

Efficient security hardware design

(design of side-channel resistant circuit design and effects of deep submicron)

Ingrid Verbauwhede

ingrid.verbauwhede-at-esat.kuleuven.be

K.U.Leuven, ESAT- SCD - COSIC
Computer Security and Industrial Cryptography
www.esat.kuleuven.be/cosic



Acknowledgements:

Benedict Gierlic, Elke Demulder, Junfeng Fan, P. Schaumont

KUL - COSIC

Dagstuhl 2008 – 1

June 2008

Outline

- Start from the title (courtesy Ahmad)
- “Efficient security hardware design”
 - Efficient hardware for security functions
 - Secure hardware
- “design of side-channel resistant circuit design”
- and “effects of deep submicron”



KUL - COSIC

Dagstuhl 2008 – 2

June 2008

Embedded Security

NEED BOTH

- Efficient Implementation
 - Within power, area, timing budgets
 - Public key: 2048 bits RSA, 200 bit ECC on 8 bit μ C and 100 μ W
 - Public key on a passive RFID tag
- Trustworthy implementation
 - Resistant to attacks
 - Active attacks: probing, power glitches, JTAG scan chain
 - Passive attacks: monitor electromagnetic radiation



Security as a design dimension

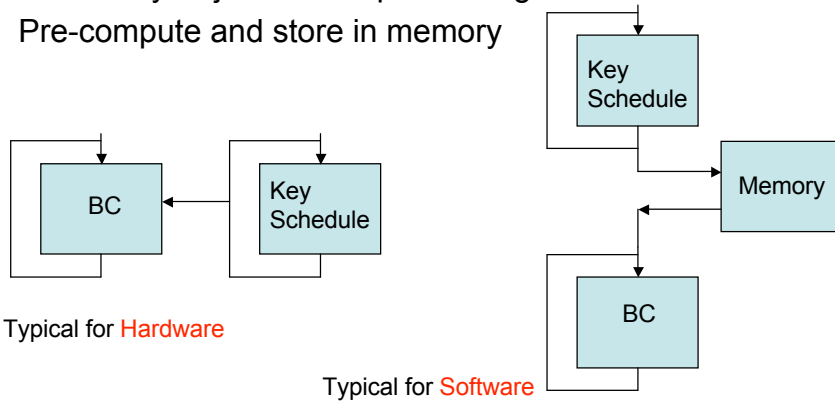
- Security consumes resources!
 - extra area, extra power, extra design time
 - E.g. communication – computation trade-off
- **Similar** to power or area optimization
 - Perfect security does not exist (zero-power design doesn't exist either)
 - Low-risk security does exist (low-power design does exist)
- **Different:** attacker will go for the easiest entry point:
 - If strong crypto algorithm: try side channel attack
 - Look at the JTAG interface
 - Monitor power consumption
 - Introduce glitches (= fault attacks)
 - Guess the password: Paris Hilton's dog
 - Bribe the security guard

Efficiency: adapt HW platform to application

Simple example: Key Schedule for secret key

Two options:

- On the “fly” = just in time processing
- Pre-compute and store in memory



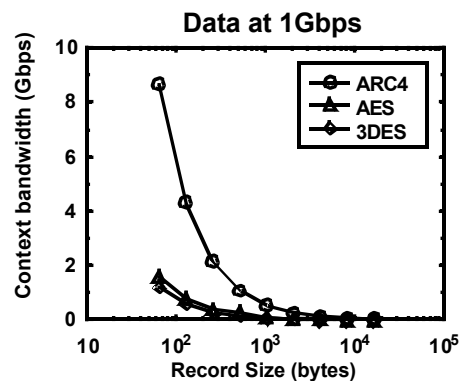
KUL - COSIC

Dagstuhl 2008 – 5

June 2008

Key schedule on the fly

- The cost of fast key context switching in SW
- Example for IPSEC router
 - one 128 bit key = 1408 bits round keys (10 rounds + initial key)
 - half of internet packets are only 64 bytes in length (512 bits)



[source: J. Goodman]

KUL - COSIC

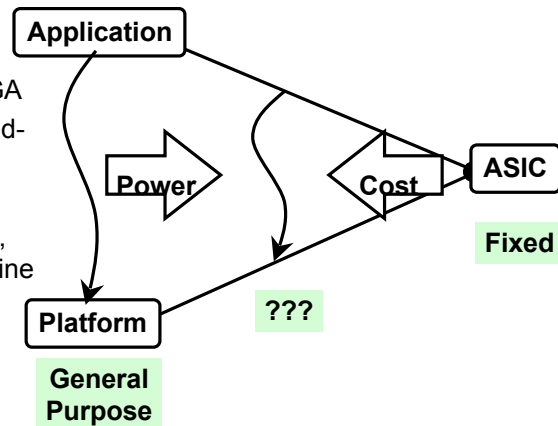
Dagstuhl 2008 – 6

June 2008

Match between algorithm & architecture

Close the gap:

- Dedicated HW: ASIC
- Programmable HW: FPGA
- Custom instructions, hand-coded assembly
- Compiled code
- JAVA on virtual machine, compiled on a real machine



KUL - COSIC

Dagstuhl 2008 – 7

June 2008

Throughput – Energy numbers

AES 128bit key 128bit data	Throughput	Power	Figure of Merit (Gb/s/W)
0.18µm CMOS	3.84 Gbits/sec	350 mW	11 (1/1)
FPGA [1]	1.32 Gbit/sec	490 mW	2.7 (1/4)
ASM StrongARM [2]	31 Mbit/sec	240 mW	0.13 (1/85)
Asm Pentium III [3]	648 Mbits/sec	41.4 W	0.015 (1/800)
C Emb. Sparc [4]	133 Kbits/sec	120 mW	0.0011 (1/10.000)
Java [5] Emb. Sparc	450 bits/sec	120 mW	0.0000037 (1/3.000.000)

[1] Amphion CS5230 on Virtex2 + Xilinx Virtex2 Power Estimator

[2] Dag Arne Osvik: 544 cycles AES – ECB on StrongArm SA-1110

[3] Helger Lipmaa: PIII assembly handcoded + Intel Pentium III (1.13 GHz) Datasheet

[4] gcc, 1 mW/MHz @ 120 Mhz Sparc – assumes 0.25 µ CMOS

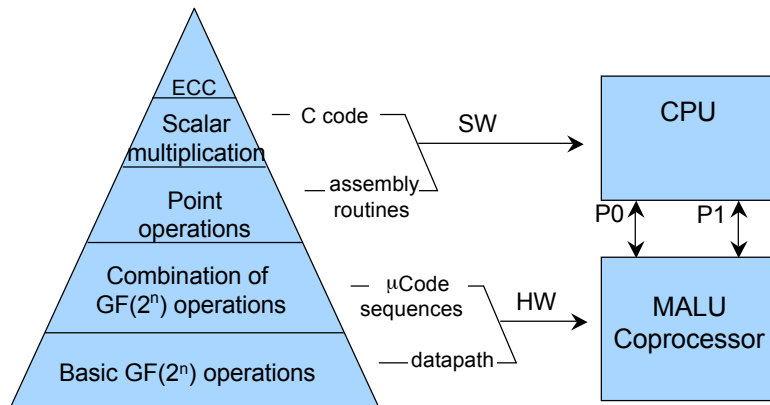
[5] Java on KVM (Sun J2ME, non-JIT) on 1 mW/MHz @ 120 MHz Sparc – assumes 0.25 µ CMOS

KUL - COSIC

Dagstuhl 2008 – 8

June 2008

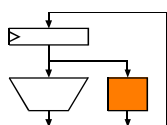
HW/SW co-design for Public Key:



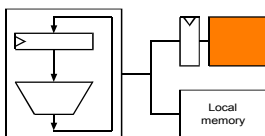
Where is boundary between SW and HW? Factor 100

[CHES 2005]

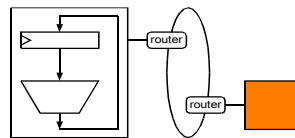
Options for HW/SW co-design



- Instruction set extensions
- Tightly coupled

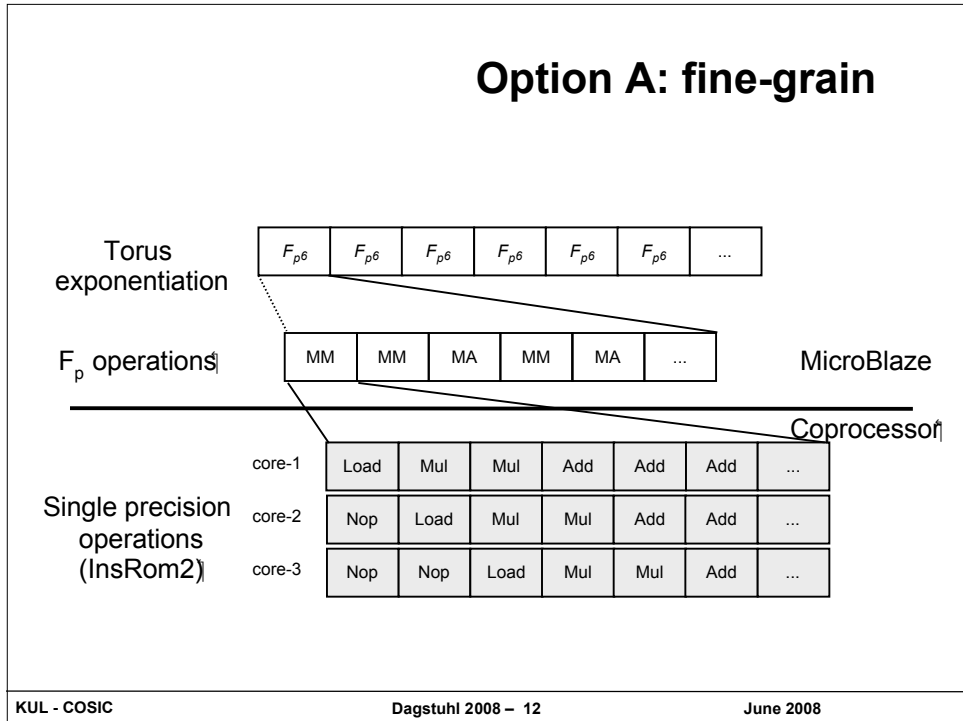
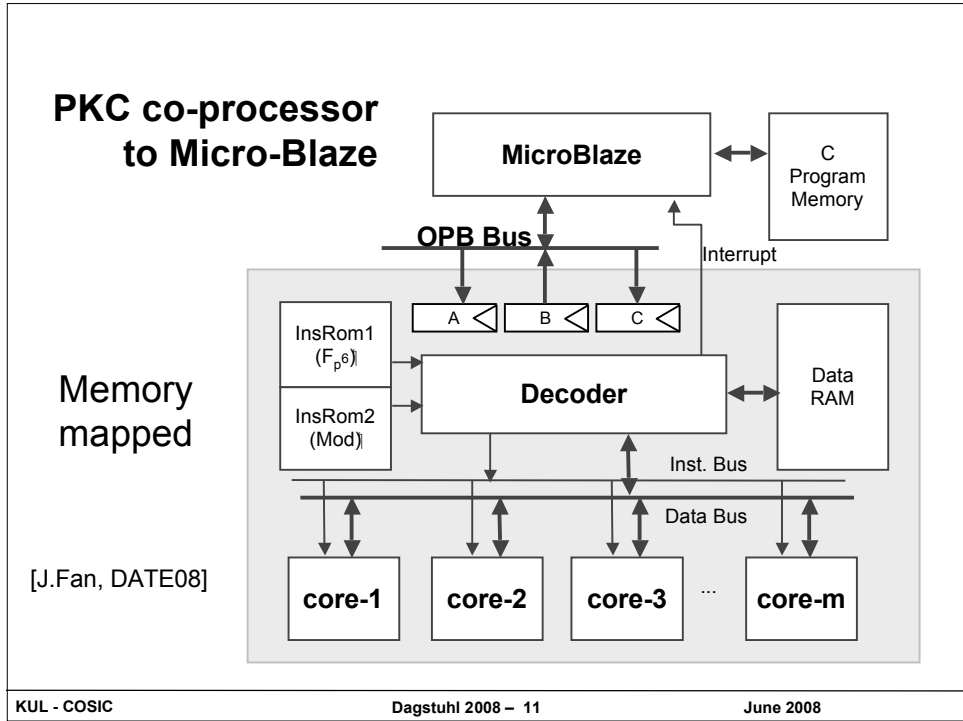


- Memory-mapped coprocessor
- Loosely coupled

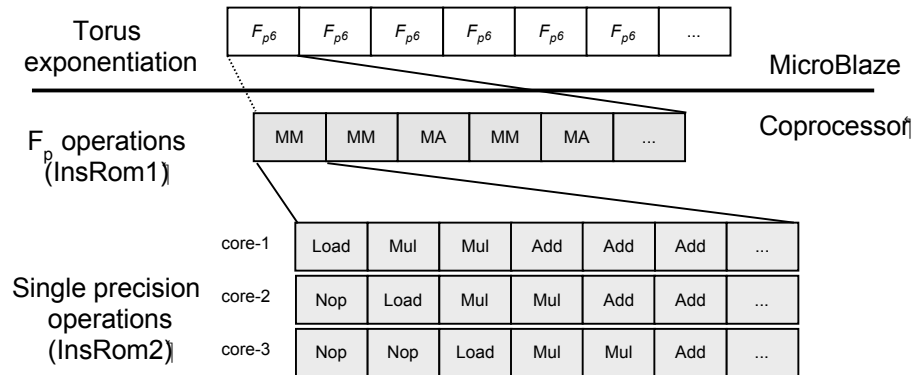


- Custom HW on NoC
- Loosely coupled
- Flexible interconnect

- Important: Prevent communication bottlenecks!
 - Otherwise, gains of custom HW could be lost



Option B: coarse grain



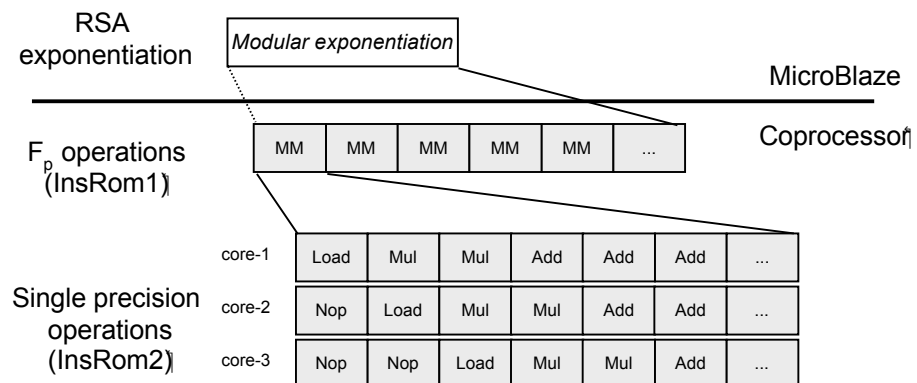
Almost 4 times faster from A to B!

KUL - COSIC

Dagstuhl 2008 – 13

June 2008

Reprogram for RSA

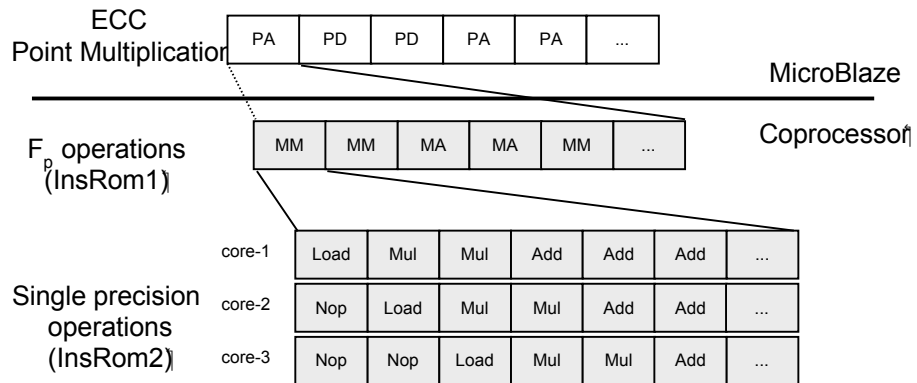


KUL - COSIC

Dagstuhl 2008 – 14

June 2008

Reprogram for ECC



Secure implementations

“design of side-channel resistant circuit design”
and “effects of deep submicron”

Many Power Analysis Attacks

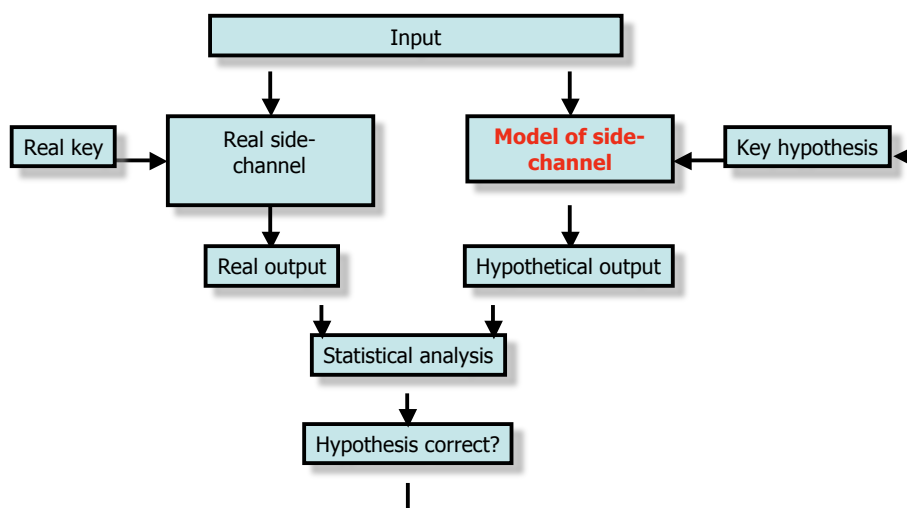
- Direct attacks (extract)
 - Simple Power Analysis (1999)
 - Single- / Multi-Bit Differential Power Analysis (1999/2002)
 - Correlation Power Analysis (2004)
 - Collision Attacks (2003)
- Two-step attacks (extract)
 - Template Attacks (2002)
 - Stochastic Model (2005)
 - Inferential Power Analysis (1999)

KUL - COSIC

Dagstuhl 2008 – 17

June 2008

Correlation DPA



KUL - COSIC

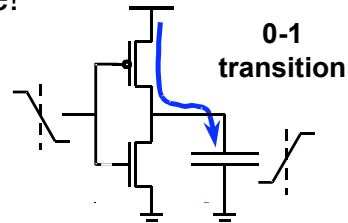
Dagstuhl 2008 – 18

June 2008

Intro to Static CMOS

- Consumes power when output makes a 0 to 1 transition = 'dynamic power'
- Most popular circuit style!

IN	OUT
0→0	0
0→1	discharge
1→0	charge
1→1	0



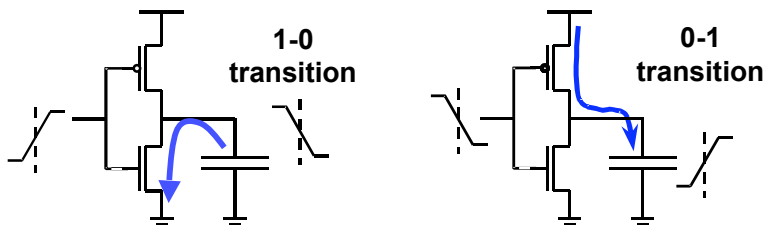
KUL - COSIC

Dagstuhl 2008 - 19

June 2008

Duplicate logic

- As suggested by famous cryptographers . . .



IN	$\overline{\text{IN}}$	OUT	$\overline{\text{OUT}}$
0→0	1→1	0	0
0→1	1→0	discharge	charge
1→0	0→1	charge	discharge
1→1	0→0	0	0

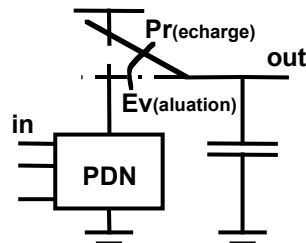
KUL - COSIC

Dagstuhl 2008 - 20

June 2008

Dynamic logic

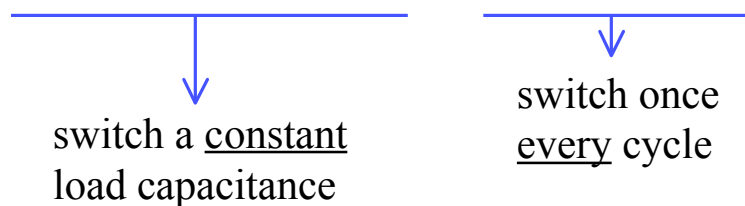
- Dynamic logic breaks input **sequence**



IN	OUT _{Pre}	OUT _{EV}	Charge
0→0	1	1	0
0→1	1	0	discharge
1→0	1	1	0
1→1	1	0	discharge

Transition independent power consumption ...

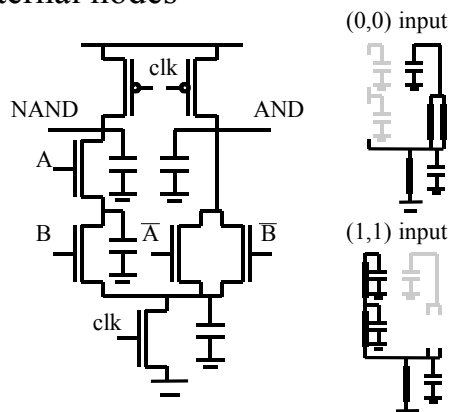
- ...doesn't create any side channel information
 - When logic values are measured by charging and discharging capacitances, we need to use a fixed amount of energy for every transition



Dynamic and Differential logic ...

- is necessary but not sufficient
 - Balance differential output nodes
 - (Dis)charge all internal nodes

→
E.g. DCVSL
is not
sufficient



[Tiri, ESSCIRC02]

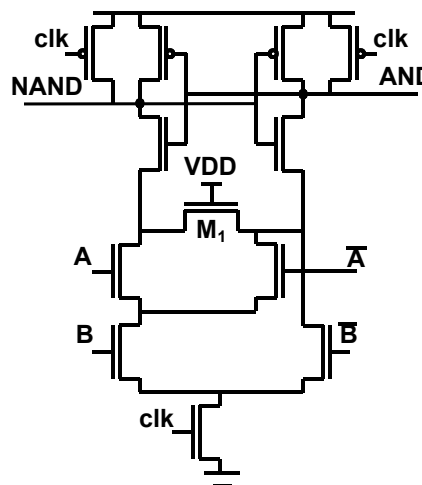
KUL - COSIC

Dagstuhl 2008 - 23

June 2008

Sense Amplifier Based Logic charges each cycle a constant load

- Balanced input and output nodes
- All internal nodes connect to an output

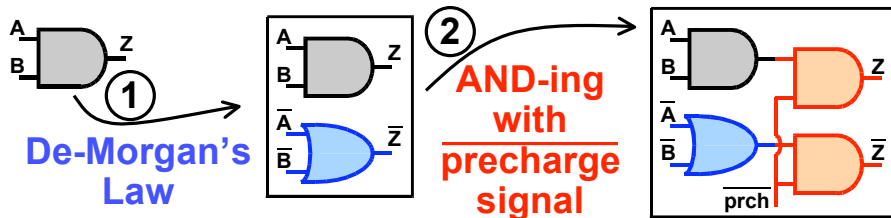


KUL - COSIC

Dagstuhl 2008 - 24

June 2008

Solution based on *Standard* cells



- false output
- with false inputs
- precharge 1: outputs are 0
- precharge 0 - evaluation: 1 output is 1

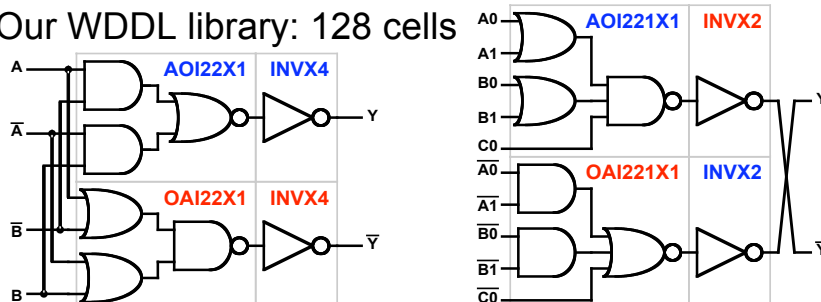
KUL - COSIC

Dagstuhl 2008 – 25

June 2008

WDDL library

- All functions of and2, or2 operator
- In addition: inverted input, output signals
- XOR2X4: OAI221X2:
- Our WDDL library: 128 cells



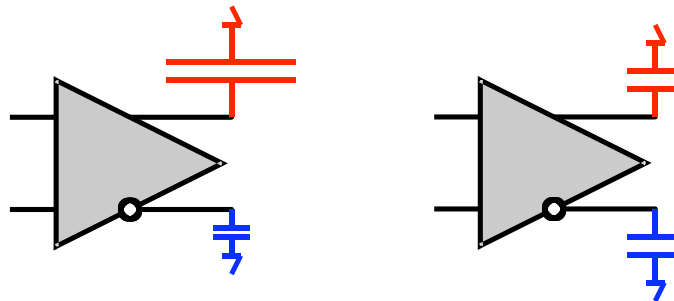
KUL - COSIC

Dagstuhl 2008 – 26

June 2008

Unbalanced capacitive loads

- For constant power consumption:
constant load capacitance.
- Match loads at differential outputs.

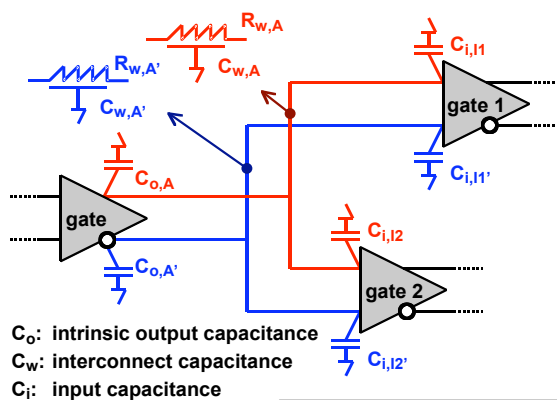


KUL - COSIC

Dagstuhl 2008 – 27

June 2008

Load capacitance breakdown



- Intrinsic caps.:
matched
- Interconnect:
dominant
(Moore's law)
- Balancing
interconnect:
crucial

$$\begin{aligned}
 C_A &= C_{A'} \\
 C_{o,A} + C_{w,A} + C_{i,I1} + \dots C_{i,Ik} \\
 &= C_{o,A'} + C_{w,A'} + C_{i,I1'} + \dots C_{i,Ik'} \\
 C_{w,A} &= C_{w,A'}
 \end{aligned}$$

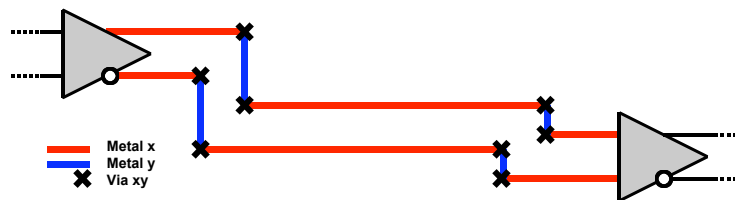
KUL - COSIC

Dagstuhl 2008 – 28

June 2008

Place & Route approach

- Parallel routes (adjacent tracks, same layer) balance geometric distances, parasitic effects
- Resistance: equal vias, wire segments
- Capacitance (to other layers): ideally same environment
exact if every other layer is a power plane



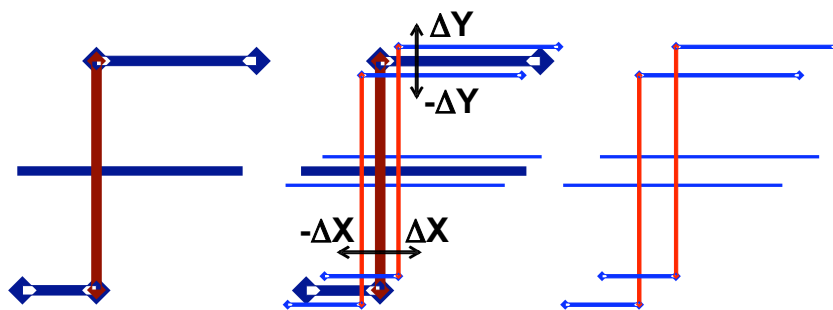
KUL - COSIC

Dagstuhl 2008 – 29

June 2008

Fat wire decomposition

- Duplicate fat wire.
- Slide apart copies.
- Reduce to normal width.



KUL - COSIC

Dagstuhl 2008 – 30

June 2008

“Effects of deep submicron”

- Variations, matching:
 - Spread: lot to lot, wafer to wafer variation
 - Parametric gradients: die to die, within die variations
 - Matching: random fluctuations, systematic offset

Random fluctuations:

- ion implantation
- dopant diffusion
- Interface states
- Edge roughness
- Poly-Si grain effects
- ...

Systematic effects:

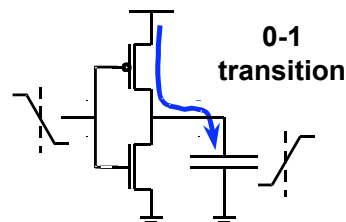
- Dimensional errors
 - Photo-mask size
 - Lens aberrations
 - Photo-resist thickness
- Topography related
- Mechanical strain variation
- ...

[Source: M. Pelgroms, M. Vertregt, NXP]

Static CMOS - below 90nm

- Dynamic + static + short circuit leakage
- Dynamic = transition
- Static = leakage = Level dependent
- Short = transition = good designers ignore it

IN	OUT
0 → 0	0
0 → 1	discharge
1 → 0	charge
1 → 1	0



Current equation

- Strong inversion: $I = \beta(V_{gs} - V_T)^2$
- V_T is function of
 - gate oxide thickness
 - Dopant concentration in channel region
- Granularity is reached, dopant variations:
 - 0.25/0.25 μm transistor = 1000 doping atoms, $\sigma = 3\%$
 - 100/65 nm transistor = 60-80 atoms, $\sigma = 11\%$
- Weak inversion, leakage current,
 - $I = I_0 \exp(q(V_{gs} - V_T)/mkT)$
- Beta = f(mobility), e.g. f(transistor orientation)

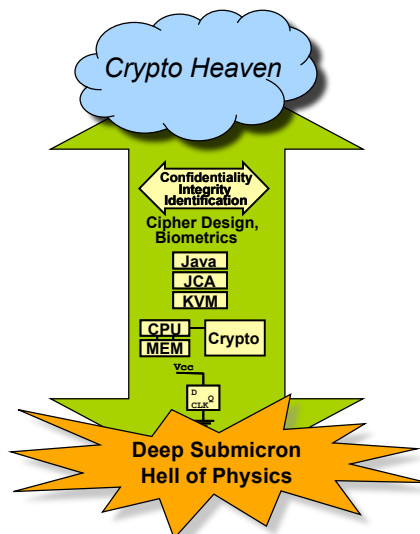
[Source: M. Pelgroms, M. Vertregt, NXP]

Mismatch at transistor level

- 10%: can use minimum devices
- 1%: need 1-10 μm^2 devices and decent layout
- 0.1%: need 10-100 μm^2 devices and very careful layout
- 0.01%: need very large area devices, extreme layout symmetry and circuit tricks
- 0.001%: forget it

[Source: M. Pelgroms, M. Vertregt, NXP]

Technology aware embedded security



CMOS:

- Adapt power models for attack
- Leakage current = static = not switching dependent
- Temperature effects
- Mismatch effects

New circuit/technology tricks:

- Security with plastic transistor
- Embrace new ideas
- ...

RINGS: Reconfigurable Interconnect Next Generation Systems

Conventional interconnect:

- space division
- time division

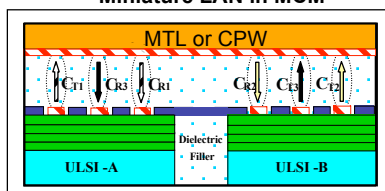
New interconnect:

- code division (CDMA)
- frequency division (FDMA)
- any combination of the above

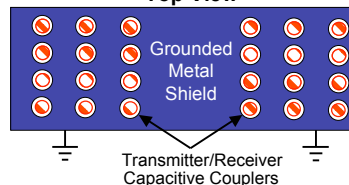
Reconfigurable!

- “Low Loss, dispersion-free, ultra-high data rate (100Gbps/channel & 20Tbps/chip)”

Miniature LAN in MCM



Top View



[M.F. Chang, Proc. IEEE 2001]

Conclusion

- Security is an extra design dimension
- Need for efficient designs
- Need for secure designs
- Deep submicron effects: change in power model, change in circuit design?
- Embrace new circuit ideas.