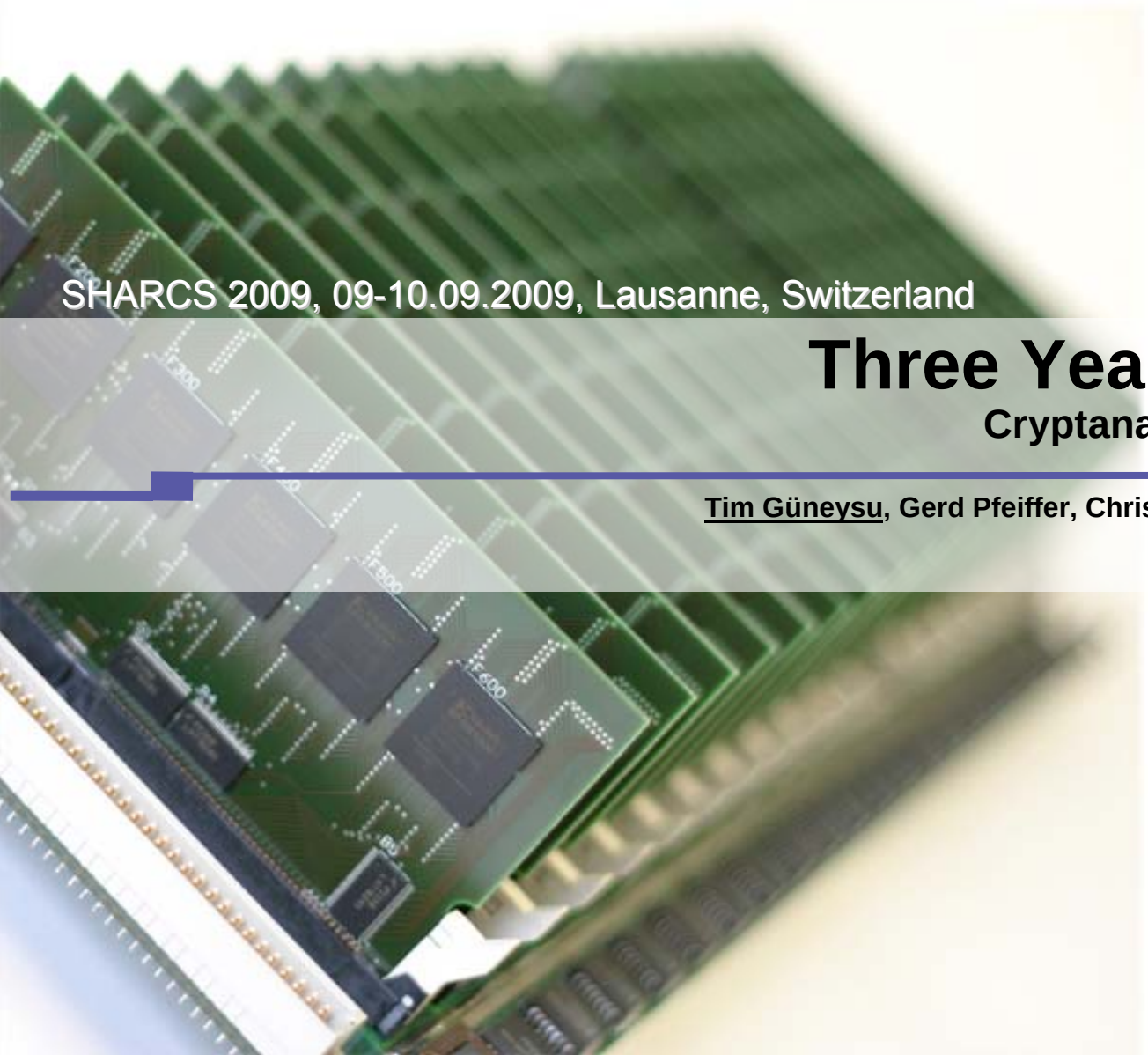
Horst Görtz Institute for IT-Security



SHARCS 2009, 09-10.09.2009, Lausanne, Switzerland

Three Years of Evolution

Cryptanalysis with COPACOBANA

Tim Güneysu, Gerd Pfeiffer, Christof Paar, Manfred Schimmler (et. al.)

Chair for Embedded Security
Ruhr-University Bochum, Germany
and
Electrical Department of
the University of Kiel, Germany

http://www.copacobana.org

Agenda

Horst Görtz Institute for IT-Security

- Introduction and Motivation
- Architecture of COPACOBANA
- Cryptanalytic Applications on COPACOBANA
- Deficiencies and Limitations
- The Next Cluster Generation: COPACOBANA v2

Agenda

Horst Görtz Institute for IT-Security

- **Introduction and Motivation**
- Architecture of COPACOBANA
- Cryptanalytic Applications on COPACOBANA
- Deficiencies and Limitations
- The Next Cluster Generation: COPACOBANA v2

Introduction and Motivation

Horst Görtz Institute for IT-Security

- Security of ciphers is related to complexity of attacks
- Complexity of attacks are determined by their asymptotic runtime and step count, e.g.,
  - Pollard-Rho Attack on ECC-160 → ≈ 2^{80} steps (average)
  - SHA-1 Collisions (EUROCRYPT '09) → ≈ 2^{52} steps (average)
- To understand complexity of a single step, its implementation on an actual system required
- Finding the platform that provides the most efficient attack implementation (w.r.t. cost and performance) allows to determine the cryptosystem's real-world security

Potential Platforms for Cryptanalysis

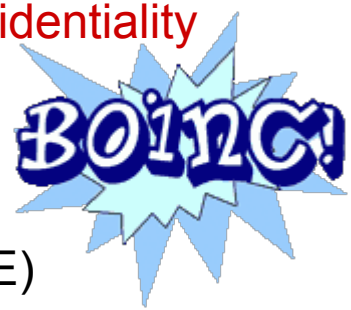
Horst Görtz Institute for IT-Security

– **Large supercomputers:**
  - Complex and expensive parallel computing architectures
  - Fast I/O, large memory
  - Examples are Cray-XD1, IBM BlueGene

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

– **Distributed computing (PCs, Playstations, Graphics Cards):**
  - Dedicated clients in clusters, or
  - Using PC‘s idle time, for example SETI@home (BOINC)

► Problem of motivating for cryptanalytic challenges, confidentiality issues, power consumption of the cluster



– **Special purpose hardware:**
  - Application Specific Integrated Circuits (ASICs, high NRE)
  - Field Programmable Gate Arrays (FPGAs, low NRE)

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

Potential Platforms for Cryptanalysis

Horst Görtz Institute for IT-Security

➔ **FPGA-based COPACOBANA Cluster**
(Cost Optimized Parallel Code Breaker)

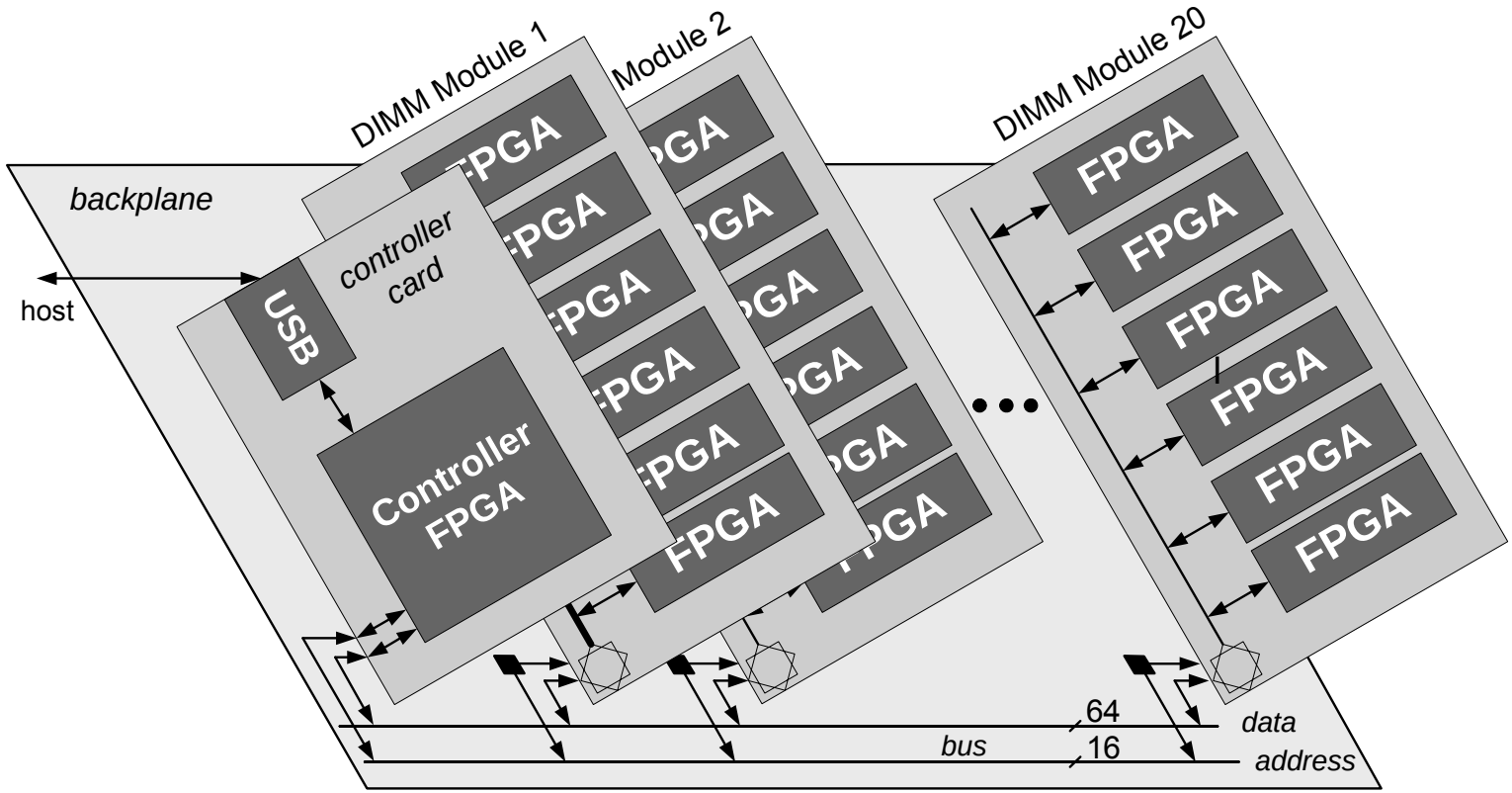
Agenda

Horst Görtz Institute for IT-Security

- Introduction and Motivation
- **Architecture of COPACOBANA**
- Cryptanalytic Applications on COPACOBANA
- Deficiencies and Limitations
- The Next Cluster Generation: COPACOBANA v2

COPACOBANA: Architecture

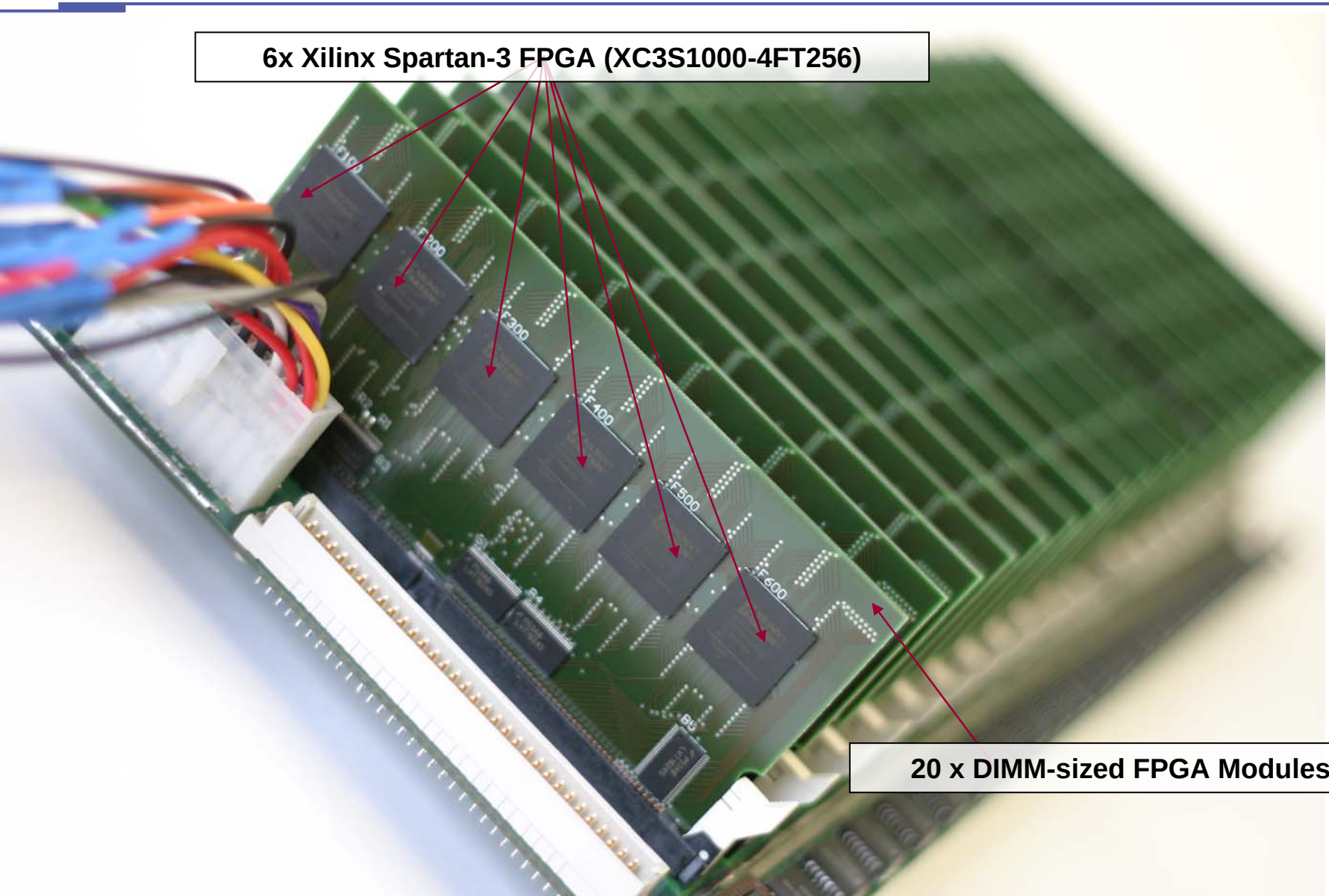
Horst Görtz Institute
for IT-Security



- Backplane with plug-in slots can host up to 20 DIMM-sized FPGA modules
- 6 x low-cost Xilinx Spartan-3 FPGAs (XC3S1000) per FPGA module
- Shared 64-bit data and 16-bit address connection on backplane (bi-directional)
- Controller connects PC with FPGAs in a slow Master-Slave scheme (3 MBit/s)

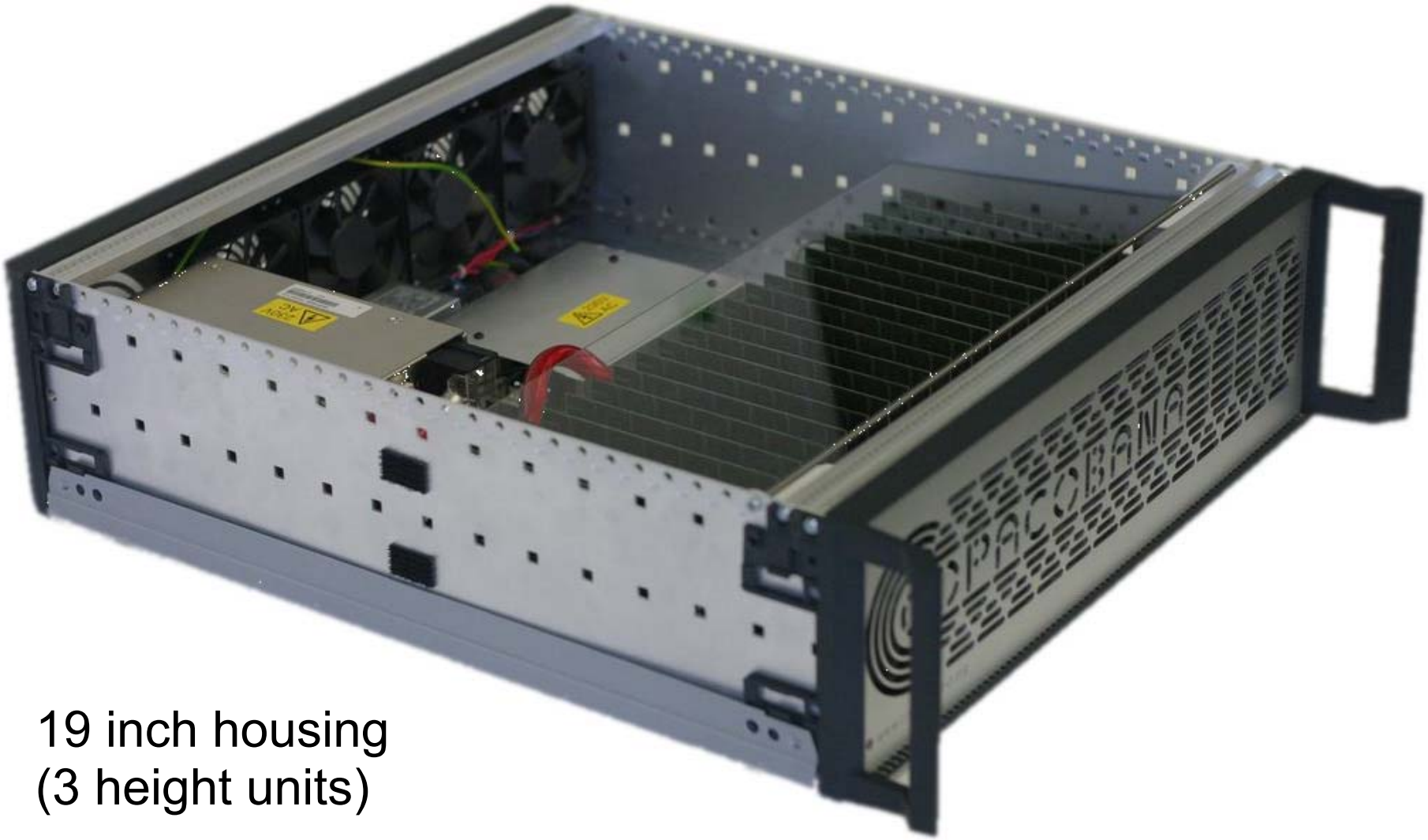
COPACOBANA: Prototype

Horst Görtz Institute for IT-Security



COPACOBANA: Release Candidate

Horst Görtz Institute for IT-Security



19 inch housing
(3 height units)

Agenda

Horst Görtz Institute for IT-Security

- Introduction and Motivation
- Architecture of COPACOBANA
- **Cryptanalytic Applications on COPACOBANA**
- Deficiencies and Limitations
- The Next Cluster Generation: COPACOBANA v2

Exhaustive Key Search with COPACOBANA

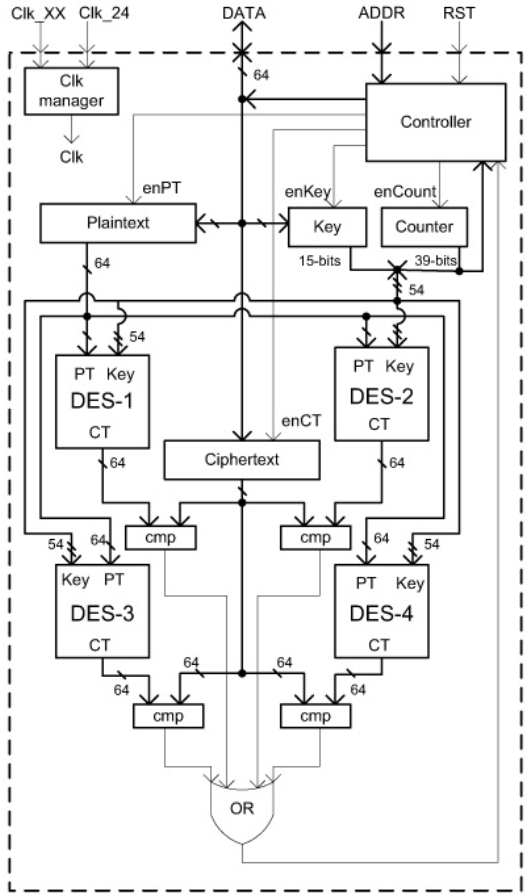
Horst Görtz Institute for IT-Security

First release shown on SHARCS/CHES 2006:

Successful Key Search on 56-bit DES for <10k€

- 4 pipelined DES engines on each FPGA
- One key per clock cycle per DES engine
- One FPGA@100MHz: **400 mio**. keys/s
- Comparison: Pentium4@3GHz ≈ **2 mio**. keys/s

- Search time **8.6 days** on average (100MHz), with further optimizations (136 MHz) search time reduced to **6.4 days!**



Exhaustive Key Search with COPACOBANA

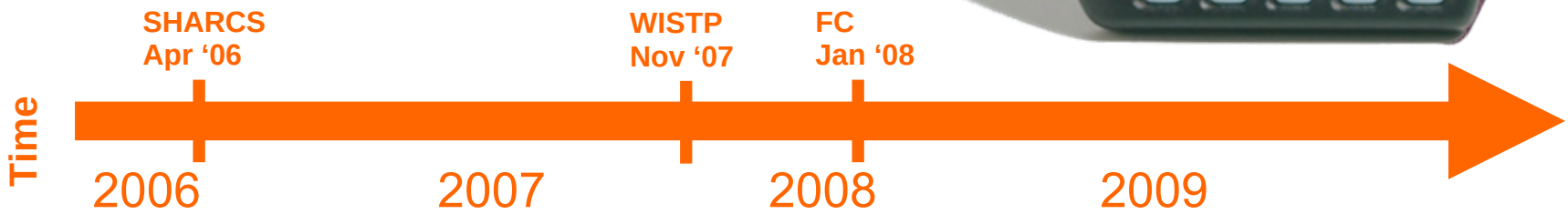
Horst Görtz Institute for IT-Security

Real-World Attacks on DES-based Systems

- Norton Diskreet Harddisk Encryption (DES)
  - Weak key derivation from passwords
  - If pwd consists only of {A, . . . ,Z,@, [, \,],, } attack requires 2^{35} ops ➔ **<1s search time**

- Attack on the Basic Access Control (BAC) of ePass
  - Little entropy in MRZ allows for brute force attack on SHA-1-TDES enc./auth.
  - Access to private data in 18 seconds (real time)

- DES-based One-Time Password Tokens
  - Key extraction from OTP tokens by knowledge of 2-3 challenge-response pairs



Smarter Attacks with COPACOBANA

Horst Görtz Institute for IT-Security

Attacking the A5/1 Stream Cipher in GSM

- Hardware-based guessing attack (CHES ’08)
  - adapted attack from Keller and Seitz
  - breaks A5/1 in about 6 hours on average
- Time Memory Data Tradeoff on A5/1 with COPACOBANA
  - Success rate 63% with 64 data points after 27s, 95.4 days of precomputation time and total table size of 4.85 TB
  - However, construction of precomputation tables is not finished due to host slow interface

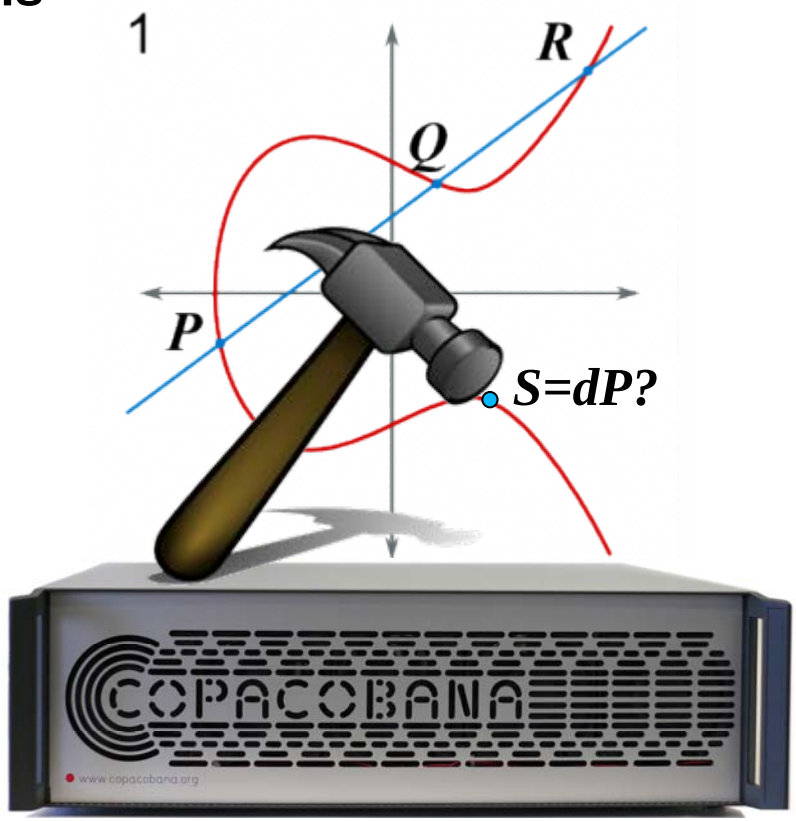
➔ Need for faster I/O

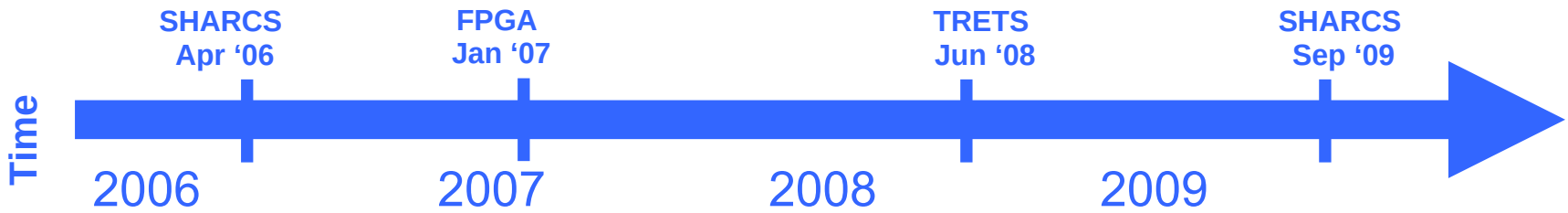
Supporting Asymmetric Cryptanalysis

Horst Görtz Institute for IT-Security

Solving Elliptic Curve Discrete Logarithms

- First Pollard-Rho Attack on ECC over prime fields in hardware (SHARCS '06/FPGA '07/ACM TRETS)
- On average, one COPACOBANA solves ECCP-97 in about three months, ECCP-109 in 24 years
- **In the next session**: Pollard-Rho for binary (Koblitz) curves ECC2-131, ECC2K-130 and ECC2/K-163





The Elliptic Curve Method on COPACOBANA

Horst Görtz Institute for IT-Security

Implementing ECM (phase 1+2) on COPACOBANA

- Using “classical” Montgomery curves
- Montgomery ladder for phase 1 and (adapted) standard continuation method for phase 2
- Acceleration of required field operations ADD/SUB/MUL with dedicated arithmetic units in FPGAs (DSP blocks)
- No DSPs in Spartan-3 XC3S1000
  ➔ FPGA module redesigned for Virtex-4 SX 35
- 24 ECM cores per Virtex SX 35
  2131 ops/s for 151 bit parameters (post-synth)

➔**I/O limits performance**

➔BRAMs limit prime table size

Factor n= 7626668401 080283463

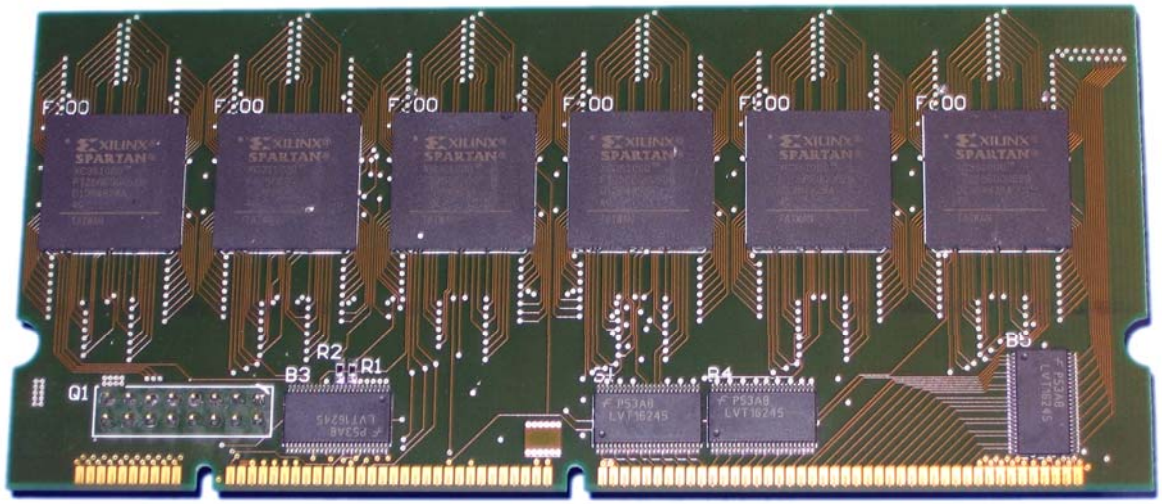
p=2349834551
q=3245619313

Evolution of FPGA modules from XC3S1000 to XCV4SX35 FPGAs

Horst Görtz Institute for IT-Security

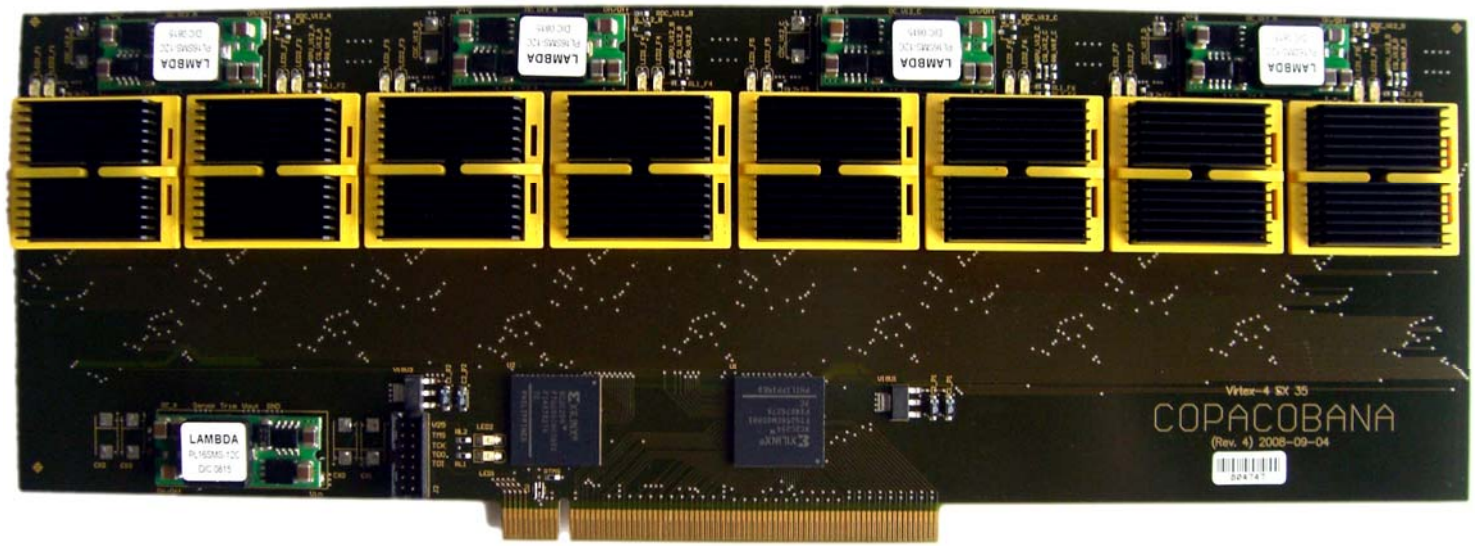
Original:

6xSpartan-3
XC3S1000



Redesign:

8xVirtex-4
XCV4SX35



Redesign with Virtex-4 FPGAs

Horst Görtz Institute for IT-Security

Significantly higher power consumption with Virtex-4 FPGAs (10W ea.)

- Enhanced power supply for 128 FPGAs: 120A@12V = 1.5kW
- Improved cooling using high-performance heat sinks and fans

Agenda

Horst Görtz Institute for IT-Security

- Introduction and Motivation
- Architecture of COPACOBANA
- Timeline of Cryptanalytic Applications on COPACOBANA
- **Deficiencies and Limitations**
- The Next Cluster Generation: COPACOBANA v2

Deficiencies and Limitations

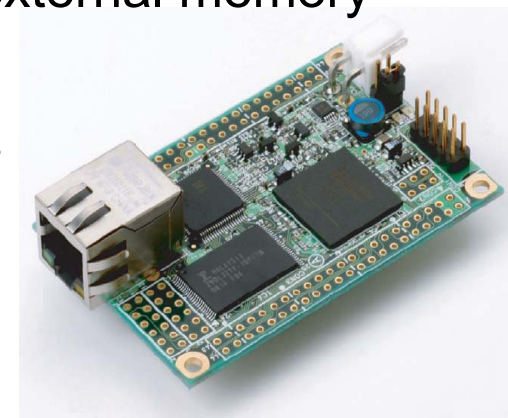
Horst Görtz Institute for IT-Security

- Spartan-3 XC3S1000 FPGAs only provide **limited amount of logic**
  → replace them by larger and recent FPGAs such as Spartan-6
  (see **Peter Alfke's talk tomorrow**)

- **Slow Master-Slave bus** system is a real issue for data-intensive apps

- Use of memory is **restricted to internal 18 kbit BRAM blocks**
  → some applications (e.g., ECM) could benefit from external memory

- **Virtex FPGAs are less appropriate** for cryptanalysis
  - More expensive w.r.t. Spartan-3 (factor of >5x).
  - Spartan-3A DSP/Spartan-6 have DSP blocks, too
  - High overhead due to cooling and power needs



Agenda

Horst Görtz Institute for IT-Security

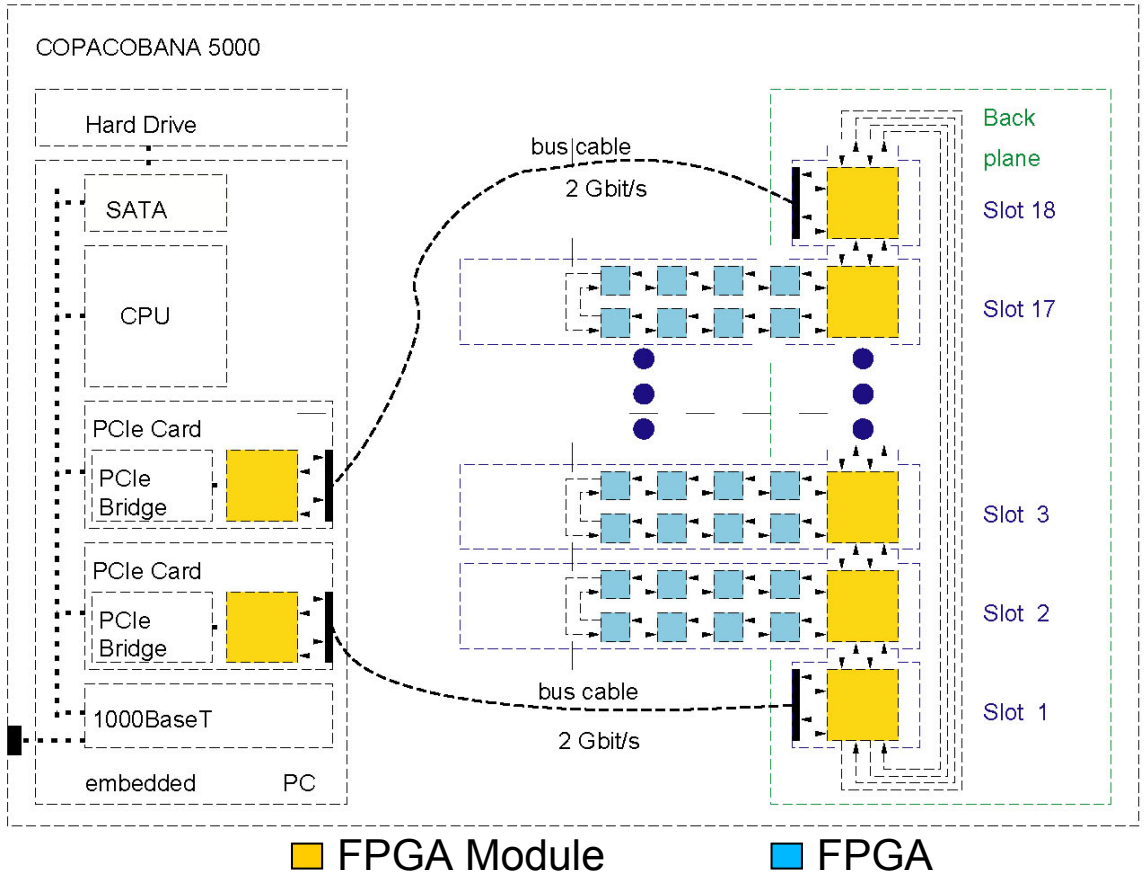
- Introduction and Motivation
- Architecture of COPACOBANA
- Timeline of Cryptanalytic Applications on COPACOBANA
- Deficiencies and Limitations
- **The Next Cluster Generation: COPACOBANA v2**

Next Generation of COPACOBANA

Horst Görtz Institute for IT-Security

- New FPGA module for **Spartan-3 5000** and (coming) **Spartan-6**
- **Integrated PC (mini-ITX)** inside the COPACOBANA housing
- Fast **PCIe-based bridge** between PC and backplane (2 GBit/s)

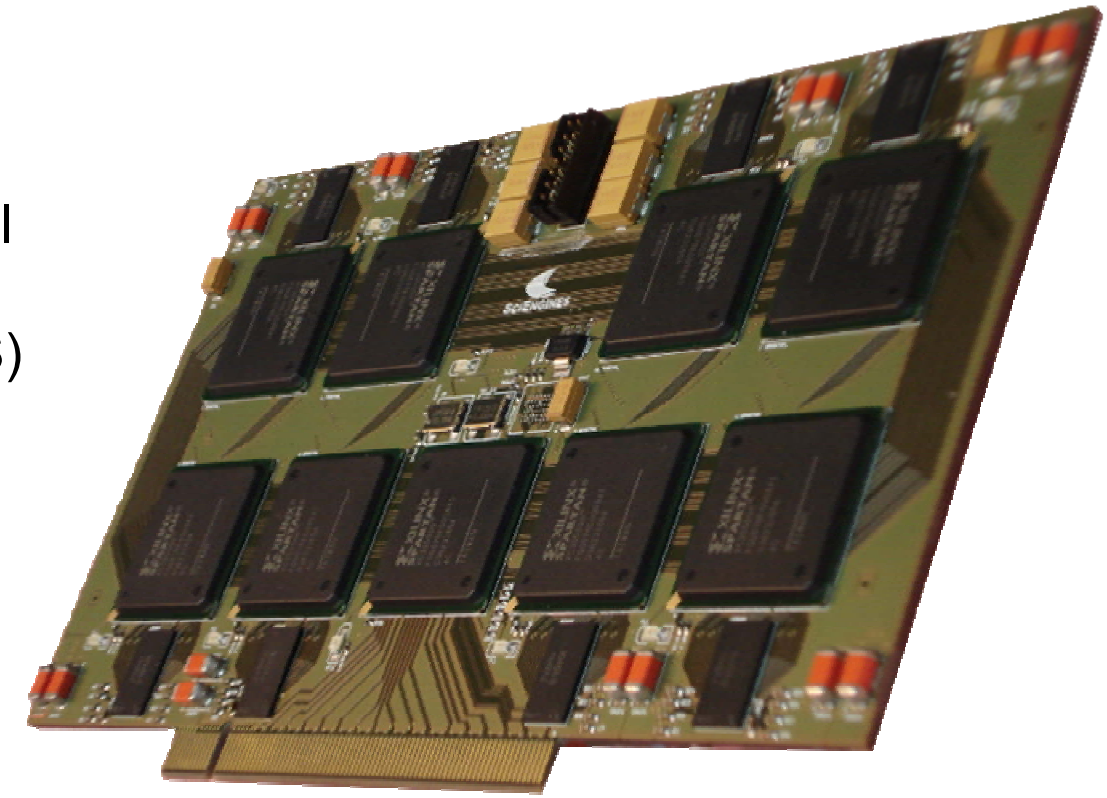
- **Simultaneous bus** access using two PCIe bridges
- Data distribution with **two serial systolic rings**
- **Attached hard disk and 32 MBit RAM** improves handling of large data



Next Generation of COPACOBANA II

Horst Görtz Institute for IT-Security

- Production is scheduled to be finished in **October 2009**
  - First FPGA module is already available
- **Data intensive attacks** will benefit most of new design
  - TMTO attacks (A5/DES)
  - Password/Dictionary Attacks
  - ECM (with Spartan-6)
  - Distributed Pollard-Rho (also with Spartan-6)
  - Further assistence to index calculus/GNFS computations



Conclusion

Horst Görtz Institute for IT-Security

- COPACOBANA has proved as a **valuable tool** to perform and to estimate real attacks on many cryptosystems
  (note that there are even some more that could **not** be published)

- New architecture eliminates obvious deficiencies concerning **limited amount of logic, slow data exchange and lack of memory**

- **New Spartan-6 generation** of FPGAs come with more logic, less power requirements and (important for arithmetic!) DSP blocks

- Further results (based on Spartan-3 5000) are hopefully available at the **end of October!**

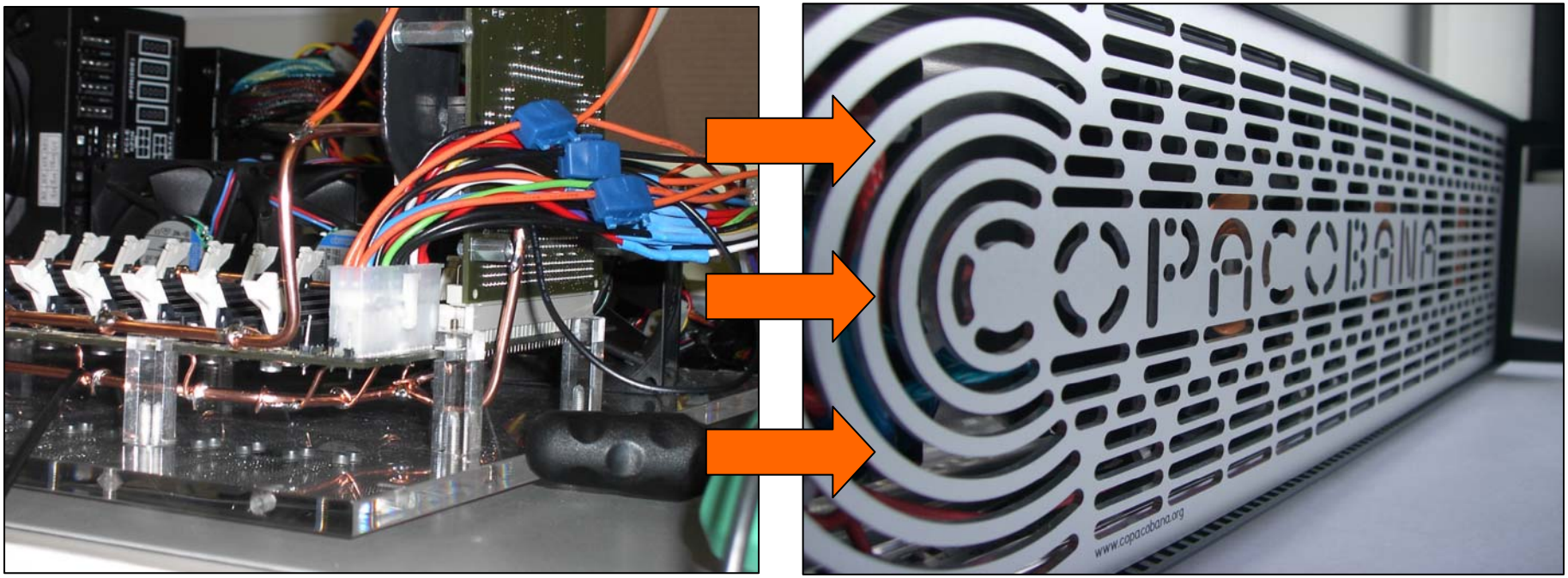
Questions?

Horst Görtz Institute for IT-Security

XILINX

Thanks to Xilinx and SciEngines for their support!

SCIENGINES



Please remember: COPACOBANA is for sale!
Just talk to Christof to purchase one or more ☺

http://www.copacobana.org