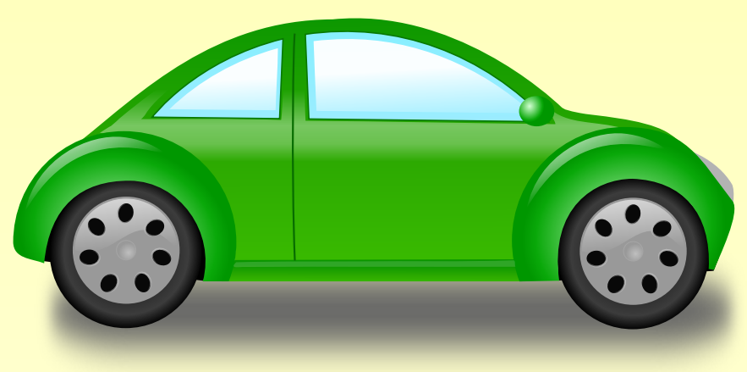
Lightweight Cipher Resistivity against Brute-Force Attack: Analysis of PRESENT

Jan Pospíšil, Martin Novotný

Nowadays ligthweight ciphers are compromised

Hitag2



BROKEN!

KeeLoq

BROKEN!

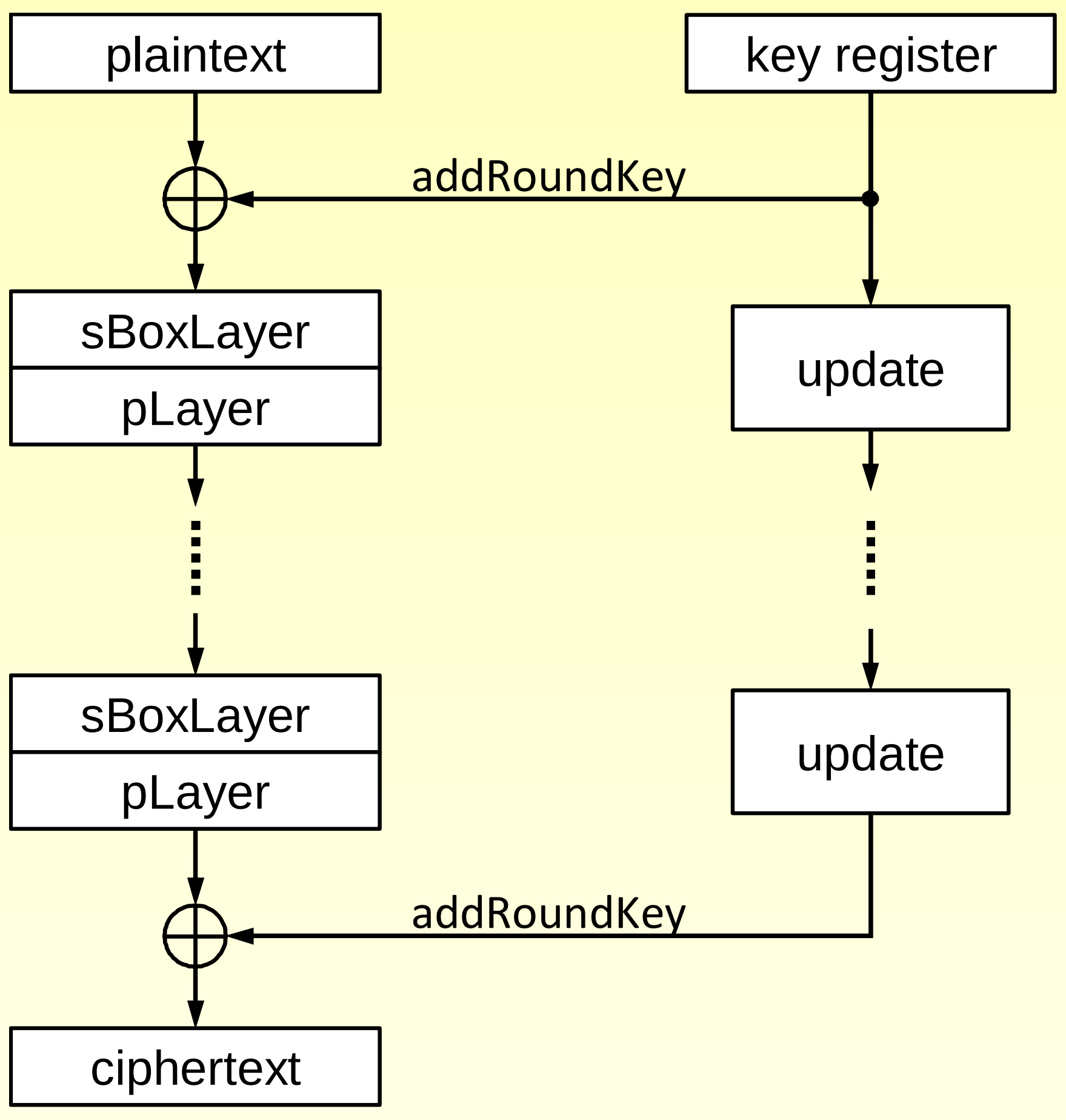
Crypto1

BROKEN!

Replacement must satisfy very strong design constrains on area and power consumption.

PRESENT cipher

- New lightweight cipher (CHES 2007)
- Symmetric block cipher — 64 bit blocks
- 80 bit or 128 bit key, 31 rounds

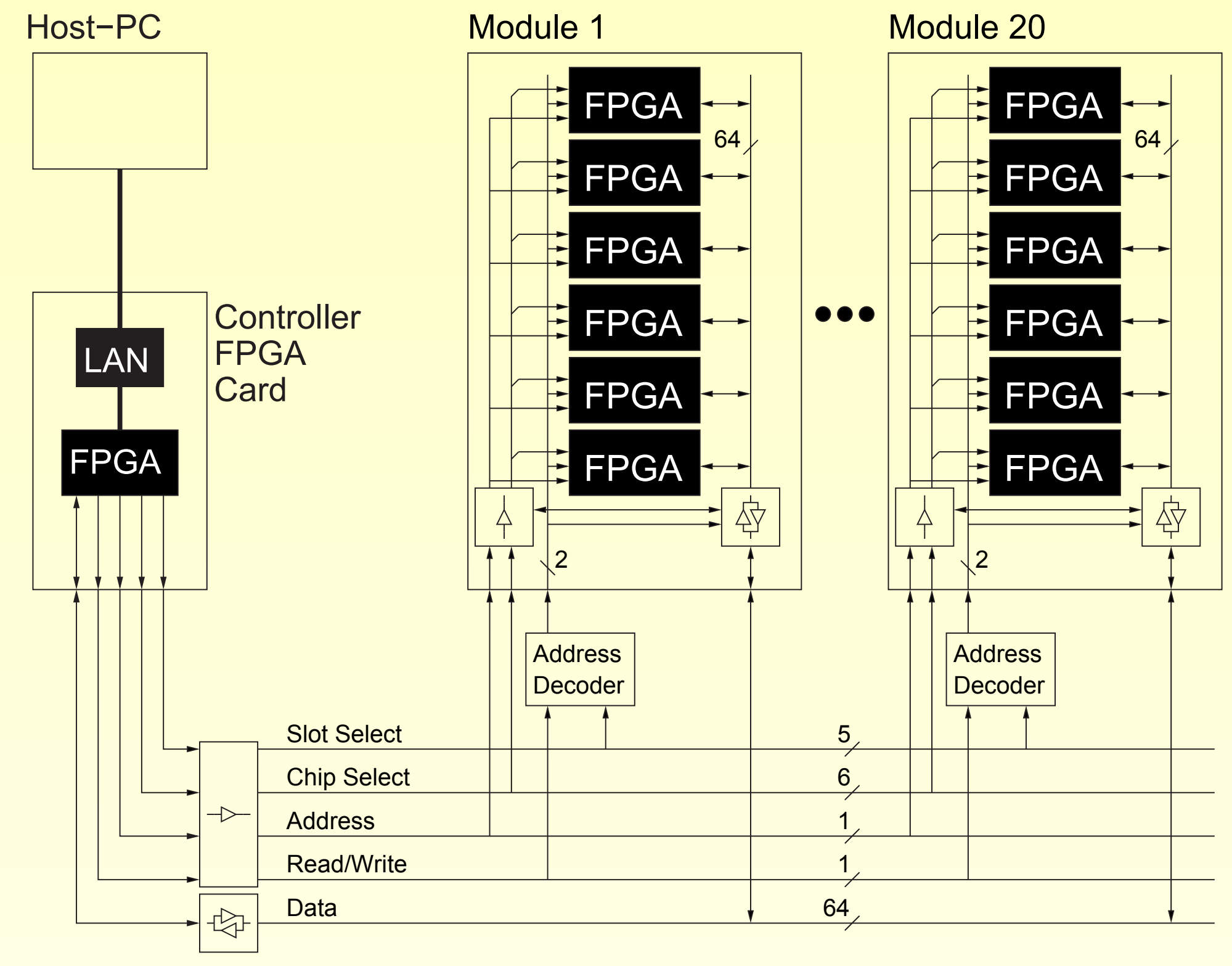


Can PRESENT be compromised, too?

?

COPACOBANA

- Cost-Optimized Parallel Code Breaker
- High-performance, low-cost FPGA cluster
- 120 × Xilinx Spartan-3 1000
- Breaks DES (6.4 days), Hitag2 (1 hour), ...



Design

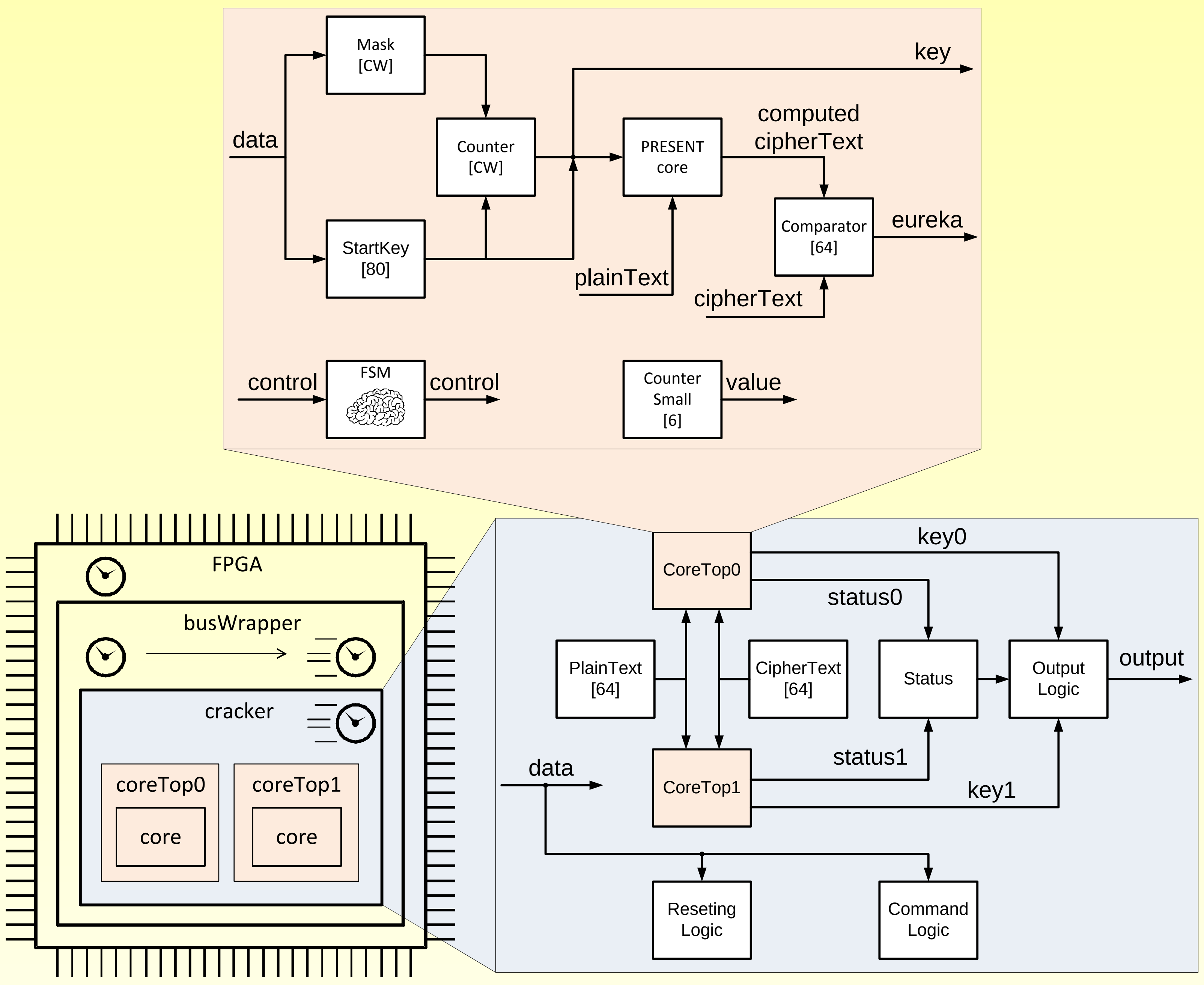
- VHDL, Xilinx ISE 11.5, brute-force approach
- 3 types of core tested: simple, **pipelined** and serial
- Search space → key subspaces — good scalability

	simple core	**pipelined core**	**serial core**
size	270 kGE	450 kGE	20 kGE
chip space	27%	45%	2%
critical path	83.3 ns	4.4 ns	5.9 ns
maximal frequency	12 MHz	227 MHz	170 MHz
speed ⋆	1	1 ⋆⋆	1/32
throughput	0.77 Gbit/s	14.53 Gbit/s	0.34 Gbit/s
maximum cores on chip	3	2	50
chip throughput	2.31 Gbit/s	29.06 Gbit/s	17 Gbit/s

⋆ results computed in each cycle

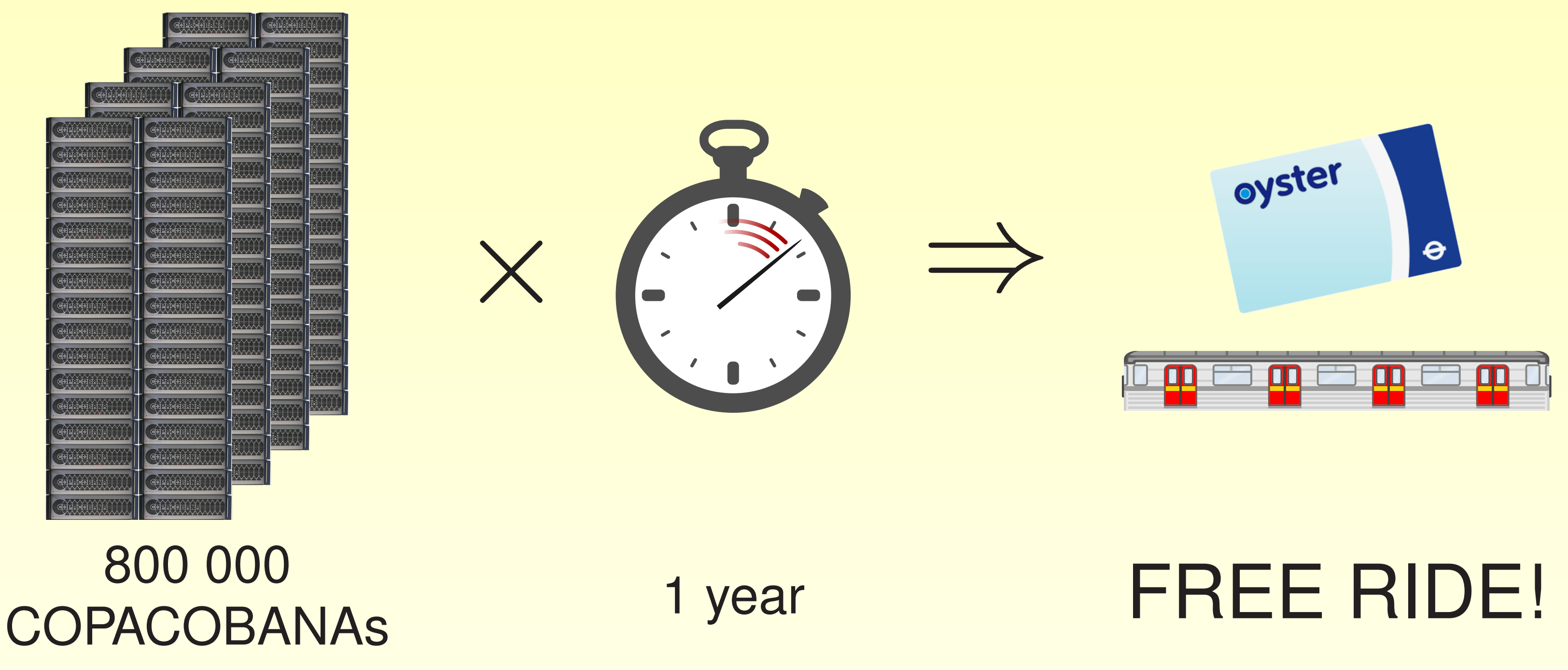
⋆⋆ with 31 cycles of setup delay (without results)

Design overview



Results

- 2 pipelined cores in FPGA ⇒ 240 cores in COPACOBANA
- 100 MHz clock ⇒ 24 billion keys per second
- 80 bit key ⇒ 800 000 COPACOBANA-years on average



Conclusions

- 800 000 COPACOBANAs ≈ GDP of Mongolia
- PRESENT is a good solution for lightweight cryptography

Acknowledgement

This work has been partially supported by grant No. SGS12/094/OHK3/1T/18 and grant No. SGS10/119/OHK3/1T/18.