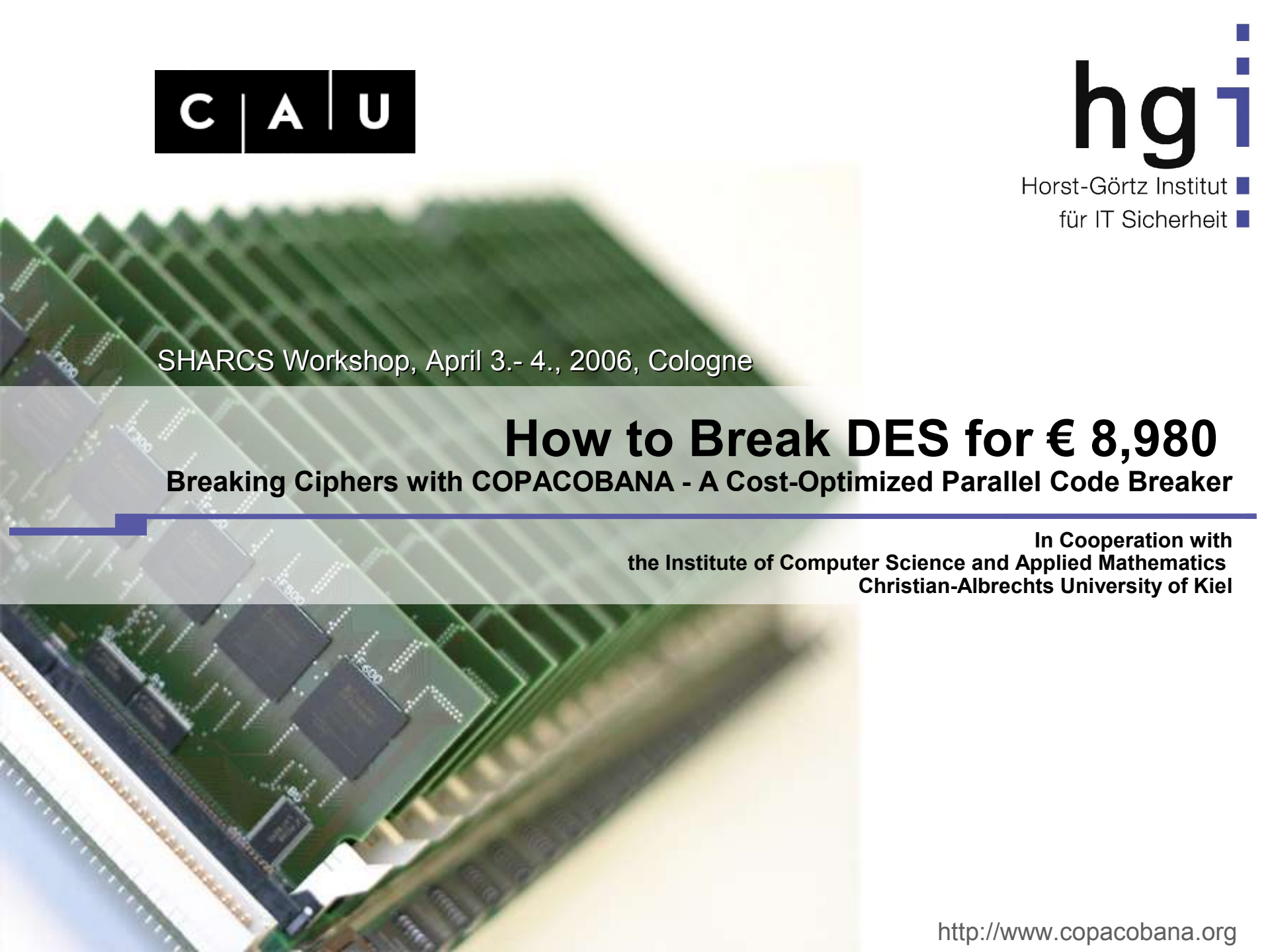


SHARCS Workshop, April 3.- 4., 2006, Cologne

How to Break DES for € 8,980

Breaking Ciphers with COPACOBANA - A Cost-Optimized Parallel Code Breaker

In Cooperation with
the Institute of Computer Science and Applied Mathematics
Christian-Albrechts University of Kiel

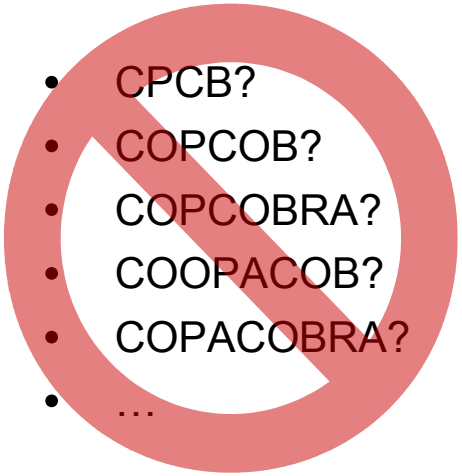
http://www.copacobana.org

Outline

Introduction: A Naming Tale

What does COPACOBANA stand for?

Possible abbr. of „Cost-optimized Parallel Code-Breaker“:



- CPCB?
- COPCOB?
- COPCOBRA?
- COOPACOB?
- COPACOBRA?
- …

► COPACOBANA

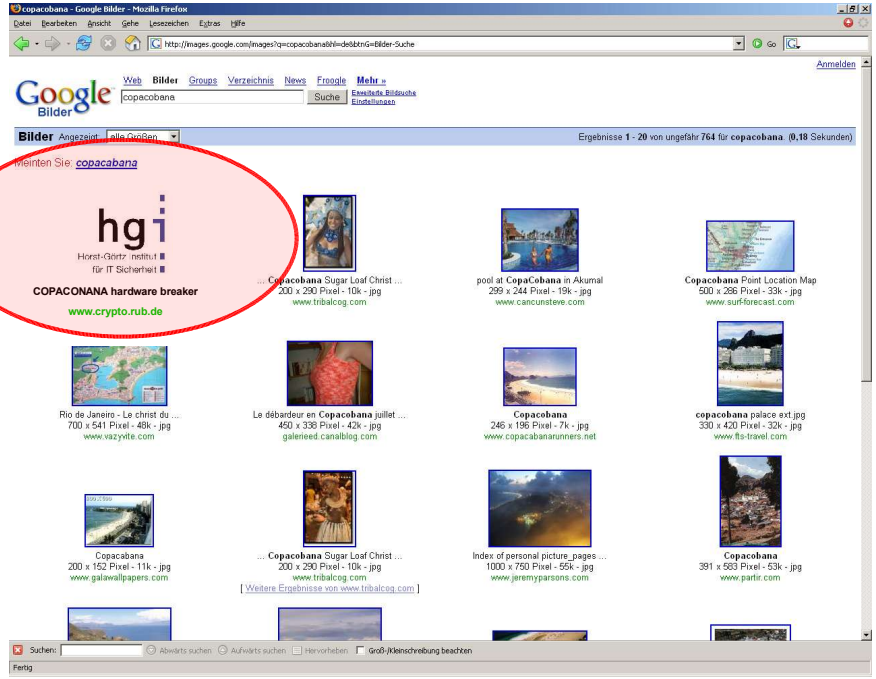
Introduction: A Naming Tale

… Easy to remember: Copacabana…

Introduction: A Naming Tale

Horst-Görtz Institut für IT Sicherheit

- Might yield nice Google-hits when misspelling copacabana…



Outline

2. Introduction

3. **Cryptanalysis of Modern Ciphers**

5. COPACOBANA

7. Brute Force Attack on DES

9. Conclusion and Outlook

Cryptanalysis of Modern Ciphers: Basics

Horst-Görtz Institut für IT Sicherheit

Security of ciphers is related to complexity of attacks:

- Symmetric ciphers:
  - usually, only exhaustive key search possible (brute force)
  - an exhaustive key search should be infeasible
  - key lengths: 112…256 bit (2^{112}…2^{256} different keys)
  - „> 80 bit are safe“
  - Data Encryption Standard (DES): 56 bit
- Asymmetric ciphers (e.g., RSA):
  - larger keys due to „smarter“ attacks
  - key lengths: 768…4096 bit
  - current WR: RSA-200
  - limit of software-based attacks: 768 bit
  - „2048 bit are safe“

Cryptanalysis of Modern Ciphers: Hardware

Possible solutions to computational extensive problems:

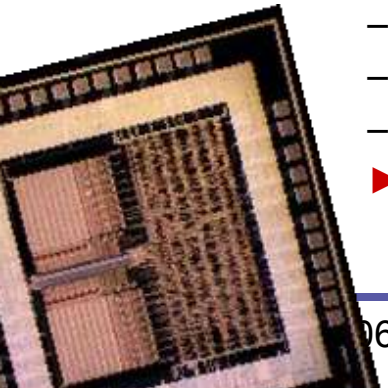
- Large supercomputers:
  - Complex and expensive parallel computing architectures
  - Fast I/O, large memory, easy to program
  - E.g., Cray-XD1

  ► Too complex for (most) cryptanalysis (bad cost-performance ratio)

- Distributed computing (conventional PCs):
  - Dedicated clients in clusters, or
  - Using PC's idle time: E.g., SETI@home (BOINC framework)

  ► Problem of motivating for cryptanalytic challenges, confidentiality issues

- Special purpose hardware:
  - Application Specific Integrated Circuits (ASICs, high NRE)
  - Field Programmable Gate Arrays (FPGAs, low NRE)
  - Optimized for one particular objective

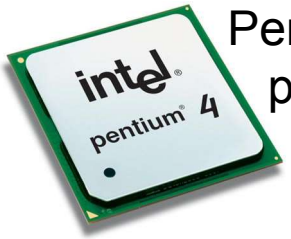


  ► Tradeoff between reprogrammability and price per piece, best cost-performance ratio

Cryptanalysis of Modern Ciphers: Example

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

- DES encryptions / decryptions per second



Pentium4@3GHz: $\approx 2 \times 10^6$
price per piece (market price): € 80

Xilinx xc3s1000@100MHz: $\approx 400 \times 10^6$
price per piece (market price): € 40

► Cost-performance ratio differs by 2-3 orders of magnitude!

1) Based on actual implementation at hand.

Outline

2. Introduction

3. Cryptanalysis of Modern Ciphers

5. COPACOBANA

7. Brute Force Attack on DES

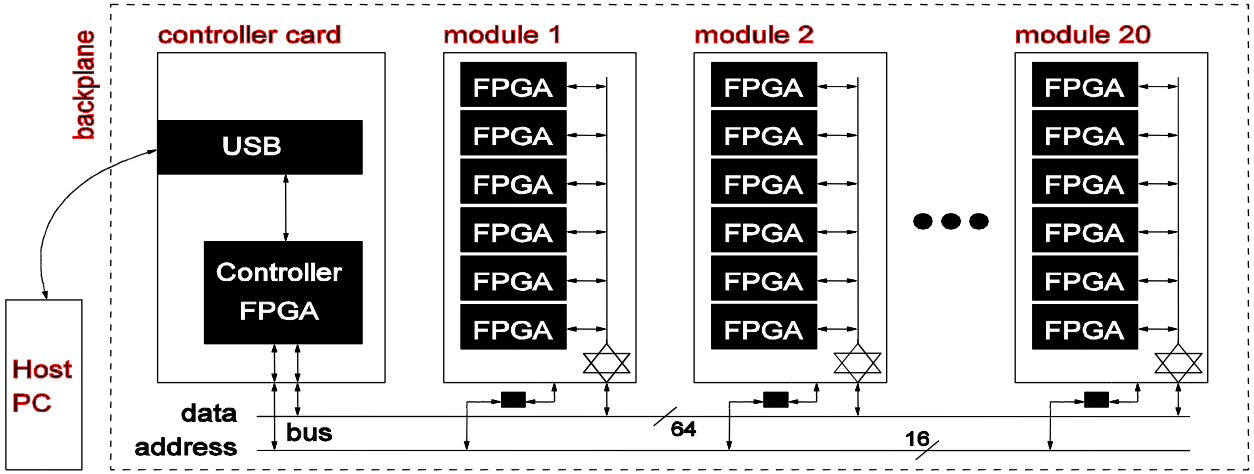
9. Conclusion and Outlook

COPACOBANA: Basic Design

- Parallel architecture built out of 120 low-cost FPGAs
- Total cost: < € 9,000 (including fabrication and material cost)
- Optimized w.r.t. computational power and monetary cost:
  - custom design with off-the-shelf hardware (low-cost)
  - no global memory
  - no high-speed communication („only“ ~ Mbit/s)

COPACOBANA: Basic Design

- Modular design:
  - Backplane
  - FPGA modules (each with 6 low-cost FPGAs)
  - Controller card with USB interface



- Easily extendable:
  - Up to 20 FPGA modules with 6 FPGAs each
  - Connect multiple COPACOBANAs via USB

COPACOBANA: FPGA Modules

Horst-Görtz Institut für IT Sicherheit

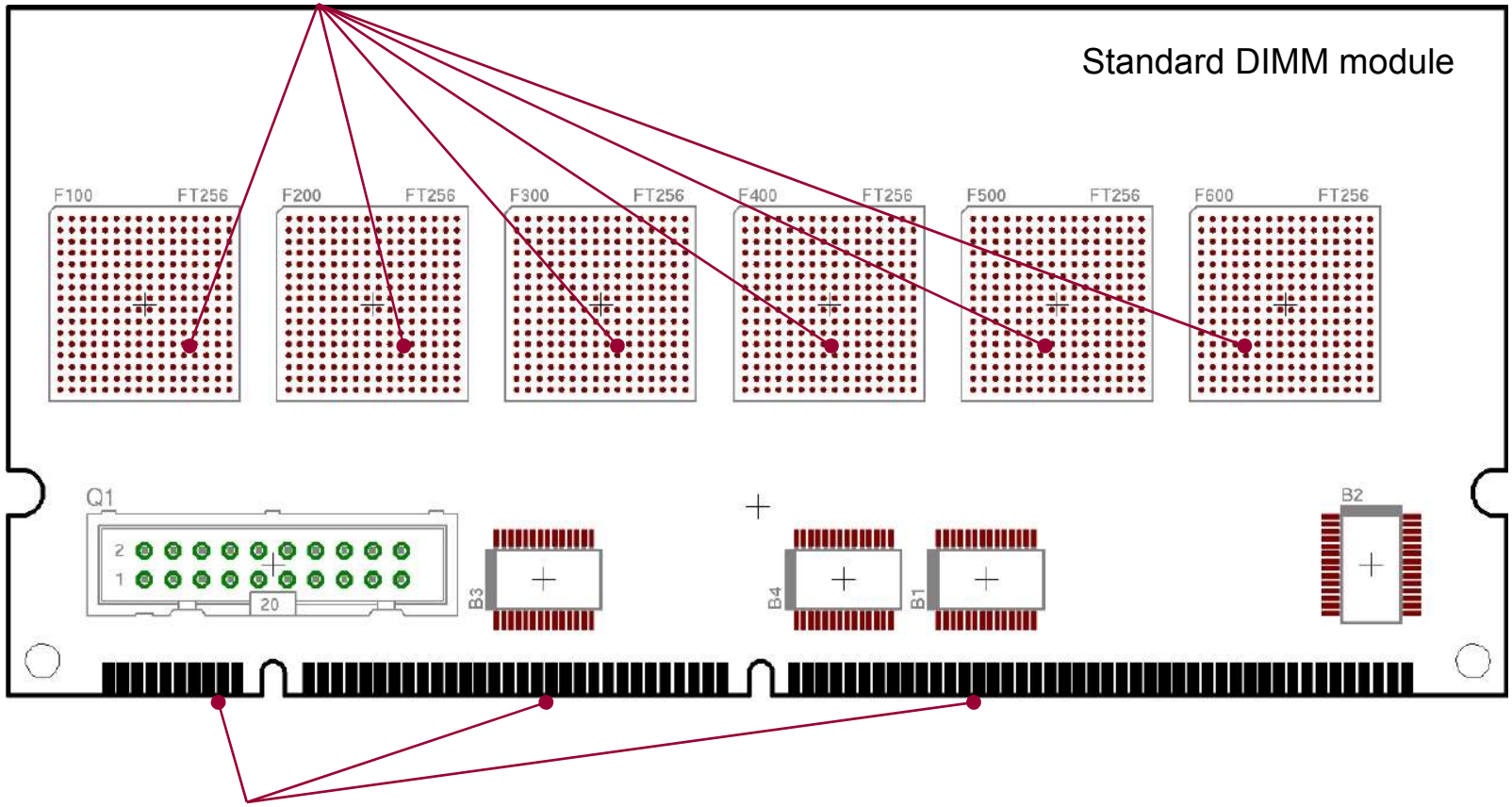
Functionality:

- 6x Spartan-3 FPGAs (xc3s1000) per module
  - BGA packaging (FT256)
  - Internal clock rate up to 300 MHz
- Addressing:
  - HW decoded adress of FPGA modules (GAL on backplane)
  - HW decoded adress of single FPGA
  - Further addresses (5-bit) for FPGA-internal processing
- 64-bit data connection to backplane (bi-directional)
- 64-bit local bus (per module)
- Host cryptanalytical applications, e.g.,
  - Key search engines for DES
  - ECM engines
  - Pollard Rho engines

COPACOBANA: FPGA Modules (Schematic)

Horst-Görtz Institut für IT Sicherheit

6x Spartan 3 FPGA (xc3s1000, FT256 packaging)

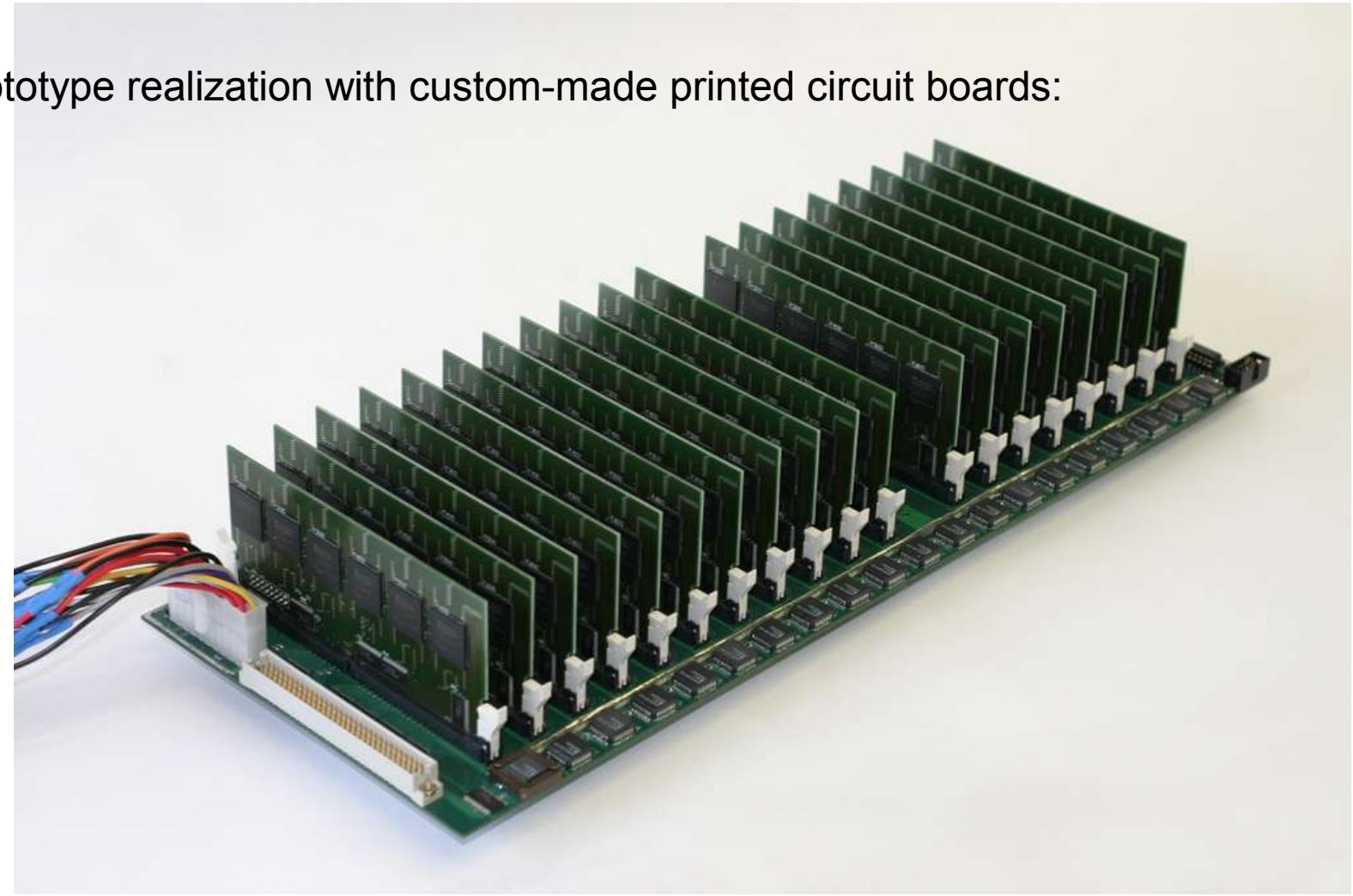


Connection to backplane (64-bit data bus)

COPACOBANA: FPGA Modules (Realization)

Horst-Görtz Institut für IT Sicherheit

Prototype realization with custom-made printed circuit boards:



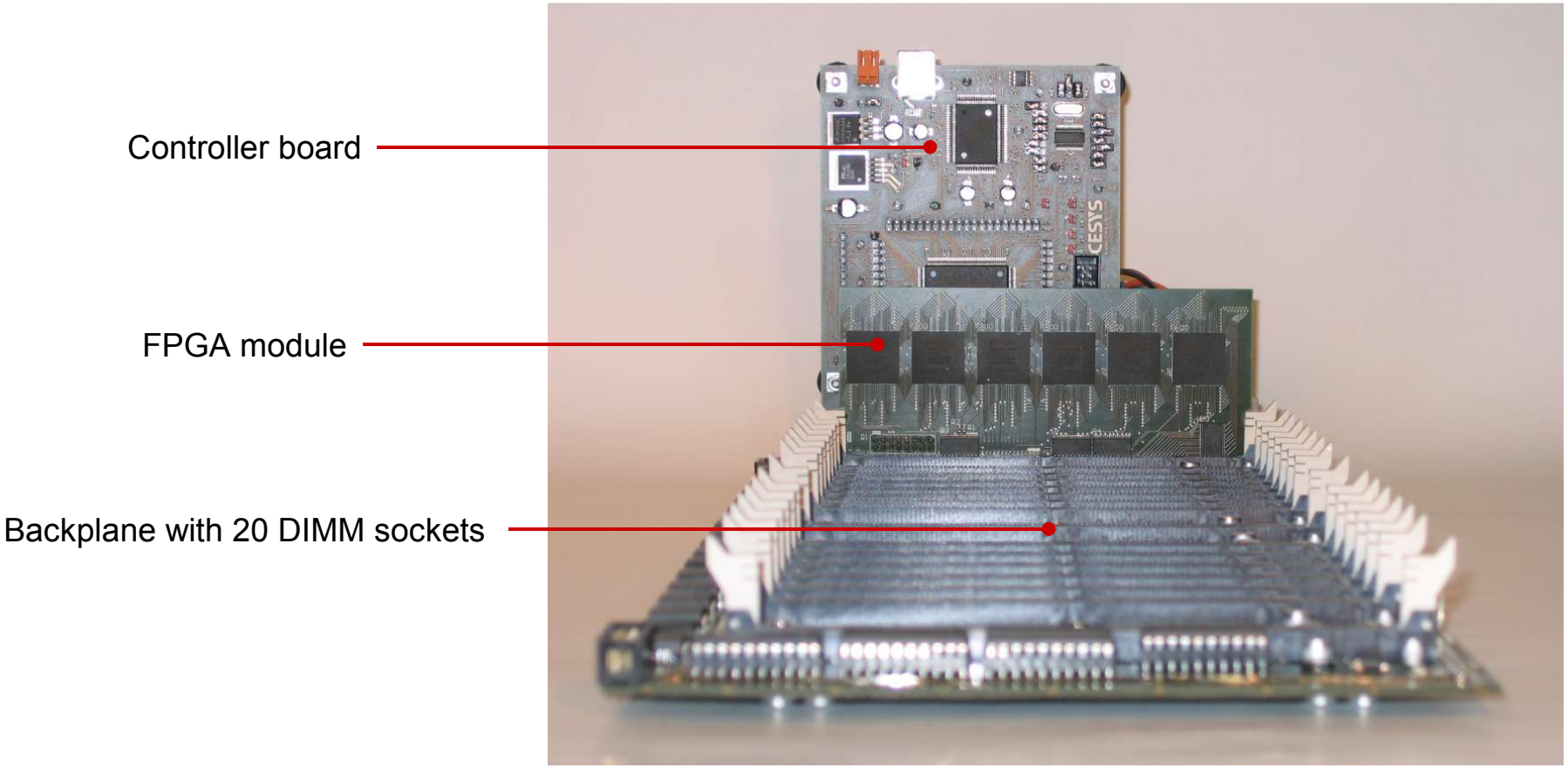
COPACOBANA: Controller Module

Horst-Görtz Institut für IT Sicherheit

Functionality:

- Programming of FPGAs:
  - Individual (download per FPGA)
  - Concurrent (download to all/ subset FPGAs)
- Communication with FPGAs:
  - Initialization of FPGA logic
  - Polling of FPGAs
- Communication with host-PC:
  - Redirecting results
  - Simple pre- and post processing

COPACOBANA: Realization



COPACOBANA: Applications

Ideal platform for cryptanalysis:

- Exhaustive key search of DES
  - Per device 48 billion keys per second (w/ 20 FPGA modules)
  - Average search time with COPACOBANA in less than 9 days
- Factorization
  - Parallelized Elliptic Curve Method (ECM)
    (see Kris' talk after lunch)
- Solving Elliptic Curve DLP
  - Parallelized Pollard's Rho (PR) (see Christof's talk this afternoon)

- can break many cryptographically weak ciphers with COPACOBANA
- can not break strong ciphers (AES, RSA-1024, ECC-163, …) BUT provide solid basis for estimates by extrapolation of COPACOBANA results!

2. Introduction

3. Cryptanalysis of Modern Ciphers

5. COPACOBANA

7. **Brute Force Attack on DES**

9. Conclusion and Outlook

Cryptanalytical Applications: Attacks on DES

Horst-Görtz Institut für IT Sicherheit

Conventional attacks on the Data Encryption Standard (DES):

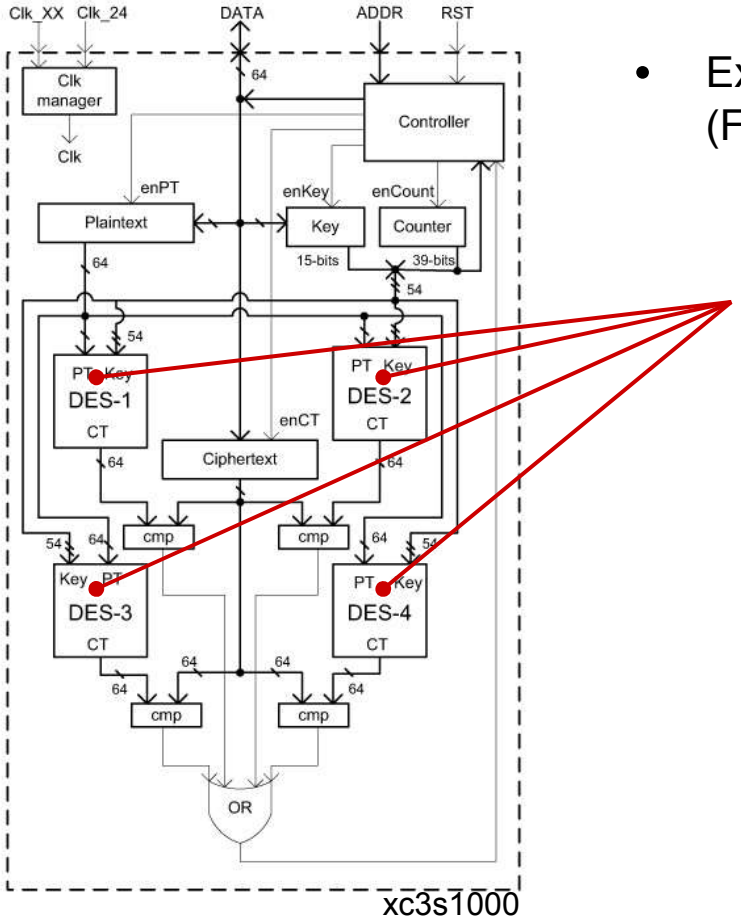
- DES:
  - Block cipher with 56-bit key
  - Expired standard, but still used (legacy products, compatibility reasons)

- Exhaustive key search (conventional technology):
  - Check 2^{55} keys on average
  - Personal Computer (e.g., Pentium4@3GHz): ~ 2 mio. keys/ sec
  - Average key search with one PC: ~ 2^{34} sec = 545 years!

► Can do much better with special-purpose hardware!

Cryptanalytical Applications: Attacks on DES

FPGA-based attacks on the Data Encryption Standard (DES):

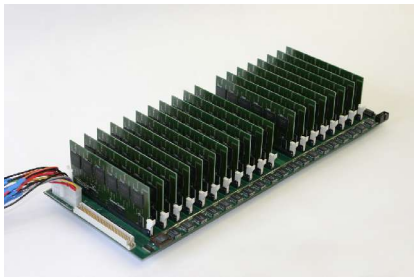


- Exhaustive key search (FPGA based):
  - 4 completely pipelined DES engines per FPGA (courtesy of the crypto group of the University of Louvain)
  - one key per clock cycle per DES engine
  - One FPGA@100MHz: 400 mio. keys/ sec

Cryptanalytical Applications: Attacks on DES

FPGA-based attacks on DES (contd.):

- Exhaustive key search (contd.):
  - Average key search with COPACOBANA (120 FPGAs): **8.7 days**!



- Comparison FPGA vs. PC for average key search in 8.7 days:
  - Need 22865 Pentium4 processors (~ 22865 · € 160 incl. overhead)

    or
  - COPACOBANA (total cost < € 9,000 incl. overhead)

► **COPACOBANA ~ 400 times more cost-efficient!**

2. Introduction

3. Cryptanalysis of Modern Ciphers

5. COPACOBANA

7. Brute Force Attack on DES

9. Conclusion and Outlook

Conclusion

Horst-Görtz Institut für IT Sicherheit

Pros and cons of COPACOBANA:

+ efficient hardware architecture
+ reprogrammable hardware (FPGAs)
+ very cheap to produce
+ extendable (per architecture, multiple architectures, …)
+ design option: local memory
+ design option: upgrade to future FPGA technologies
+ not restriced to code-breaking

- no global memory (only controller/ host-PC)
- relatively slow communication
- suited only for particular problems (e.g., cryptanalysis)
- requires programming in VHDL

Outlook

Future work includes

- Completion of the COPACOBANA platform:
  - harden communication framework
  - run complete DES key search with 120 FPGAs
  - run (previous) ECC challenges on COPACOBANA, analyze SECG 80, 112, 128
  - implement parallel ECM for COPACOBANA
- Optimization of VHDL implementations
- Optimization of hardware platform (beyond prototype)
- Hardware based attacks demand for re-evaluation of security of, e.g., ECC
- Further applications: Smith-Waterman algorithm for scanning DNA sequences against databases

Thanks!
Demonstration of COPACOBANA tomorrow (?)