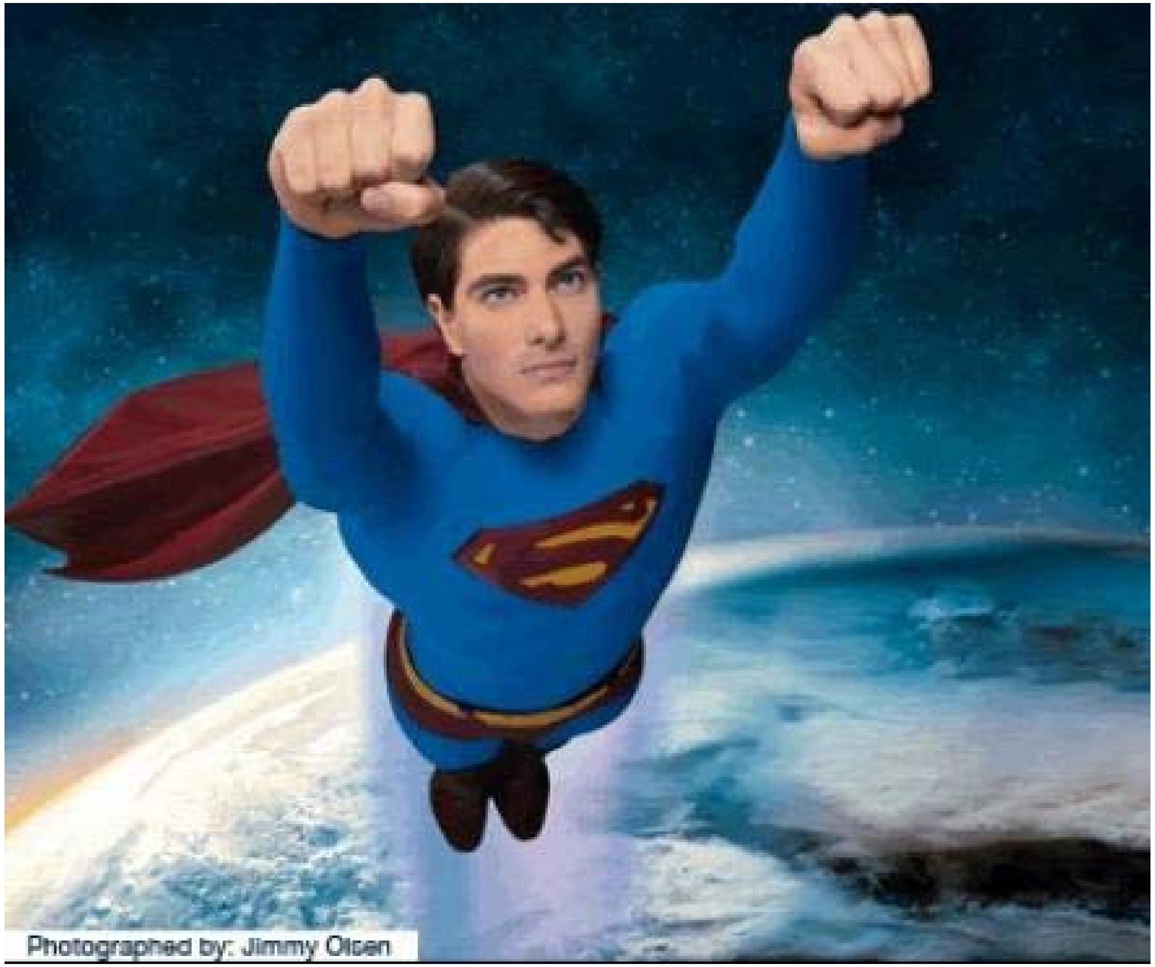
Breaking Ciphers

with Special Purpose Hardware

hgi
Horst Görtz Institute
for IT-Security

PC‘s = slow…

POWER!



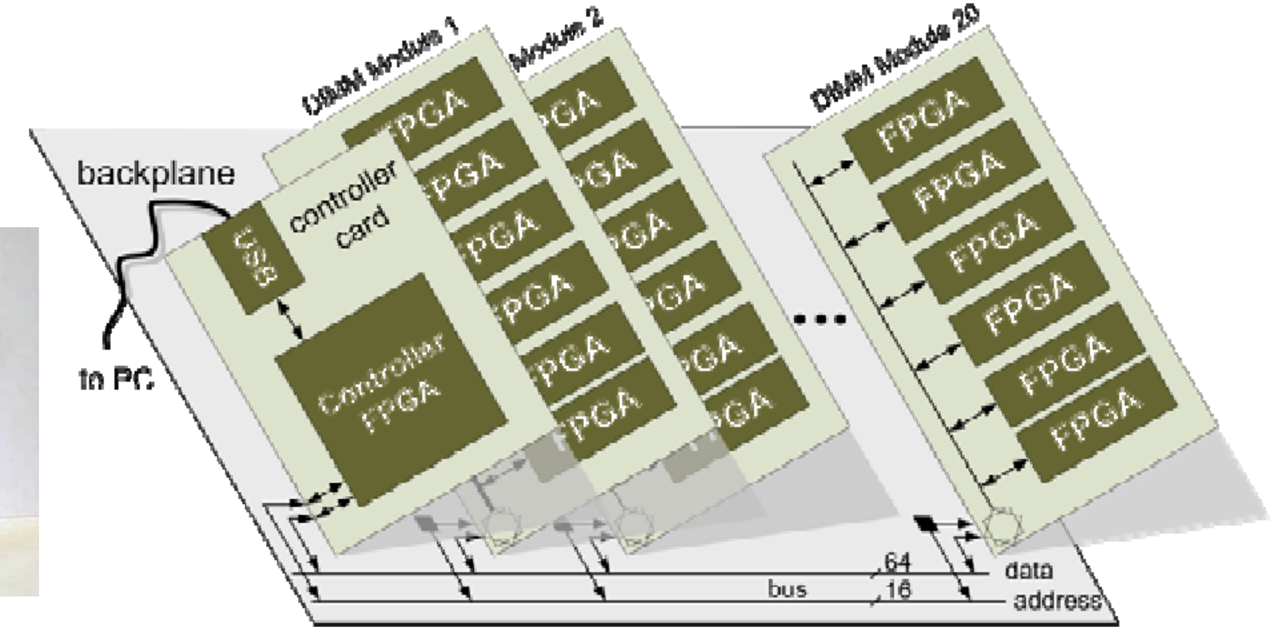
Steal Secrets & Break Ciphers !

New Invention!

- very fast hardware
- cost-optimized !
- parallelized !

Special Purpose Hardware

- FPGA-based reconfigurable machine for cryptanalysis
- Parallel architecture built out of **120 Xilinx Spartan3 FPGAs**
- Modular design:
  - Backplane with FPGA modules (each with 6 low-cost FPGAs)
  - Controller card with USB interface or TCP/IP Interface

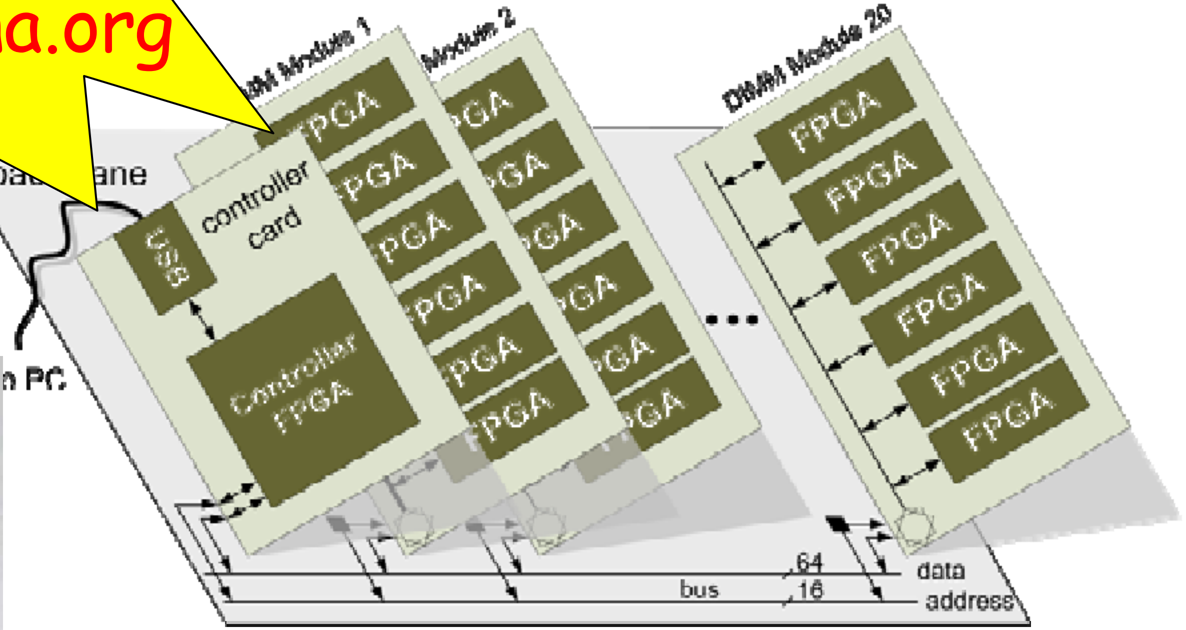


Special Purpose Hardware

- FPGA-b   ed   onfigurable machine for cryptanalysis
-    ralle   ur   uilt out of **120 Xilinx Spartan3 FPGAs**
-
  A modules (each with 6 low-cost FPGAs)
  USB interface or TCP/IP Interface

available from

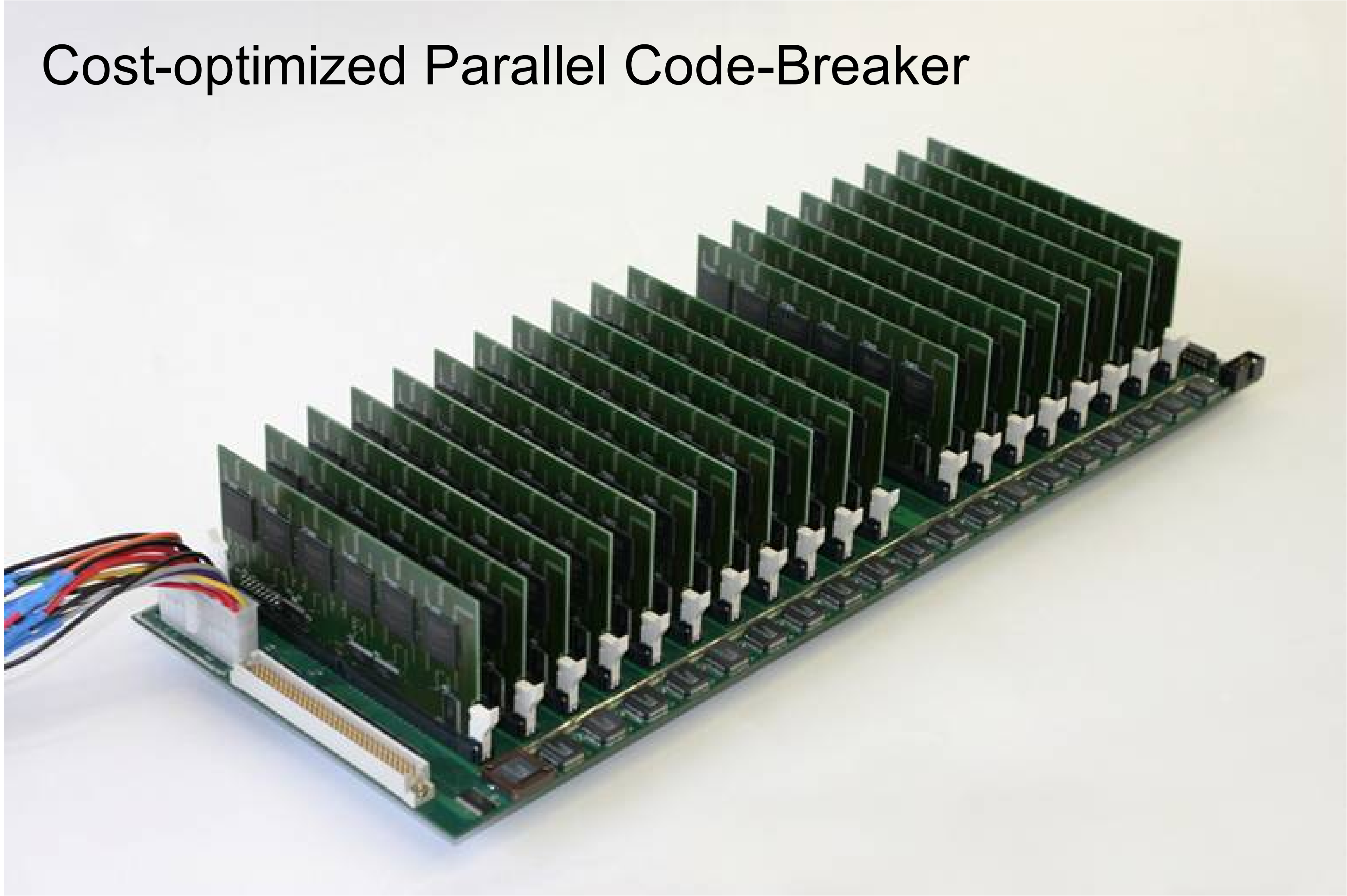
www.copacobana.org



Fastest Machine of the Summer!

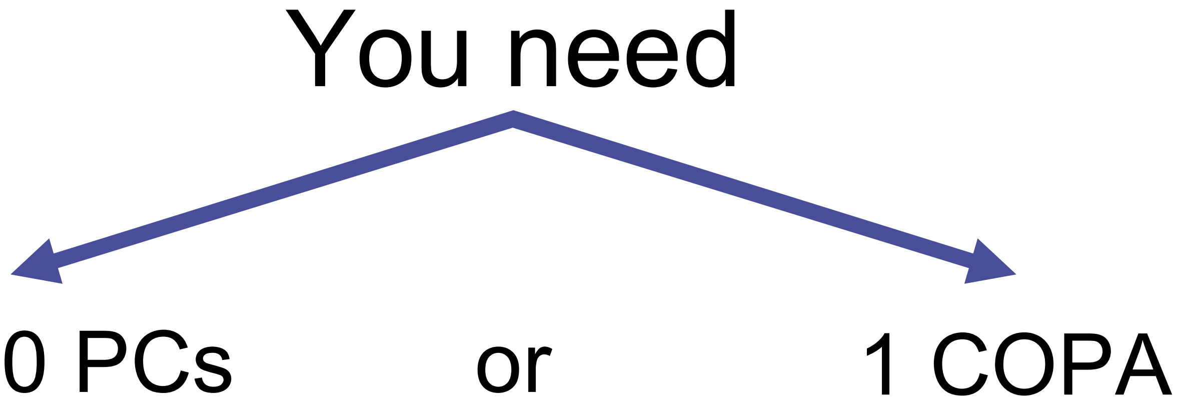
… Easy to remember: Copacobana…

COPACOBANA: FPGA Modules



Cost-optimized Parallel Code-Breaker

To break DES in 6.4 days in average



You need

32,640 PCs or 1 COPA

Consumption-performance ratio of DES[1]: PC vs. FPGA

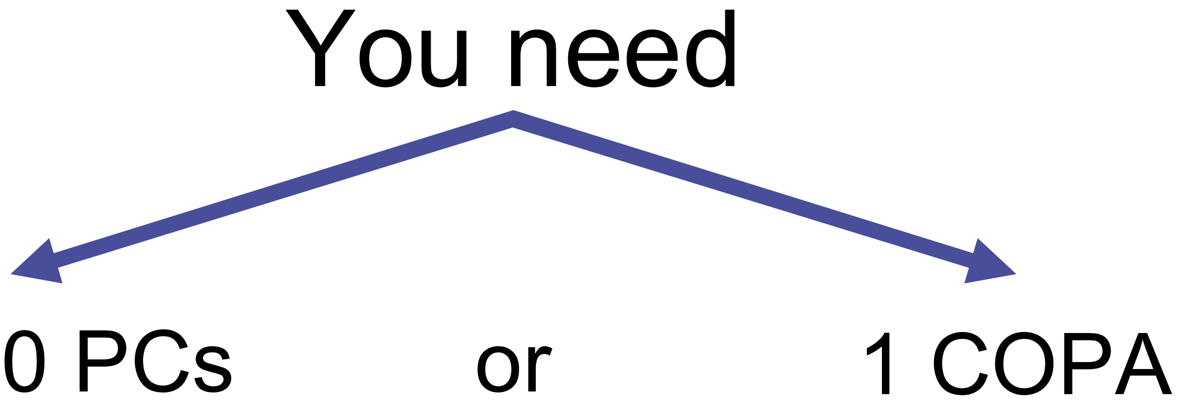
– consumption per the average DES brute-force attack

	Pentium4@3GHz:	≈ 750 MWh
	Xilinx XC3S1000@136MHz:	≈ 92 kWh

► Consumtion-performance ratio differs by 3-4 orders of magnitude!

[1] Based on actual optimized implementations

To break DES in 6.4 days in average



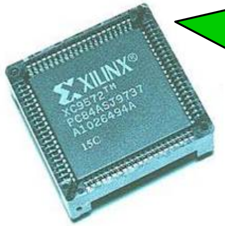
You need

32,640 PCs or 1 COPA

Consumption-performance ratio of DES[1]: PC vs. FPGA

– consumption per the averag ES force attack

Pentium4 h



kWh

Green cryptanalysis:
Our contribution to
global warming

► Consumtion-performance ratio differs by 3-4 orders of magnitude!

[1] Based on actual optimized implementations

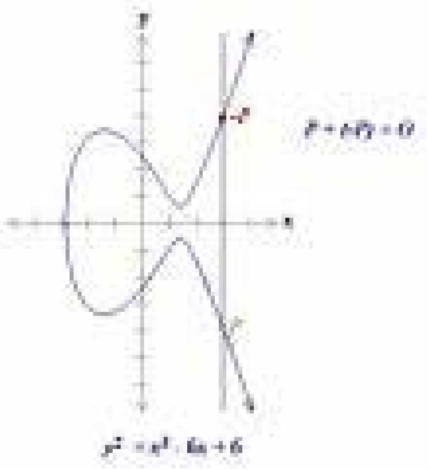
Play NSA

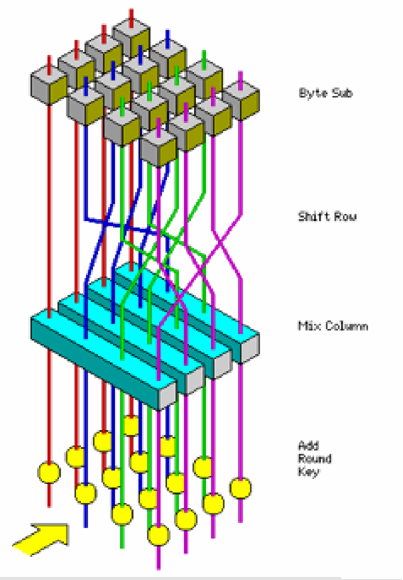
9 of 10 spies recommend COPACOBANA

It is POWERFUL

Break all kinds of ciphers!

Z A B C D E F G H I J K L M N O P Q R S T U V W X Y
M N O P Q R S T U V W X Y Z A B C D E F G H I J K L





Break electronic Passports!

Very cool: Steal Identities! Track People!

Breaking the A5/1

Guess complete content of **R1**, **R2**

Derive content of **R3** step-by-step:

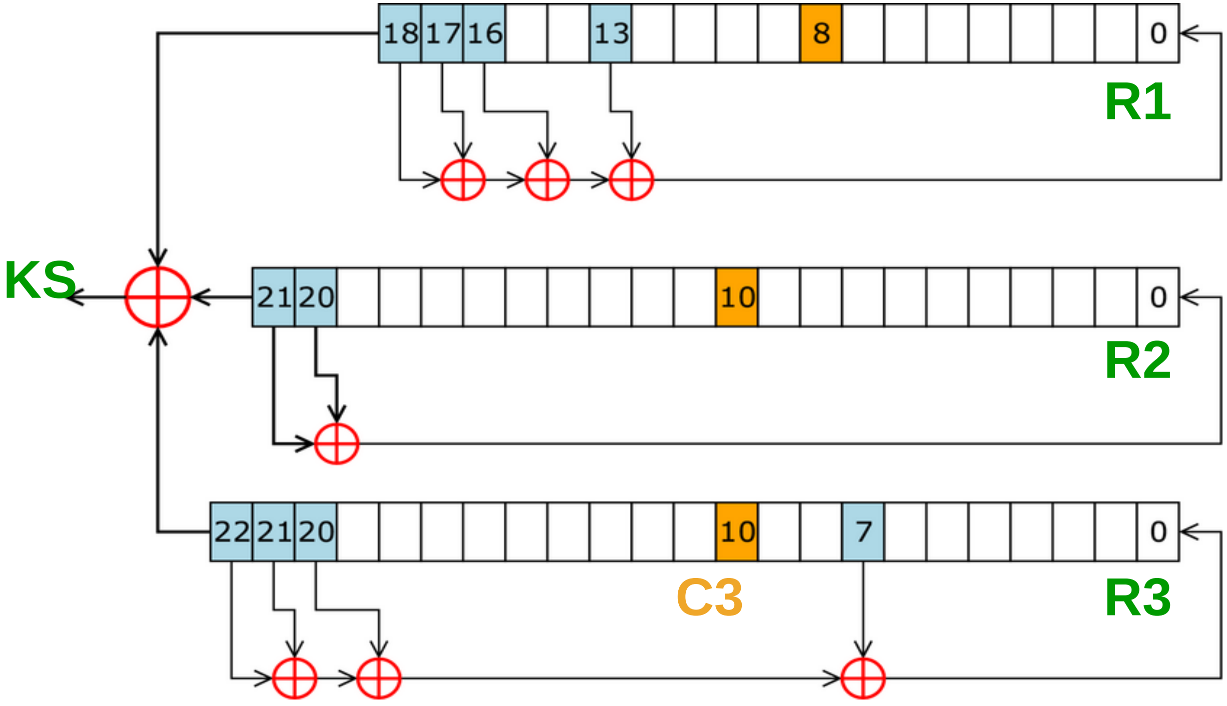
a. Derive **MSB** of **R3** from **R1**, **R2**, and known **KS**

b. Guess C3 (clocking bit of R3)

until **R3** is completely determined.

Continue clocking A5/1 & compare generated **KS** against known **KS**

If **64** bits of generated **KS** match, then **CANDIDATE FOUND**



Have (il)legal fun!

Beamter beim Lauschen mit einem Richtmikrofon

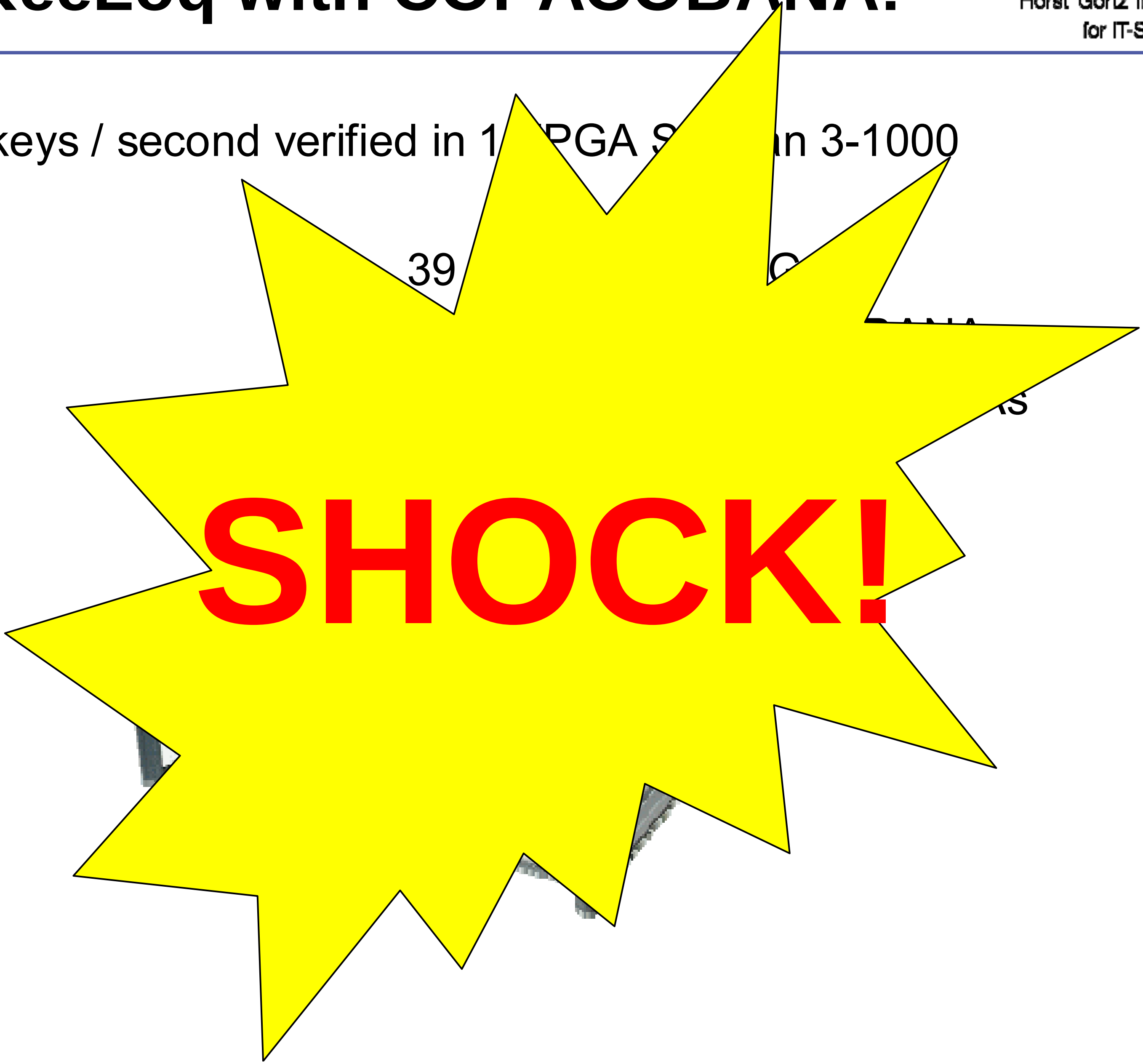
Break KeeLoq with COPACOBANA!

110 million keys / second verified in 1 PGA S an 3-1000

32 bit seed: 39 C

48 bit seed: ANA

60 bit seed: s

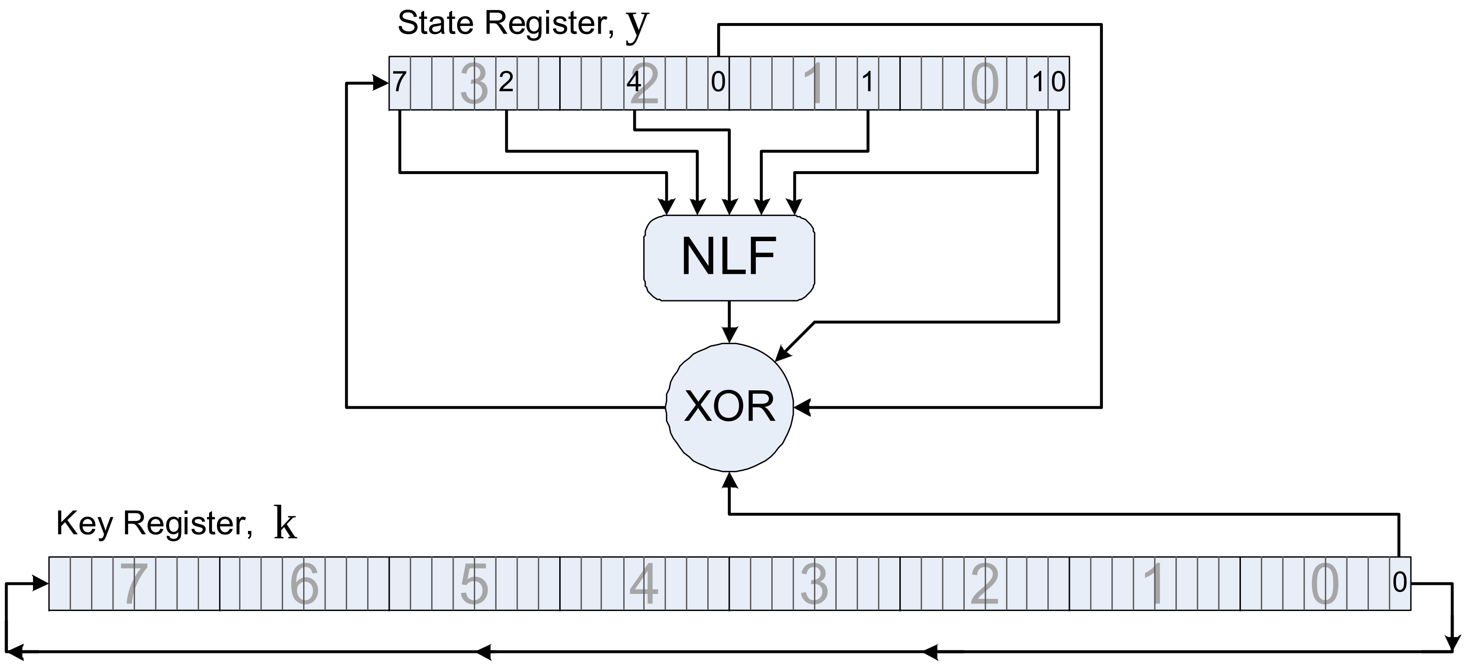


SHOCK!

Break KeeLoq with COPACOBANA!

110 million keys / second verified in 1 FPGA Spartan 3-1000

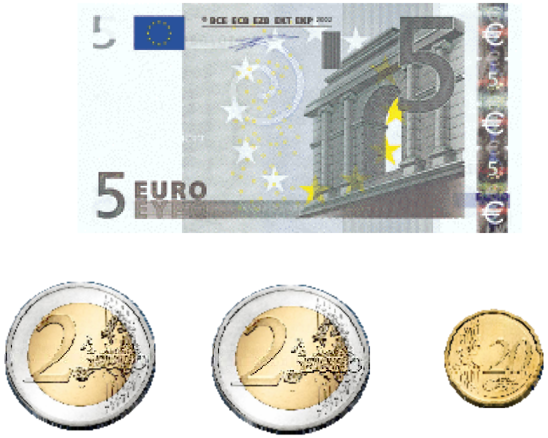
32 bit seed:	39 seconds / 1 FPGA
48 bit seed:	5.9 hours / 1 COPACOBANA
60 bit seed:	101 days / 10 COPACOBANAs



To break DES

You pay for electricity

€ 75 000 or € 9.20



9 of 10 economists recommend COPACOBANA

It is CHEAP

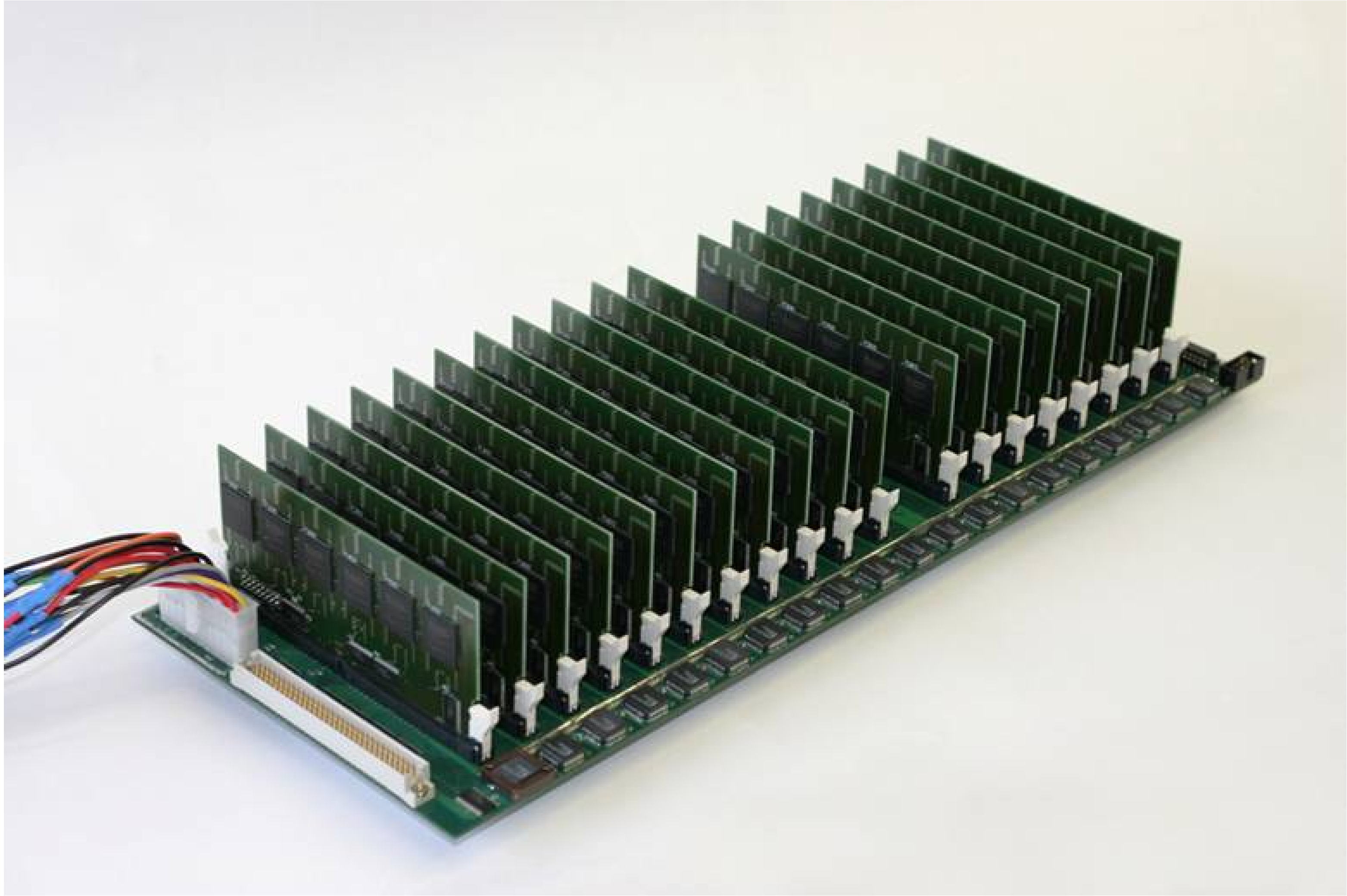
Fastest Machine of the Summer!

… Easy to remember: Copacobana…

COPACOBANA!

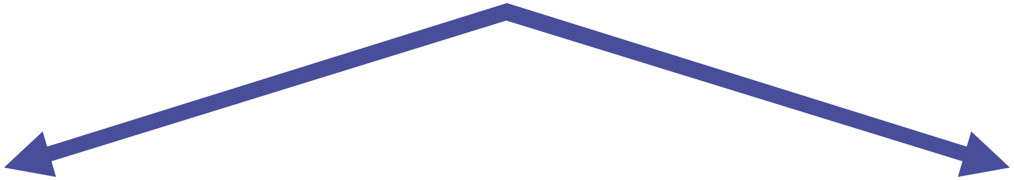
► COPACOBANA

COPACOBANA: FPGA Modules



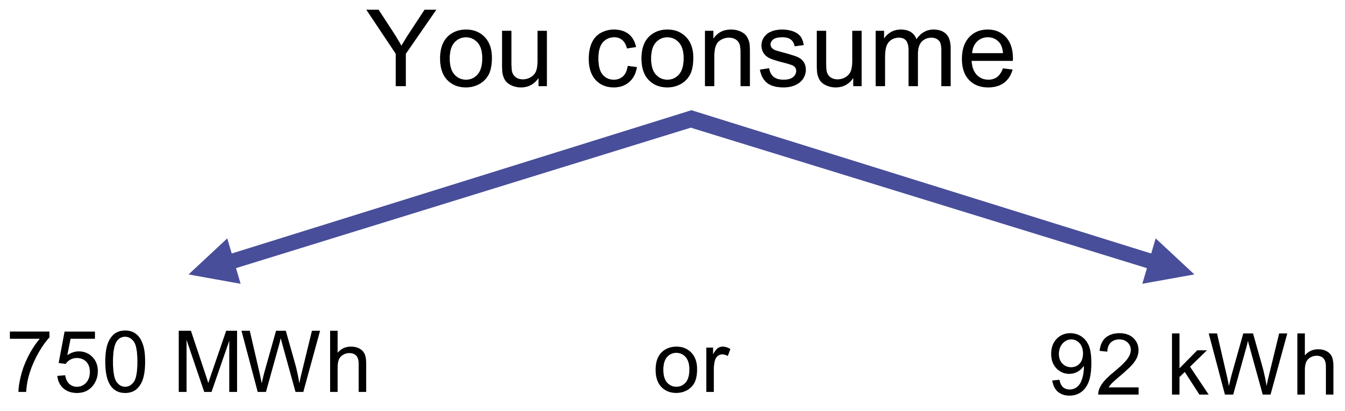
To break DES in 6.4 days in average

You need



32,640 PCs or 1 COPA

To break DES

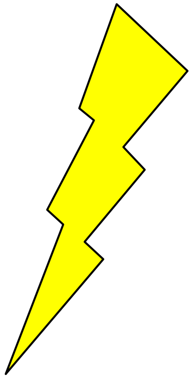


You consume

750 MWh

or

92 kWh

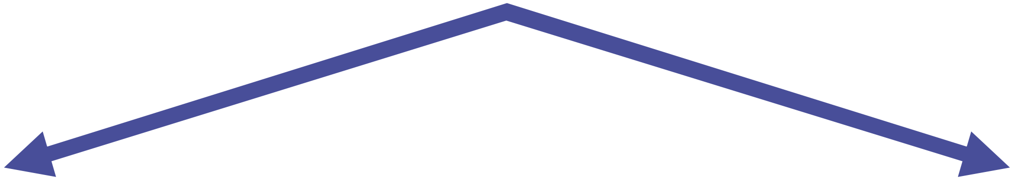


9 of 10 environmentalists recommend COPACOBANA

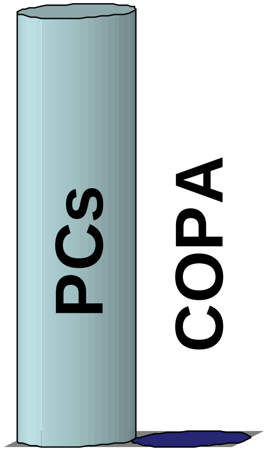
It is GREEN

To break DES

You produce CO_2



459,262 kg or 56 kg



Play NSA

SLOW!

CRAY
RESEARCH, INC.

CRAY-1

COMPUTER SYSTEM®

HARDWARE REFERENCE MANUAL
2240004

Fastest Machine of the Summer!

www.copacobana.org