RUHR-UNIVERSITÄT BOCHUM

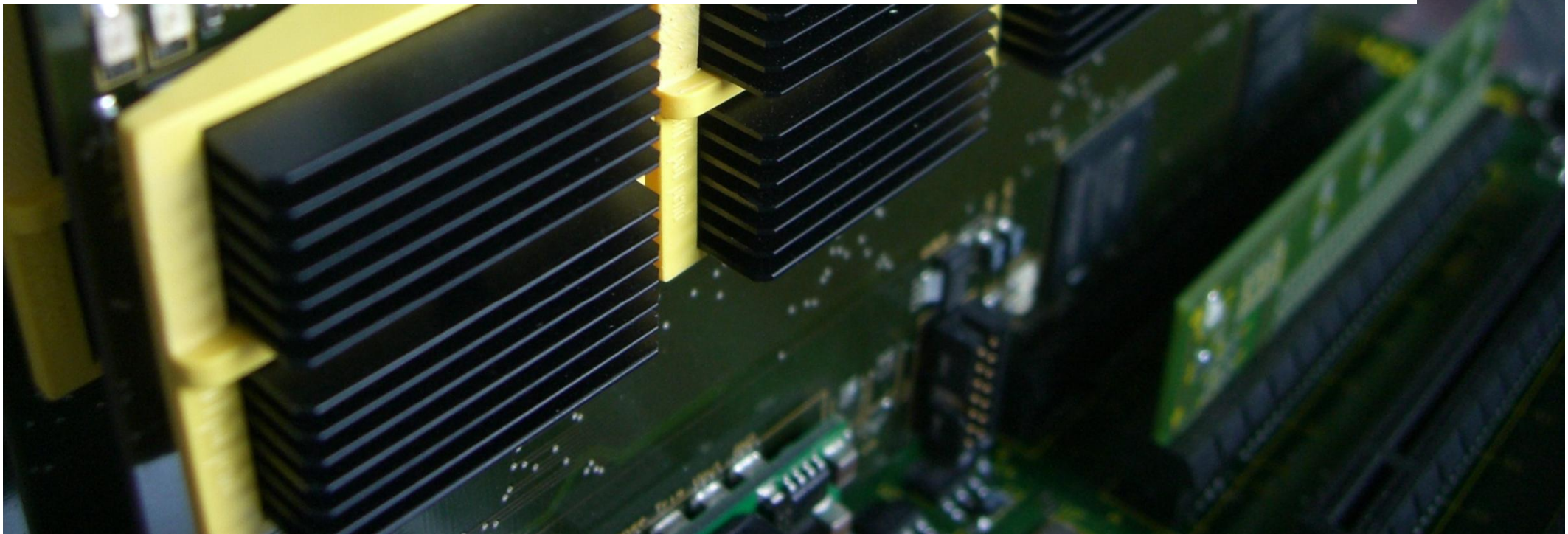
RUB

High-Performance Integer Factoring with Reconfigurable Devices

CryptArchi 2011 - Bochum

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security
Horst Görtz Institute for IT Security, Ruhr-University Bochum

16.06.2011



High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Outline

- Introduction
- Arithmetic using Modern FPGAs
- COPACOBANA / ECM System Layout
- Results
- Conclusions

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Introduction

Factorization Problem

- **Factorization Problem**
  - $2^{512} - 1 =$ é ?
  - Ancient problem
  - Mathematically hard
- **RSA**
  - Based on factorization problem
  - Online Banking (HBCI w/ RSA Keydisk/Chipcard)
  - Set-Top-Box (DigitalTV)
  - SSL certificates

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Introduction
Elliptic Curve Method

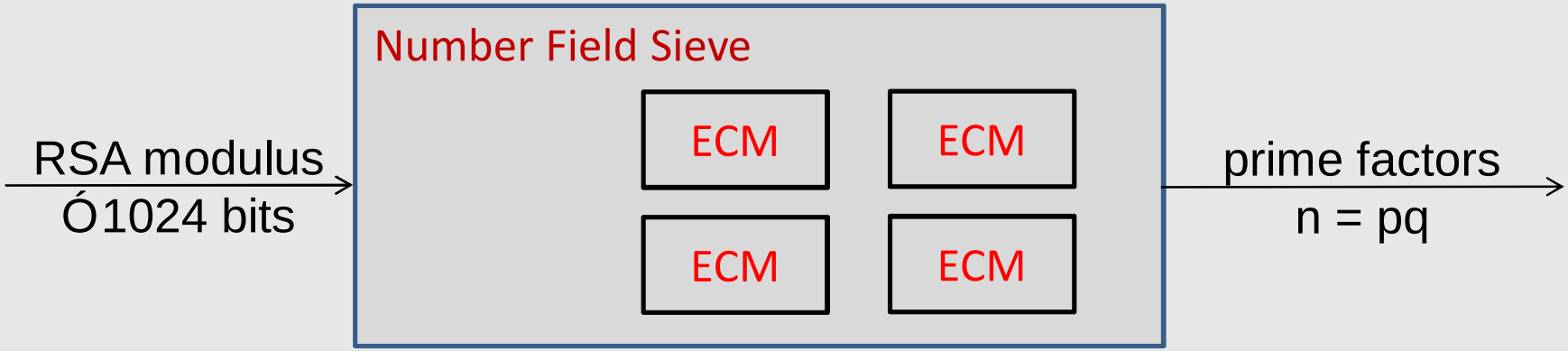
- Why use ECM?
- Factor small numbers
- Low memory requirements

- Nice to know é but é ~200 bits? Importance?

Introduction

Elliptic Curve Method

- Why use ECM?
- Factor small numbers
- Low memory requirements



- Nice to know é but é useful for co-factorization (NFS)

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Introduction
ECM Algorithm

- **Phase 1**
  - One scalar multiplication
  - But: scalar of 1300++ bit
- **Phase 2**
  - Uses phase 1 result
  - Repeated scalar multiplications
  - Iterative product computation

Algorithm 1 The Elliptic Curve Method

Input: Composite $n = f_1 \cdot f_2 \cdot \ldots \cdot f_n$.
Output: Factor f_i of n.

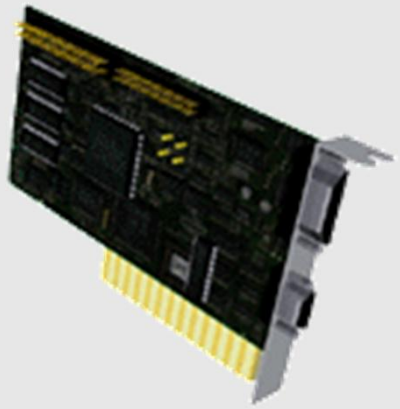
1: **Phase 1:**
2: Choose arbitrary curve $E(\mathbb{Z}_n)$ and random point $P \in E(\mathbb{Z}_n) \neq \mathcal{O}$.
3: Choose smoothness bounds $B1, B2 \in \mathbb{N}$.
4: Compute $e = \prod_{p_i \in \mathbb{P}; p_i < B1} p_i^{\lfloor \log_{p_i}(B1) \rfloor}$
5: Compute $Q = eP = (x_Q; y_Q; z_Q)$.
6: Compute $d = gcd(z_Q, n)$.
7: **Phase 2:**
8: Set $s := 1$.
9: **for** each prime p with $B1 < p \leq B2$ **do**
10: Compute $pQ = (xpQ : ypQ : zpQ)$.
11: Compute $d = d \cdot zpQ$.
12: **end for**
13: Compute $f_i = gcd(d, n)$.
14: **if** $1 < f_i < n$ **then**
15: A non-trivial factor d is found.
16: return f_i
17: **else**
18: Restart from Step 2 in Phase 1.
19: **end if**

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Introduction

Existing implementations

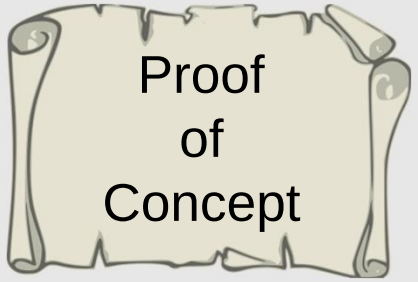
- Software: GMP-ECM (P. Zimmermann *et al.*)
- Variant: GMP-EECM (Bernstein *et al.* 2008)
- GPUs: GPU-ECM (Bernstein *et al.* 2008)



Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Introduction
Existing implementations

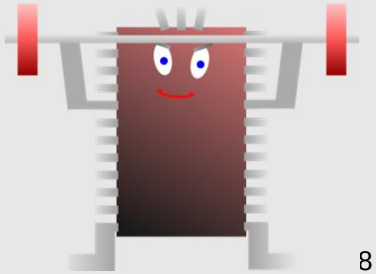
- **Simka *et al.* (FPL 2005)**
  - Montgomery curves
  - Virtex-E 2000 w/ embedded micro-controller
  - Proof-of-concept implementation



- **Gaj *et al.* (CHES 2006, IEEE ToC (Sep 2010))**
  - Implementation on high and low cost FPGAs
  - Suggestions on phase 2 implementation

2nd Phase

- **De Meulenaer *et al.* (FCCM 2007)**
  - Uses DSP hardcores to implement phase 1
  - No implementation of phase 2 (possible?)



Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Introduction

Design Goals and Decisions

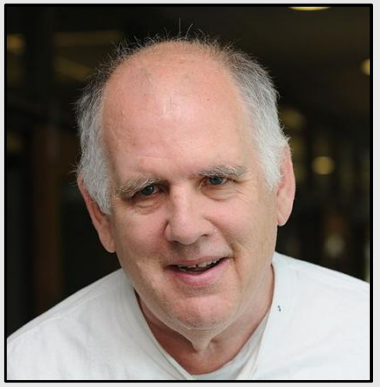
Usage of Elliptic Curve Method (ECM) in **co-factorization**

Goals

- Implement both phase 1 and 2
- Usable on COPACOBANA v4

Curves in Montgomery Form

- Efficient formulas for hardware
- Computation/storage of y-coordinate can be omitted



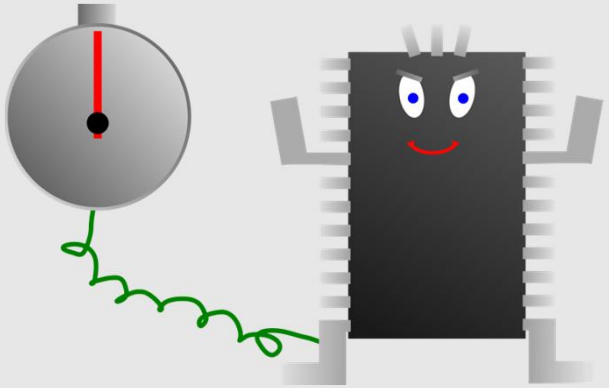
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Arithmetic using Modern FPGAs

Xilinx Virtex FPGAs

- Virtex-4 (announced 2004)
- Virtex-5 (announced 2006)
- Virtex-6 (announced 2009)

- Generic Logic (LUT, Flipflop)



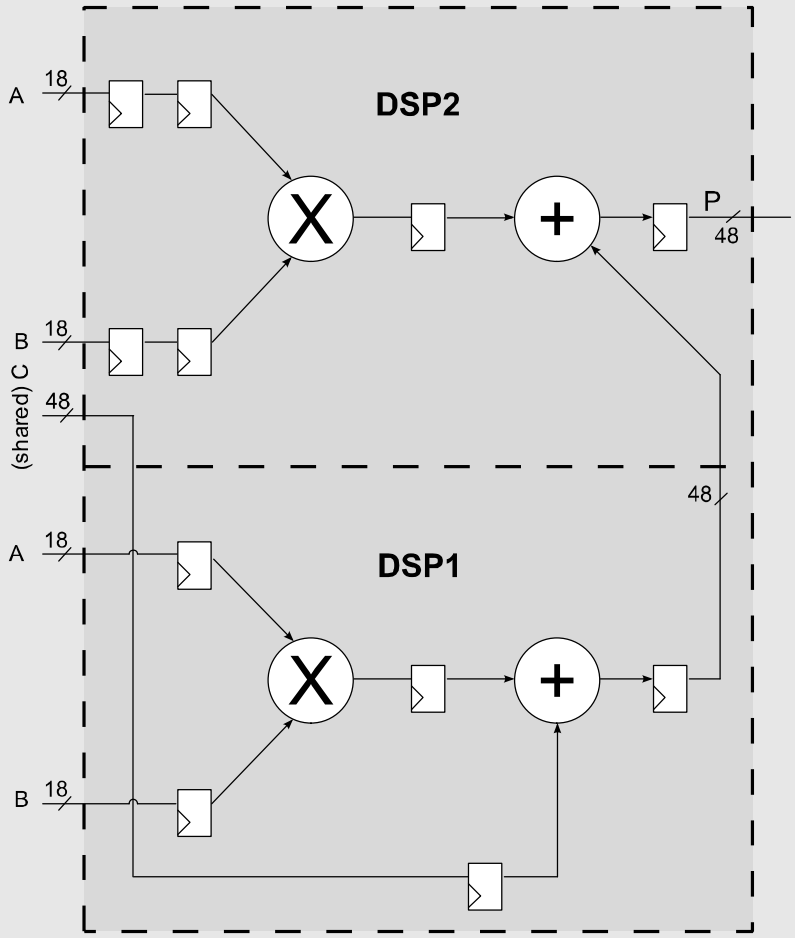
- Dedicated memory elements
- Arithmetic hardcores,
- Embedded PowerPC processors
- High-speed I/O transceivers

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Arithmetic using Modern FPGAs

Digital Signal Processing Slices on Virtex-4

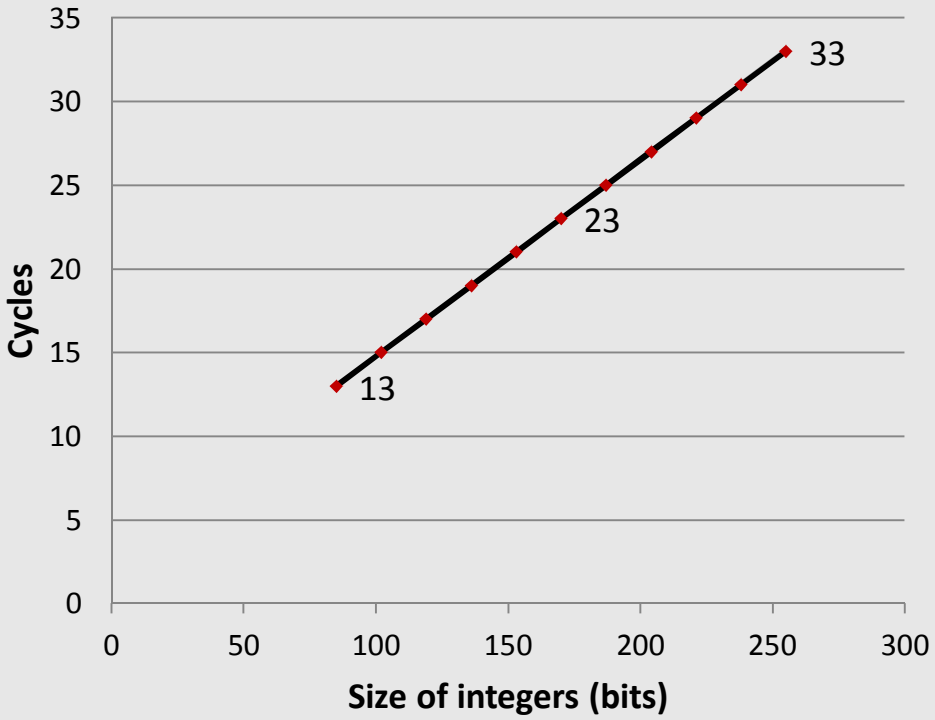
- DSP Slice: two adjacent DSP
- Fast signed 18x18-bit multiplication and signed 48-bit addition/subtraction (400 MHz)
- Integrated pipeline register
- Controllable by an OPMODE signal
- DSP elements can be cascaded



Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Arithmetic using Modern FPGAs

Implemented Mod. Addition/Subtraction

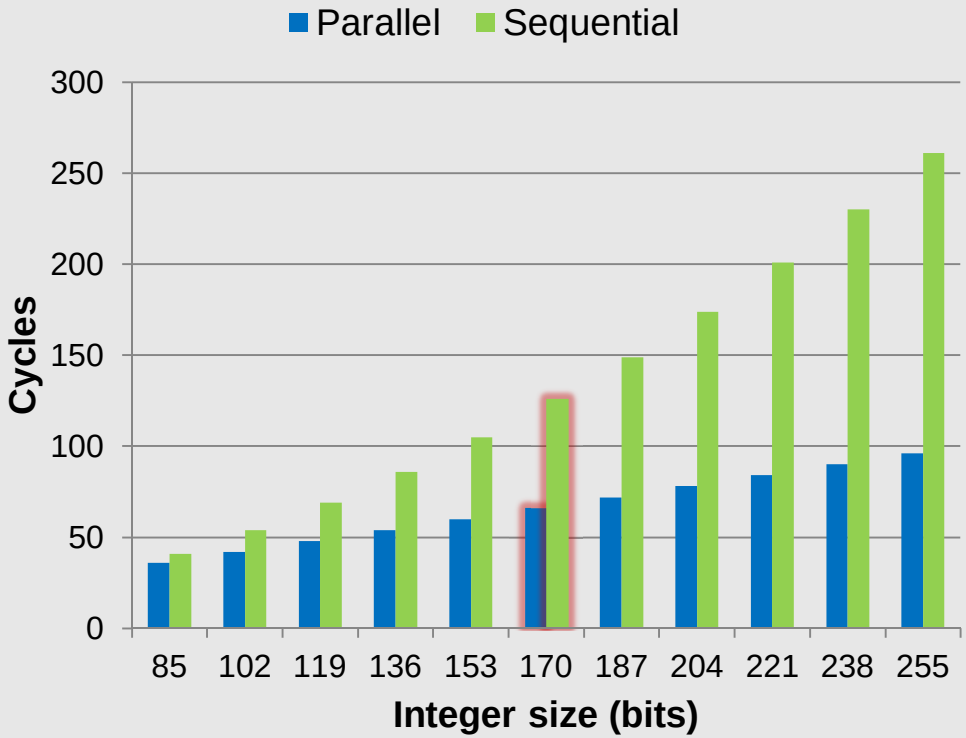


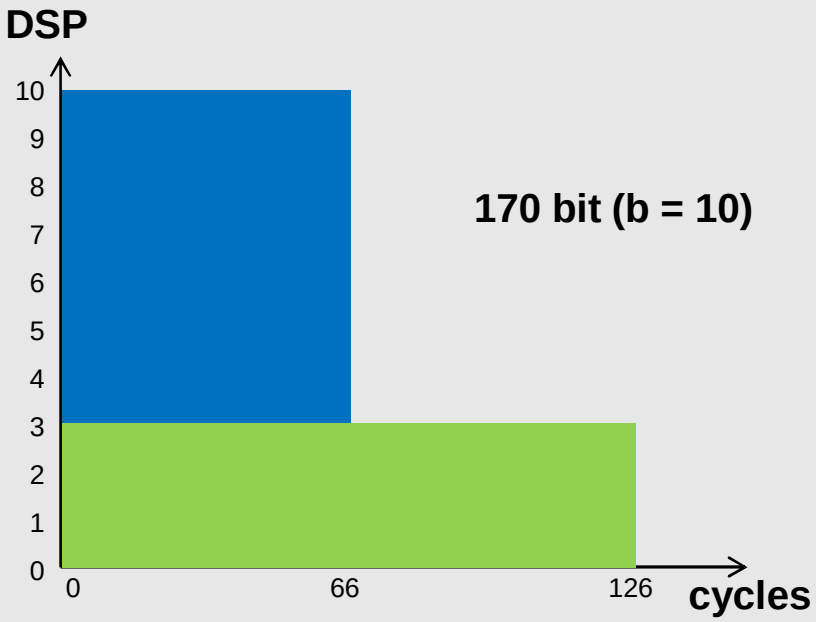
	Virtex-4	Virtex-4*
Flipflops	143	106
Slices	104	67
LUTs	123	88
DSPs	2	
Cycles	2*b+3	
Frequency	400	

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Arithmetic using Modern FPGAs

Multiplication: Parallel vs. Sequential

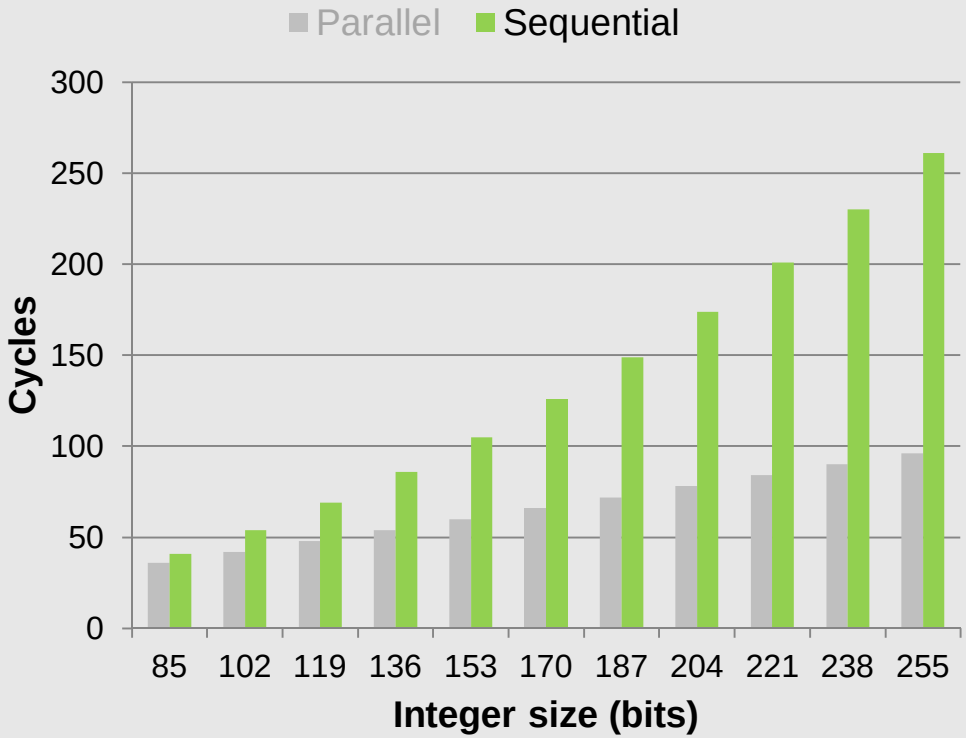




Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Arithmetic using Modern FPGAs

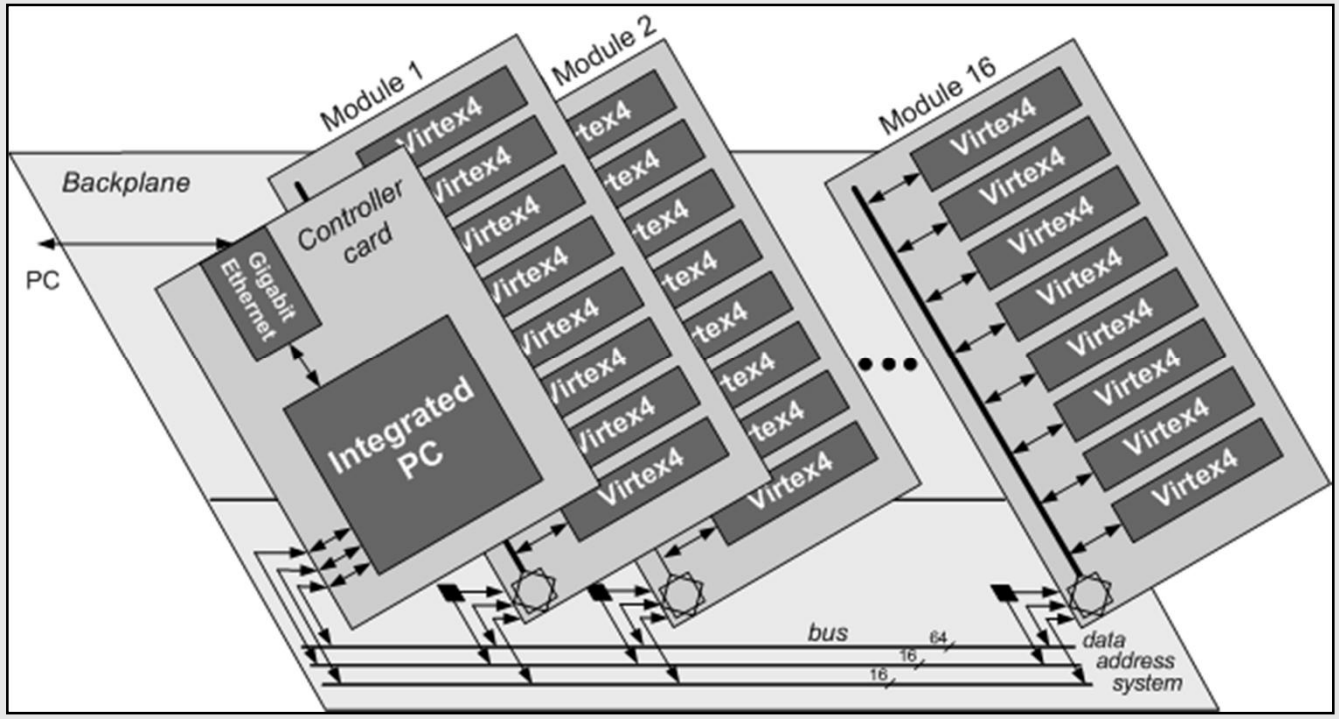
Multiplication: Parallel vs. Sequential



	Virtex-4
Flipflops	131
Slices	73
LUTs	83
DSPs	3
Cycles	b*(b+2)+6
Frequency	400 MHz

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

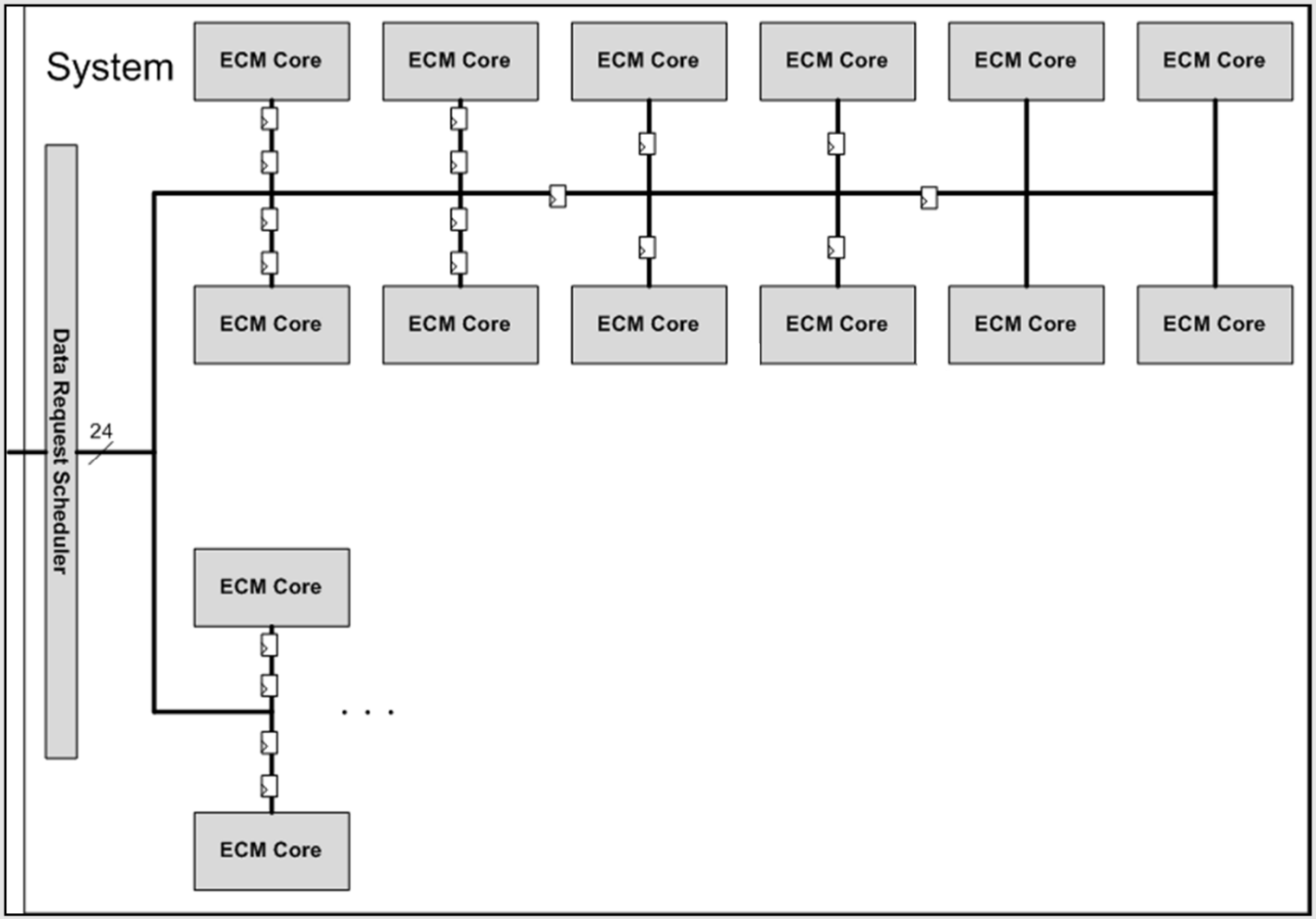
COPACOBANA: Original Architecture



- Backplane with plug-in slots can host up to 16 FPGA modules
- 8 x Xilinx Virtex-4 FPGAs (XC4VSX35) per FPGA module
- Controller connects Integrated PC with FPGAs in a Master-Slave scheme
- Gigabit Ethernet interface

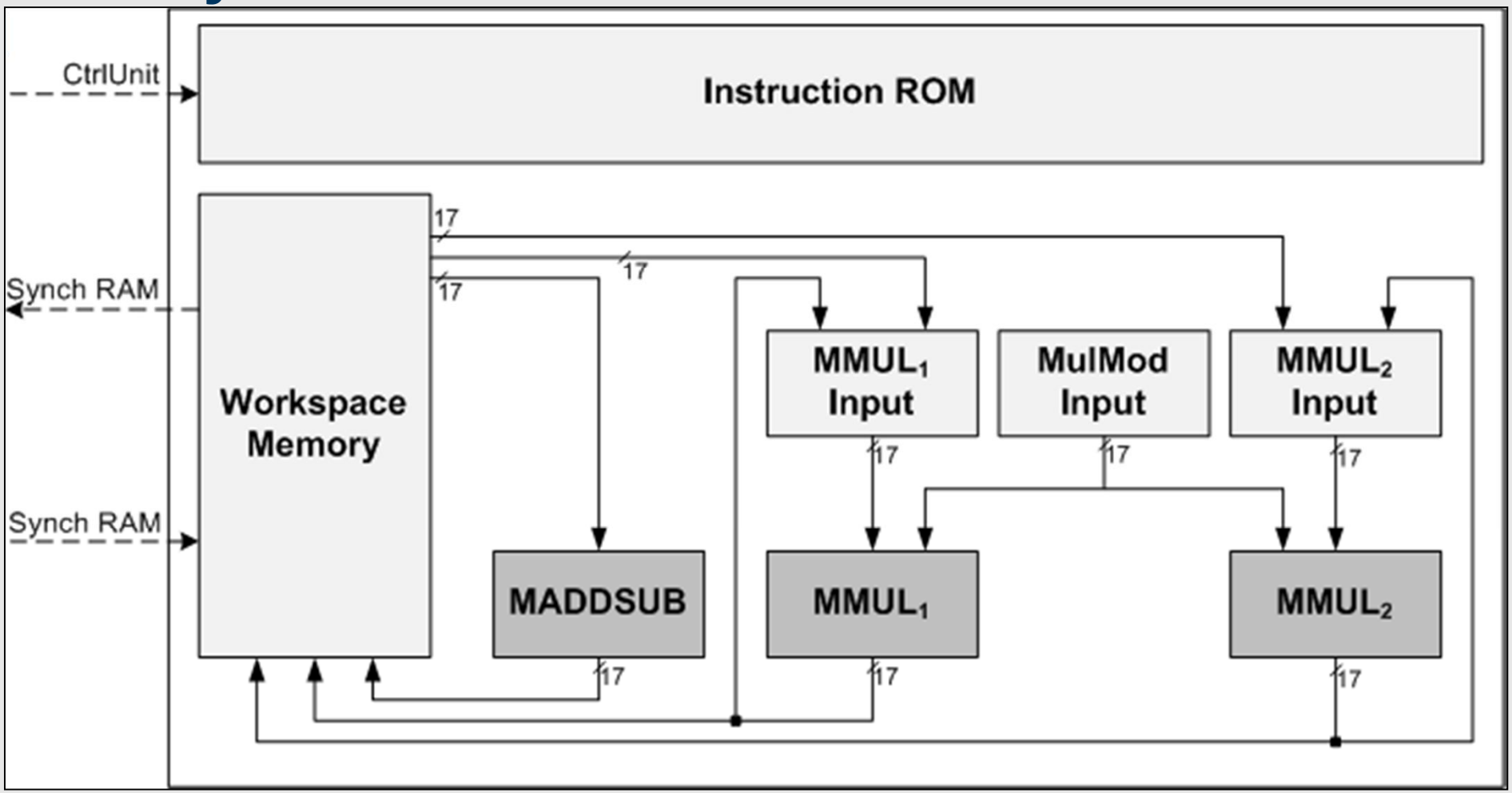
High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

ECM System Architecture



High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

ECM System Architecture



High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Results

ECM Phase 1 + 2

FPGA Type	Virtex-4 SX 35
Target Bitlength	151
Number of ECM units	24
Maximal clock frequency	200
Number of instructions for ECM Phase 1 + 2	1,969,878
Time for ECM Phase 1 + 2	9.85 ms
Number of calculations per second	**2424**

ECM Phase 1 + 2 using B1 = 960, B2 = 57000 [1374 bit k]

310,272 ECM calculations / second on COPACOBANA[1]

[1] ñOptimalòCOPACOBANA using 16 FPGA modules (= 128 FPGA)

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Results
Scalability

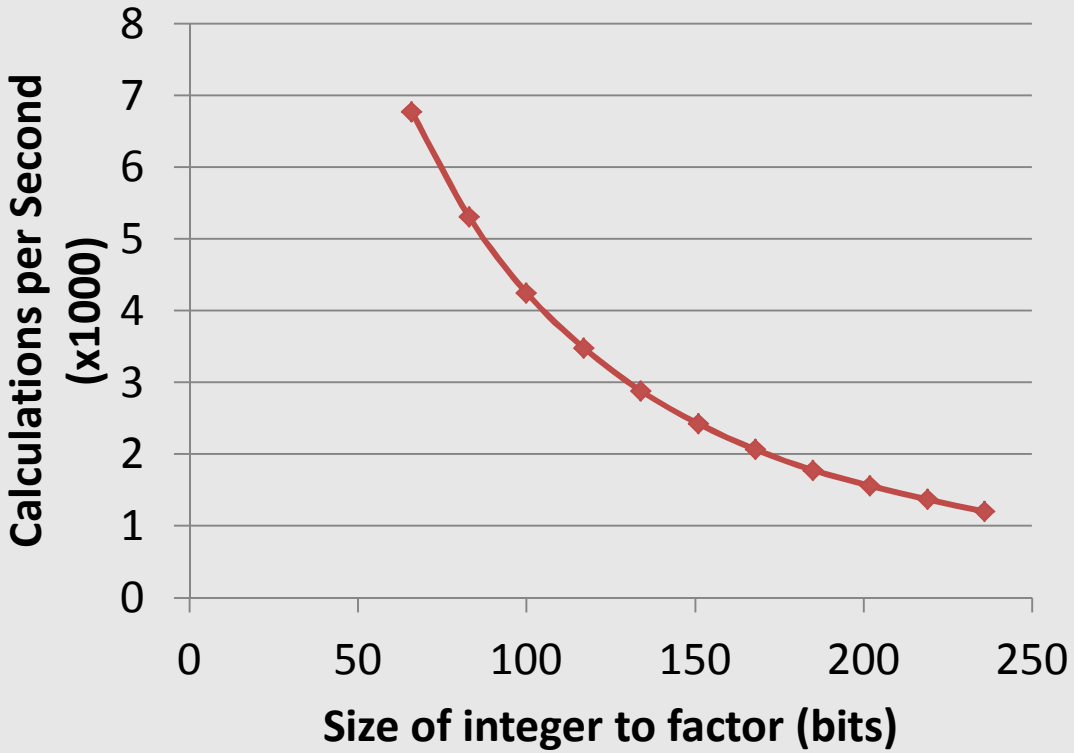
- Related work - bit-length ?
  - Å Scalable system
  - Å Fixed layout
  - Å Exchangeable ROM

		Phase 1		Phase 2		Calc / Second	
b	max. Bits	cycles	time (ms)	cycles	time (ms)	Phase 1	ECM
5	66	340,916	1.70	367,199	1.84	14,064	6,768
6	83	434,390	2.17	468,413	2.34	11,040	5,304
7	100	541,610	2.71	584,703	2.92	8,856	4,248
8	117	662,576	3.31	716,069	3.58	7,224	3,480
9	134	797,288	3.99	862,511	4.31	6,000	2,880
10	**151**	**945,746**	**4.73**	**1,024,029**	**5.12**	**5,064**	**2,424**
11	168	1,107,950	5.54	1,200,623	6.00	4,320	2,064
12	185	1,283,900	6.42	1,392,293	6.96	3,720	1,776
13	202	1,473,596	7.37	1,599,039	8.00	3,240	1,560
14	219	1,677,038	8.39	1,820,861	9.10	2,856	1,368
15	236	1,894,226	9.47	2,057,759	10.29	2,520	1,200

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Results
Scalability

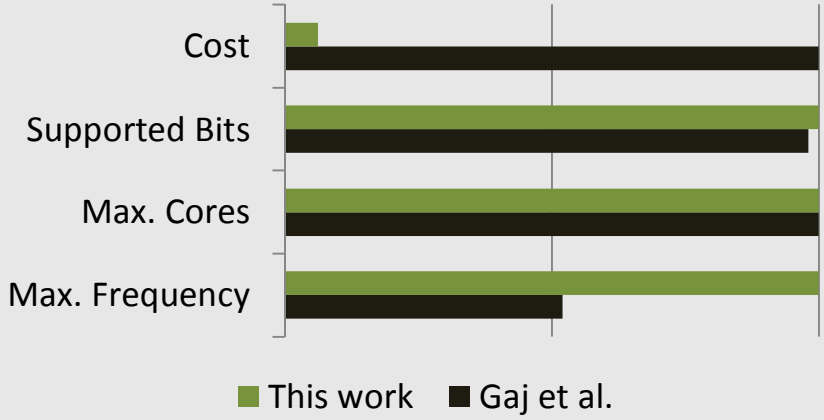
- Related work - bit-length ?
  - Å Scalable system
  - Å Fixed layout
  - Å Exchangeable ROM

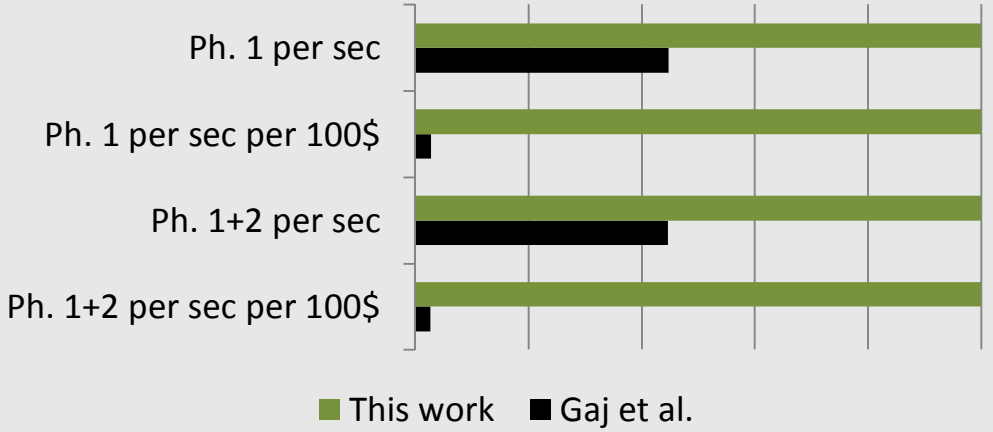


High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Results

Comparison (Gaj *et al.*)



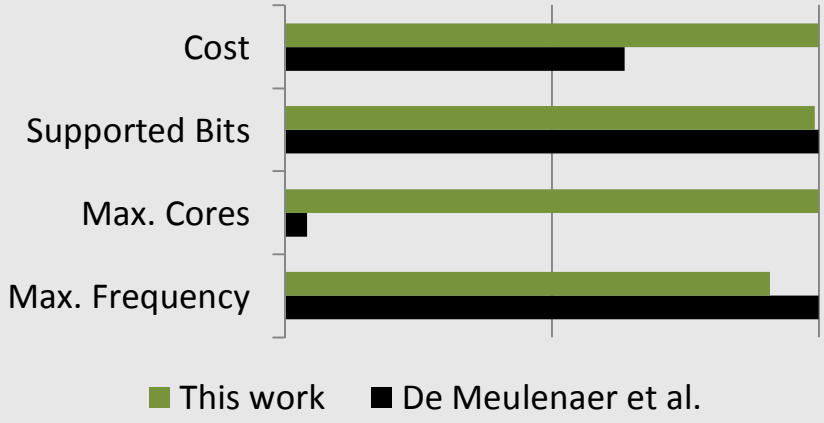


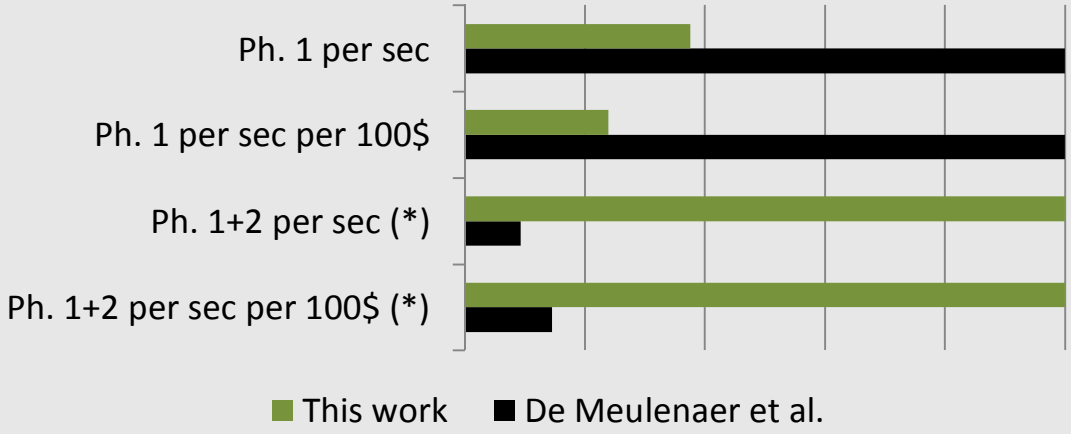
- 198 bits vs 202 bits
- Arithmetic: Fabric vs. DSPs
- Improvement by factor 2.24 resp. 37

Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Results

Comparison (De Meulenaer *et al.*)



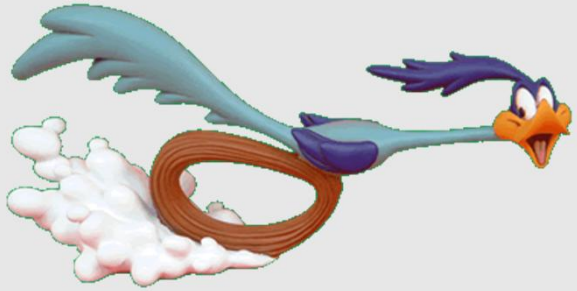


- 135 bits vs 134 bits
- Fully pipelined vs non-pipelined
- DSP arithmetic: Mult vs Mult+Add
- (*) Equal results: Phase 1+2 ~ 59.68 x Phase 1

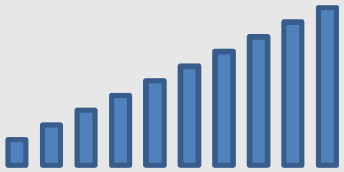
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Conclusion

- **Complete implementation**
  - Å Fastest implementation of phase 1 + 2 on FPGAs
  - Å Place & route results



- **Generic and scalable system**
  - Å Supports 66..236 bit integers
  - Å Exchangeable instruction ROM
  - Å Powerful scalable modular arithmetic



- **Highly parallel architecture for co-factorization**
  - Å Multiple ECM-units per FPGA (24 units on Virtex-4 SX 35)
  - Å COPACOBANA: max 128 Virtex-4 SX 35

RUHR-UNIVERSITÄT BOCHUM

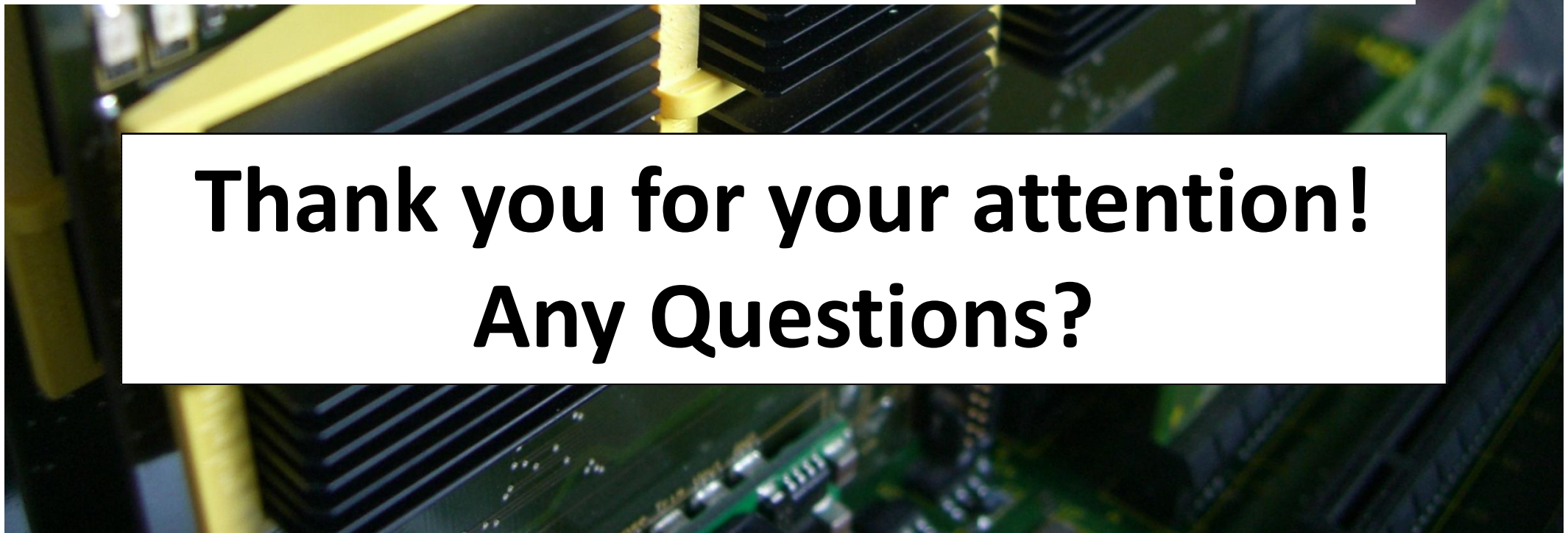
RUB

High-Performance Integer Factoring with Reconfigurable Devices

CryptArchi 2011 - Bochum

Dipl.-Inform. Ralf Zimmermann,
Chair for Embedded Security
Horst Görtz Institute for IT Security, Ruhr-University Bochum

16.06.2011



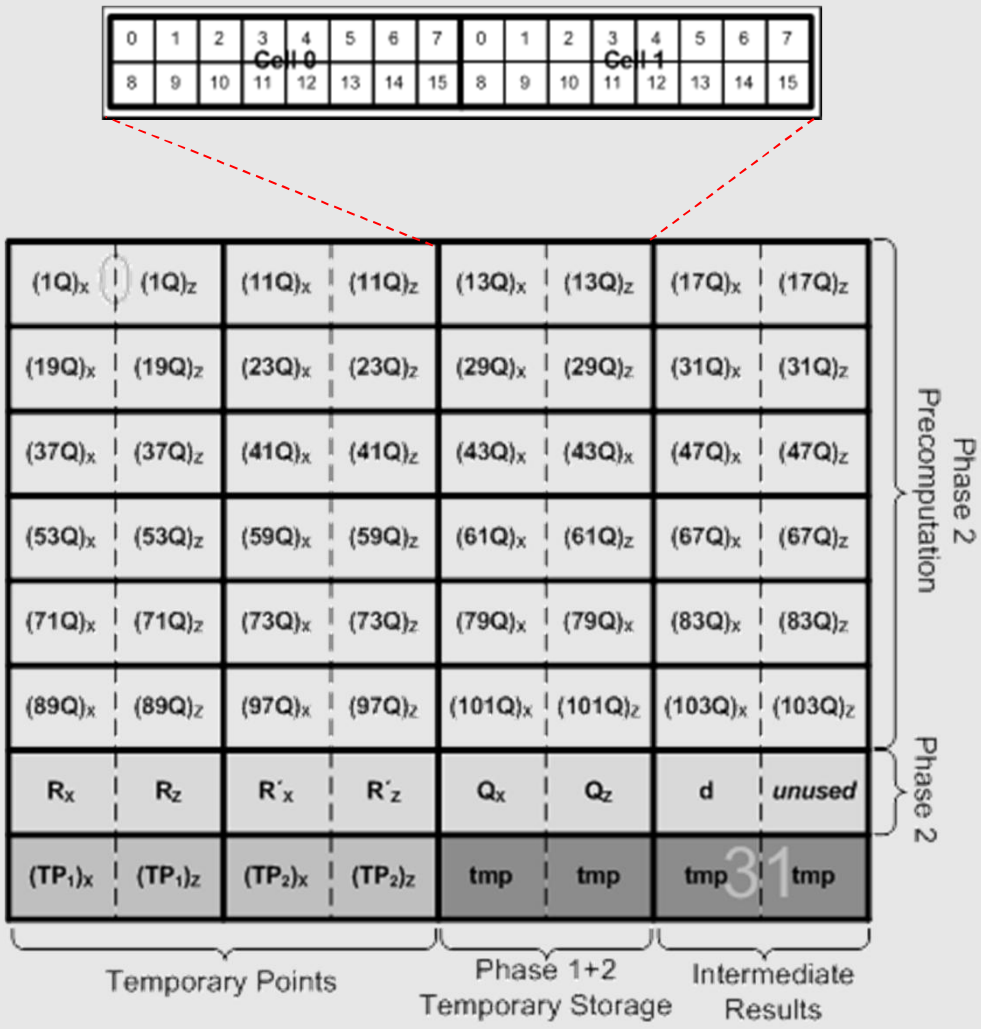
Thank you for your attention!

Any Questions?

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

ECM System Architecture
Workspace Memory

- Cell = 16 times 17-bit = 272 bit
- Block = 2 Cells = one Point
- Addressed by instruction ROM
- Fast in/out for arithmetic Units

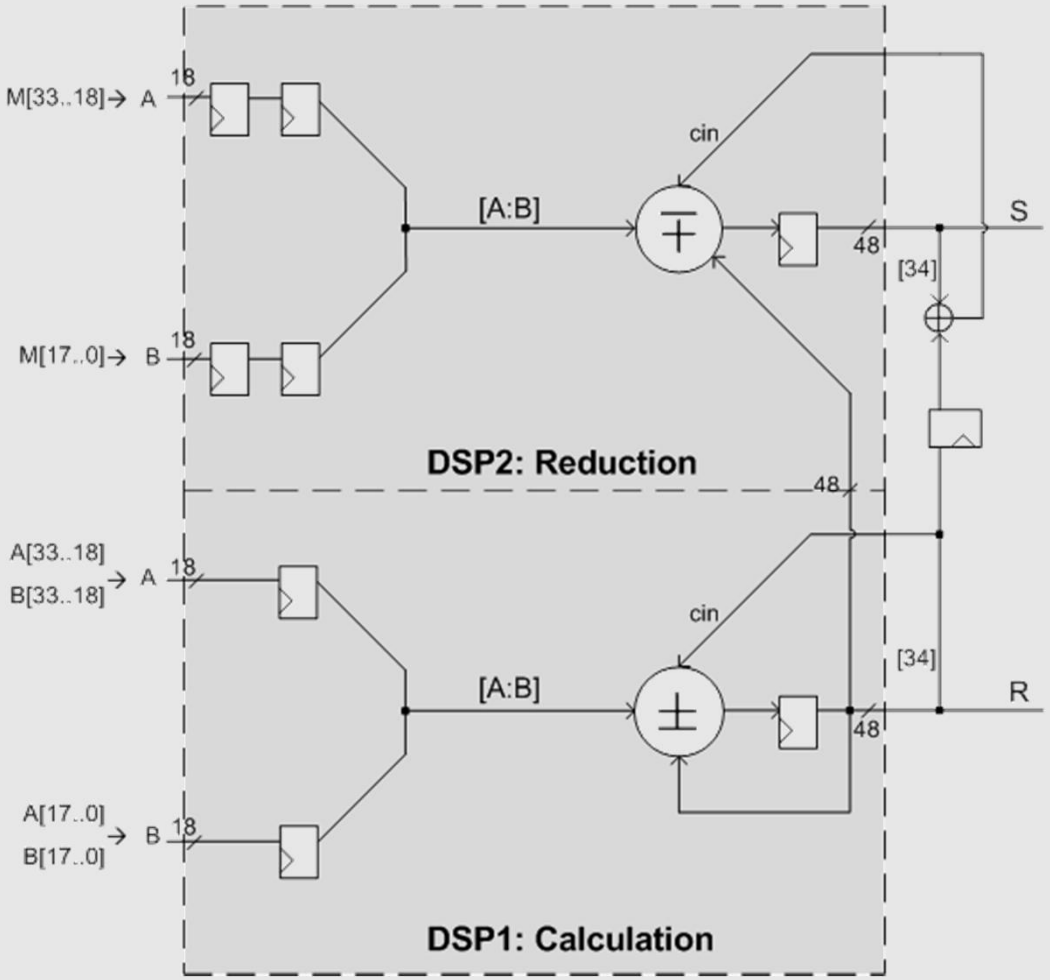


High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

ECM System Architecture

Modular Addition/Subtraction

- Computes addition/subtraction with (parallel) reduction
- Fixed amount of 2 DSPs

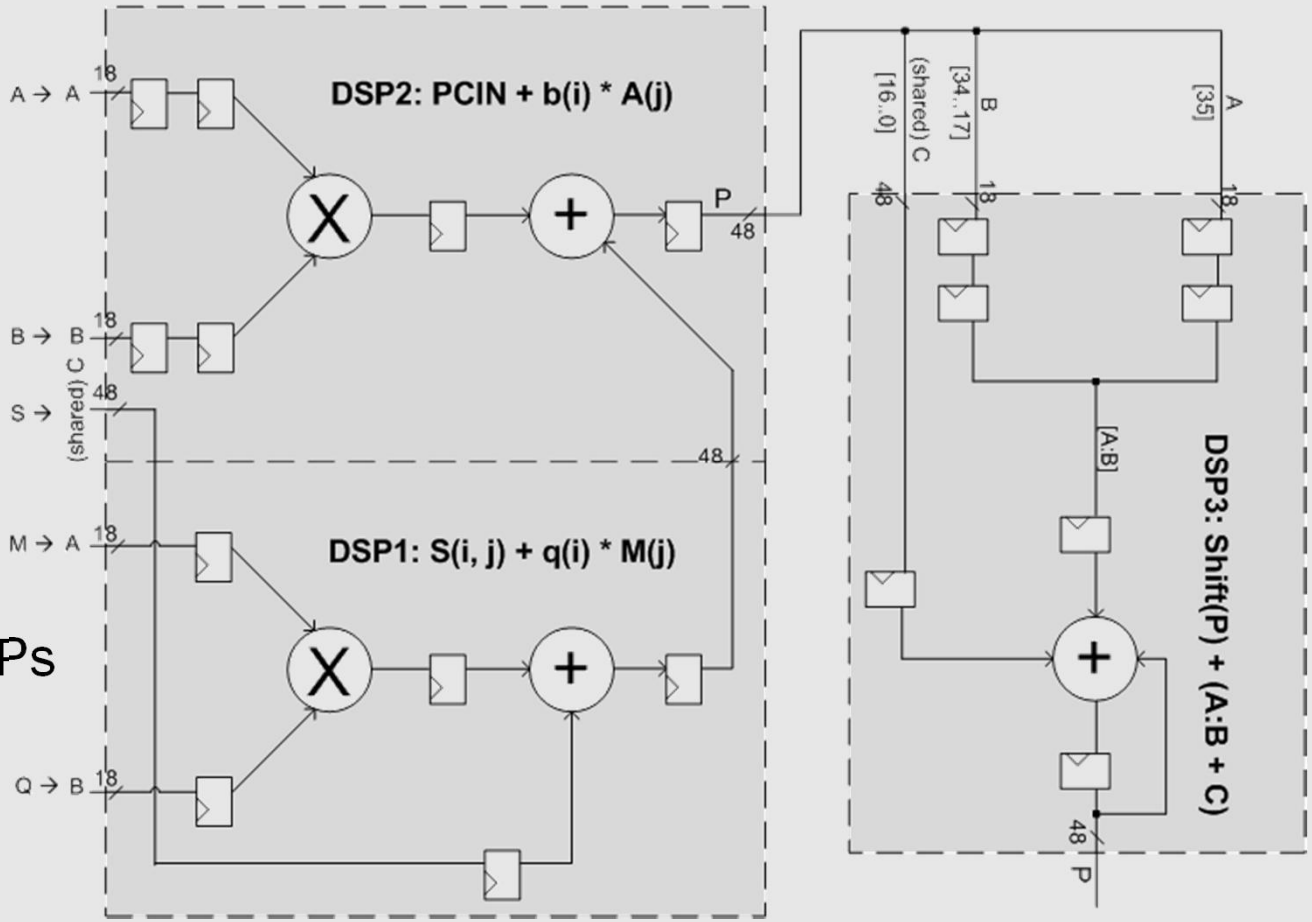


High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

ECM System Architecture

Modular Multiplication

- Computes Orup's Modular Multiplication (Quotient Pipelining with d = 0)
- Fixed amount of 3 DSPs



High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

Results

Comparison to CPUs (GMP-ECM)

PC System

Intel Core2Ê Quad CPU Q9400 @2.66 GHz
4 GB DDR2 RAM @800 MHz

ECM configuration

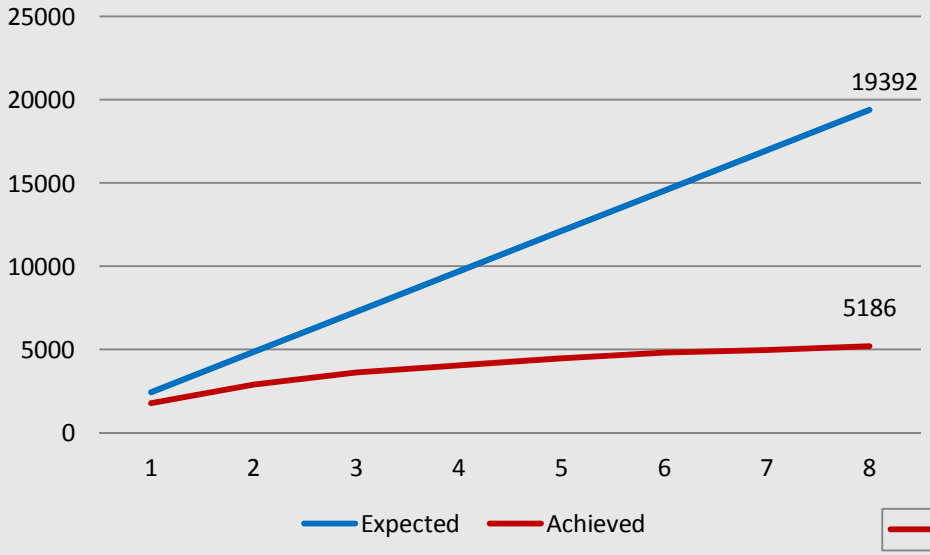
B1 = 960, B2 = 57012
45000 computations

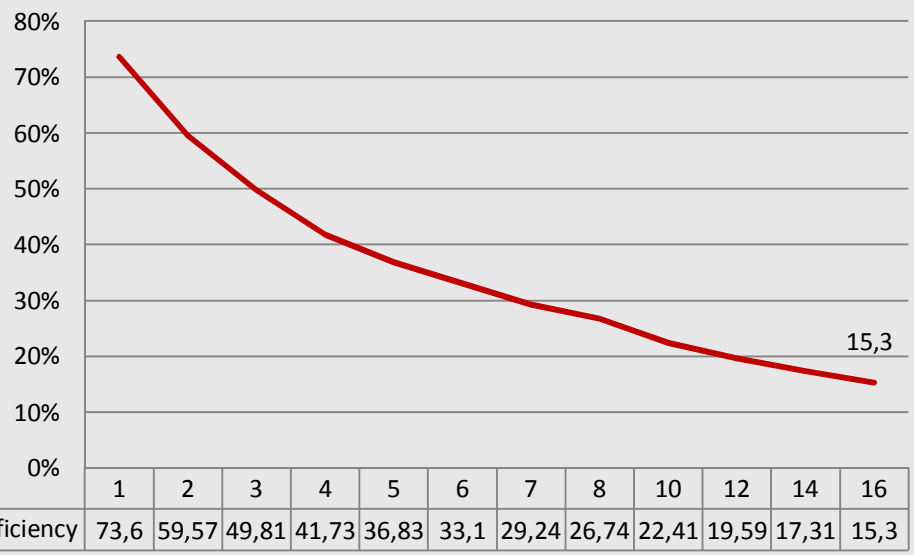
Implementation	Virtex-4 SX 35	PC
Target Bitlength	151	151
Number of ECM units	24	4
Maximal clock frequency	200	2,667
Time for ECM Phase 1 + 2	9.85 ms	2.22 ms
Number of calculations per second	**2424**	**1804**

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

COPACOBANA v4 Results

Is there a bottleneck?





	1	2	3	4	5	6	7	8	10	12	14	16
Efficiency	73,6	59,57	49,81	41,73	36,83	33,1	29,24	26,74	22,41	19,59	17,31	15,3

Bottleneck: COPACOBANA v4 Interface

High-Performance Integer Factoring with Reconfigurable Devices
Ralf Zimmermann, Tim Güneysu, Christof Paar
Chair for Embedded Security

COPACOBANA v4 Results

Explaining the bottleneck

- Bus Architecture
  - Å Slow single master bus → no interrupts
  - Å No parallel read/write operations

Solution: Rivyera

  - Å No PCI-Express
  - Å → USB with ~40 Mbps

- Processor
  - Å Slow CPU
  - Å Additional host
  - Å Power consumption, Network latency, é