Cryptanalysis with a cost-optimized FPGA cluster

Jan Pelzl, Horst Görtz Institute for IT-Security, Germany

hgi
Horst-Görtz Institut
für IT Sicherheit

UCLA IPAM Workshop IV

Special Purpose Hardware for Cryptography: Attacks and Applications

December 4 – 8, 2006

Acknowledgements

Special thanks to

Tim Güneysu, Christof Paar, Christian Schleiffer
(Horst Görtz Institute, University of Bochum)

Gerd Pfeiffer, Manfred Schimmler
(University of Kiel, hardware layout)

Jean-Jacques Quisquater, François-Xavier Standaert
(Universitè Catholique de Louvain, DES-core)

Xilinx
(generous donations of Spartan3 devices)

Agenda

- Security vs. Cost
  - Design of the *COPACOBANA* FPGA Cluster
    - Application 1: DES Brute-Force
    - Application 2: Attack on ECC
  - Conclusion and Outlook

When is a Cipher Secure?

Symmetric crypto

- (hopefully) **only brute-force attack possible**
- „secure key lengths“: 112…256 bits (attack compl. 2^{112}…2^{256})
- but in practice wide variety of keys: AES, DES, RC4, A5, …
- attack complexities: 2^{56}…2^{256}
- security of hash functions (MD5, SHA-1, …)?

Asymmetric crypto (RSA, ECC, DL)

- **algorithmic attacks** (e.g., factorization) dictate larger keys
- „secure key lengths“: > 2048 bits (> 160 bits for ECC)
- key lengths in practice:
  - RSA, DL: 1024 … 4096 bits
  - ECC: 160 … 256 bits
- attack complexities: 2^{80} (?) … 2^{128}

Security and Computation

- Traditional: security of ciphers = **complexity** of attacks
- However: what really matters are the **costs** of an attack
- State-of-the-art:
  - < 2^{50} steps can be done with PC networks (more or less conveniently)
  - > 2^{80} steps are very hard with today's technology (probably also for intelligence agencie

► **Major question: cost of attack for ciphers with 50…80 bits security?**
(RSA1024, ECC160, SHA-1, DES, A5, …)

Introduction: Massive Computing

Supercomputers (Cray, SG, SRC…)

- General (= complex & expensive) parallel computing architectures
- fast I/O, large memory, easy to program

► **poor cost-performance ratio for (most) cryptanalysis**

Distributed computing (conventional PCs)

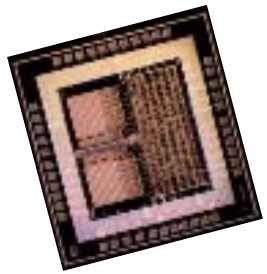
- Dedicated clients in clusters, or
- Using PC's idle time: E.g., SETI@home (BOINC framework)

► **problem of motivation, confidentiality issues**

Special-purpose hardware

- ASIC - Application Specific Integrated Circuits (high NRE)
- FPGA - Field Programmable Gate Arrays (low NRE)

► **best cost-performance ratio**



Introduction: Advantage of Hardware

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

- DES encryptions / decryptions per second

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

Xilinx XC3S1000@100MHz $\approx 400 \times 10^6$
price per device (retail): € 40

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

Based on actual implementations is software and hardware

Agenda

- Security vs. Cost
  - Design of the *COPACOBANA* FPGA Cluster
    - Application 1: DES Brute-Force
    - Application 2: Attack on ECC
  - Conclusion and Outlook

What‘s in a name?

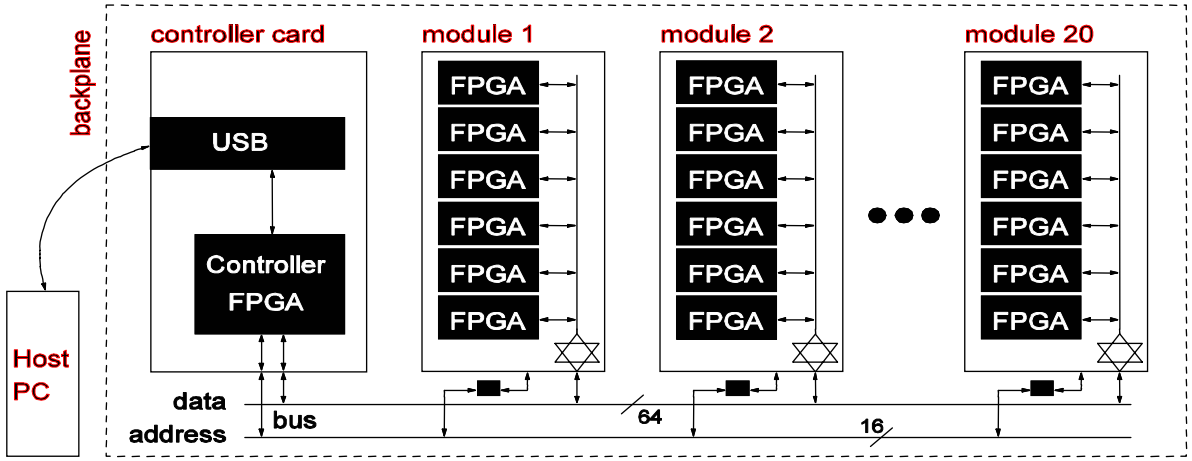
Copacobana

COPACOBANA: Design Principles

- Ability to perform $\geq 2^{56}$ **crypto operations**
- **Re-programmable**: applicable to many ciphers (other apps.?)
- Strictly optimized **cost-performance ratio**:
  - off-the-shelf hardware (low-cost)
  - many logic resources (performance)
- **Modular** design
- **< 10,000 €** (including fabrication and material cost)
- **Parallel** architecture, based on 120 low-cost FPGAs
- Sacrifices
  - no global memory
  - no high-speed communication („only“ Mbit/s)

COPACOBANA: Basic Design

- **Modular design**:
  1. Backplane
  2. FPGA modules (each with 6 low-cost FPGAs)
  3. Controller card with USB/ Ethernet interface

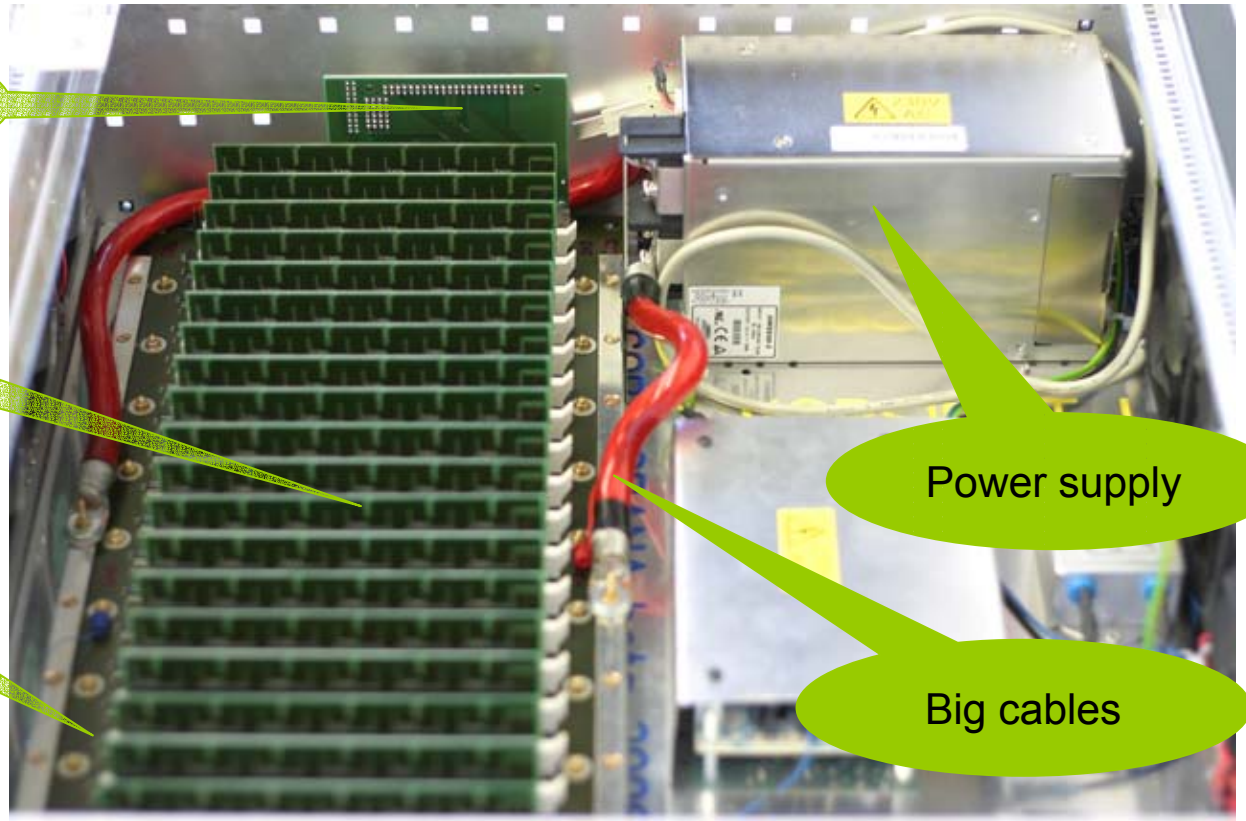


- Easily **extendable**:
  - Up to 20 FPGA modules with 6 FPGAs each
  - Connect multiple COPACOBANAs via USB/ Ethernet

COPACOBANA: Alpha Prototype

COPACOBANA: Beta Version

COPACOBANA: What‘s inside?

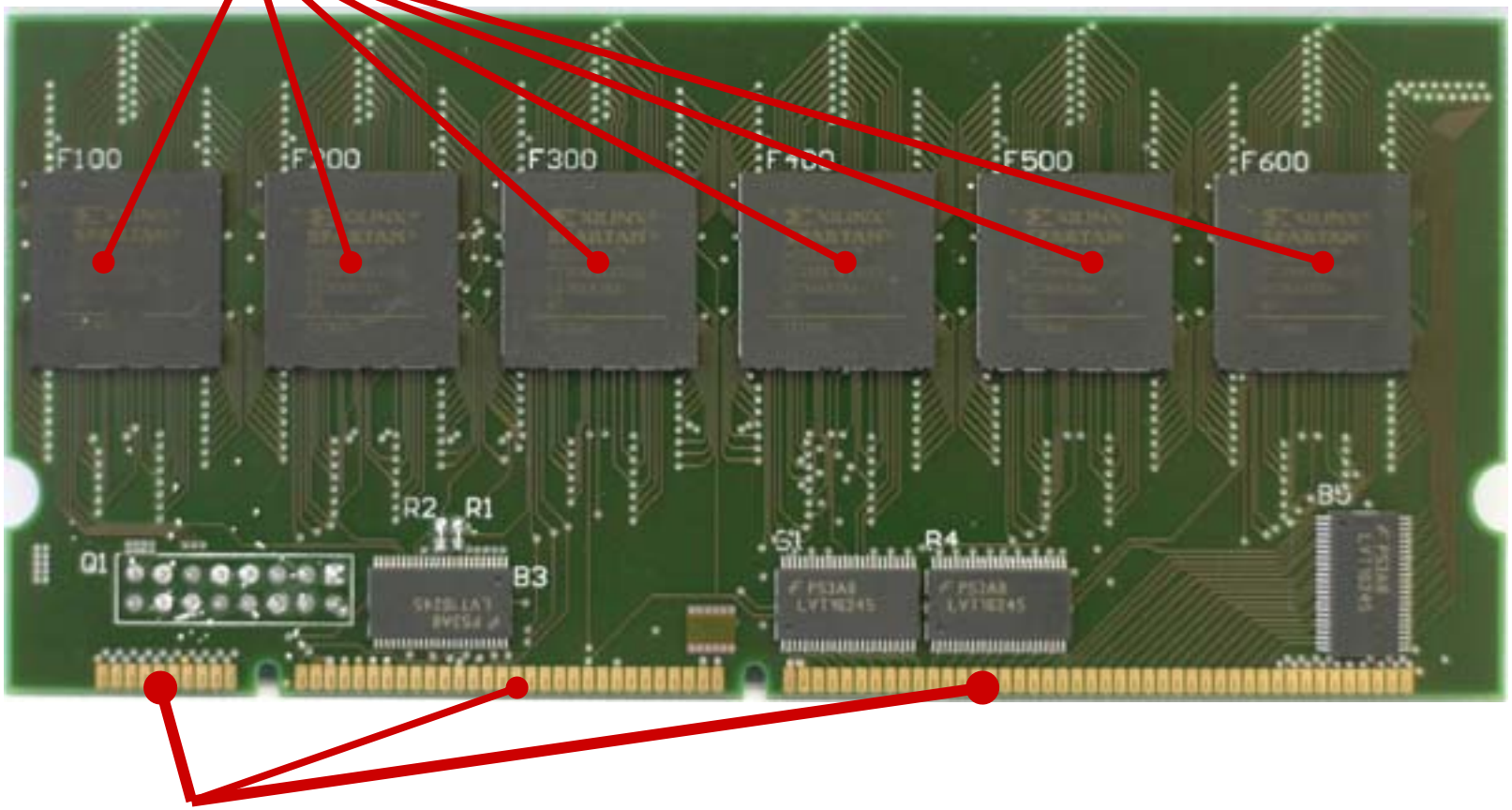


Scales easily:

- 20 FPGA modules/machine (120 FPGAs/ machine)
- multiple machines via USB/ Ethernet

COPACOBANA: FPGA Modules

6x Spartan 3 FPGA (xc3s1000, FT256 packaging)



Connection to backplane (64-bit data bus)

COPACOBANA: FPGA Modules

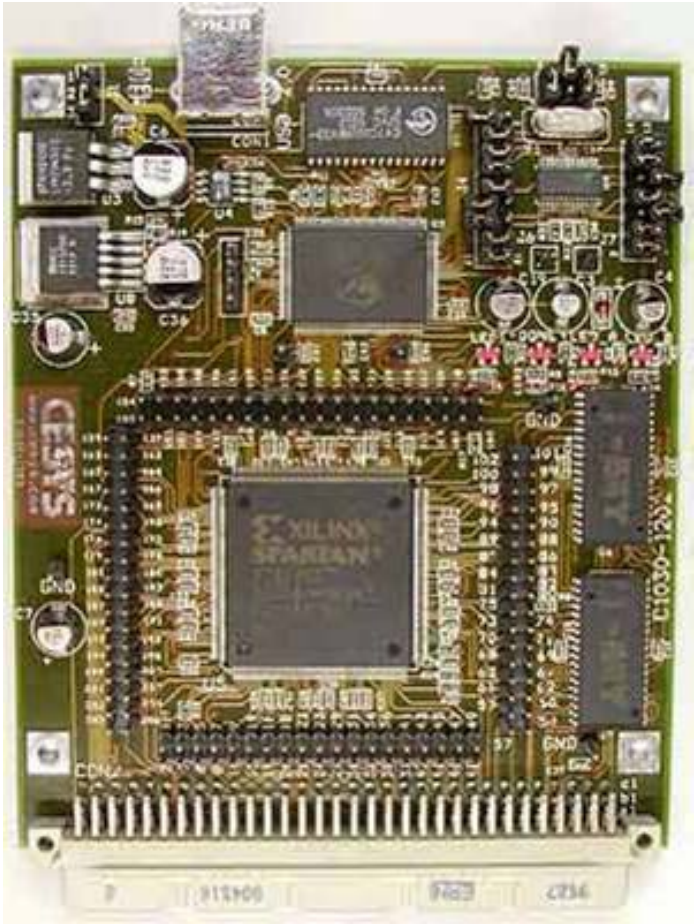
Horst-Görtz Institu
für IT Sicherhe

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

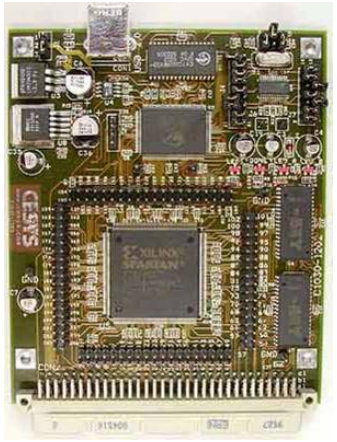
COPACOBANA: Controller Module

Proprietary board (Cesys USB2FPGA w/ Spartan II)



COPACOBANA: Controller Module

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
- New controller being developed (Ethernet, MicroBlaze, …)

COPACOBANA: Applications

First flexible cryptanalytical machine outside government agencies

1. **Exhaustive key search of DES**
   - ciphers with 2^{56}…2^{64} attack steps possible
2. Real-world systems such as **ePass, Norton Diskreet, CSA**…
3. **Elliptic Curve Discrete Logarithm Problem (ECDLP)**
   - Parallelized Pollard's Rho
4. **Factorization**
   - Parallelized Elliptic Curve Method (ECM) as subroutine for GNFS (see GMU's talk later)

Attacks feasible

Robust security estimations

Improves other attacks

Agenda

- Security vs. Cost
- Design of the *COPACOBANA* FPGA Cluster
- Application 1: DES Brute-Force
- Application 2: Attack on ECC
- Conclusion and Outlook

Cryptanalytical Applications: Attacks on DES

Data Encryption Standard (DES):

- Block cipher with 56-bit key
- Expired standard, but still used (legacy products, ePass, Norton Diskreet, …)

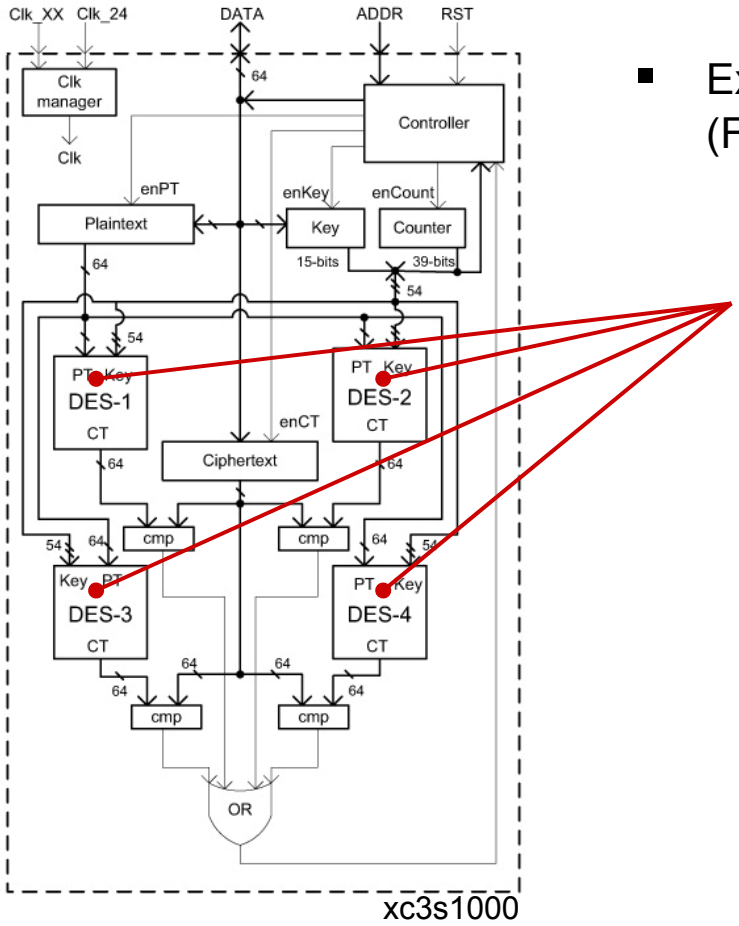
Exhaustive key search (conventional technology):

- Check 2^{55} keys on average
- PC (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!**

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 UCL)
  - one key per clock cycle per DES engine
  - One FPGA@100MHz: 400 mio. keys/ sec

Attacks on DES

- COPACOBANA: average key search of **8.7 days** @ 100 MHz

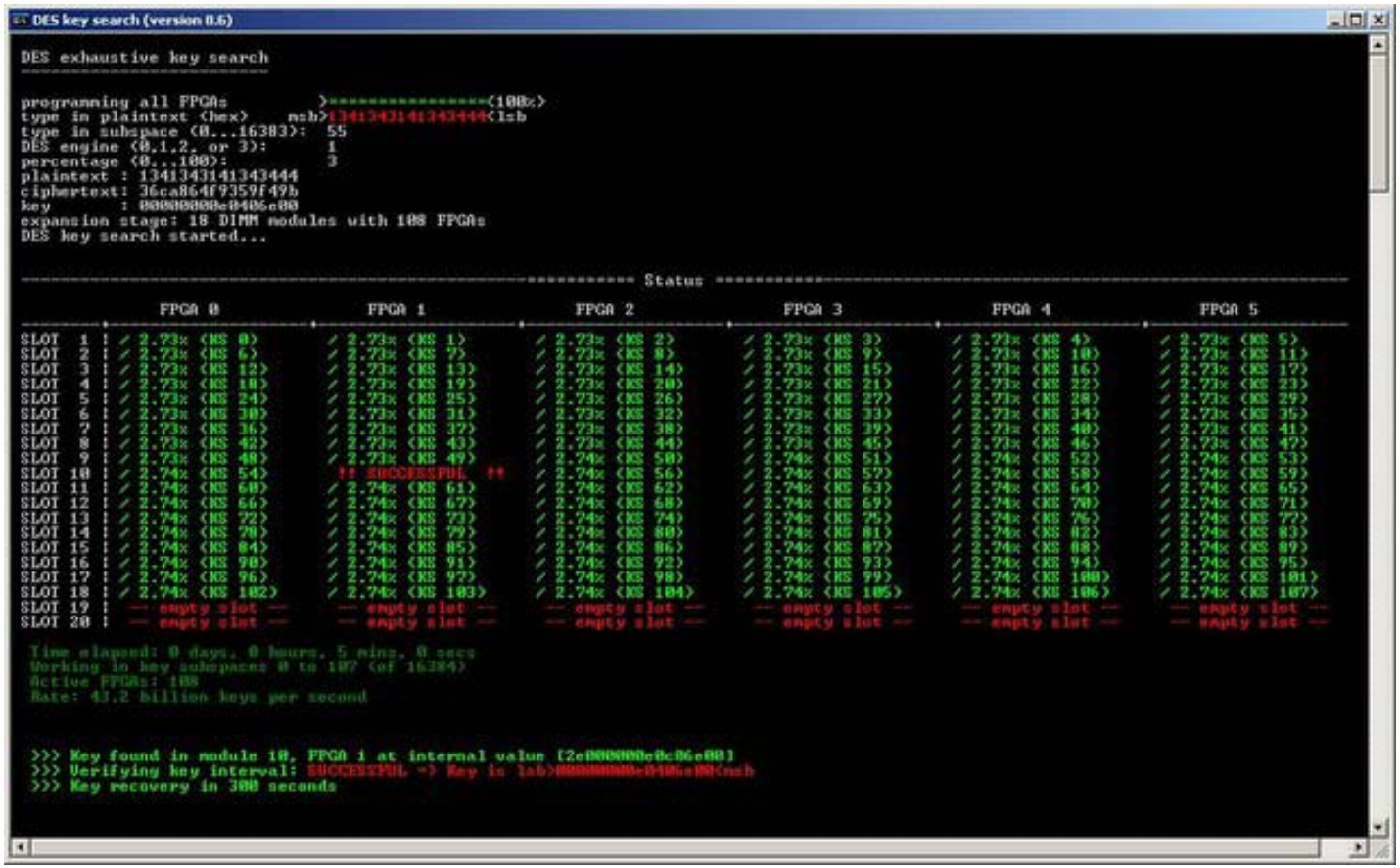
- Somewhat higher clock rates possible

- FPGA vs. PC (average key search in 8.7 days)
  - 22,865 Pentium 4 (**€ 3.6 million** incl. overhead)

    or
  - COPACOBANA (total cost **€ 9000** incl. overhead)

Attacks on DES

Host-PC application (console output):



A Historical Perspective: The Power of Moore‘s Law

Breaking DES in days:

DeepCrack, 1998

$250,000

COPACOBANA, 2006

$10,000

Moore‘ Law: 50% cost reduction / 1.5 years

2006-1998 = 8 years ≈ **5** x 1.5 years

Prediction: $250,000 / 2^5 ≈ $8,000 (close to actual $10,000)

Agenda

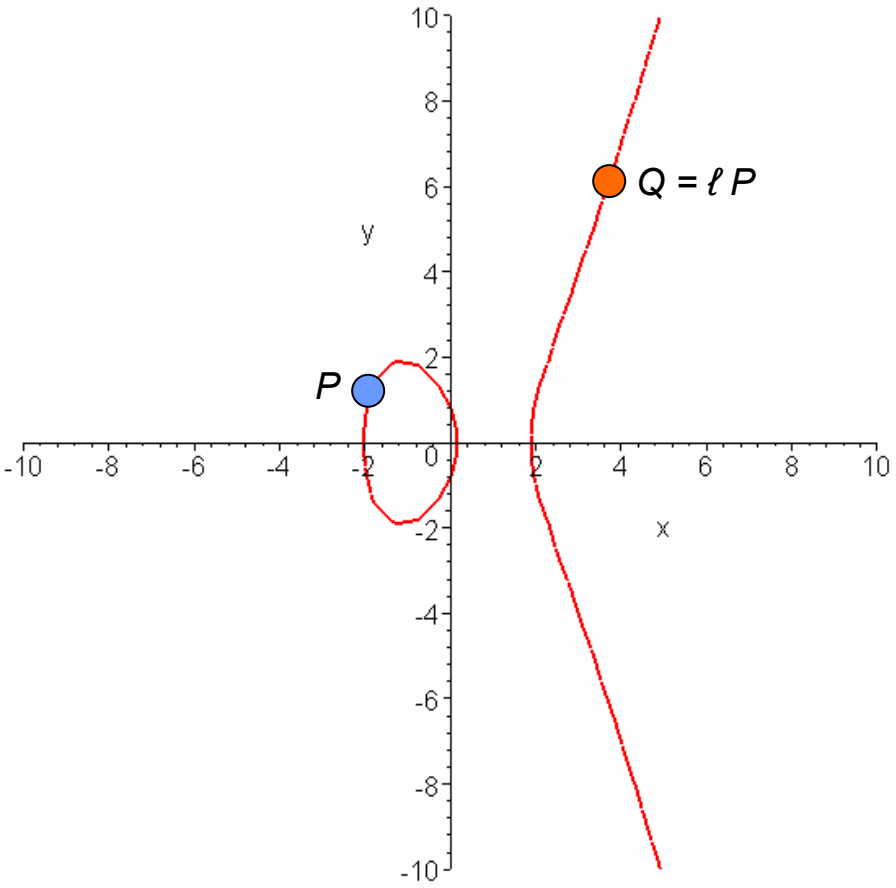
- Security vs. Cost
- Design of the *COPACOBANA* FPGA Cluster
- Application 1: DES Brute-Force
- Application 2: Attack on ECC
- Conclusion and Outlook

ECDL Problem

- Many real-world applications rely on hardness of ECDLP
  - ECDSA,
  - ECDH,
  - …

- Let P be a generator. Determine *discrete logarithm* ℓ of a point Q such that

$$Q = \ell P.$$



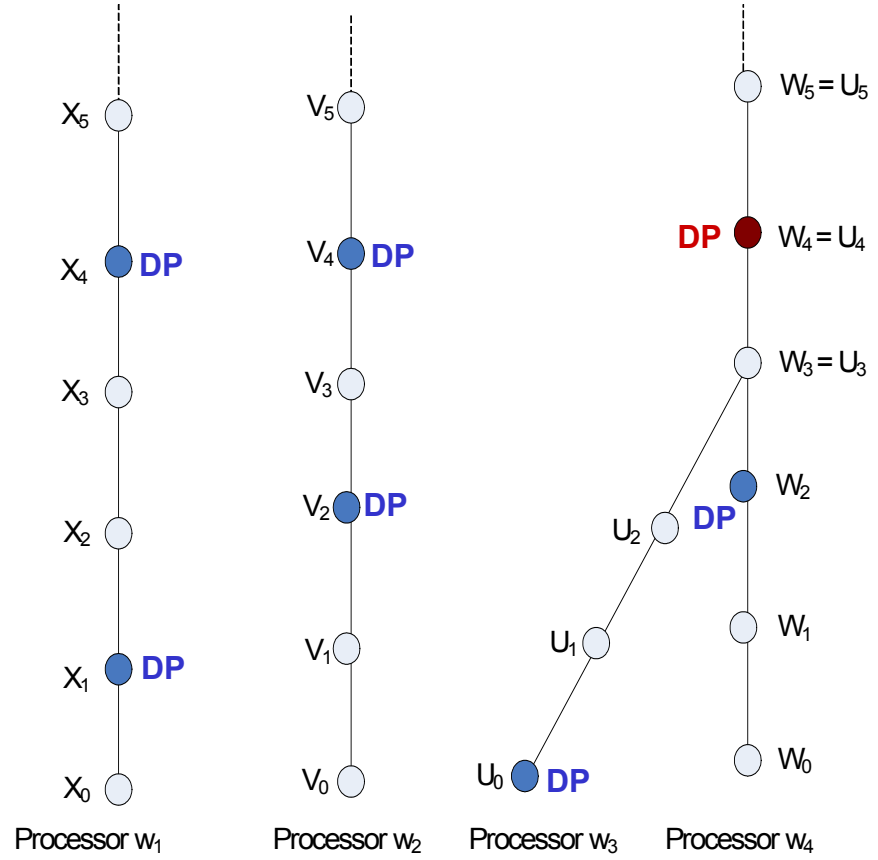
Generic ECDLP Attacks

If parameters are chosen with care, only generic attacks are possible

1. **Naïve Search**: Sequentially test P, *2P, 3P, 4P*,…
   - Brute force attack is infeasible if $\#E \geq 2^{80}$
2. **Shank's Baby-Step-Giant-Step Method**
   - Complexity in time AND memory of about $\sqrt{\#E}$
3. **Pollard's Rho method** (ρ)
   - Most efficient algorithm for general ECDLP
   - Complexity of $\sqrt{\#E}$

Note: All attacks are **exponential** in the bit length of the group order

Multi Processor Pollard Rho (MPPR)



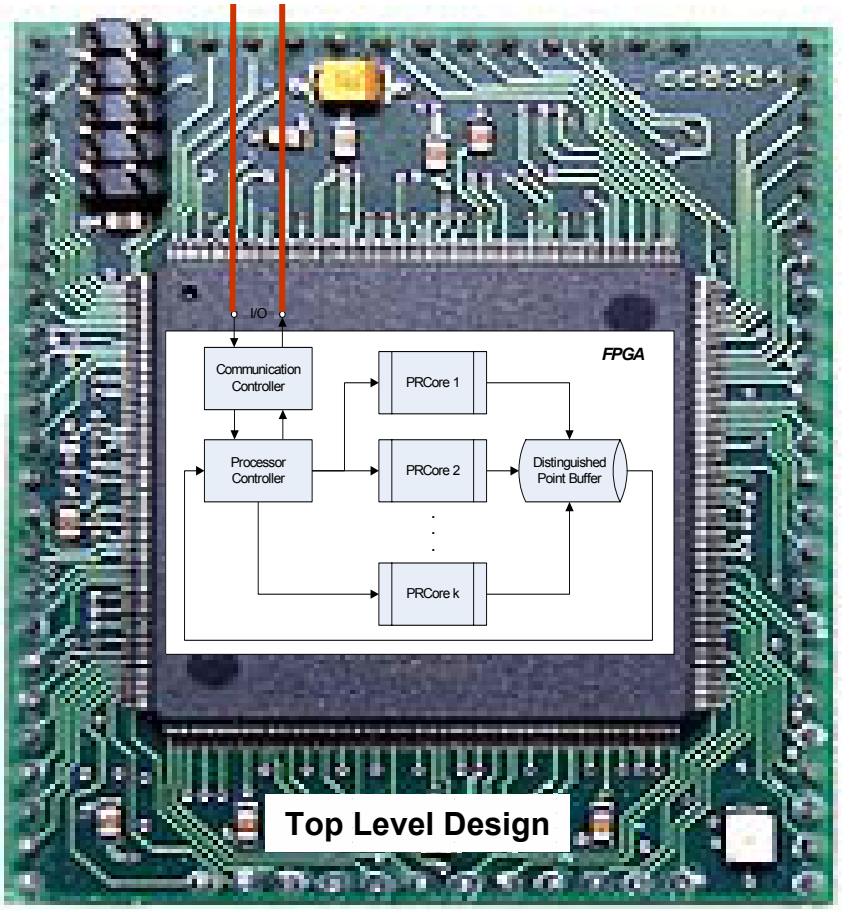
Colliding DP trails of multiple processors w_i

- Best known attack against general ECC
- Proposed by van Oorschot/Wiener in 1999
- Processors have individual search paths for “Distinguished Points” (DP)
- DP are stored at central server
- Duplicate DP = ECDLP solution

Parallelization idea: speed up linear in number of employed processors

Hardware Implementation (Top Layer)

Central Server



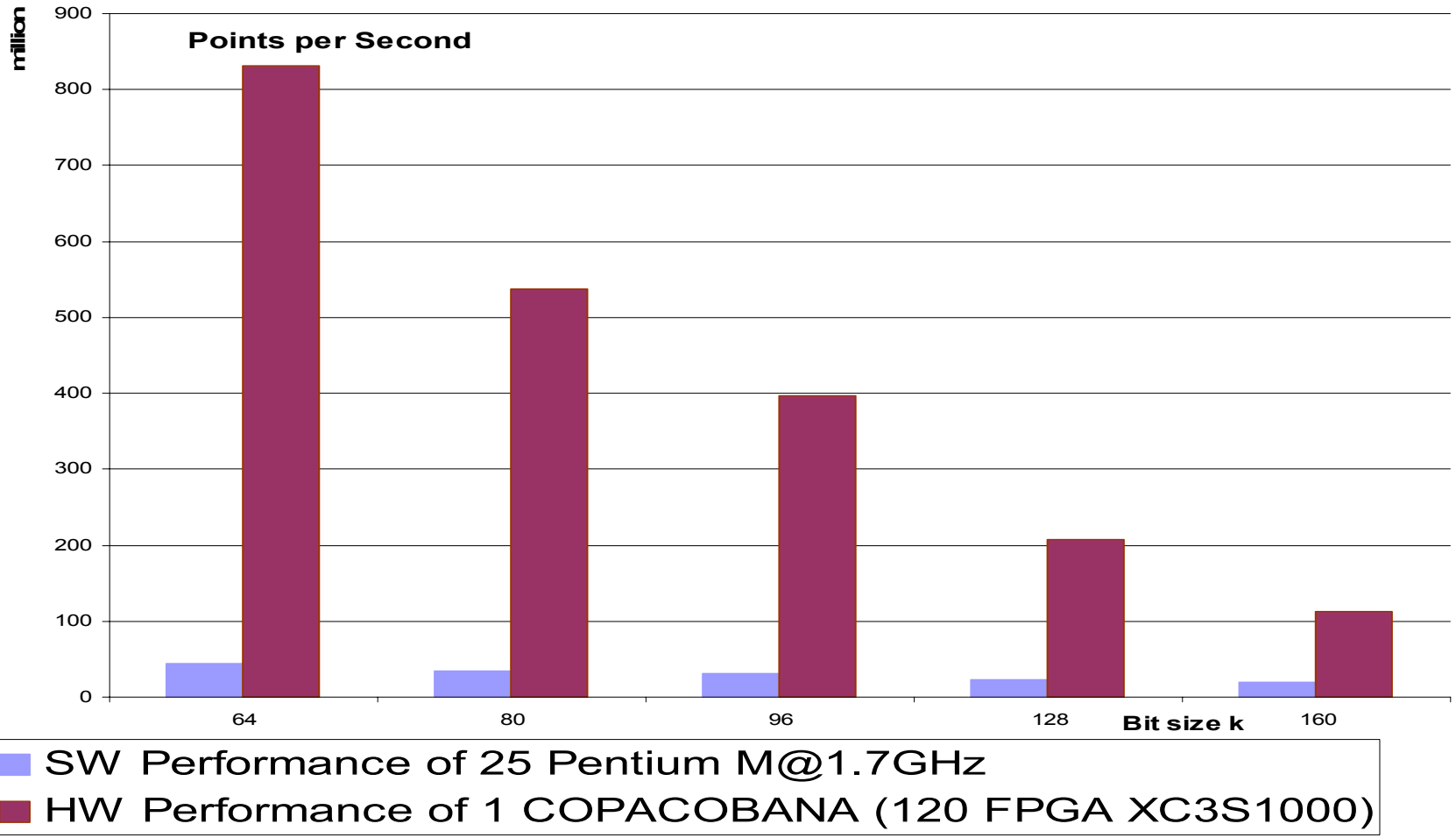
Top Level Design

Neither

- fastest, nor
- smallest
- implementations is needed, but
- **Time-Area Optimum**.

- Each FPGA: multiple point engines (PRCore) each computing a separate trail.
- All cores store distinguished points in a shared point buffer.
- Buffer locking & host communication are needed to transfer DPs to the server.
- FPGA to Host communication via serial (for debugging) or proprietary bus interface.

ECDLP Attack Comparison: SW vs. HW for $10.000



ECDLP Attacks for US$ 1 million

Bit size k	PC Cluster	COPACOBANA (estimate)	ASIC (estimate)
80	40.6 h	2.58 h	-
96	8.04 d	14.8 h	-
112 (SEC-1)*	**6.48 y**	**262 d**	**1.29 d**
128	1.94 $x10^3$ y	213 y	1.03 y
160	**1.51 x 10^8 y**	**2.58 x 10^7 y**	**1.24 x 10^5 y**

* SECG (STANDARDS FOR EFFICIENT CRYPTOGRAPHY)

Agenda

- Security vs. Cost
- Design of the *COPACOBANA* FPGA Cluster
- Application 1: DES Brute-Force
- Application 2: Attack on ECC
- Conclusion and Outlook

Conclusion – COPACOBANA

- Results
  - DES in 8.6 days (possibly 50% speedup in near future)
  - ECC-p163 attack currently ≈ $ 1 trillion ($10^{12})
    - Moore‘s Law: ECC 160 will stay secure for ≈ 20 years
  - ECC-112 (SEC-1 standard): insecure!
  - possibly real-time attack against ePass
- Many marginally weak ciphers are breakable
- „Strong“ ciphers (AES, RSA-1024, ECC-163, …) not breakable, but robust estimates by extrapolation of COPACOBANA results
- Several future applications are currently investigated
- Pictures, papers, and much more at www.copacobana.org
- We are looking for partners for other applications

Outlook

Future work includes

- Optimization of the COPACOBANA platform:
  - harden communication framework (almost done)
  - 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


Questions?