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

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

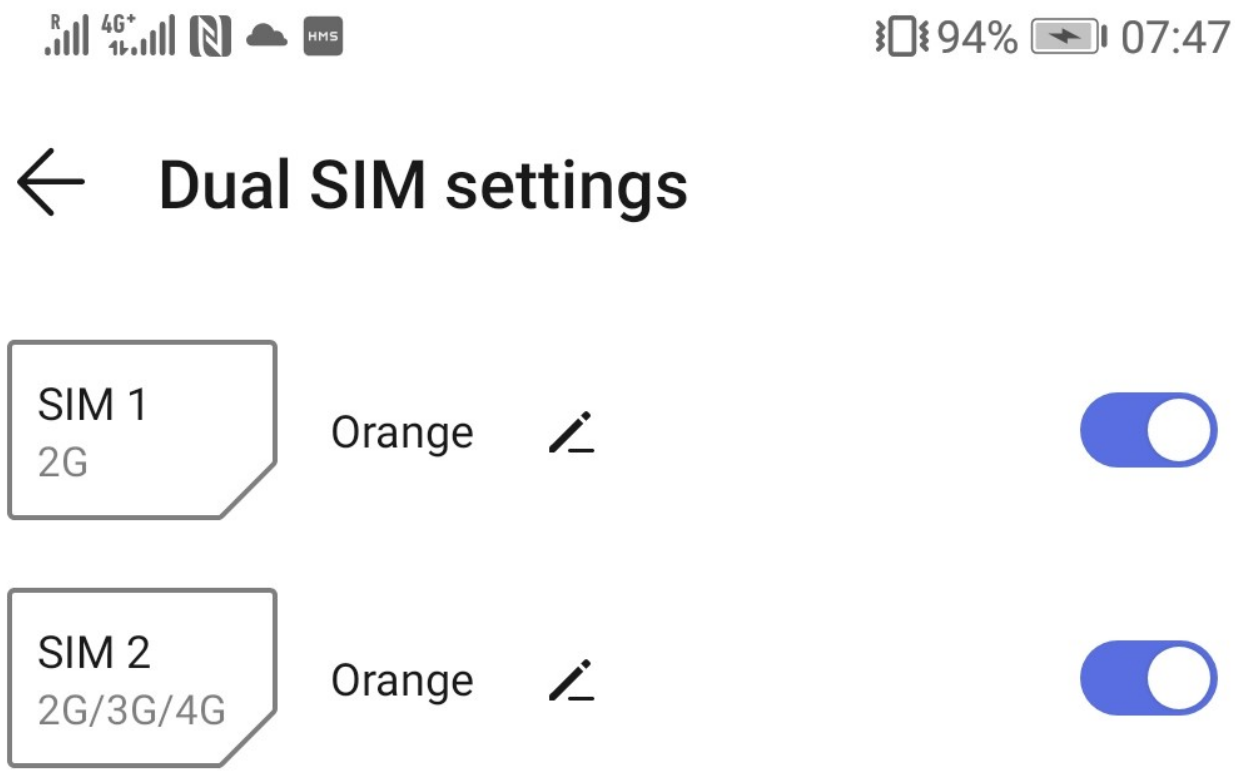
[1]DiS Group, Radboud University, Nijmegen, The Netherlands

[2]imec-COSIC - ES&S, ESAT, KU Leuven, Belgium

[3]LIACS, Leiden University, The Netherlands

13th International Conference on Cryptology
AFRICACRYPT 2022, July 18-20, 2022 - Fes, Morocco

2G Networks still in use



- 2G networks are still used in most parts of Europe, Africa, Central America and South America as a fallback service.

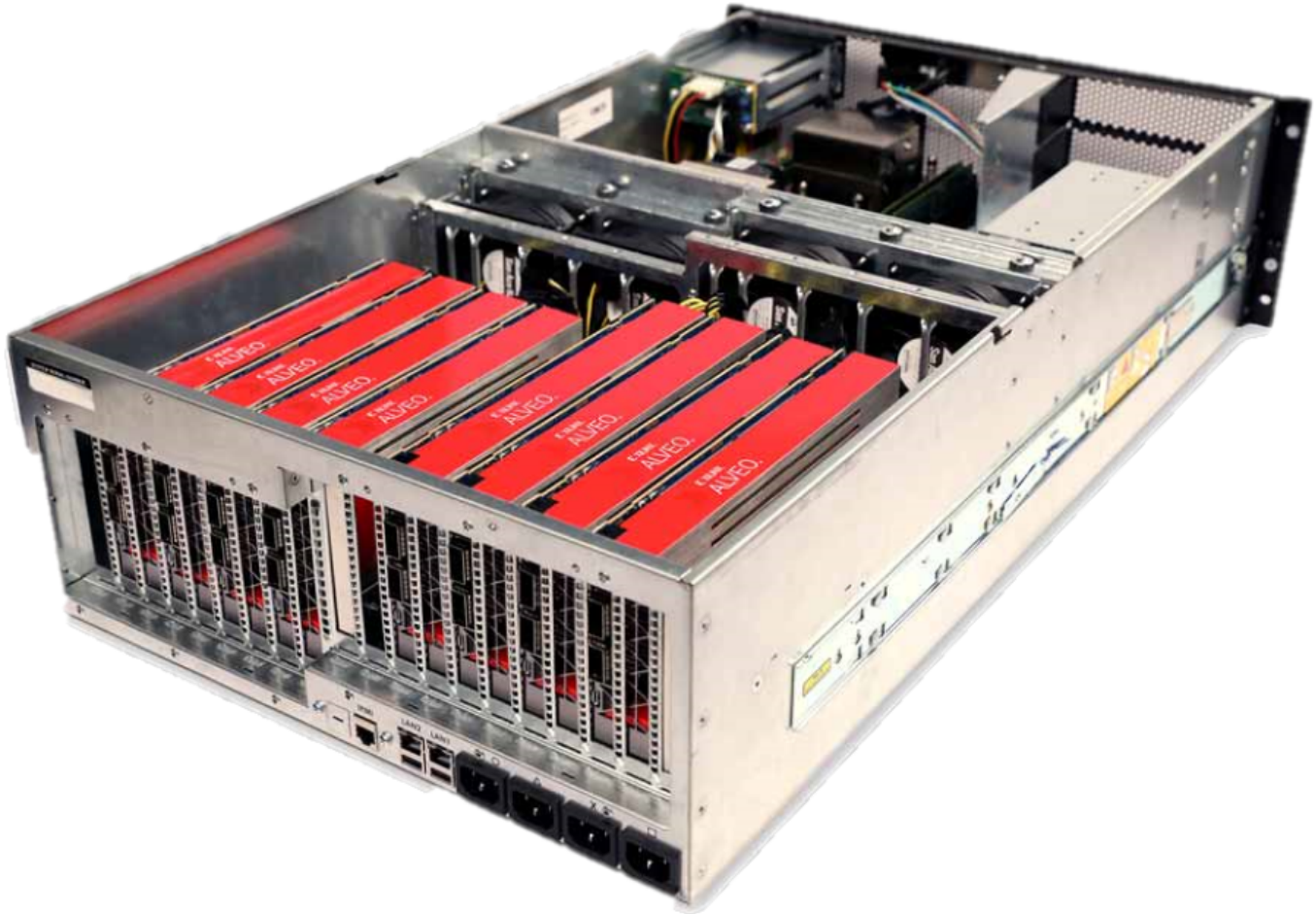
Security in 2G Networks

- A5/3 algorithm is used in 2G (GSM) and 3G (UTMS) mobile networks.
- A5/3 is based on KASUMI block cipher.
- 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.

Research Question

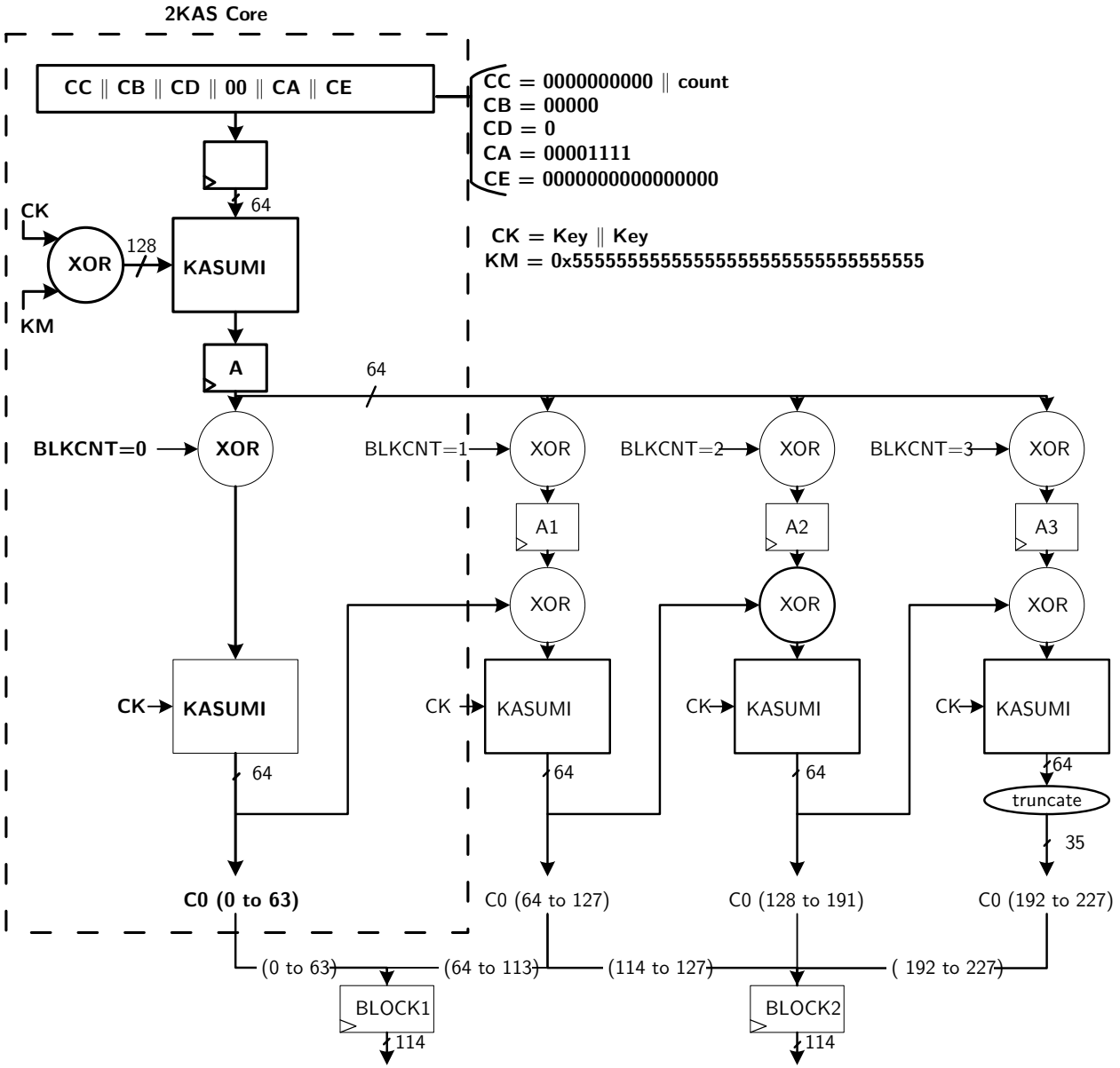
- If we do a brute-force attack, how fast can we recover the key depending on the available computing power we have?

The computing power!

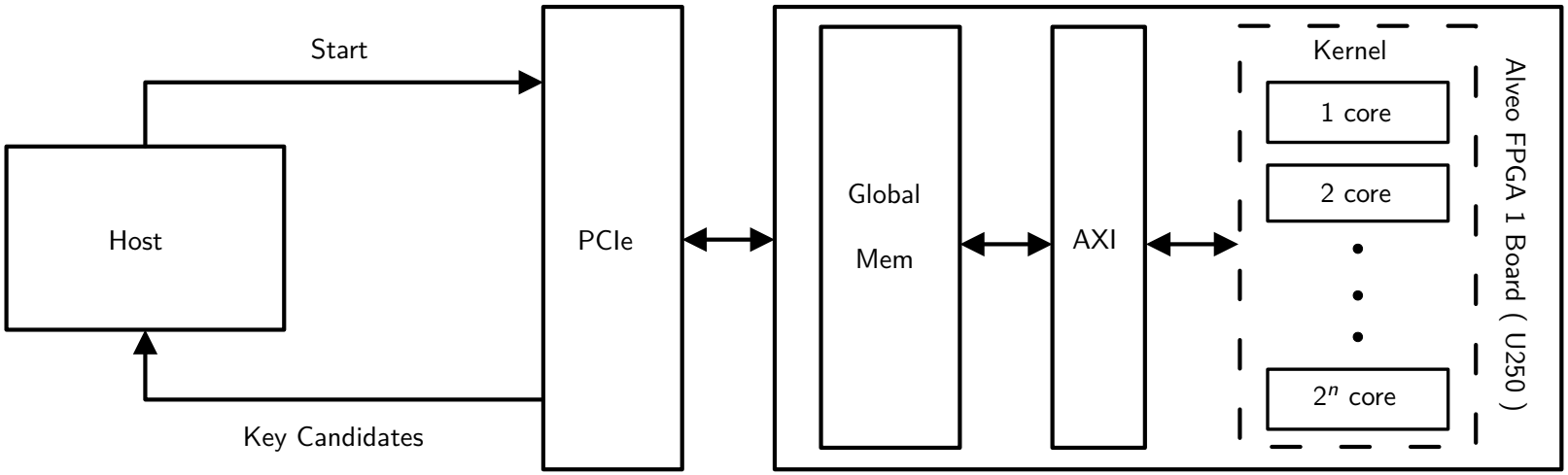


- A "typical" cloud computation server with 8 FPGA ALVEO U250 boards.

The idea of partial A5/3 algorithm

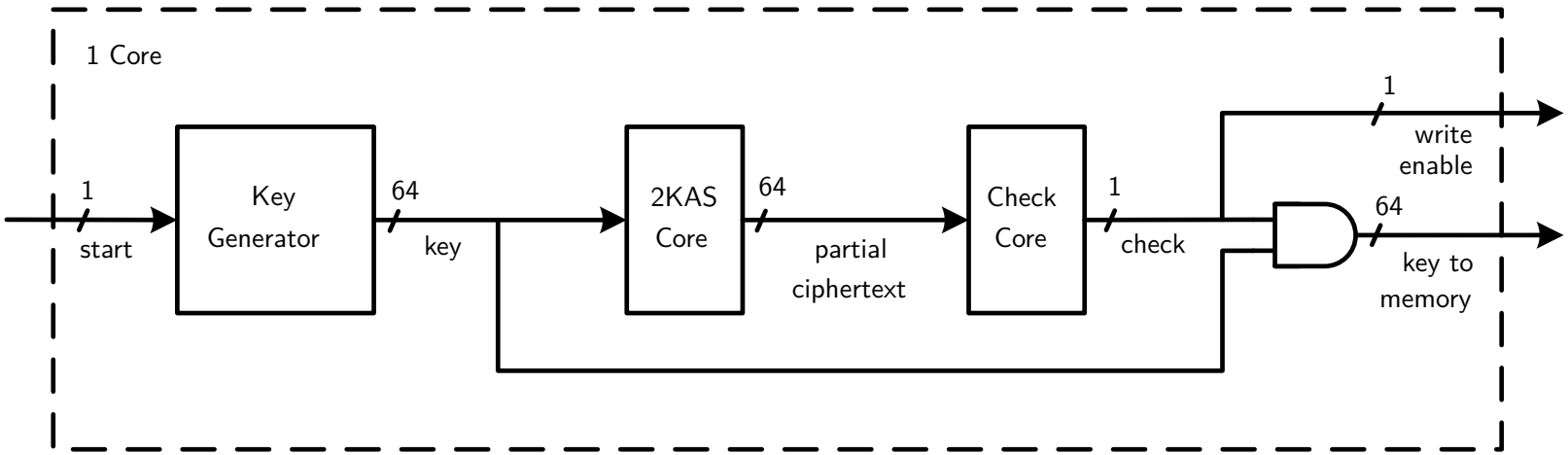


Top-level design



- Number of cores $\rightarrow$ power of two (2^n):
  - no need for extra control for key space allocation
  - each core searches its own key subspace

Basic core



- Fully pipelined design, checks one key per clock cycle

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: 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%

Average Expected Run Time

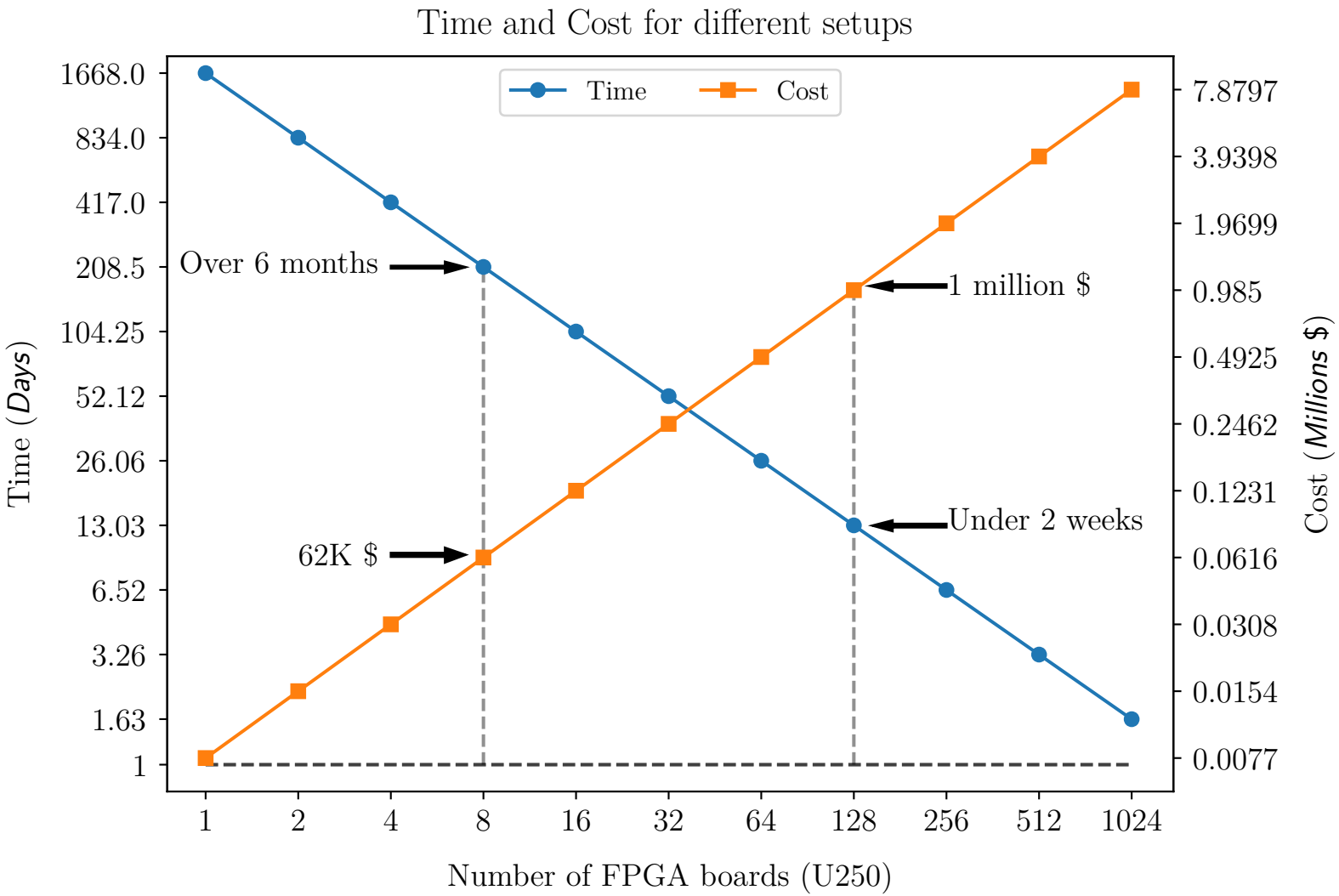
- The expected run time of exhaustive key search is:

$$\approx \frac{K * t}{2 * c}$$

  - with $K = 2^{64}$ the number of possible keys,
  - t the time for 1 key evaluation and
  - c the number of cores.
  - On average we expect to recover the key in half way of the search.

Time and Cost evaluation

- The current unit cost of Alveo U250 is 7695$.



Merci!