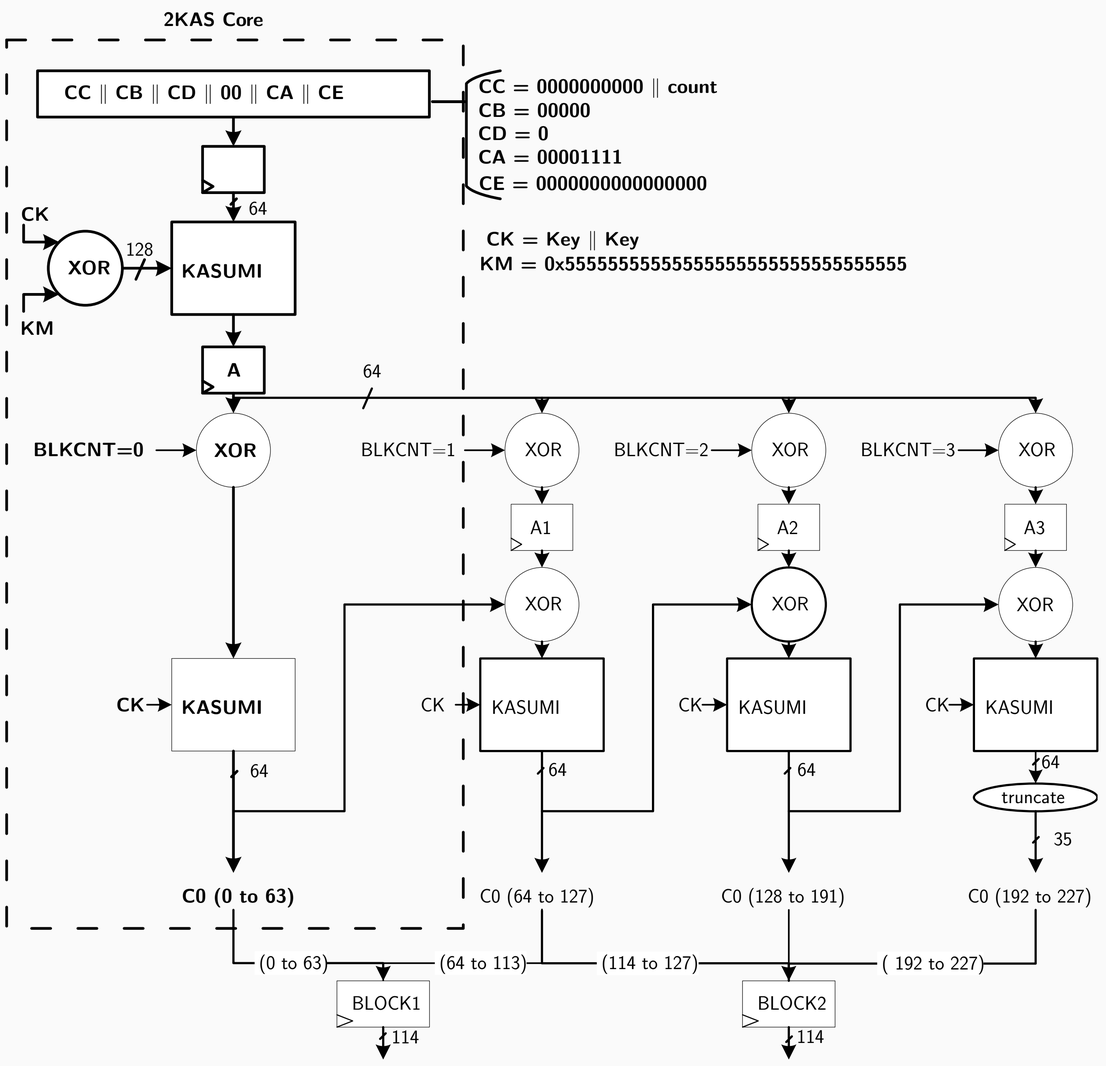

Figure 1: The A5/3 algorithm and the 2KAS core (2 blocks of KASUMI).

- This approach requires less resources which is a prerequisite for achieving a high level of parallelism.
- Also, it creates the conditions to have a low-latency hardware architecture.

Proposed Hardware Architecture

- **Top-level design**

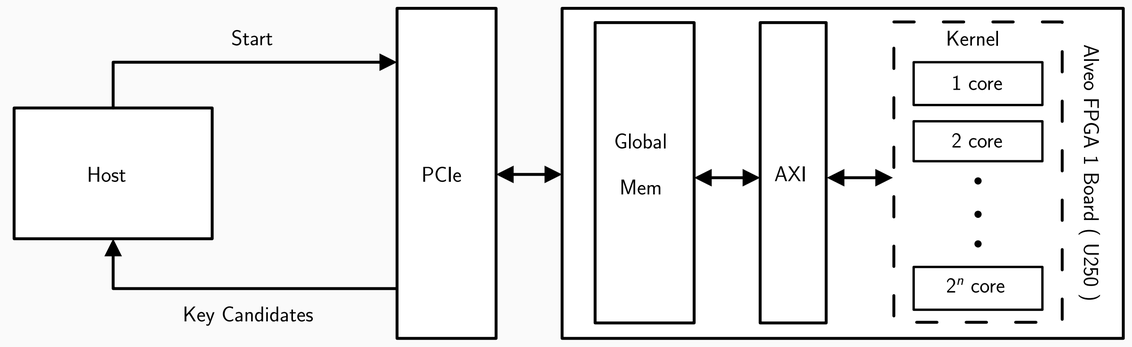

Figure 2: Top-level design on Alveo U250 AMD-Xilinx FPGA board

- **Basic core**

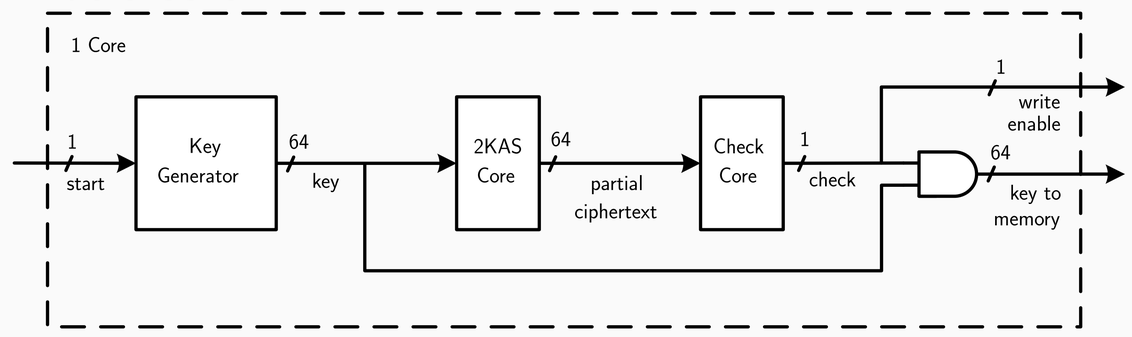

Figure 3: Hardware architecture of one core that performs the key search

Results

- Frequency: 500 Mhz $\rightarrow$ evaluate 1 key every 2ns.
- 128 cores fit in 1 Alveo U250 $\rightarrow$ evaluate $64 * 10^9$ keys/second.

Table 1: Resources

#	LUTs	Util. on Alveo	Regs	Util. on Alveo	BRAMs	Util. on Alveo
1 core	10462	0.61%	5598	0.16%	16	0.6%
128 cores	1348131	78%	721462	20.9%	16	0.6%

- The expected run time of exhaustive key search is $\approx K * t/(2 * c)$, where K the number of possible keys, t the time for 1 key evaluation and c the number of cores.

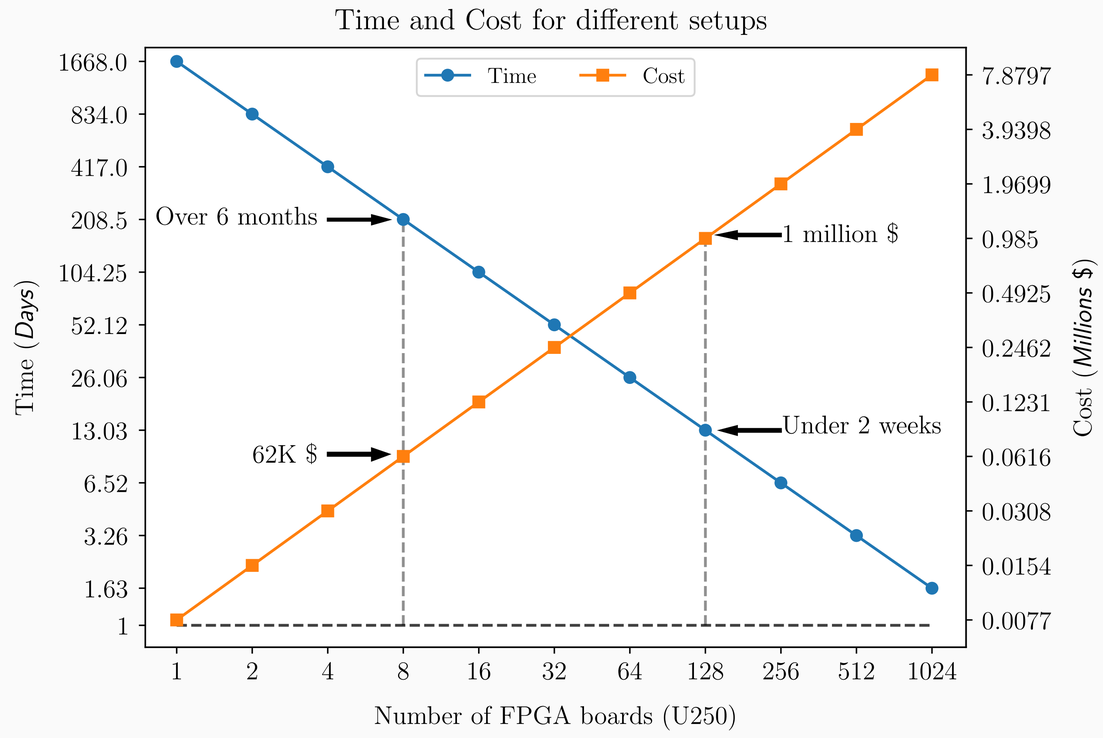

Figure 4: Time and Cost for different setups. All axes are in log scale.

- The current unit cost of Alveo U250 is 7695$.
- A cloud based FPGA has hourly cost 1.65$ which leads to a cost for one attack around $66K.

CESCA Laboratory

Radboud University