Universität Karlsruhe (TH)
Research University · founded 1825

Karlsruhe Institute of Technology

Exploiting Dynamic and Partial Reconfiguration for Cryptographic Applications

Michael Hübner, Jürgen Becker

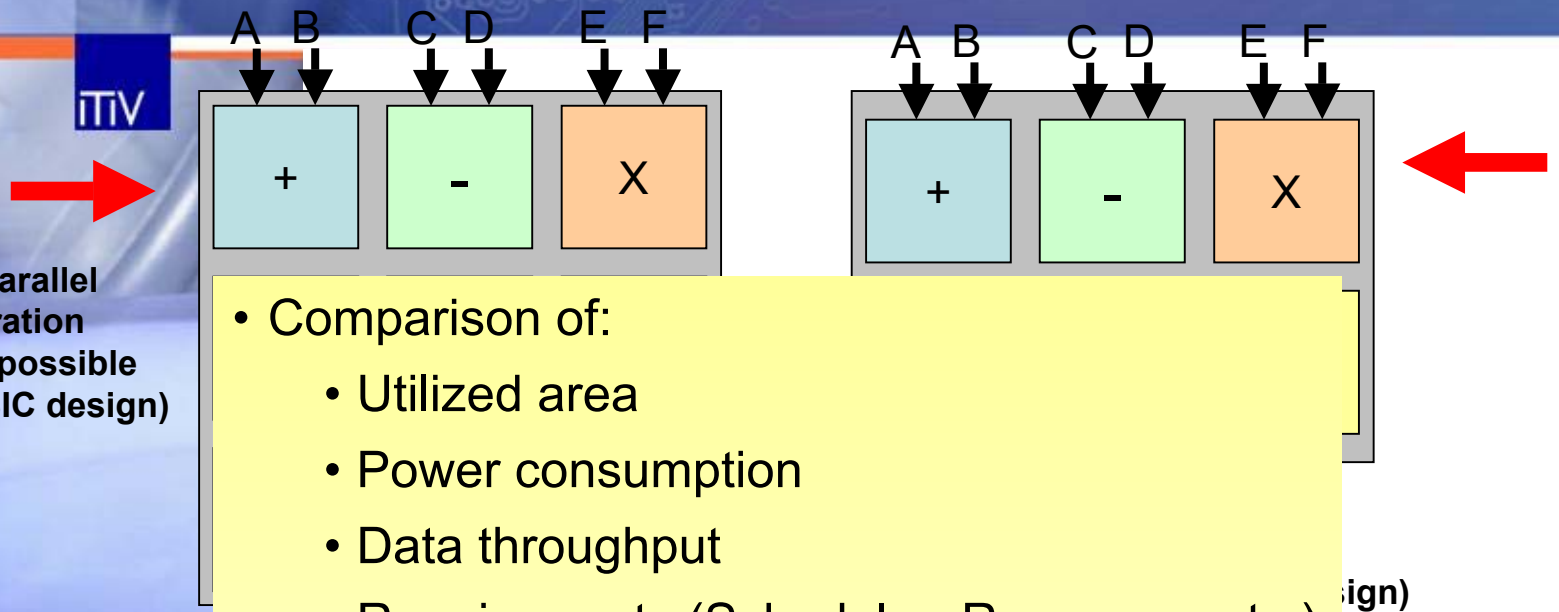
June 20st, Montpellier 2007

Heads of Institute:
Prof. Dr.-Ing. K.D. Müller-Glaser
Prof. Dr.-Ing. J. Becker

Contents

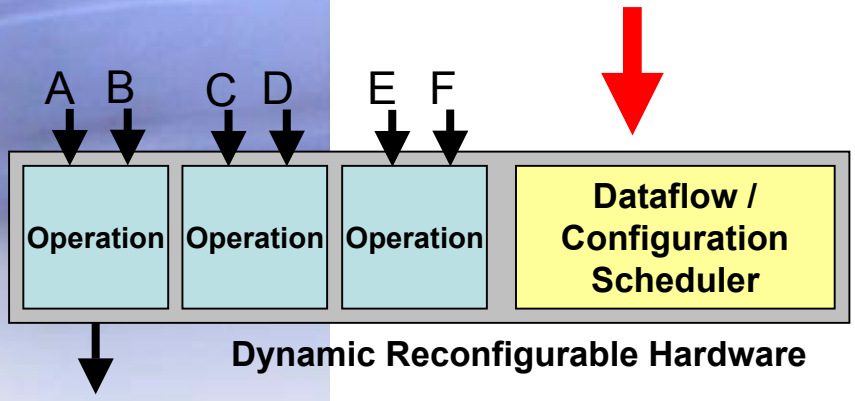
- Motivation
- Hardware Basics
- Configuration Manipulation
- Run-Time Component
- Methods for Side-Channel Attack Defense
- Conclusion and Future Work

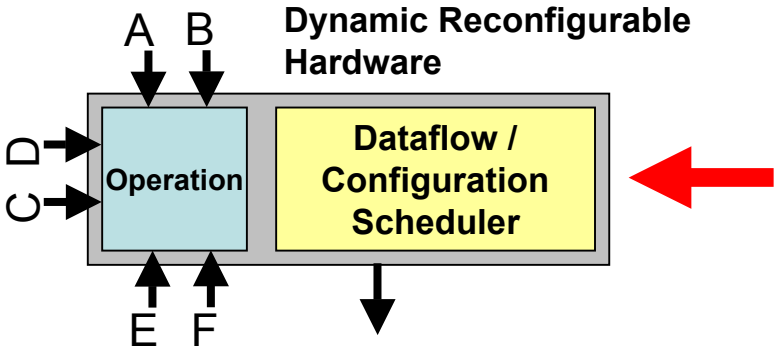
Why Dynamic and Partial Reconfiguration?



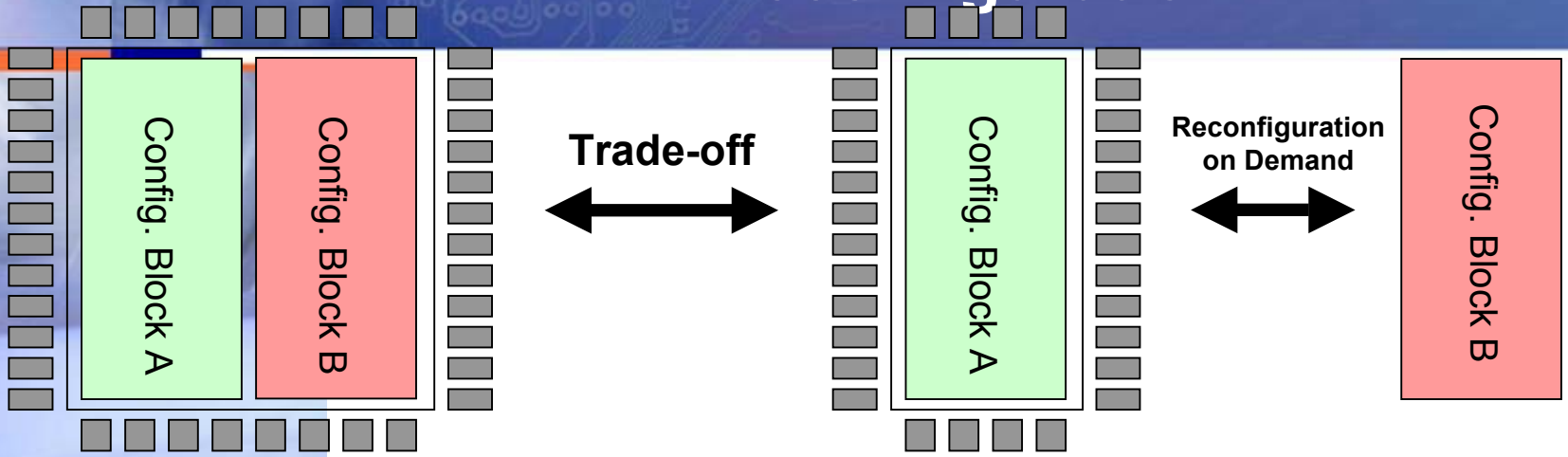
Full parallel integration (also possible as ASIC design)

- Comparison of:
  - Utilized area
  - Power consumption
  - Data throughput
  - Requirements (Scheduler, Resources etc.)





Why Dynamic and Partial Reconfiguration?



- **High static and dynamic Power Consumption**
- **No Run-Time Reconfiguration Management necessary**

- **Optimal size of FPGA** (depends on the size of the greatest Module to implement)
- **Less static and dynamic Power Consumption** but additional Power loss by increased external Memory
- **Caution: Additional Power Consumption while Reconfiguration**

(Median Power Dissipation increases with the Frequency of Reconfiguration)

Secure Hardware for Cryptography

Side-Channel Attacks

Secure Hardware?

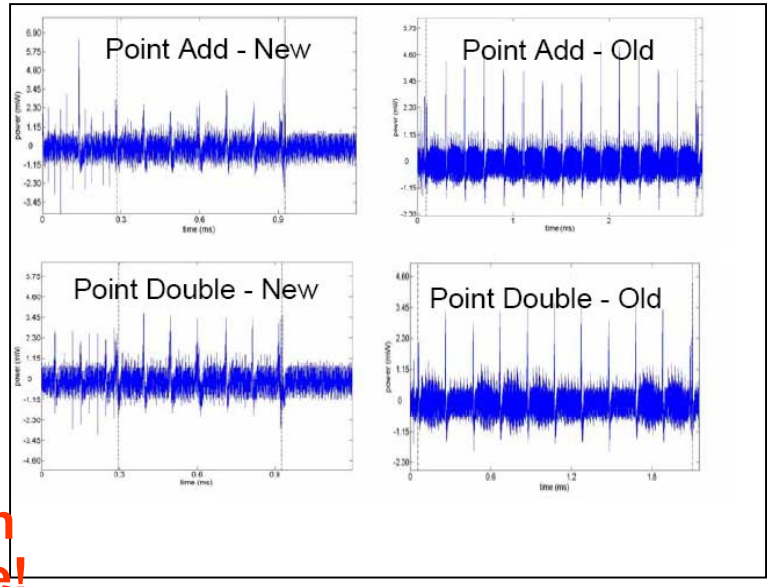
Robust against Side-Channel Attacks (power consumption, timing, electromagnetic radiation)

SPA Attack

Pattern in power consumption reveals information about Algorithm and sequence of operations. Key can possibly be extracted.

Countermeasures:

- **Use of balanced Algorithms**
- **Physical Measures to avoid Patterns**



Secure Hardware and Implementation is gaining more and more Importance!

Source: Alexander Klimm, ITIV

Secure Hardware for Cryptography
Increase of Security against Side-Channel Attacks

Ideal world:

- Secure Hardware doesn't reveal ANY Information over Side-Channels (electromagnetic radiation, power consumption, …)

The real world:

- Every switching operation affects power consumption and creates electromagnetic radiation
- Change in Capacity in the routing channels can be measured and reveals information

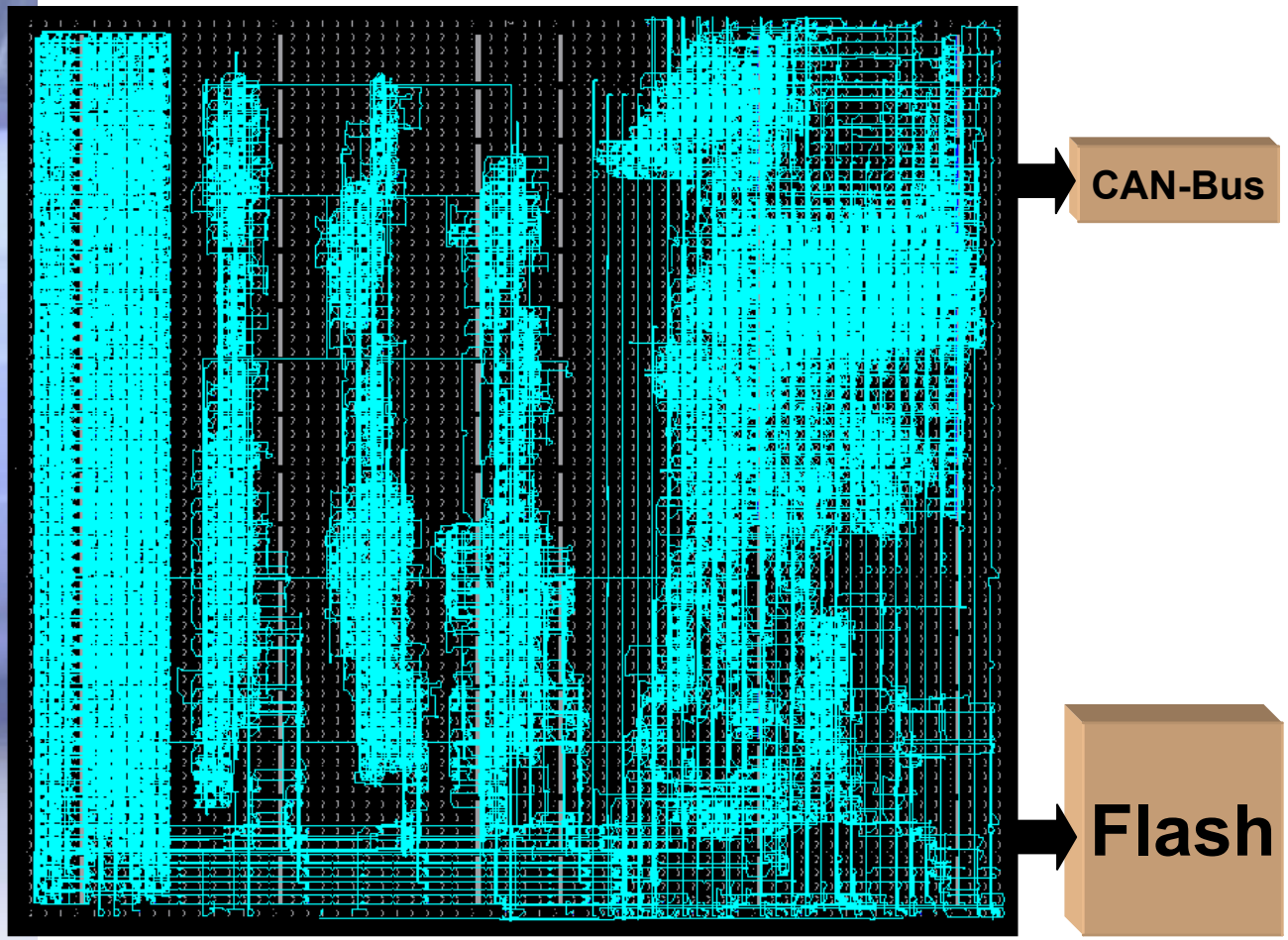
Possible Solutions:

- For every Gate exists an „inverted" Gate (well known in ASIC design)
- Either one of the two is switched every clk-cycle. Switching operations are „neutralized"!

- Wiring of LUT's is critical (Capacities change)
- Dedicated routing in FPGA necessary to guarantee wire lengths

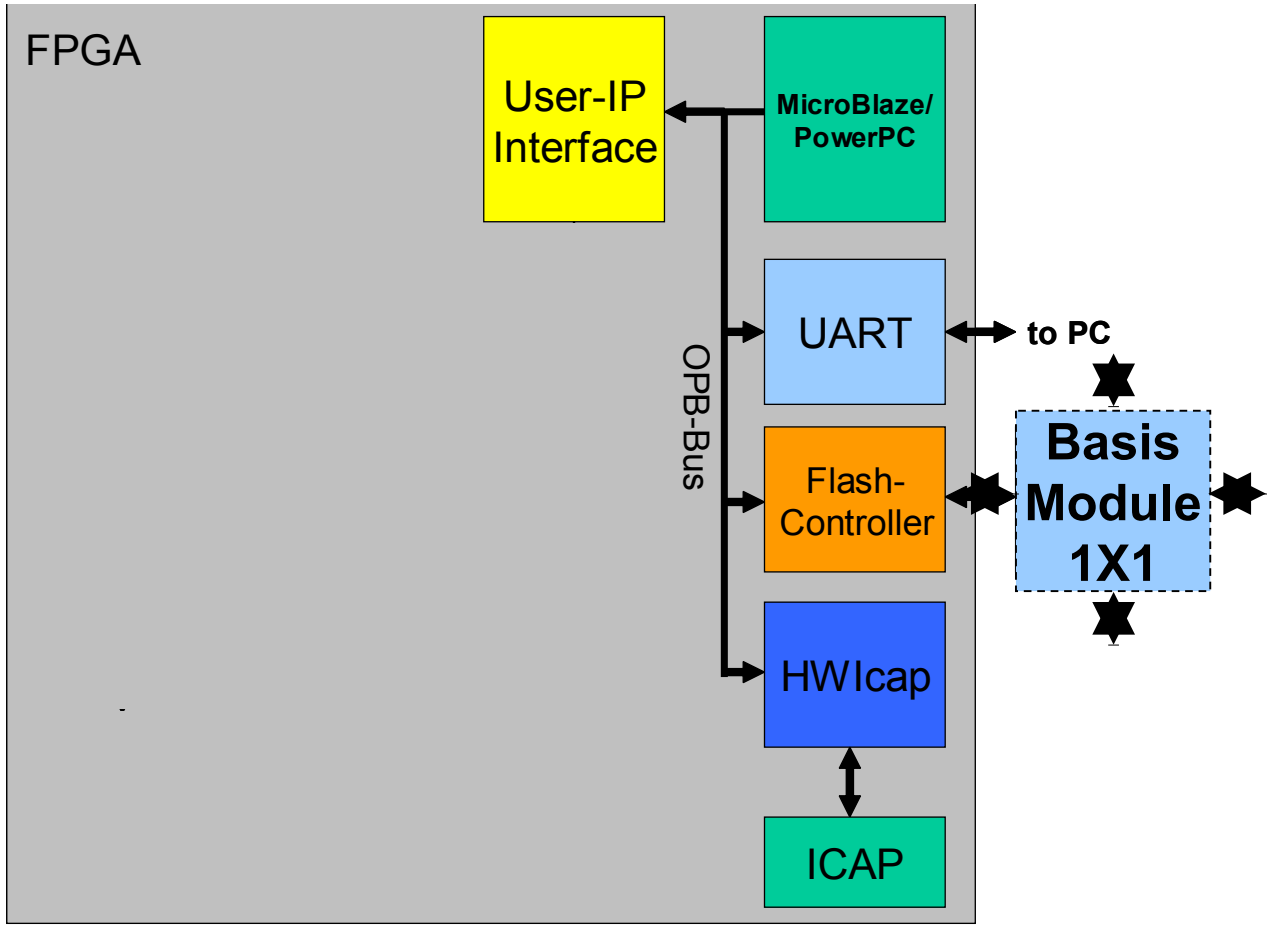
Source: Alexander Klimm, ITIV

1D Reconfiguration: Automotive Inner Cabin Functions

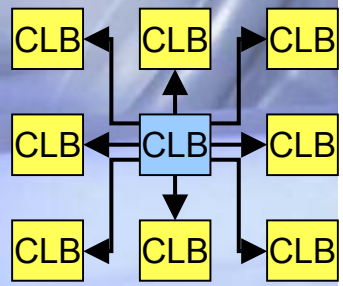


2D On-Line Placement Process

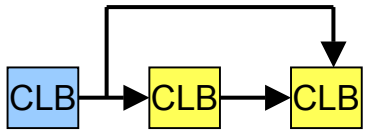
- Control Unit initiates load-process from external memory
- Run-time system calculates necessary and available area for placement
- After placement communication primitives were established



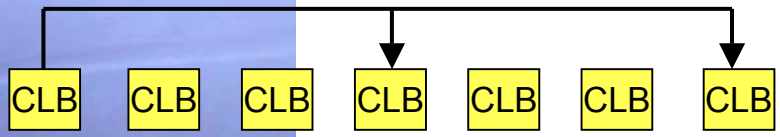
Power/Performance Analysis - Motivation



Direct Lines



Double Lines

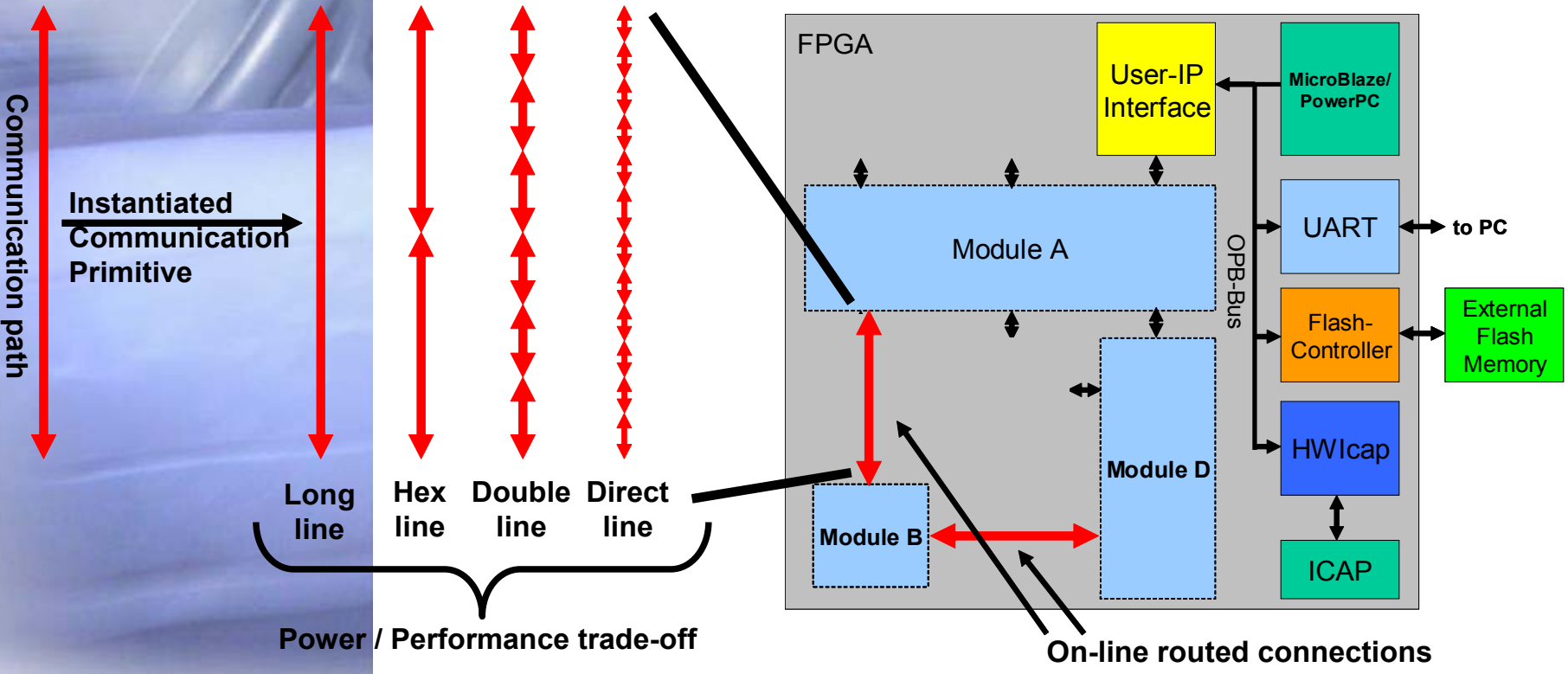


Hex Lines

- Longer communication lines cause higher power consumption (due to capacity) while providing higher performance
- Power consumption and delay was estimated for the different lines
- This information can be exploited during run-time to change the power consumption of integrated algorithms while keeping performance conditions

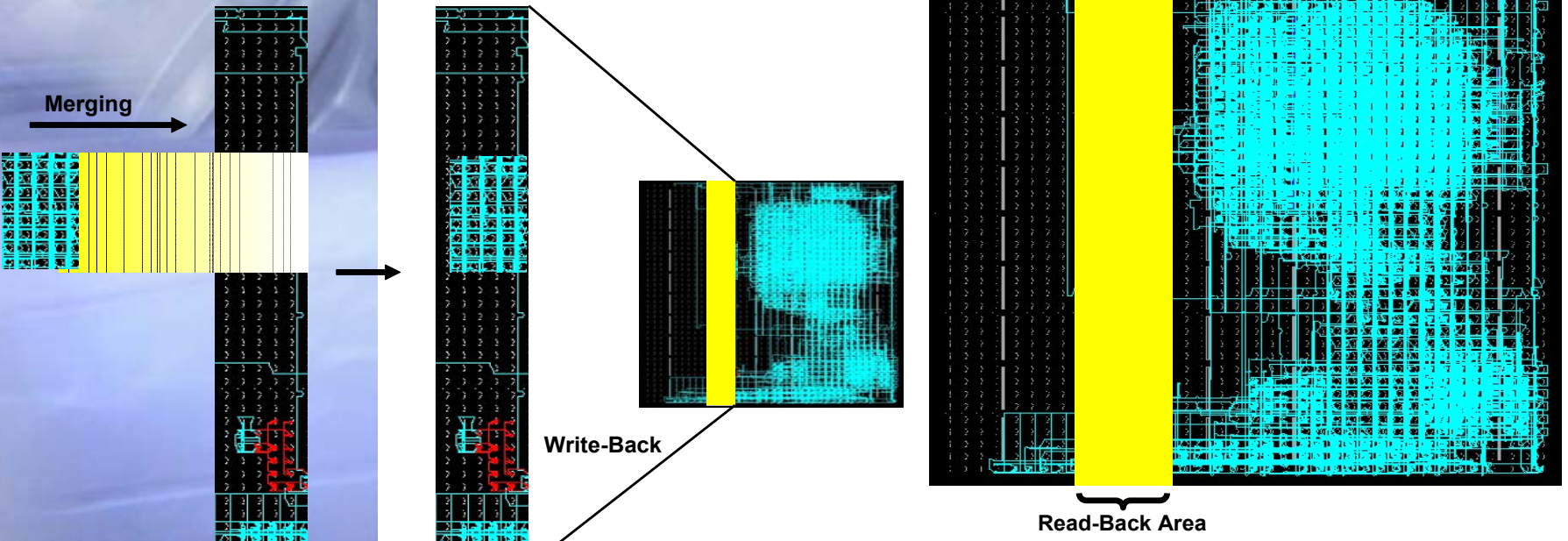
Investigation of communication lines on standard reconfigurable hardware

Power/Performance Analysis – Motivation



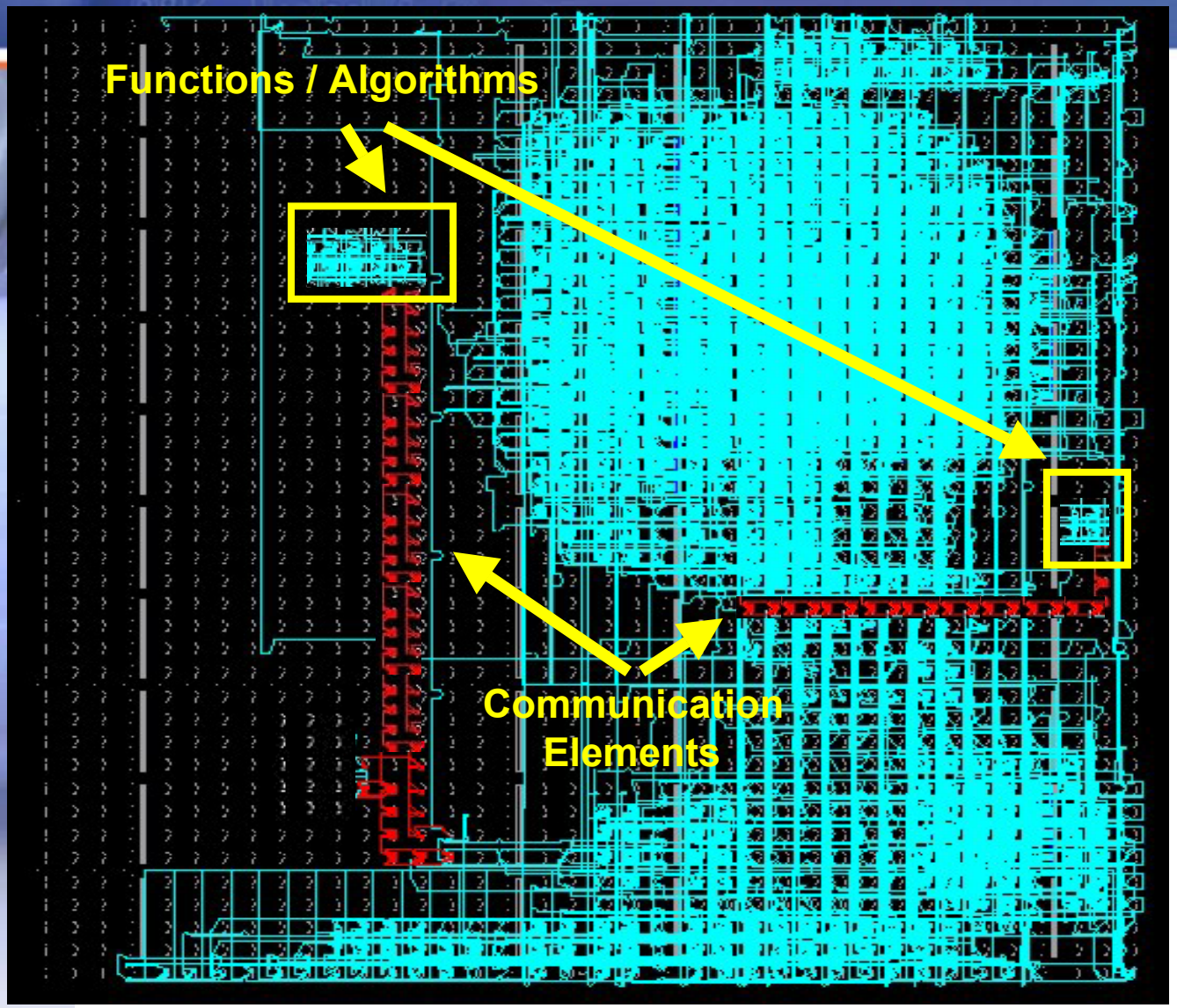
Substitution of communication primitives by considering Power ←→ Performance Trade-Off

Run-Time Manipulation of Configuration



Exploiting Read-, Modify- and Writeback Method for run-time resource adaptation

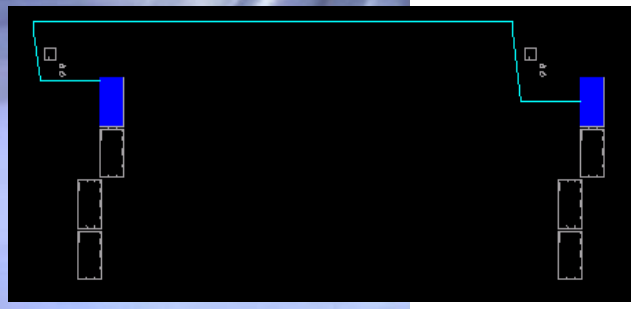
Feature for Future: Online Routing



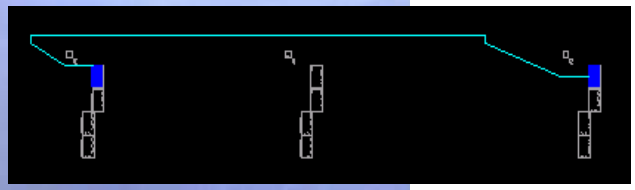
Power/Performance Estimation of FPGA Communication Primitives

LUT - based macros for implementing the different communication lines on a Virtex II – 2000 FPGA (Xilinx)

VCD*-File

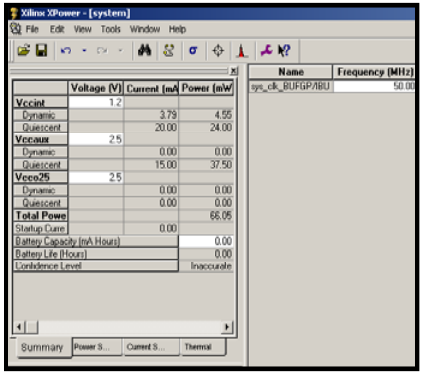


Direct line

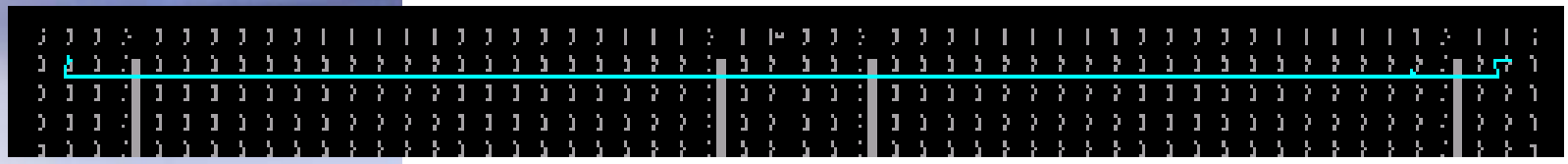


Double line

Hex line



XPower for estimating the power consumption based on timing simulation in ModelSim



Long line

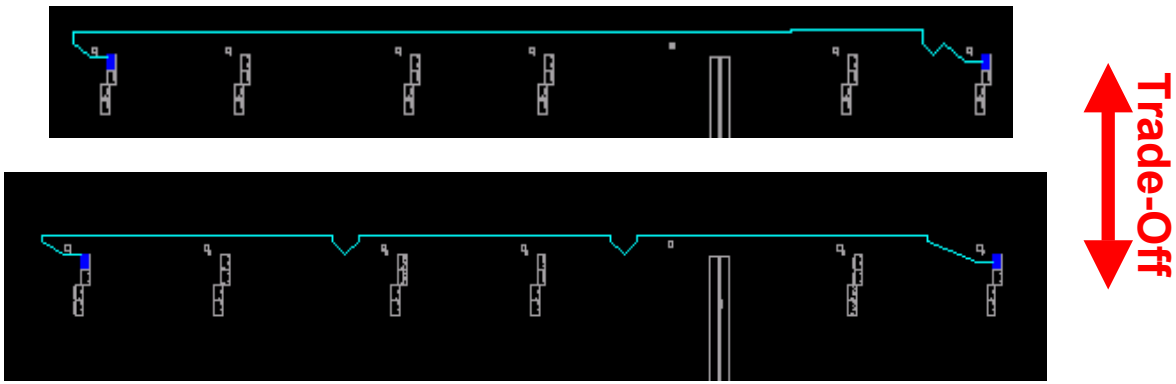
Power/Performance Trade-off

Macro	Max. delay	Power Consumtion	Frequency
Direct	0.581 ns	0.125 mW	17 MHz
Double	0.590 ns	0.126 mW	17 MHz
Hex	0.755 ns	0.134 mW	17 MHz
Long	1.271 ns	0.280 mW	17 MHz

Power consumption and delays of different FPGA signal lines

Different communication lines can be exploited for cryptographic domain

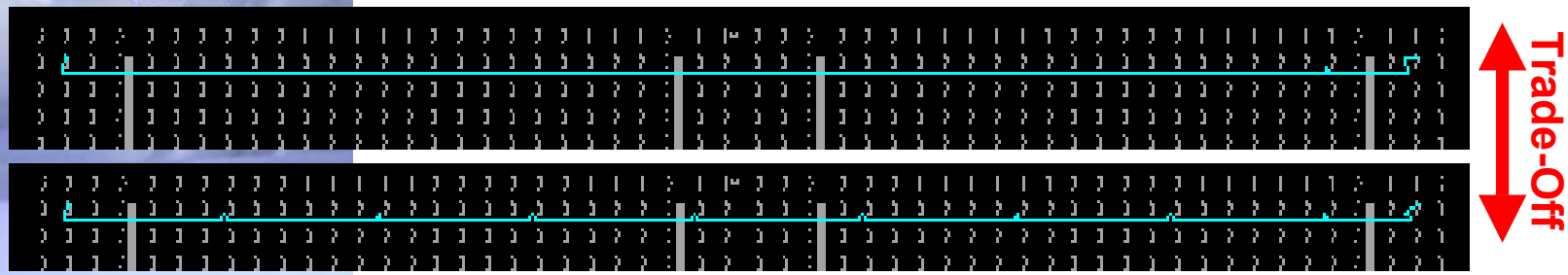
Example1:



Hex line or
3 double lines?

Power/Performance Trade-Off

Example2:



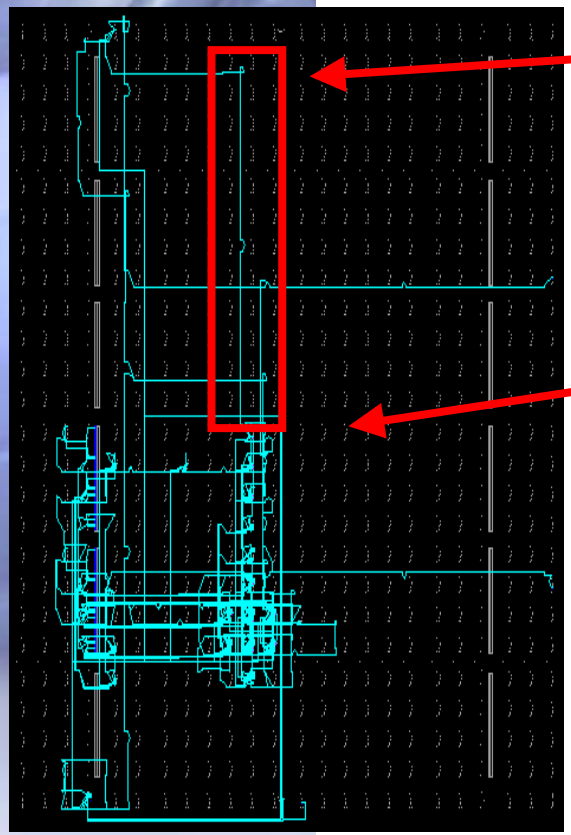
Results from estimating the power consumption:

Macro	Max. delay	Power consumption	Frequency
1 Hex	0.755 ns	0.134 mW	17 MHz
3 Double	0.798 ns	0.125 mW	17 MHz
1 Long	1.271 ns	0.280 mW	17 MHz
Mult. Hex	1.828 ns	0.223 mW	17 MHZ

Long line or multiple hex lines?

Multiple hex lines instead of 1 long line reduces ca. 20% of power consumption!

Power Optimized Routing – Example1



Long net consisting of hex lines, could be replaced by double lines

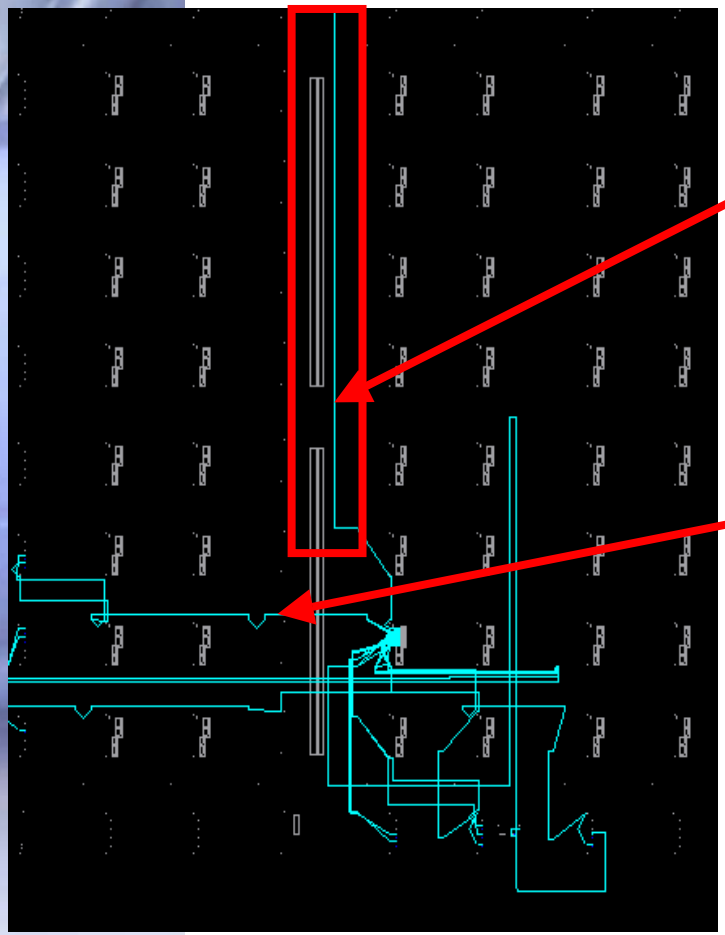
Worst delay: 1.848 ns

Hex line, could be replaced by double lines

Worst delay: 1.701ns

Optimization possibilities can easily be identified in the FPGA Editor; using a text file could simplify this process

Power Optimized Routing – Example2



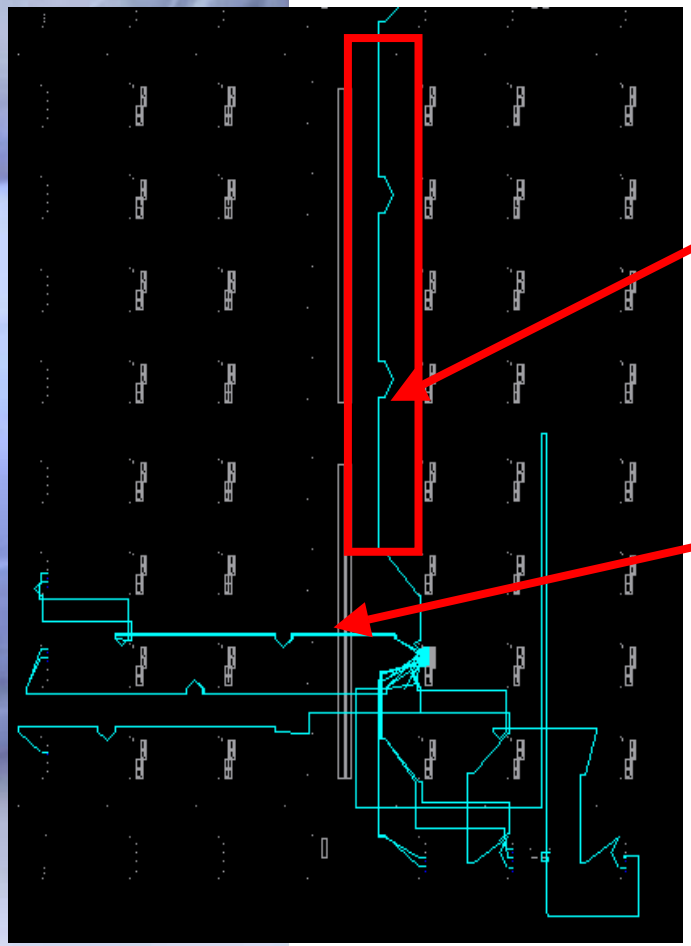
Long net consisting of a hex line, could be replaced by double lines

Worst delay: 1.562 ns

2 Hex lines, could be replaced by double lines

Worst delay: 1.381/1.113ns

Power Optimized Routing – Example2



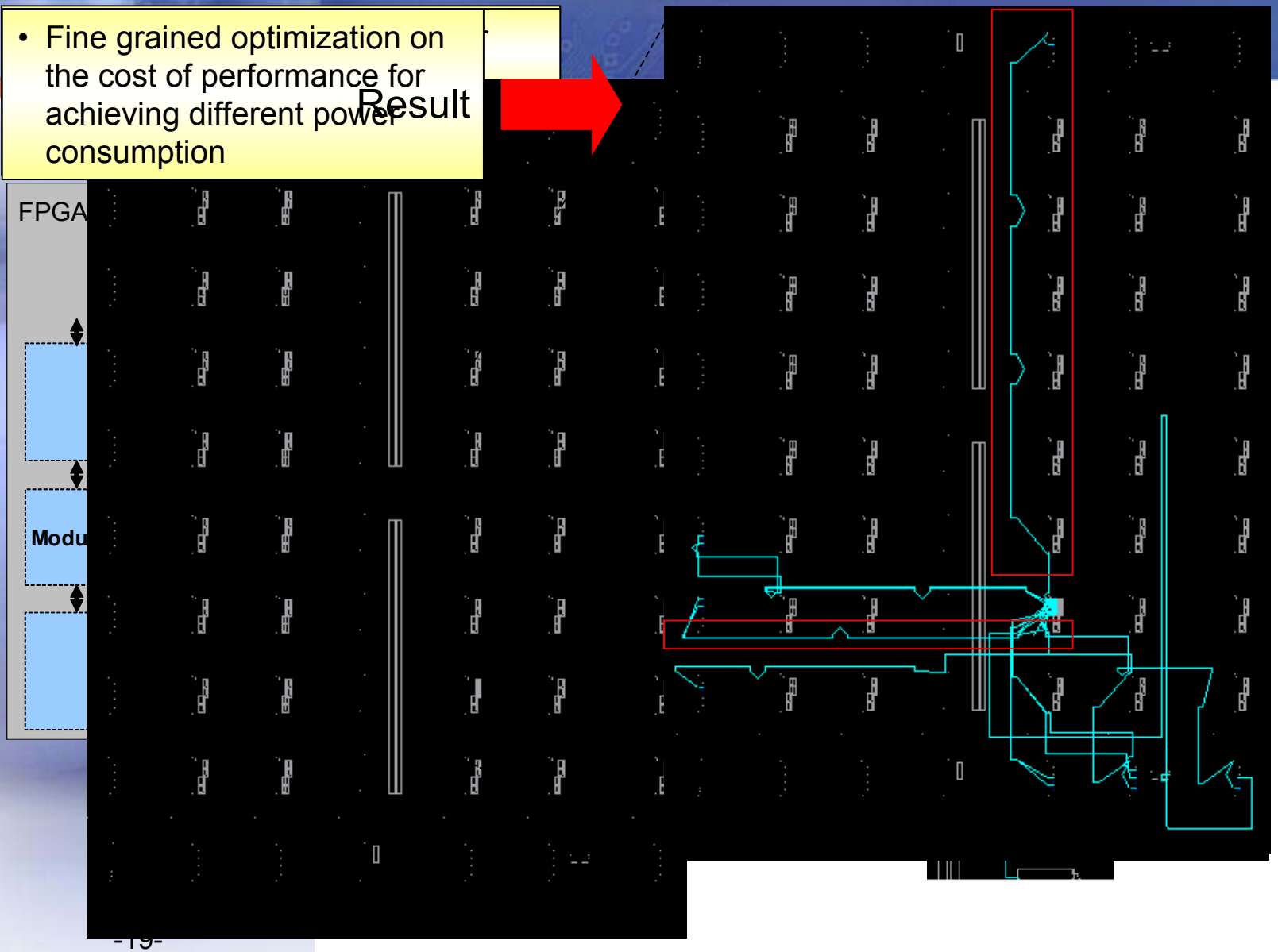
1 hex line net replaced
by three double lines

2 Hex line nets, each
replaced by 2 double lines

Power estimated with XPower:
11% power reduction on signal lines,
after adapting only three lines

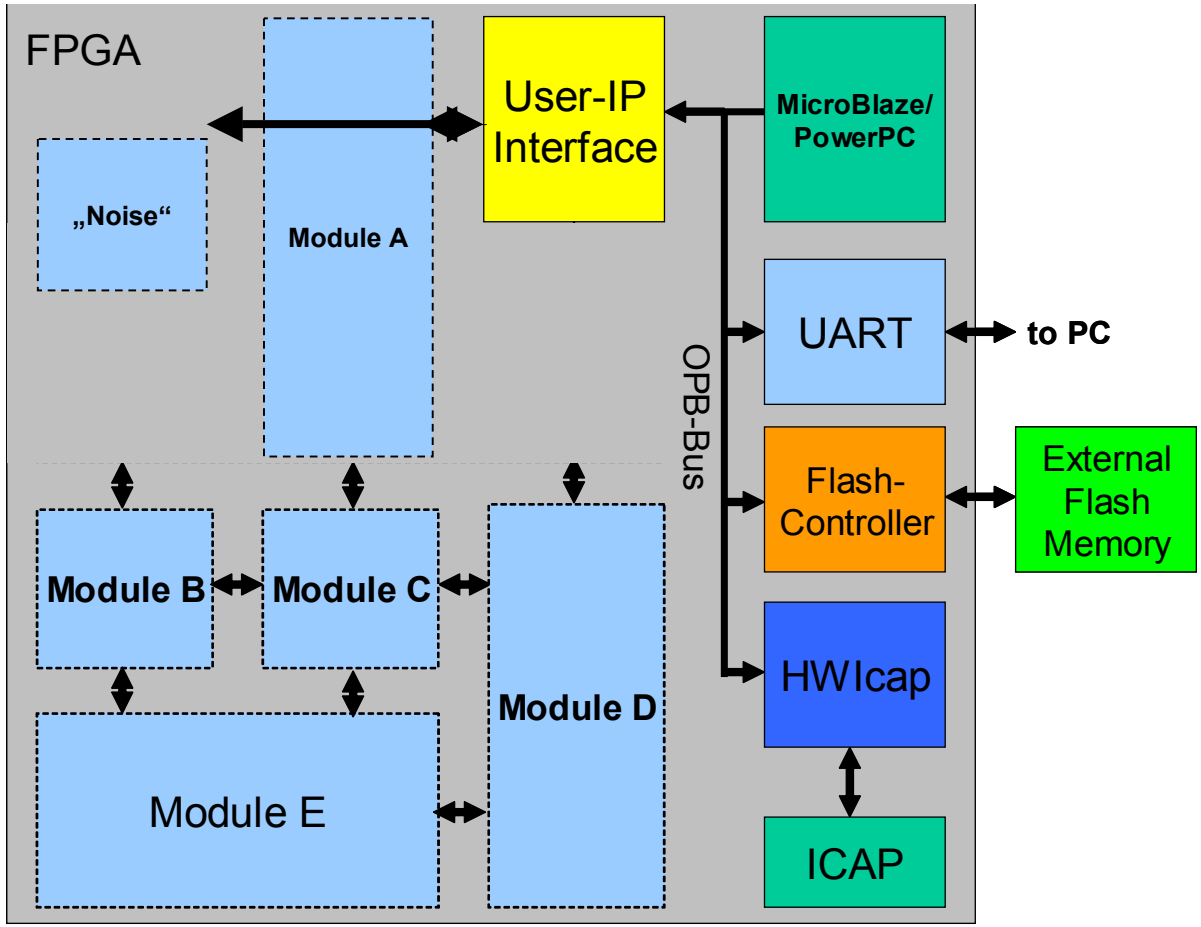
Outlook – Power/Performance Optimized On-line Routing

- Fine grained optimization on the cost of performance for achieving different power consumption



Different Methods for Side-Channel Attack Defense

- Alternative Mapping of algorithms
- Implementation of “noisy” modules
- Exchange of single wires within algorithm modules
- Relocation of modules



Conclusions

- Simulations and estimations show clear difference in power consumption and maximum delay time for different kinds of signal lines
- Routing manipulation during the design phase can be exploited for Side-Channel Attack Defense while still maintaining performance requirements
- The Xilinx Description Language (XDL) file can be used for re-routing signal lines on Xilinx FPGAs
- This power/performance information can be included in an on-line router for self-adaptive cryptographic domain related system approach
- Various methods for “secure hardware” exploiting fine grained configuration manipulation and 2D reconfiguration

Thanks for your attention!

Contact:

Michael Hübner, Jürgen Becker
ITIV – Universität Karlsruhe (TH)
(huebner, becker@itiv.uni-karlsruhe.de)