VLSI System Design

Vincent Immler
vincent.immler@oregonstate.edu

Prepared for: ECE474/574, Spring 2024

Oregon State University

rootoftrust.io

> *“They say data is the new oil. If so, maybe advanced chip foundries are the new nukes. Ten years from now, superpower status is going to be defined by the ability to make semiconductors.”*
>
> 2021 – BHARAT KAPOOR, KEARNEY [1]

…to make and to break the most recent semiconductors!

This includes: chip design skills and software, manufacturing, reverse-engineering, etc.

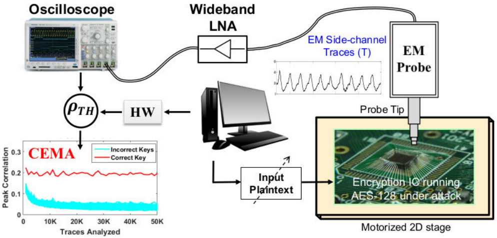
[1] https://spectrum.ieee.org/tech-talk/semiconductors/devices/south-koreas-450billion-investment-latest-in-chip-making-push

About Me: Vincent Immler

- **Since 12/2021: Assistant Professor at OSU, focus on hardware/physical security**
  - Physical security: dealing with physical quantities (time, electromagnetic emanation, ...)
  - Hardware=physical implementation and low-level embedded code; debug interfaces
- **04/2019-12/2021: Subject Matter Expert in cryptanalysis at ZITiS**
  - German government agency supporting law enforcement and intelligence community
  - R&D to access protected/encrypted data, e.g., for digital forensics and lawful interception
  - Led the effort to build a new hardware security lab for government-level needs
  - Exploration/Exploitation: classified software/hardware projects on systems security
- **10/2013-03/2019: Security researcher/project lead at Fraunhofer Institute AISEC**
  - Fraunhofer = Europe's largest research organization (not a university)
  - R&D with industry and government agencies on security
  - Acquired major research project: 'self-funded' PhD from Technical University Munich
- **At ESCRYPT Inc., worked on V2X projects; IBM R&D (Extreme Blue)**
- **Before 2013: BS/MS in IT-Security from Ruhr-University of Bochum (Germany)**

“My Other Business” at OSU: Hardware/Physical Security

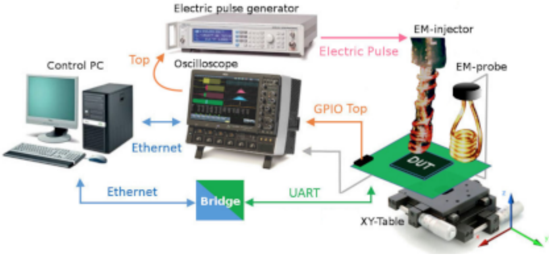
Non-invasive Attacks



(source: “STELLAR: A Generic EM Side-Channel Attack […]”)

- Eavesdrop sensitive data
- Limited hardware / weak attacker model
- Massive data analysis (‘big data’)
- Statistics that make you happy!

Semi-invasive Attacks

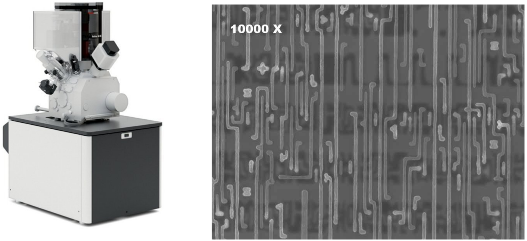


(source: “Studying EM Pulse Effects on Superscalar Microarchitectures at ISA Level”)

- Change data or control flow
- Voltage or clock glitches
- Laser for front-/backside of the chip
- High voltage/short rise EM pulses

“My Other Business” at OSU: Hardware/Physical Security

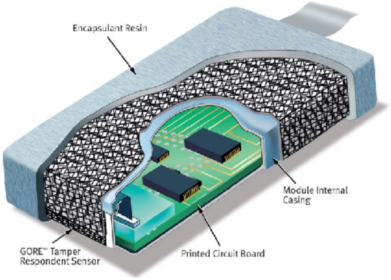
Fully-Invasive Attacks



(source: “Reverse engineering, how to use SEM full-vision imaging”)

- Advanced equipment needed
- Focused Ion Beam → ‘chip-edit’
- Scanning Electron Microscope → ‘chip-RE’
- Most powerful attacks; substantial resources!

Anti-Tamper Enclosures



(source: GORE commercial brochure)

- Physical ‘Access Denial System’
- Highest security, e.g., for banking
- Extremely challenging

VLSI System Design?

Chips are hugely important – one of the top-most traded commodities, CHIPS Act, etc.

- Relevant coursework at OSU includes but not limited to:
  - ECE474/574: VLSI System Design (digital, front-end design)
  - ECE499: Special Topics: Hardware Verification (digital, verification-only)
  - ECE471/571: Energy-Efficient VLSI (mixed analog/digital)
  - ECE422/423/520/522/523: CMOS-* (analog, back-end design)
- In this course: focus on digital design using FPGAs

Why focus on FPGAs?

- Most/all digital designs (or parts of it) are prototyped on FPGAs
- FPGAs are great for all applications where MOQ [2] of a custom chip cannot be met

Why VLSI/FPGAs for security?

- Security point of view: learn how things are put together …
- …to also know how to take them apart (chip reverse-engineering)!
- FPGAs are field-programmable, i.e., your HDL design can be kept secret

[2] Minimum Order Quantity (MOQ). Manufacturing a chip is a serious business that often requires MOQs of 1M chips or more

Proprietary vs. Open-Source

Research vs. industry vs. government:

- Proprietary software often used in industry; but things are changing!
- Difficult to learn skill and retain proficiency w/o access to proprietary software
- Free and open-source EDA software gaining a lot of momentum
- Digital sovereignty in Europe and many countries of increasing importance

Learning fundamentals vs. career readiness:

- Getting your degree is about fundamentals (not specific software)
- Software, languages, and paradigms keep evolving
- Industry has their own corporate coding styles and procedures
- Prevent ecosystem lock-in ("LabView", "Matlab")
- Do not list "Matlab" as a skill in your resume, list *experience*!

This course: open-source and Xilinx Vivado (FPGA); can continue practicing!

Linux/Unix Philosophy

Why you should start using Linux (if not already done so):

- User knows better …so he must specify how things work
- Provide mechanisms, not policy
  - Mechanism: long life time
  - Policy: short life time
- Its not the most friendly to use, but it is efficient (for advanced users)
  - Do not confuse ease of use with efficiency
  - Consumer OS are locking users into one interface policy
- Easy things are easy, hard things are possible

Most (if not all) in the chip industry use Linux!

Basic Terminology and Mindset

Nuanced differences you should be aware of:

- Course with large focus on Hardware Description Language (HDL)
- In a narrow sense, this is not “coding”; instead: *describing* a design
- In a narrow sense, FPGAs are not “programmed”; instead: *configured*
- Most people use these terms interchangeably (including myself)
- Proper terminology is recommended, especially for job interviews
- In this class, we write HDL *code* and use FPGA *programmers* (JTAG)

Mindset:

- Hardware development != software; we do not want to hustle it
- Avoid technical debt in your designs; do it properly the first time
- Follow a consistent coding style [3] (make this graded?!)
- Verilog-2001 (online sources often use Verilog-1995 standard) or SystemVerilog-2017
- Note: Xilinx Vivado supports SystemVerilog (but predecessor Xilinx ISE does not!)

[3] `https://github.com/lowRISC/style-guides/blob/master/VerilogCodingStyle.md`

Selected Languages and Projects

Hardware Description Languages (HDLs):

- (System)Verilog: most popular in US industry unless aerospace/defense related
- VHDL: most popular elsewhere, especially Europe; and US aerospace/defense related
- Chisel: popularity mostly around RISC-V processor design
- Amaranth HDL: augmented Python popular for Yosys; has its own Playground

Selection of projects I consider worth mentioning:

- EDA Playground: synthesis/simulation in your browser – part of your next job interview?
- GTKWave: open-source `.vcd` viewer
- Verilator: open-source Verilog simulator
- Glasgow Explorer: Amaranth-powered FPGA-based multitool (from Eugene! Hello Piotr!)
- RapidWright: Low-level control over placement and routing in Xilinx FPGAs

Why Vivado anyhow? Fully-integrated workflow, access Xilinx primitives, …

Community Efforts and Related Initiatives

Hack@DAC: Capture-The-Flag (CTF)

- Co-located with Design and Automation Conference (DAC) – a major EDA conference
- Previous contests around a SoC design (OpenTitan) with the goal to find security flaws
- Verilator for simulation; please ask me if you plan participating in 2025 (graduate school?)

MITRE: embedded CTF (eCTF)

- Combines development and security track (software and hardware)
- Not necessarily EDA-specific, but could be of interest for students of this course

Zero to ASIC Course

- Ultra-cheap open-source process development kit and training (starts at $650)
- Uses Skywater and OpenLane ASIC tools from Efabless
- I'm unaware of any equivalent that also gets you a real chip in the end

I'm neither affiliated with any of these efforts nor are they endorsed be me!

Organizational Aspects

Your ECE 474/574 team:

- TA: Dongjun Lee, leedongj@oregonstate.edu (your primary TA for weeks 1-6)
- TA: Gabriel Cojocaru, cojocarg@oregonstate.edu (your primary TA for weeks 5-10)
- myself, vincent.immler@oregonstate.edu

Office hours:

- Dongjun Lee: Monday + Tuesday, 1pm-2pm, KEC 3110
- Gabriel Cojocaru: TBD, announced for 2nd half of this course
- Vincent Immler: *only by appointment and only 10 min*, unrelated to assignments

Friday labs act as de facto office hours during which I will be taking questions.
This is exactly the same structure as in previous years when taught by Houssam Abbas.

Syllabus

Important aspects:

- If you have any question, please check the syllabus first
- If it is a question related to assignments, *only* reach out to the TA
- For disagreements about grading, *only* reach out to the TA
- For disputes (=TA and you cannot settle it), get me involved

Online repositories and distribution of instructional content:

- For version control of your code, please only use a *private* repository
- All instructional content, including assignments, is ©Vincent Immler
- Some content may be from previous instructors or unknown origin
- For some of which, I may not have the right to distribute further
- Do Not Upload This Content Online – You Do Not Own it

For obvious reasons: especially do not upload solutions!

Grading (Proposal)

Plan for grading (subject to minor adjustments):

- 10% for each assignment (5 assignments total)
- 20% for each project (3 projects)
- Graduate students: discuss additional difficulty / effort

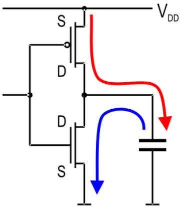
Some extra information:

- I do not cap at 100%. You may be able to achieve 110% in this course
- More than 100% cannot be honored in OSU's grading system
- However, this is a good story to tell in a letter of recommendation
- This will not feel like any other class: "not achieving everything but still getting 100%"
- Reasoning: if everyone gets 100%, I do not know how to adjust level of difficulty

Power Consumption of a Circuit (Job Interview Question)

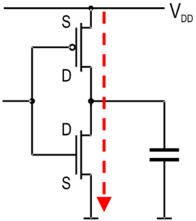
- World relies on CMOS transistors (Complementary Metal Oxide Semiconductor)
- Power consumption (VLSI-point of view): $P_{\mathrm{v,tot}} = P_{\mathrm{v,dyn}} + P_{\mathrm{v,leak}} + P_{\mathrm{v,short-circuit}}$
- Power consumption dominated by dynamic part $P_{\mathrm{v,dyn}}$
- Circuit active = high dynamic power consumption
- Circuit inactive = low static power consumption (due to leakage)
- CMOS has high noise-immunity, and other benefits

Dynamic power



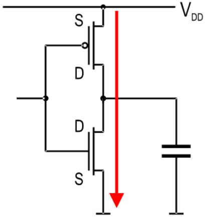
charging and discharging capacitors

Leakage power



leaking transistors

Short-circuit power

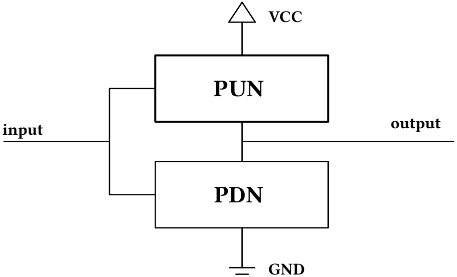


short circuit path

CMOS Basics

A CMOS logic gate is built using two networks

- Pull-up and pull-down network (PUN/PDN)
- Pull-up part made from PMOS transistors
- Pull-down part made from NMOS transistors
- Complementary: always PMOS and NMOS!



Result: only one network is active

- Static power consumption will be low
- Inactivity should not decrease battery life
- Static power consumption more of a problem in newer technology nodes (higher leakage)

Dynamic Power Consumption (Job Interview Question)

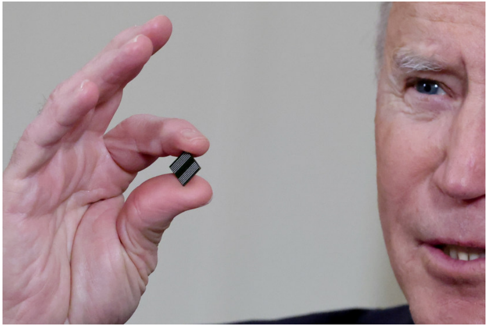
$$P_{\mathrm{v,dyn}} = \overbrace{\alpha}^{\text{Activity Factor}} \cdot \underbrace{C_{\mathrm{L}}}_{\text{Capacitive Load}} \cdot \overbrace{(V_{\mathrm{DD}})^2}^{\text{Operating Voltage}} \cdot \underbrace{\mathrm{f}}_{\text{Frequency}} \tag{1}$$

- **Activity Factor $\boldsymbol{\alpha}$**: Probability of logic level change causing charging of the load
- **Capacitive Load C_{L}**: Capacitive load, parasitic capacitances of transistor
- **Operating Voltage V_{DD}**: Limited by threshold voltage V_{th}
- **Frequency f**: Switching speed (clock frequency) at which circuit is operates

Activity factor also expressed as: $\alpha \cdot C_{\mathrm{L}} = C_{\mathrm{eff}}$ whereas $C_{\mathrm{eff}} = \sum_i P_{(0 \to 1)i} \cdot C_i$

Fab Trends

- Highly political topic
- Race for smaller technology nodes
- New transistor designs (e.g., Fin, GAA)
- Europe: “1.5-ish” nm in 2026 (Intel)
- US: “3-ish” nm in 2026 (TSMC)
- Asia: “2-ish” nm in 2025 (TSMC)
- Access to ≤ 7nm equipment restricted



(source: Reuters)

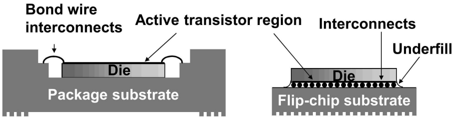
However: too narrow focus on fabs with ‘only’ fewer nm is ill-advised! [4]

Lower nm race mostly relevant for digital part of a design. Mixed-Signal is a different story!

[4] https://www.stiftung-nv.de/sites/default/files/eu-semiconductor-manufacturing.april_.2021.pdf

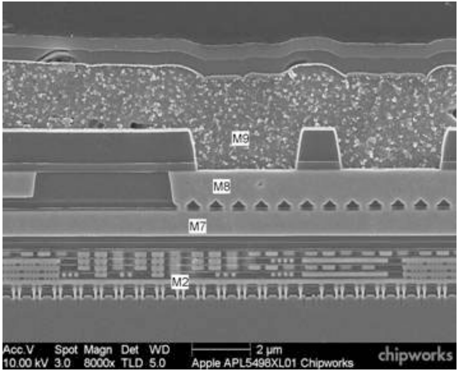
Chips and Traditional Package Integration

- Silicon dies manufactured ‘bottom-up’
- Top: metal and active layer (few μm)
- Bottom: bulk silicon (hundreds of μm)
- Integration type #1: ‘wirebond’
- Integration type #2: ‘flip-chip’



Wirebond package die

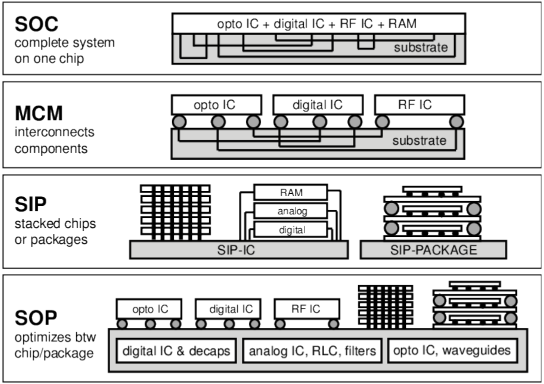
Flip-chip packaged die



(Cross section of Apple A5X. Source: Chipworks)

More than Moore: Improved Packaging/Integration

- Applications often need:
- …higher signal integrity
- …higher integration density
- …improved power distribution
- …shorter time to market
- → 2.5D and 3D integration of chips
- ‘*Scaling diversity*’ – not just transistors

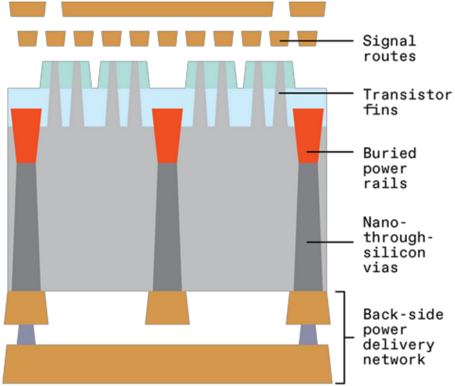


Increasingly more common, especially stacked DRAM for SoCs. [5]

[5] Figure source: Thermal and Crosstalk-Aware Physical Design for 3D System-On-Package by Minz et al.

More than Moore: Power Delivery Network (PDN)

- Traditional chip: signals and power delivery only on top-side
- Problem: conflict over resources
- Solution: find other ways of power delivery – leverage unused backside?
- Idea #1: Buried Power Rails (BPR)
- Idea #2: Fully-Backside PDN

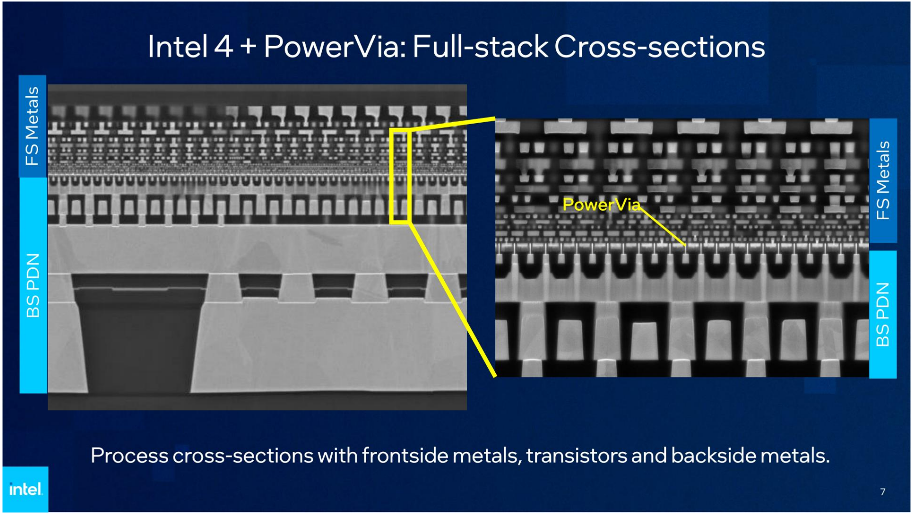


Promising but manufacturing this is very challenging! [6]

Expecting Intel's ArrowLake (15th gen, 20A process) in late 2024 / early 2025

[6] https://spectrum.ieee.org/next-gen-chips-will-be-powered-from-below

More than Moore: Power Delivery Network (PDN)

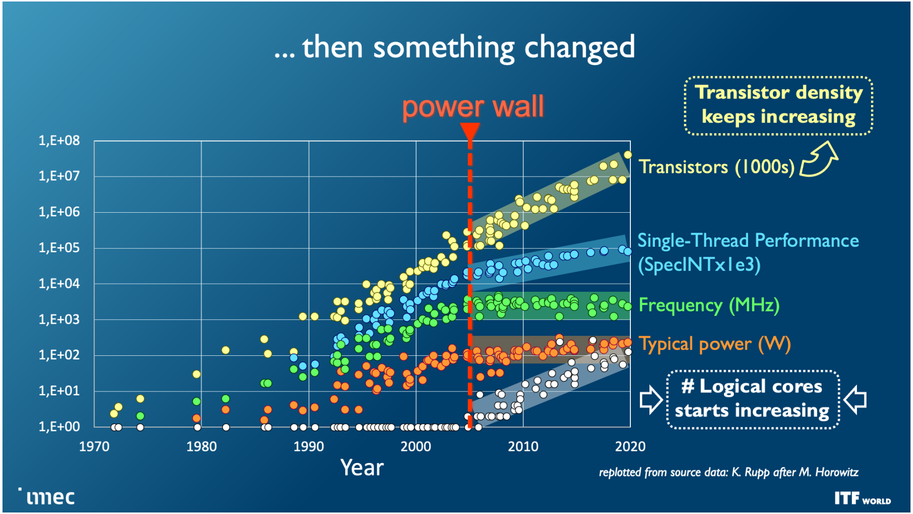


Intel 4 + PowerVia: Full-stack Cross-sections

Process cross-sections with frontside metals, transistors and backside metals.

Where did the silicon go? White thin line only!

Other Scaling Problems: Power Wall



... then something changed

Transistor density keeps increasing

Logical cores starts increasing

replotted from source data: K. Rupp after M. Horowitz

Result: more application-specific instruction sets, more cores, . . .