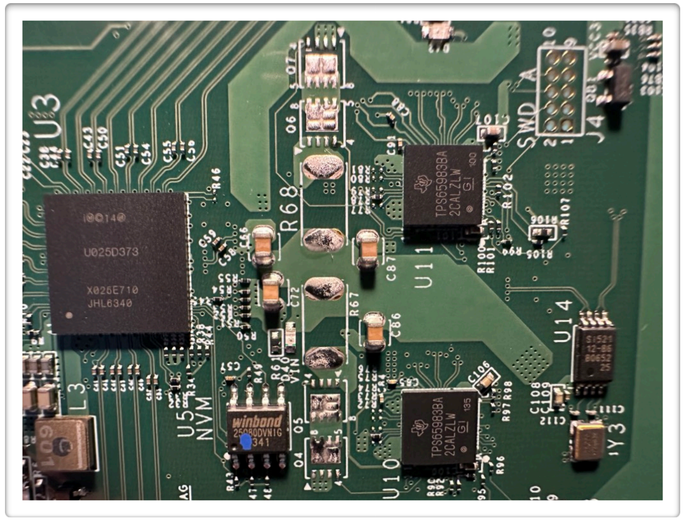


Platform Security Meetup

- March 2026

Tomáš Rosa

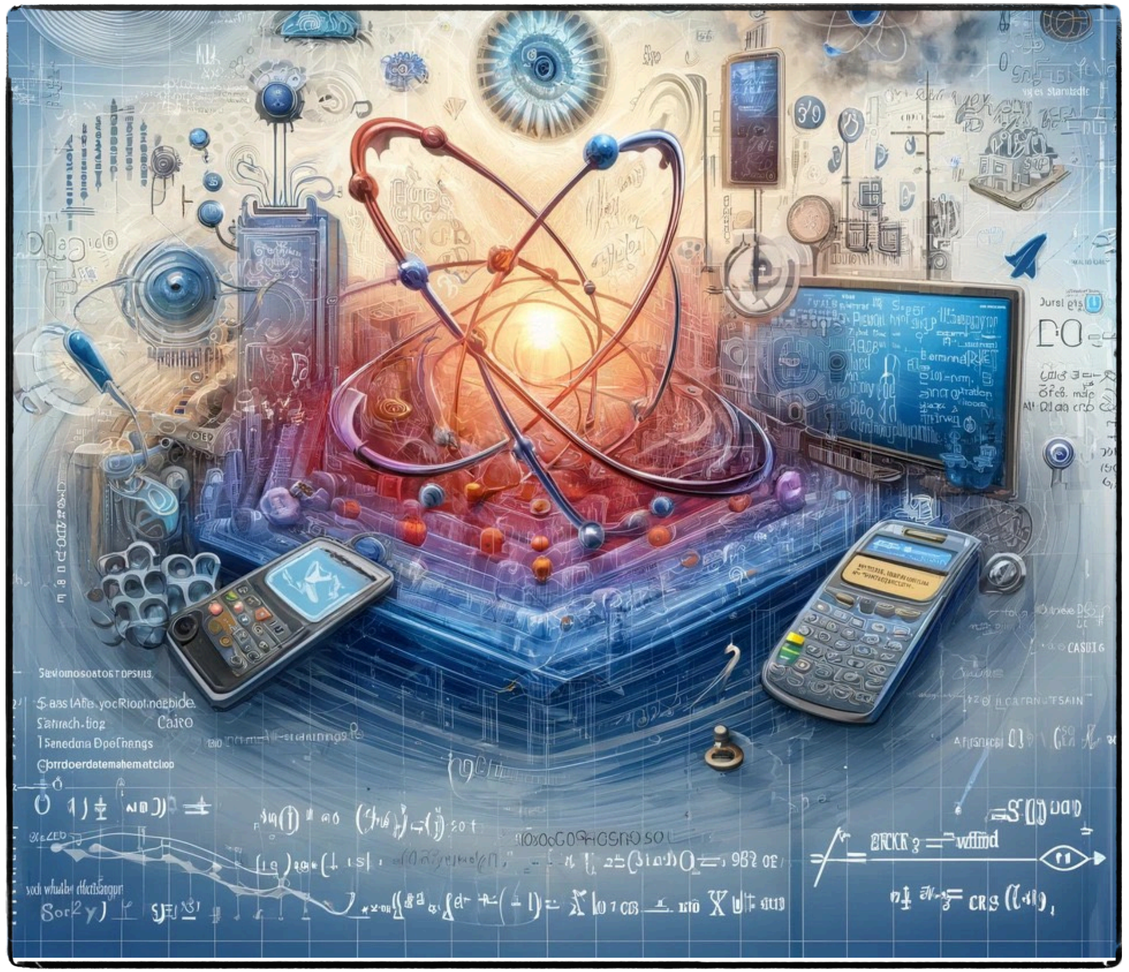
Cryptology and Biometrics Competence Centre of Raiffeisen Bank International

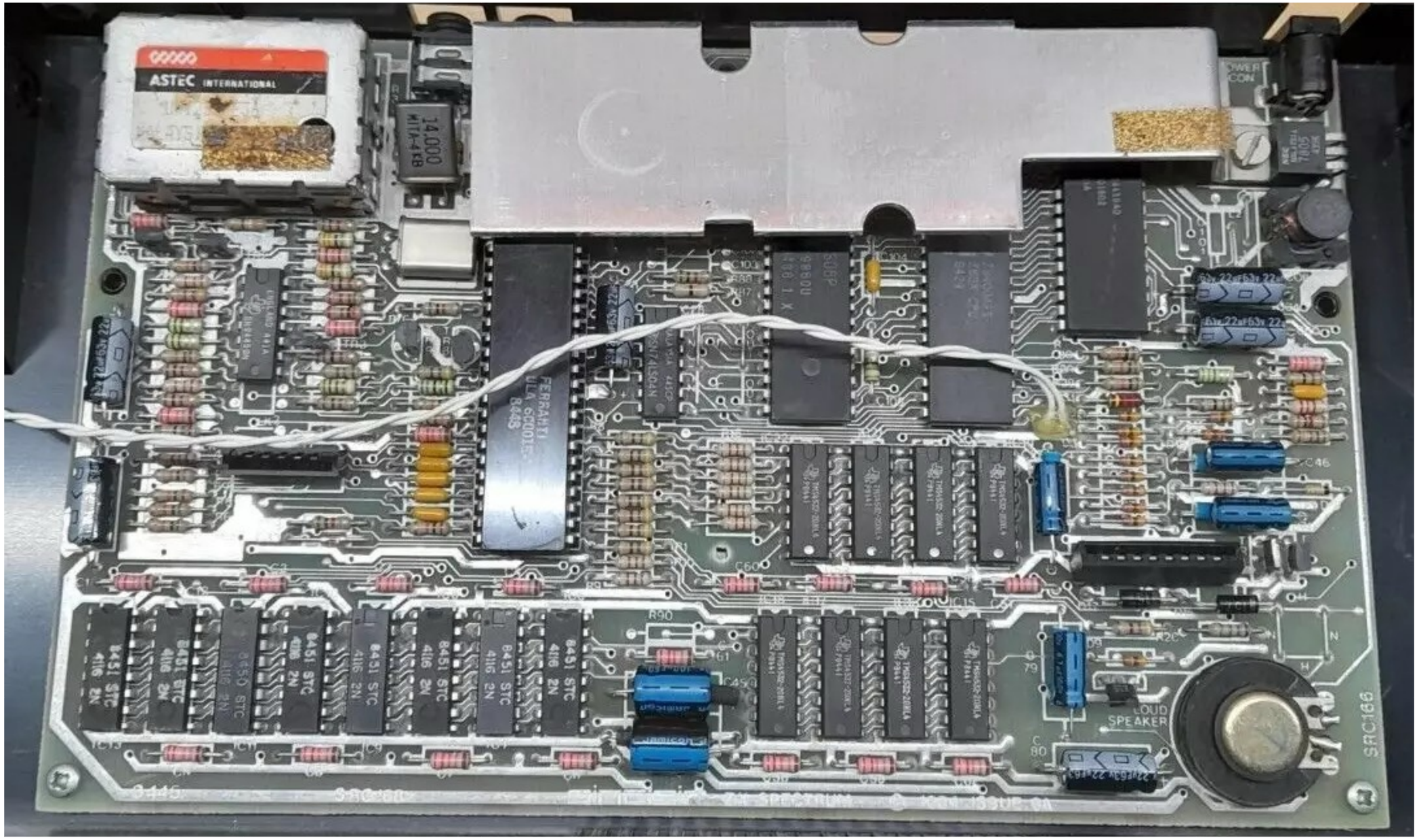
Department of Algebra, Faculty of Mathematics and Physics, Charles University in Prague

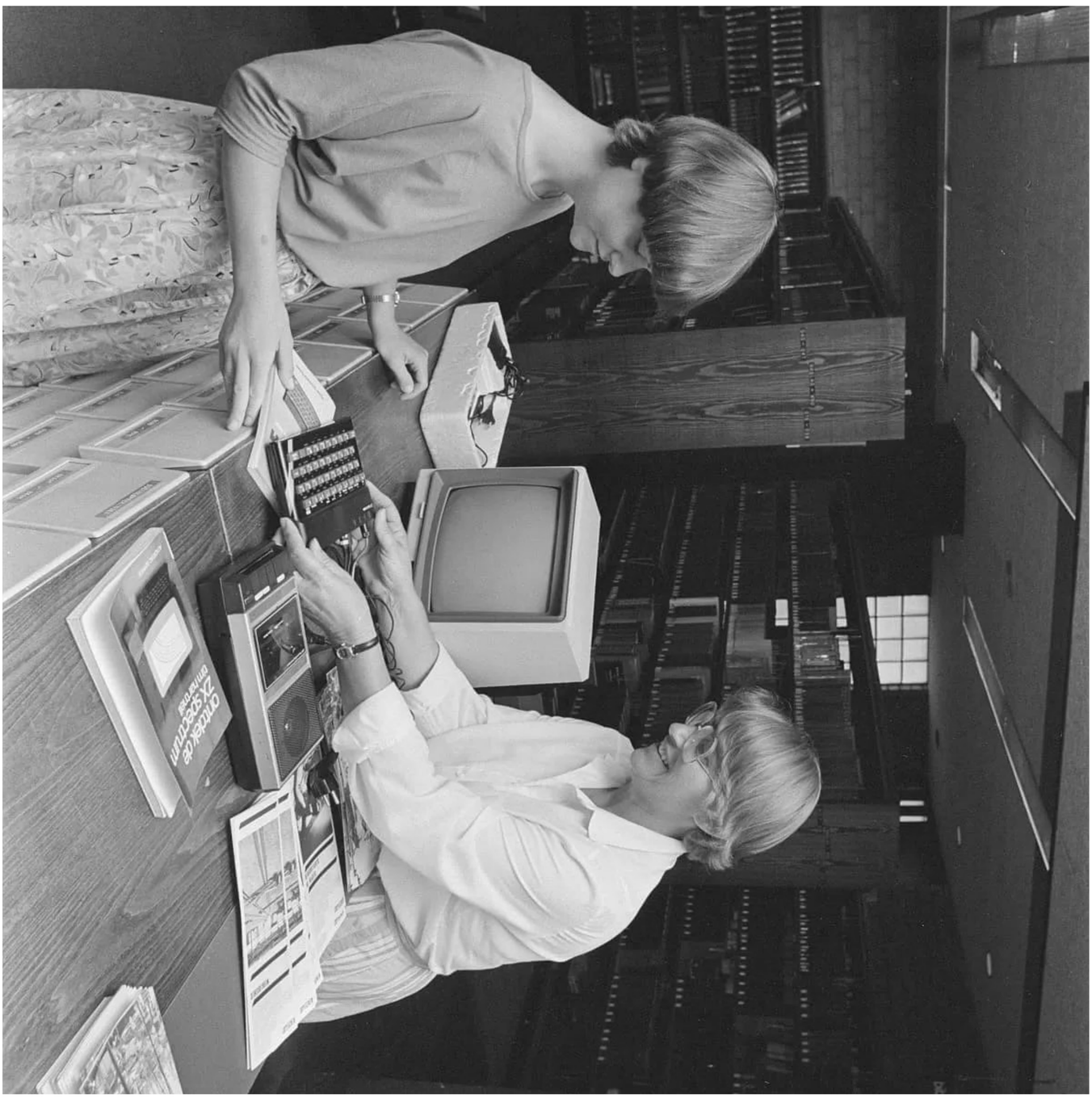
-- extended version: https://ok1sfu.cz/files/rosa-platform-security-2025.pdf

About Us as of **March 2026**

- Active research topics
  - Post-quantum cryptography, classical and quantum cryptanalysis
  - Platform security, tactical radio
- Secondary research areas
  - Electronics design and vulnerabilities, FIDO2
  - Radio, NFC, and telecommunication networks
- Maintained competence background
  - Classical and quantum computer science
  - Graduate applied mathematics and physics
  - Security modeling, primary focus on cryptology




ASTEC INTERNATIONAL
14.000
FERRANTI
ULA 6C001E-
8448
LOUD
SPEAKER
SAC166

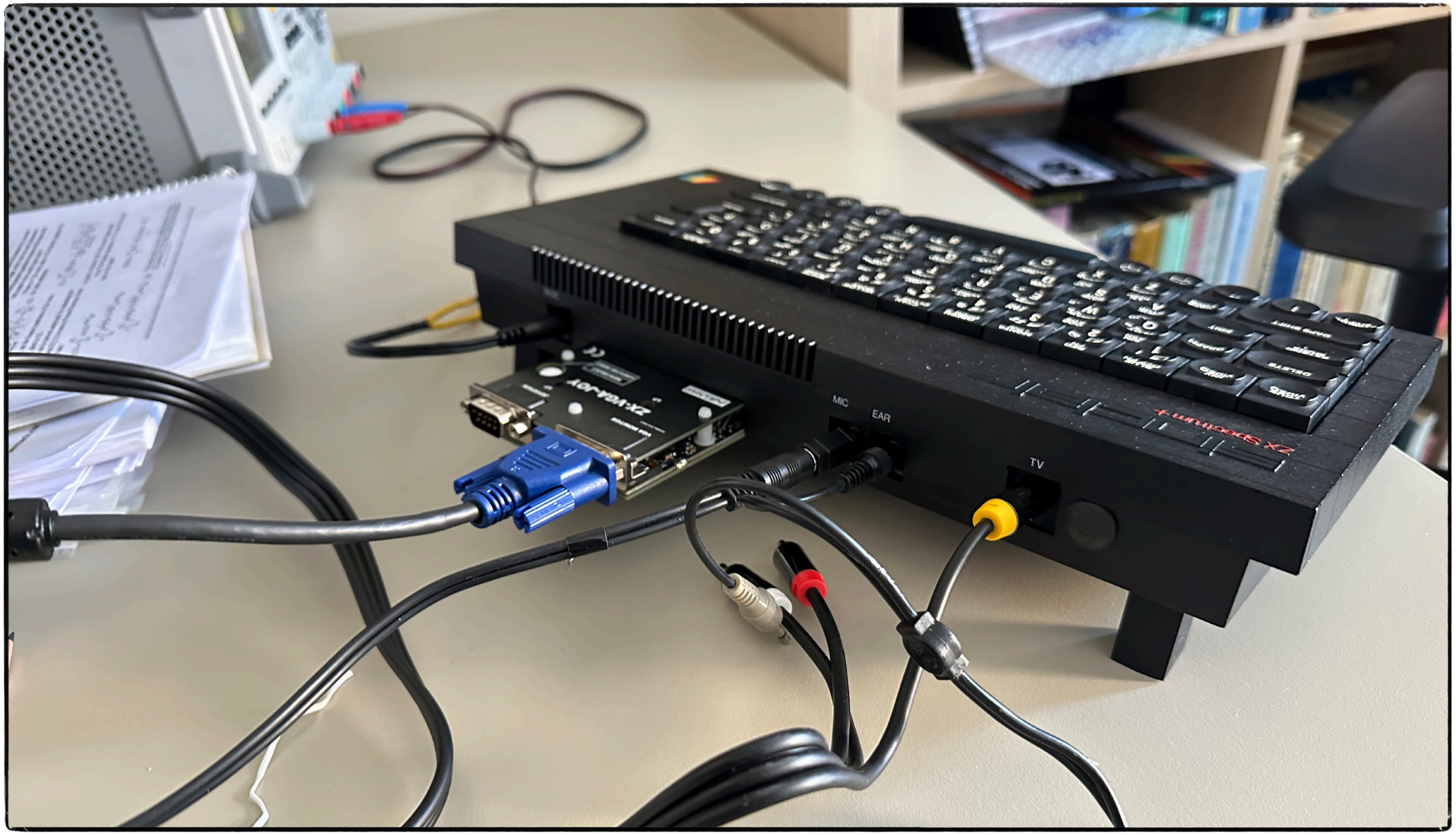


-- Librarian loaning a woman a Sinclair ZX-Spectrum in 1984, NL

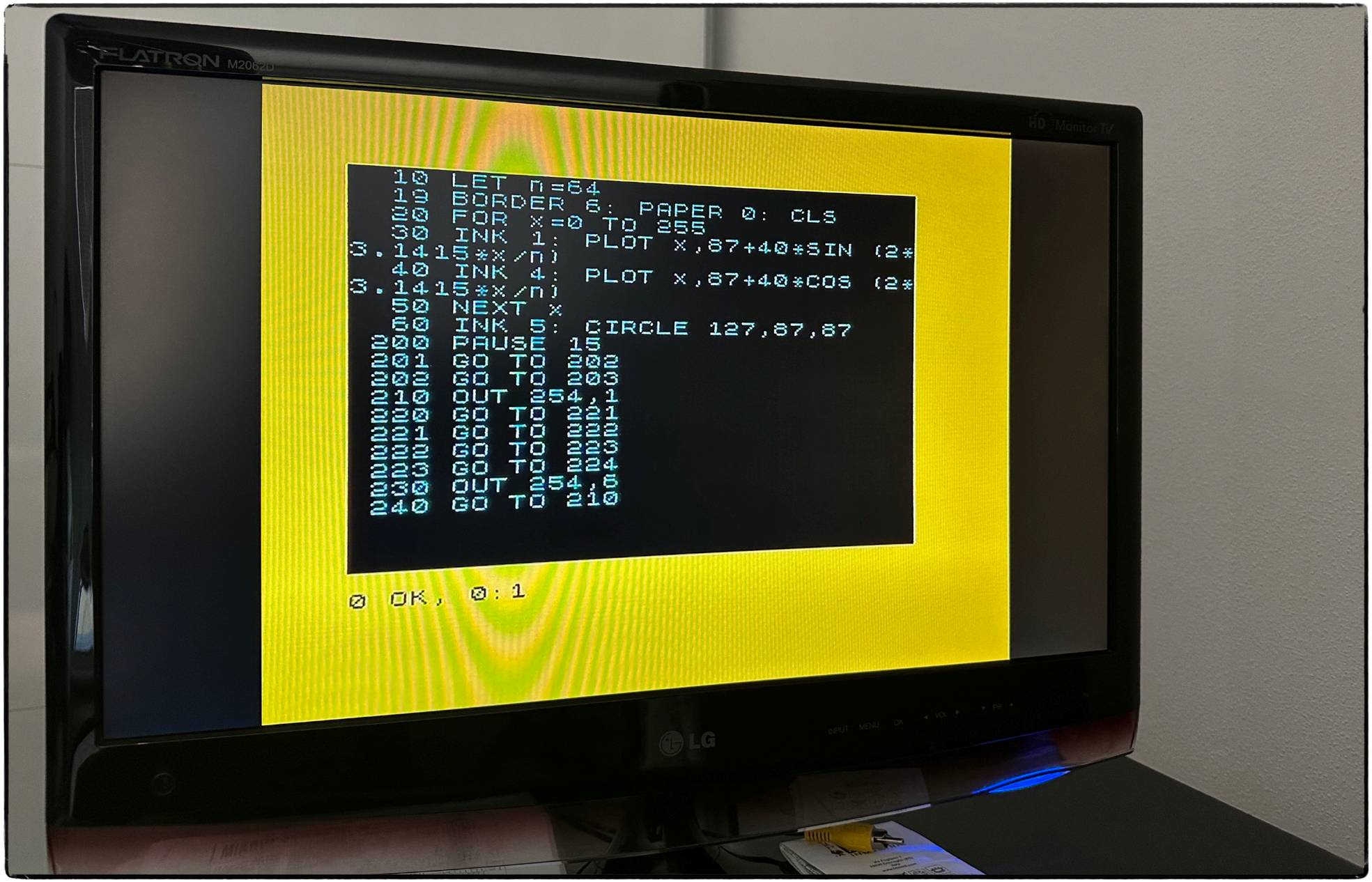
-- https://80sheaven.com/sinclair-zx-spectrum/

Na výstavě „Elektronizace a automatizace 83" byly vystaveny i osobní mikropočítače PMD-85 se zobrazovací jednotkou určené pro školní výuku. Jejich praktické předvádění při zahájení výstavy se zájmem sledoval i předseda vlády ČSSR L. Štrougal, tajemníci ÚV KSČ M. Jakeš a J. Havlín a další soudruzi.

-- Věda a technika mládeži, 01, 1984


MIC
EAR
TV
ZX Spectrum+

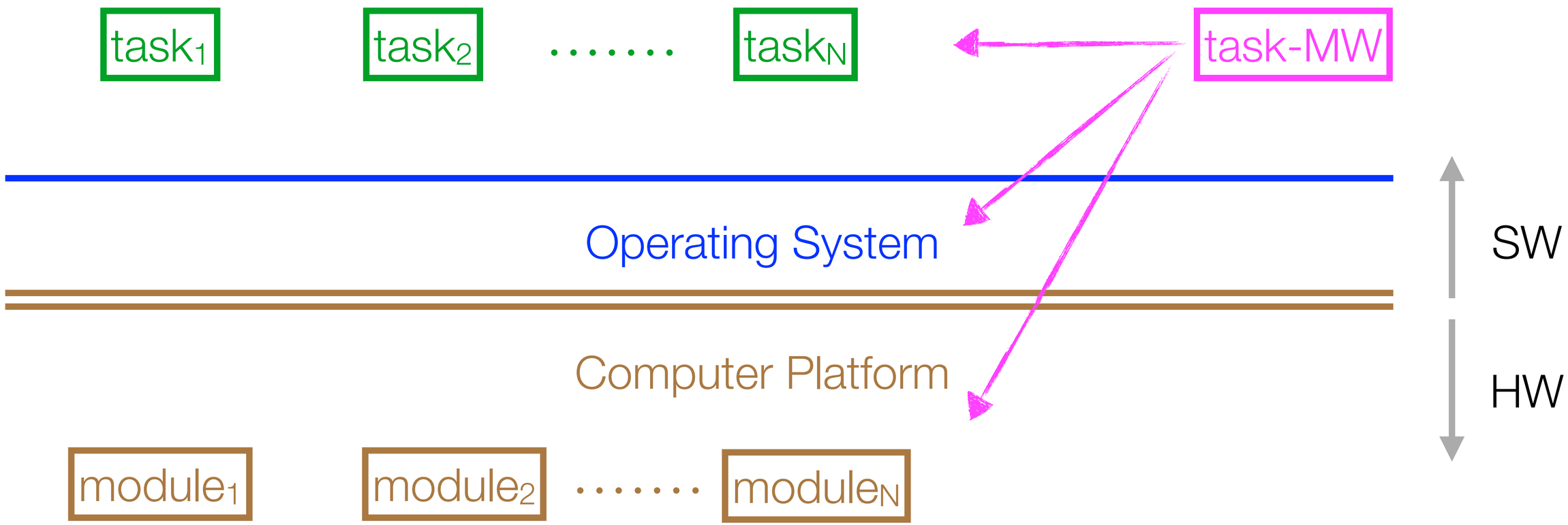

Ø OK, 60:2
Ø OK, 60:2
LoRa
RF


FLATRON M2062D
HD Monitor TV
10 LET n=84
19 BORDER 6: PAPER 0: CLS
20 FOR x=0 TO 255
30 INK 1: PLOT x,87+40*SIN (2*
3.1415*x/n)
40 INK 4: PLOT x,87+40*COS (2*
3.1415*x/n)
50 NEXT x
60 INK 5: CIRCLE 127,87,87
200 PAUSE 15
201 GO TO 202
202 GO TO 203
210 OUT 254,1
220 GO TO 221
221 GO TO 222
222 GO TO 223
223 GO TO 224
230 OUT 254,6
240 GO TO 210
0 OK, 0:1
LG
INPUT MENU OK VOL PR

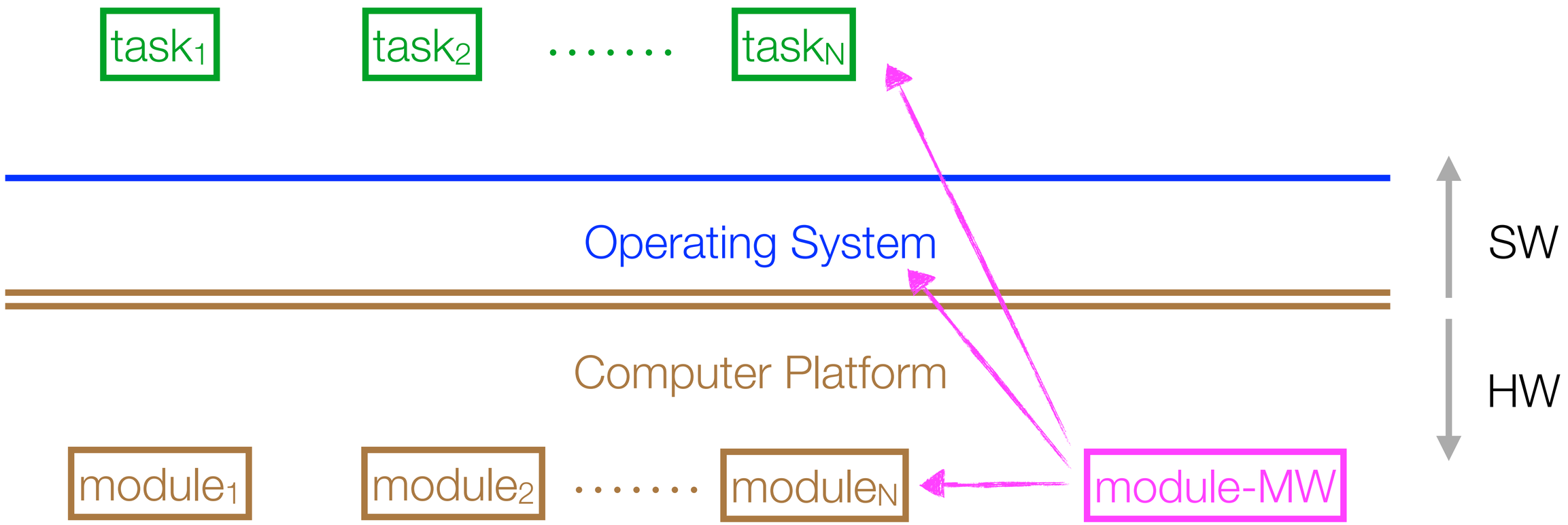
“Despite modern marketing buzzwords, the computing machines principles stay basically the same.”

“Secure hardware enables secure software, not the other way round.”

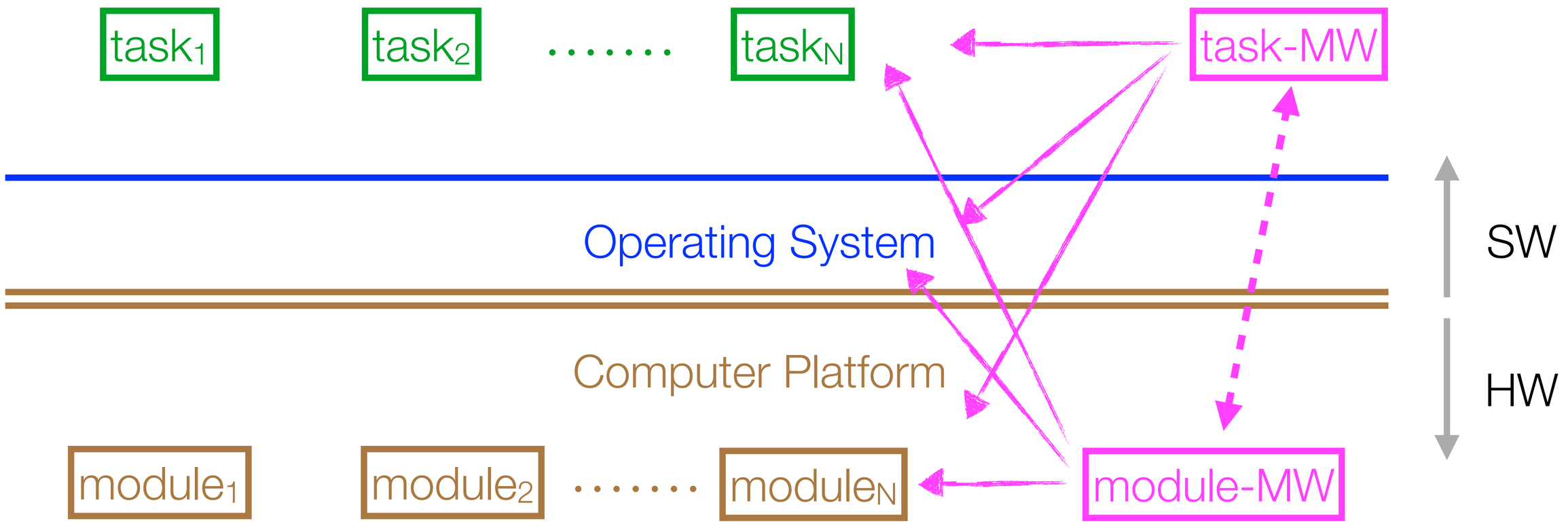
Purely User-Space SW Attack Model



Evil HW Attack Model



HW-SW Attack Model



Reliability, not Perfection

- We do not require the computer platform to be perfect
- We need to have a clearly defined system security policy
- We shall be able to rely on the HW obeying that system policy
- The operating system than strives to compensate the weak points while empowering the strong ones

Thunderbolt, USB4, PCI Express, and NVMe

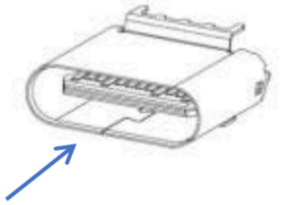
Glossary

- **DFP** - Downstream Facing Port; USB host-side port or hub downstream port
- **UFP** - Upstream Facing Port; USB device-side port or hub upstream connection
- **DRP** - Dual Role Port; USB port that may operate as either a DFP or a UFP
- **Source** - the provider of VBUS power in a USB connection
- **Sink** - the consumer of VBUS power in a USB connection
- **USB PD** - USB Power Delivery
- **SOP*** - Start of Frame field in a USB Power Delivery; indicates the intended recipient of the packet
- **VCONN** - the dedicated power supply rail for cables and accessories
- **BMC** - Biphase Mark Coding
- **CDR** - Clock (and) Data Recovery

-- Application Note, AN1974, Microchip Technology Inc., 2015

USB Type-C® – Functional Model

- USB 3.2 / *USB4™* data bus
  - Two sets of TX/RX pin pairs, supports x1 and x2 operation
- USB 2.0 data bus
  - Two pin sets on host, one set on device – strapped together within the host and device
- Two power buses
  - VBUS and VCONN
- Two sideband pins (SBU1/SBU2)
  - *SBTX / SBRX for USB4*
- CC – Configuration Channel
  - Two CC pins in connector
  - One CC wire in cable



Looking into the product receptacle:

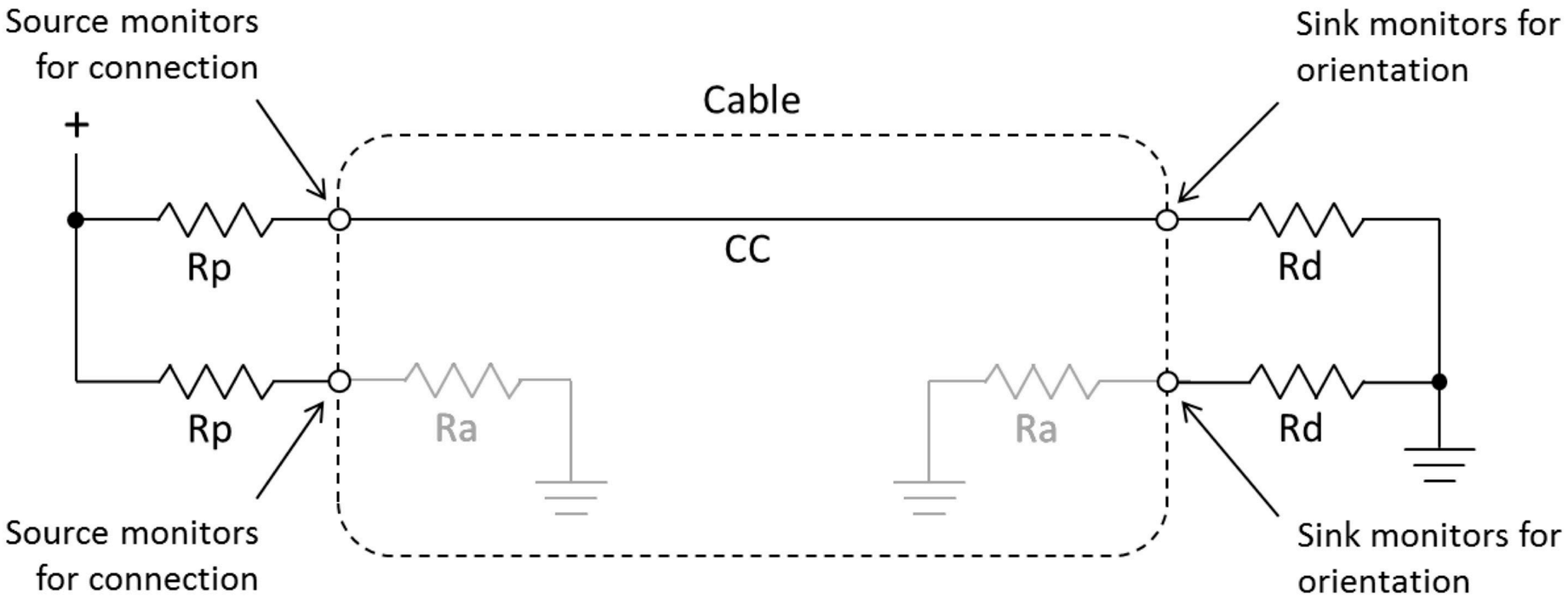
A1	A2	A3	A4	A5	A6	A7	A8	A9	A10	A11	A12
GND	TX1+	TX1−	VBUS	CC1	D+	D−	SBU1	VBUS	RX2−	RX2+	GND
GND	RX1+	RX1−	VBUS	SBU2	D−	D+	CC2	VBUS	TX2−	TX2+	GND
B12	B11	B10	B9	B8	B7	B6	B5	B4	B3	B2	B1

Looking into the cable or product plug:

A12	A11	A10	A9	A8	A7	A6	A5	A4	A3	A2	A1
GND	RX2+	RX2−	VBUS	SBU1	D−	D+	CC	VBUS	TX1−	TX1+	GND
GND	TX2+	TX2−	VBUS	VCONN			SBU2	VBUS	RX1−	RX1+	GND
B1	B2	B3	B4	B5	B6	B7	B8	B9	B10	B11	B12

Lane 1 ***Lane 0***

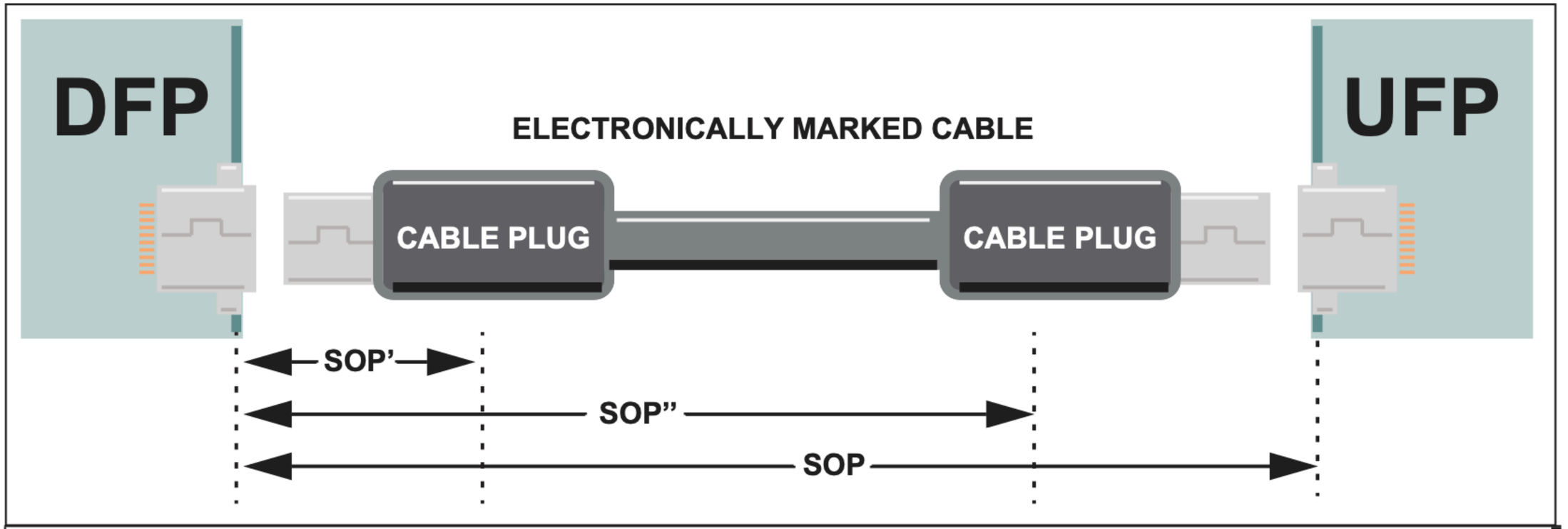
USB Type-C® – Pull-Up/Pull-Down CC Model



- Host side can substitute current sources for Rp
- Powered cables and accessories introduce Ra at the “unwired” CC pins which are used to indicate the need for VCONN

Source also monitors for orientation this way. Sink monitors for a connection via V_{BUS}.

FIGURE 2: SOP* SIGNALING



Note: SOP' is assigned to one plug of the cable while SOP'' is assigned to the other. The cable plugs cannot tell which side that they are connected to, just that one end may respond to SOP' addressed messages and the other may respond SOP'' addressed messages.

The DFP is the Bus Master and initiates all communication.

-- Application Note, AN1974, Microchip Technology Inc., 2015

FIGURE 1: POWER DELIVERY PROTOCOL PACKET FORMAT

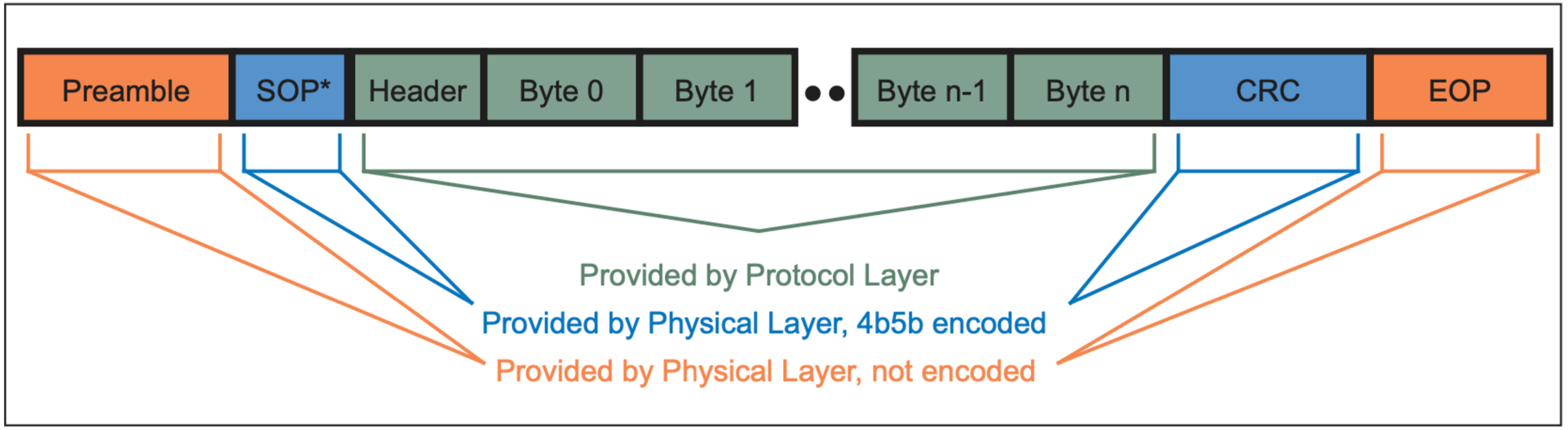
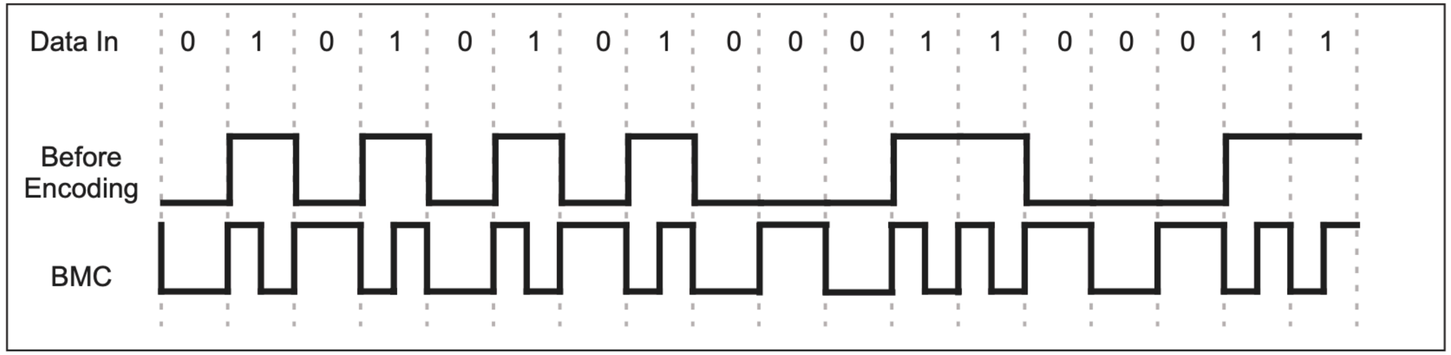


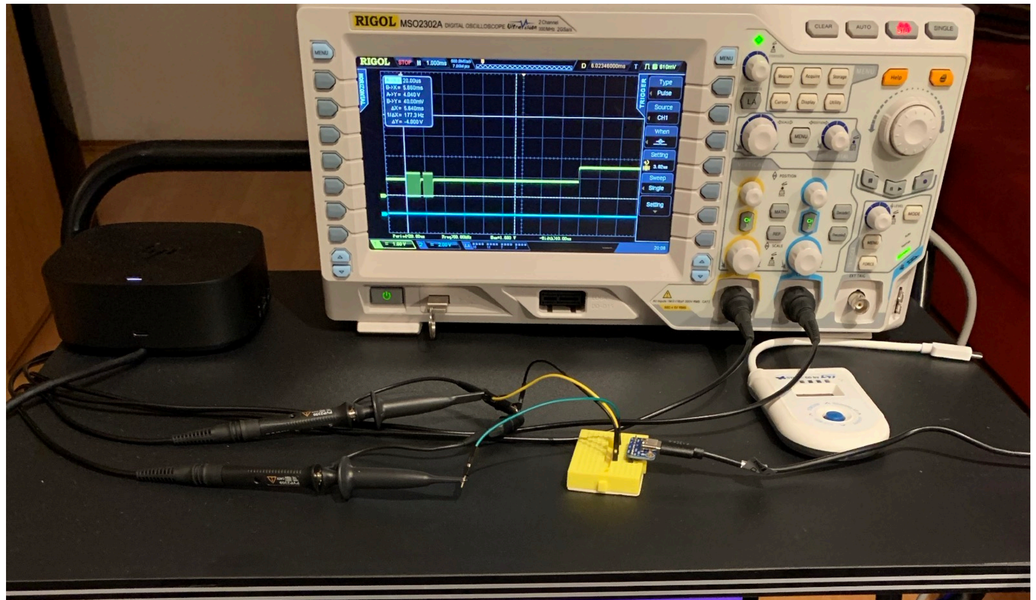
FIGURE 5: BMC SIGNALING



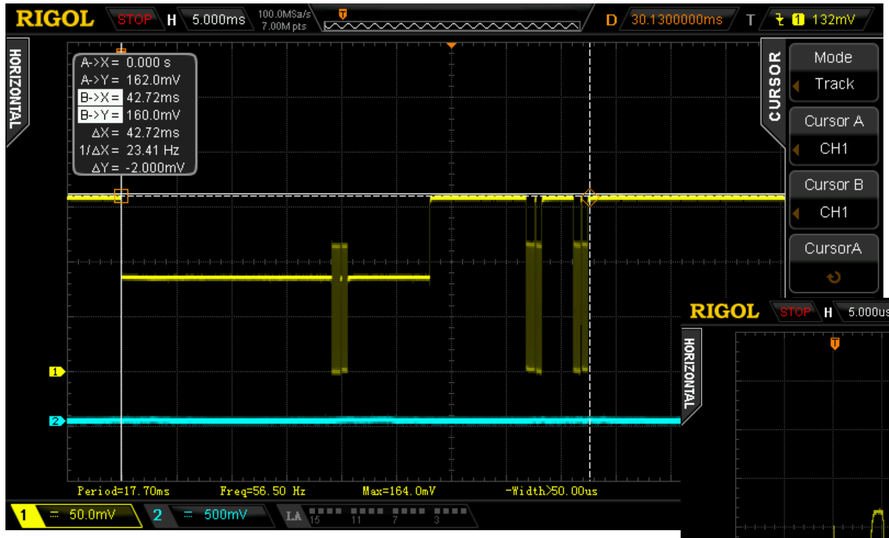
Biphase Mark Coding

Differential Manchester coding, 300 kbps, DC balanced with a nominal voltage swing of 1.125V

-- Application Note, AN1974, Microchip Technology Inc., 2015

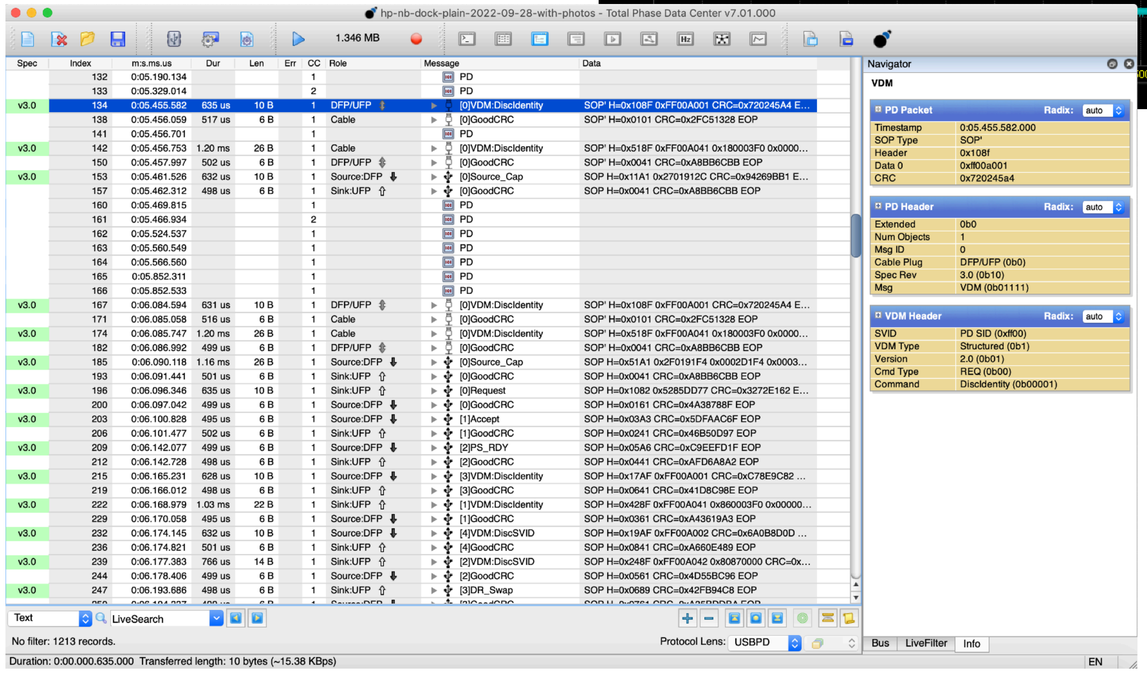

RIGOL MSO2302A


ubuntu


RIGOL
STOP
H 5.000ms
100.0MSa/s
7.00M pts
D 30.1300000ms
T 1 132mV
HORIZONTAL
A->X= 0.000 s
A->Y= 162.0mV
B->X= 42.72ms
B->Y= 160.0mV
ΔX= 42.72ms
1/ΔX= 23.41 Hz
ΔY= -2.000mV
CURSOR
Mode
Track
Cursor A
CH1
Cursor B
CH1
CursorA
Period=17.70ms
Freq=56.50 Hz
Max=164.0mV
-Width>50.00us
1 = 50.0mV
2 = 500mV
LA

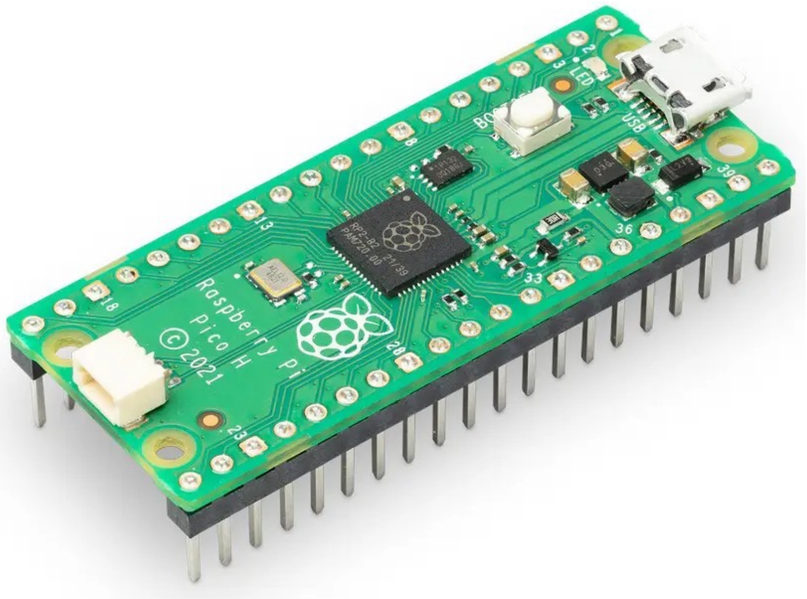

USB
Power Delivery
Analyzer
TOTALPHASE


RIGOL
STOP
H 5.000us
1.000GSa/s
700k pts
D 24.8000000us
T 1 71.0mV
HORIZONTAL
CURSOR
23:33

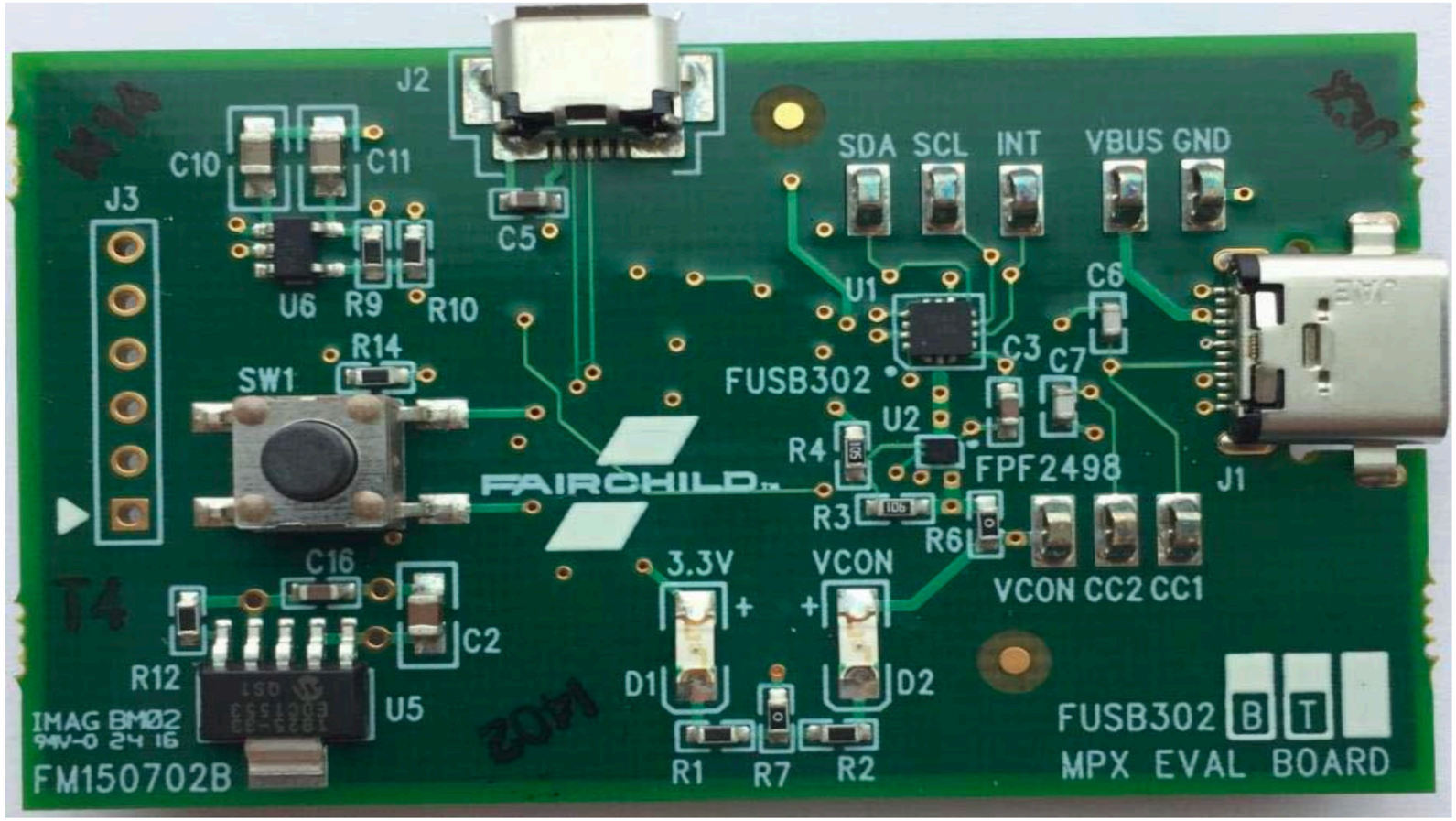

hp-nb-dock-plain-2022-09-28-with-photos - Total Phase Data Center v7.01.000
1.346 MB
Spec Index m:s.ms.us Dur Len Err CC Role Message Data
132 0:05.190.134 1 PD
133 0:05.329.014 2 PD
v3.0 134 0:05.455.582 635 us 10 B 1 DFP/UFP [0]VDM:DiscIdentity SOP' H=0x108F 0xFF00A001 CRC=0x720245A4 E...
138 0:05.456.059 517 us 6 B 1 Cable [0]GoodCRC SOP' H=0x0101 CRC=0x2FC51328 EOP
141 0:05.456.701 1 PD
v3.0 142 0:05.456.753 1.20 ms 26 B 1 Cable [0]VDM:DiscIdentity SOP' H=0x518F 0xFF00A041 0x180003F0 0x0000...
150 0:05.457.997 502 us 6 B 1 DFP/UFP [0]GoodCRC SOP' H=0x0041 CRC=0xA8BB6CBB EOP
v3.0 153 0:05.461.526 632 us 10 B 1 Source:DFP [0]Source_Cap SOP H=0x11A1 0x2701912C CRC=0x94269BB1 E...
157 0:05.462.312 498 us 6 B 1 Sink:UFP [0]GoodCRC SOP H=0x0041 CRC=0xA8BB6CBB EOP
160 0:05.469.815 1 PD
161 0:05.466.934 2 PD
162 0:05.524.537 1 PD
163 0:05.560.549 1 PD
164 0:05.566.560 1 PD
165 0:05.852.311 1 PD
166 0:05.852.533 1 PD
v3.0 167 0:06.084.594 631 us 10 B 1 DFP/UFP [0]VDM:DiscIdentity SOP' H=0x108F 0xFF00A001 CRC=0x720245A4 E...
171 0:06.085.058 516 us 6 B 1 Cable [0]GoodCRC SOP' H=0x0101 CRC=0x2FC51328 EOP
v3.0 174 0:06.085.747 1.20 ms 26 B 1 Cable [0]VDM:DiscIdentity SOP' H=0x518F 0xFF00A041 0x180003F0 0x0000...
182 0:06.086.992 499 us 6 B 1 DFP/UFP [0]GoodCRC SOP' H=0x0041 CRC=0xA8BB6CBB EOP
v3.0 185 0:06.090.118 1.16 ms 26 B 1 Source:DFP [0]Source_Cap SOP H=0x51A1 0x2F0191F4 0x0002D1F4 0x0003...
193 0:06.091.441 501 us 6 B 1 Sink:UFP [0]GoodCRC SOP H=0x0041 CRC=0xA8BB6CBB EOP
v3.0 196 0:06.096.346 635 us 10 B 1 Sink:UFP [0]Request SOP H=0x1082 0x5285DD77 CRC=0x3272E162 E...
200 0:06.097.042 499 us 6 B 1 Source:DFP [0]GoodCRC SOP H=0x0161 CRC=0x4A38788F EOP
v3.0 203 0:06.100.828 495 us 6 B 1 Source:DFP [1]Accept SOP H=0x03A3 CRC=0x5DFAAC6F EOP
206 0:06.101.477 502 us 6 B 1 Sink:UFP [1]GoodCRC SOP H=0x0241 CRC=0x46B50D97 EOP
v3.0 209 0:06.142.077 499 us 6 B 1 Source:DFP [2]PS_RDY SOP H=0x05A6 CRC=0xC9EEFD1F EOP
212 0:06.142.728 498 us 6 B 1 Sink:UFP [2]GoodCRC SOP H=0x0441 CRC=0xAFD6A8A2 EOP
v3.0 215 0:06.165.231 628 us 10 B 1 Source:DFP [3]VDM:DiscIdentity SOP H=0x17AF 0xFF00A001 CRC=0xC78E9C82 ...
219 0:06.166.012 498 us 6 B 1 Sink:UFP [3]GoodCRC SOP H=0x0641 CRC=0x41D8C98E EOP
v3.0 222 0:06.168.979 1.03 ms 22 B 1 Sink:UFP [1]VDM:DiscIdentity SOP H=0x428F 0xFF00A041 0x860003F0 0x00000...
229 0:06.170.058 495 us 6 B 1 Source:DFP [1]GoodCRC SOP H=0x0361 CRC=0xA43619A3 EOP
v3.0 232 0:06.174.145 632 us 10 B 1 Source:DFP [4]VDM:DiscSVID SOP H=0x19AF 0xFF00A002 CRC=0x6A0B8D0D ...
236 0:06.174.821 501 us 6 B 1 Sink:UFP [4]GoodCRC SOP H=0x0841 CRC=0xA660E489 EOP
v3.0 239 0:06.177.383 766 us 14 B 1 Sink:UFP [2]VDM:DiscSVID SOP H=0x248F 0xFF00A042 0x80870000 CRC=0x...
244 0:06.178.406 499 us 6 B 1 Source:DFP [2]GoodCRC SOP H=0x0561 CRC=0x4D55BC96 EOP
v3.0 247 0:06.193.686 498 us 6 B 1 Sink:UFP [3]DR_Swap SOP H=0x0689 CRC=0x42FB94C8 EOP
Navigator
VDM
PD Packet Radix: auto
Timestamp 0:05.455.582.000
SOP Type SOP'
Header 0x108f
Data 0 0xff00a001
CRC 0x720245a4
PD Header Radix: auto
Extended 0b0
Num Objects 1
Msg ID 0
Cable Plug DFP/UFP (0b0)
Spec Rev 3.0 (0b10)
Msg VDM (0b01111)
VDM Header Radix: auto
SVID PD SID (0xff00)
VDM Type Structured (0b1)
Version 2.0 (0b01)
Cmd Type REQ (0b00)
Command DiscIdentity (0b00001)
Text LiveSearch
No filter: 1213 records.
Protocol Lens: USBPD
Bus LiveFilter Info
Duration: 0:00.000.635.000 Transferred length: 10 bytes (~15.38 KBps)
EN

RPi Pico H

(RP2040)



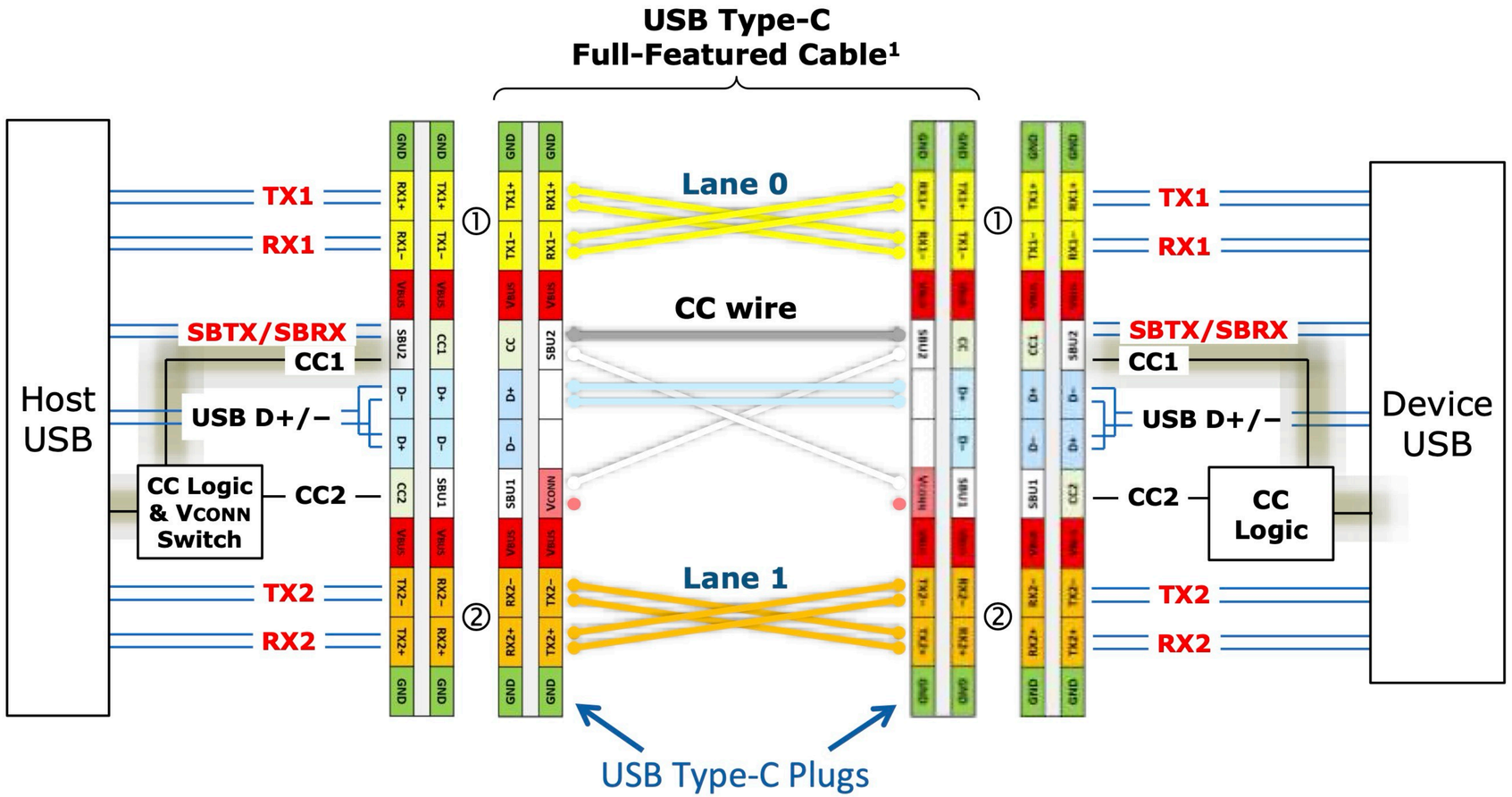
FUSB302BGEVB



-- https://hackaday.com/2023/02/14/all-about-usb-c-talking-low-level-pd/

USB Type-C® – Functional Model

- USB Type-C Full-Featured Cable supports all USB operating modes



Note: 1. Required VBUS and Ground wires not shown in this illustration

8.3.2 USB 3.1 and 2 Lanes of DisplayPort

The TUSB1046-DCI operates in USB3.1 and 2 Lanes of DisplayPort mode when the CTL1 pin is high and CTL0 pin is high.

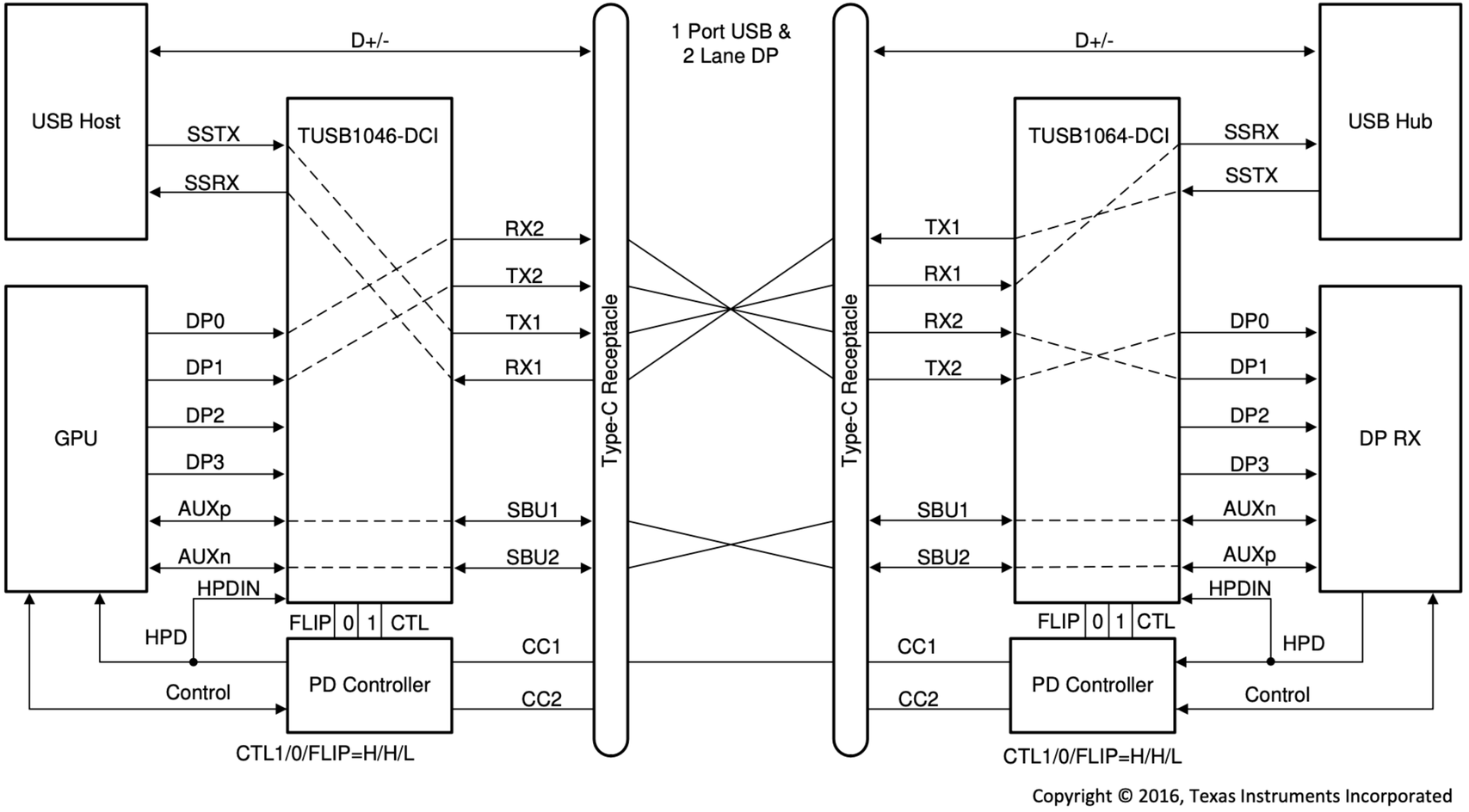
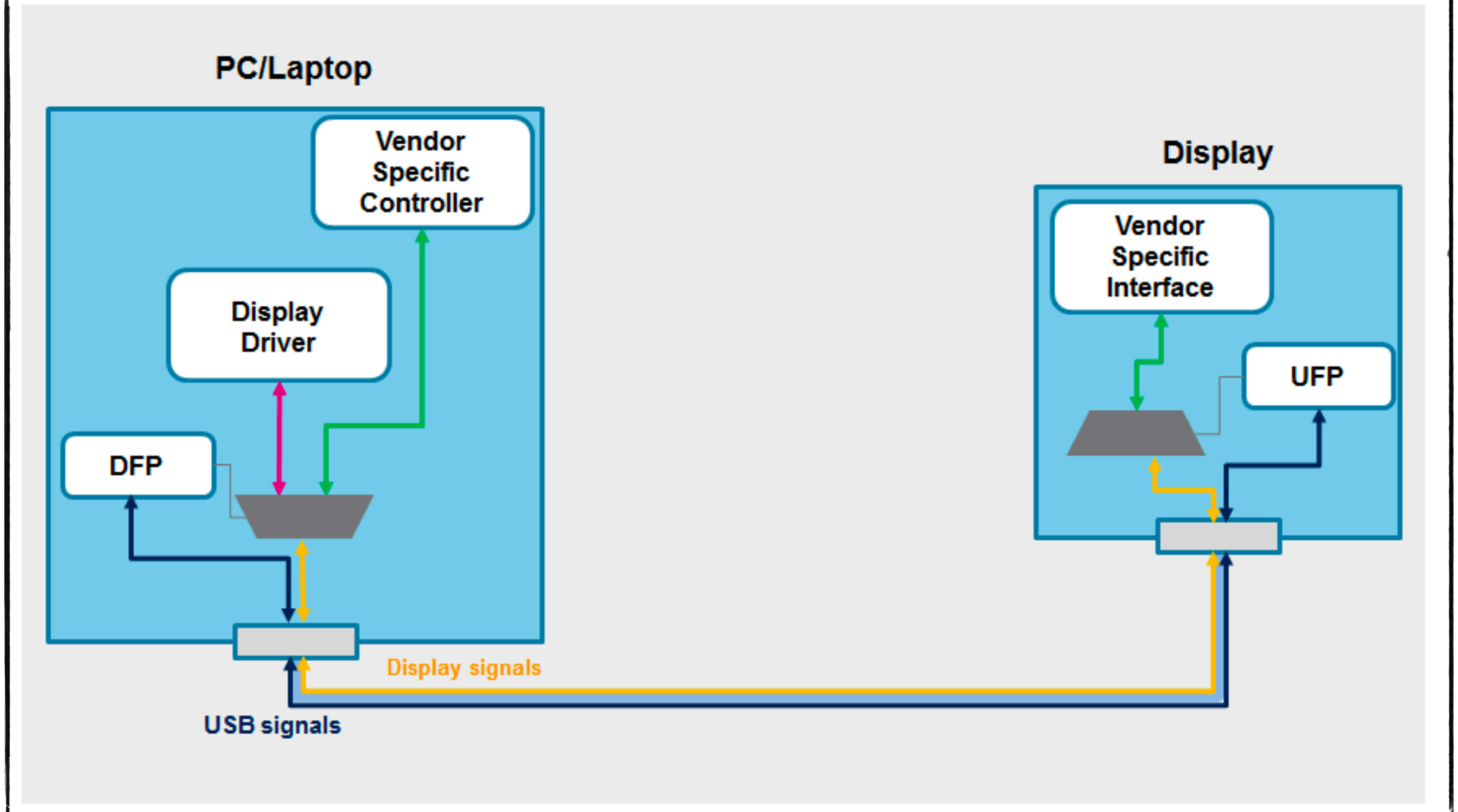


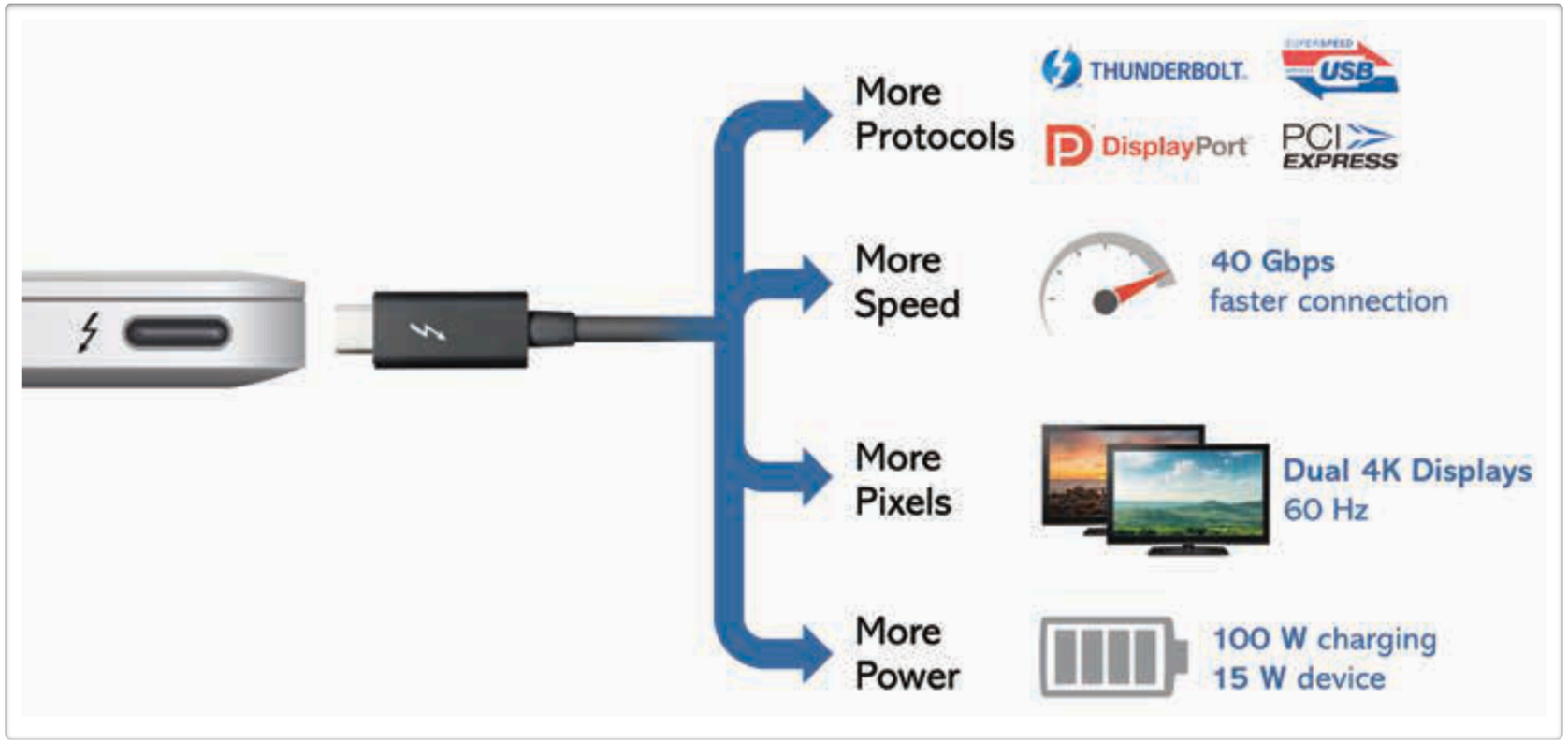
Figure 8-6. USB3.1 + 2 Lane DP – No Flip (CTL1 = H, CTL0 = H, FLIP = L)

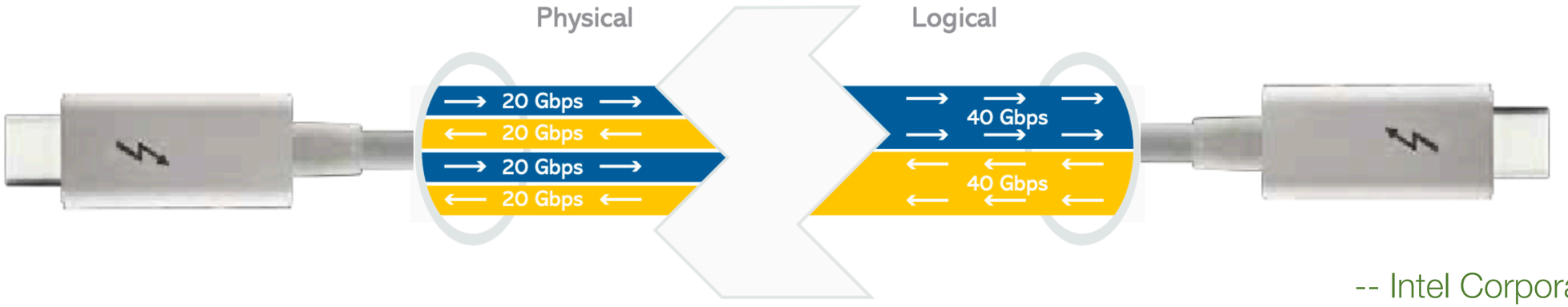
Figure 3. Typical scenario using Alternate Mode to drive a display



-- Technical Article, TA0356, STMicroelectronics, 2018

-- Intel Corporation, 2016





-- Intel Corporation, 2016

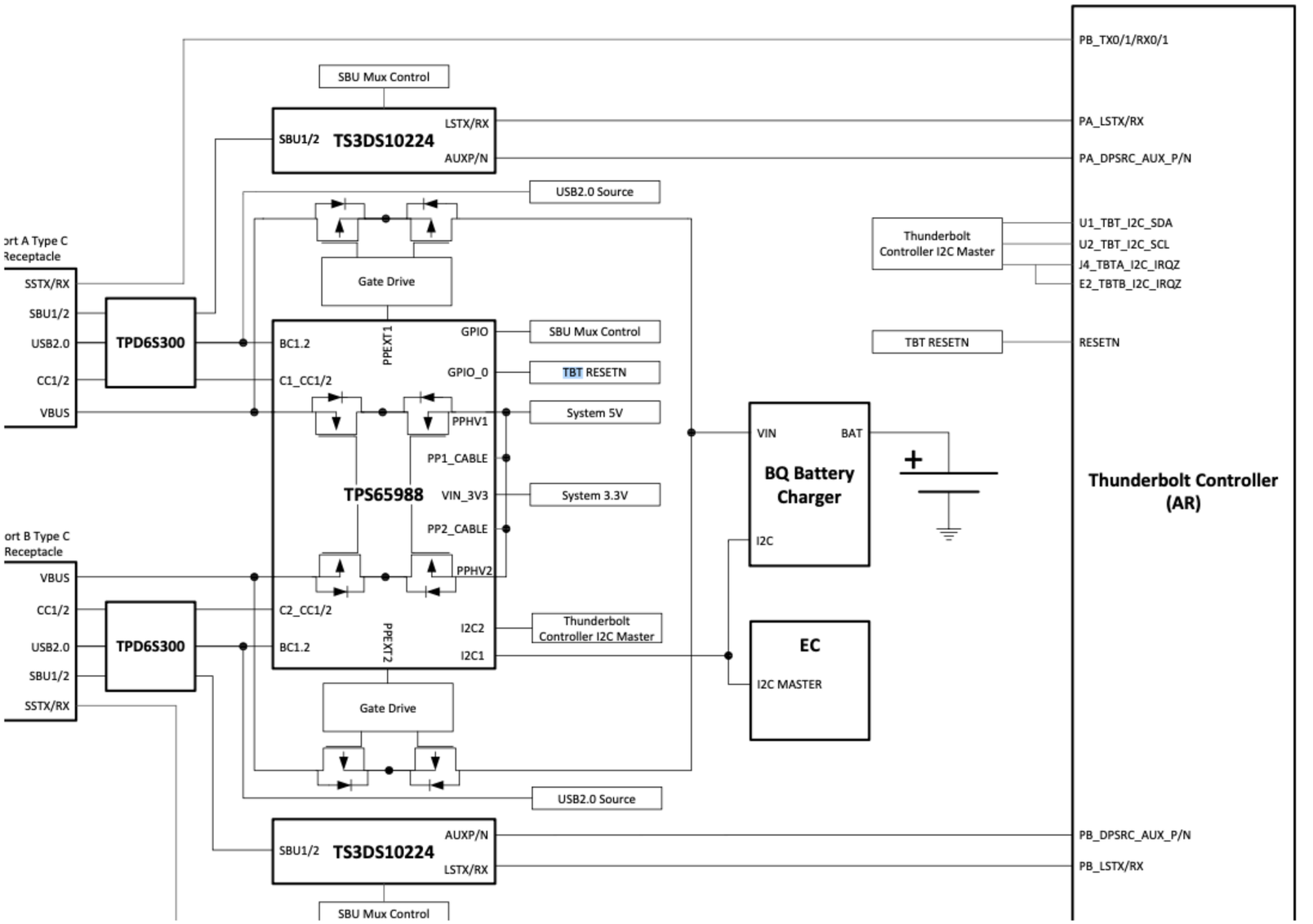
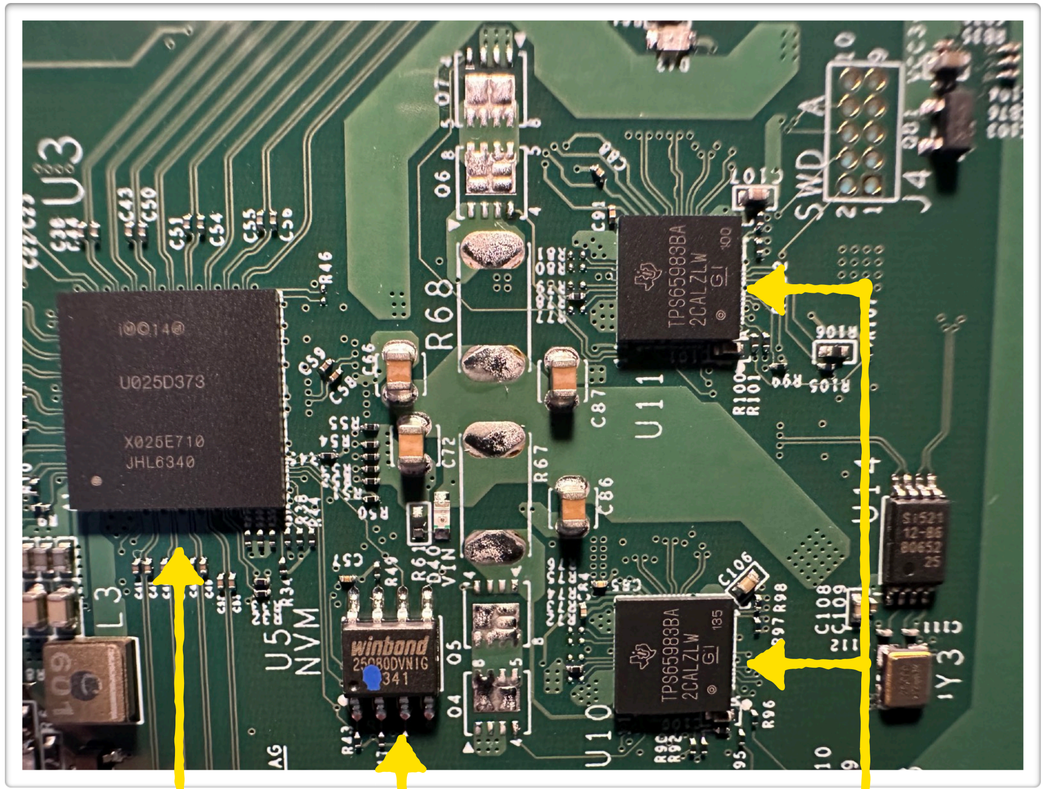


Figure 9-7. TBT Notebook with PD Charging

Thunderbolt 3 to PCI Express Expansion Chassis



TBT controller

Flash FW

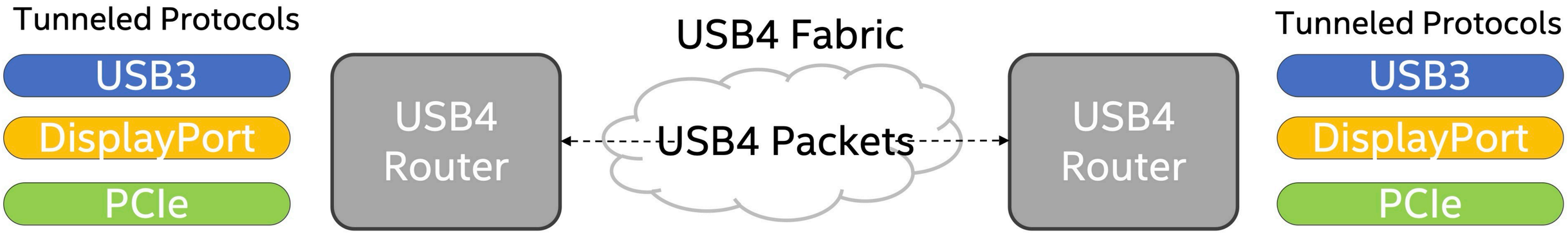
USB Type-C controllers

-- https://www.startech.com/en-eu/usb-hubs/tb31pciex16

10,000 Foot View

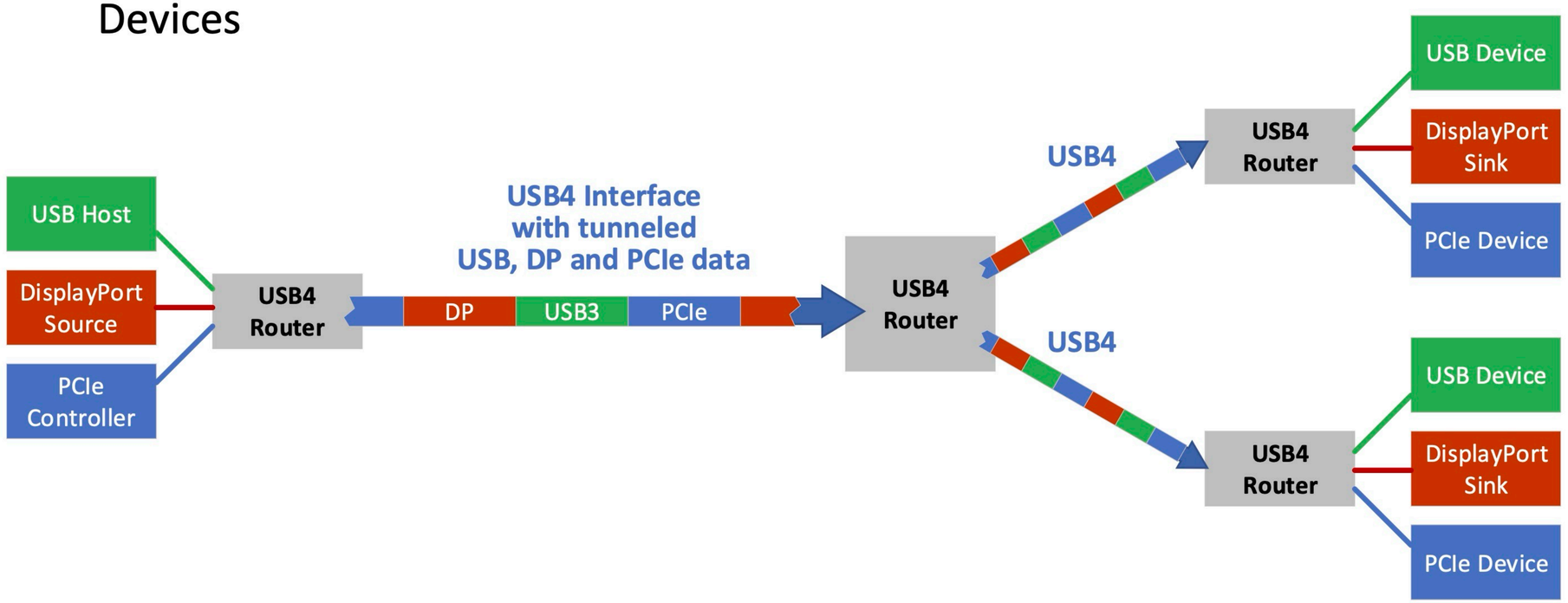
Here comes… USB4

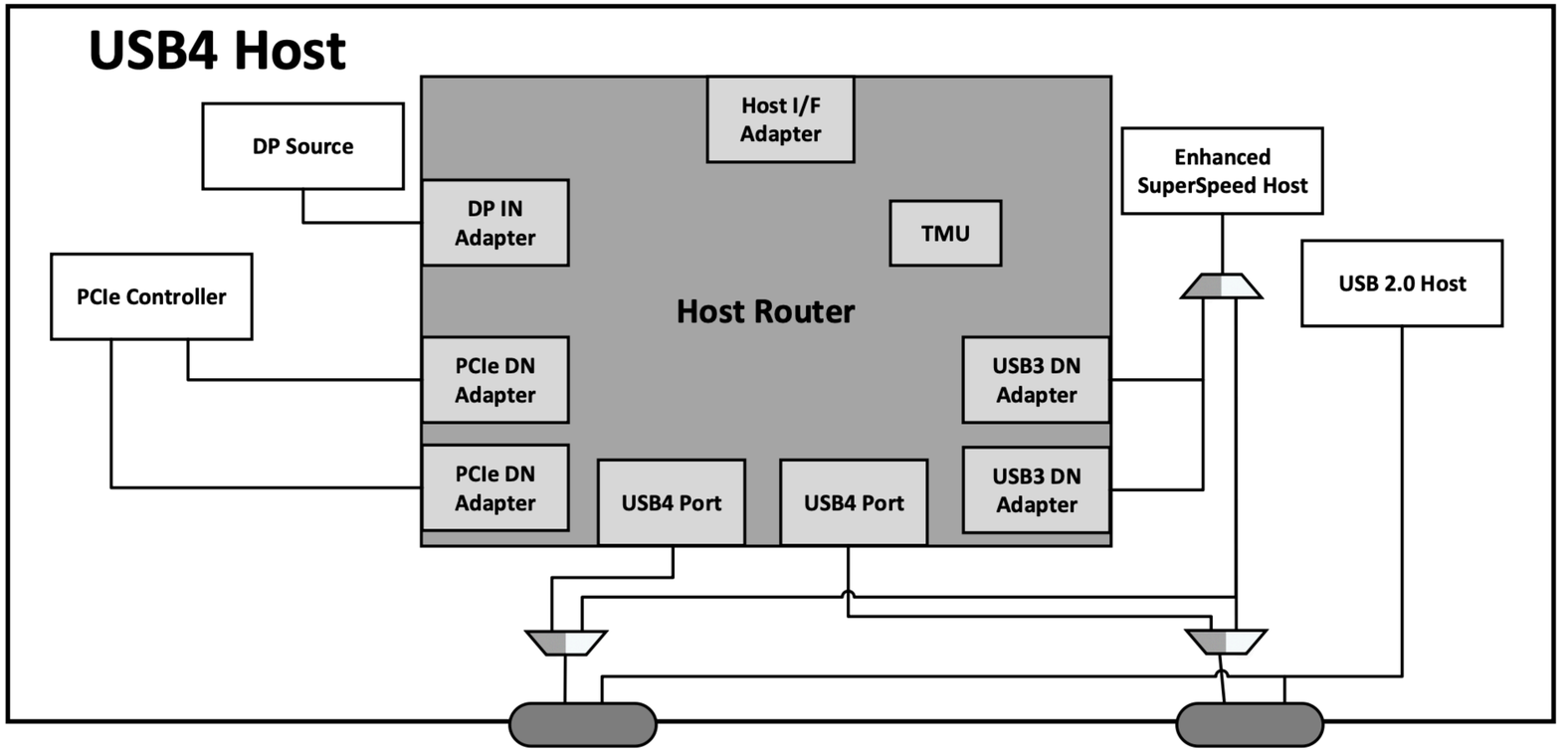
- Runs over USB Type-C® interconnect
- Tunnels USB3, PCIe and DP protocols
- Signaling rates of 10 or 20 Gbps (10 to 40Gbps aggregated b/w)
- Utilizes passive and active cables (longer reach)
- Topologies with up to 6 routers
- Time sync accuracy support across USB4™ Fabric

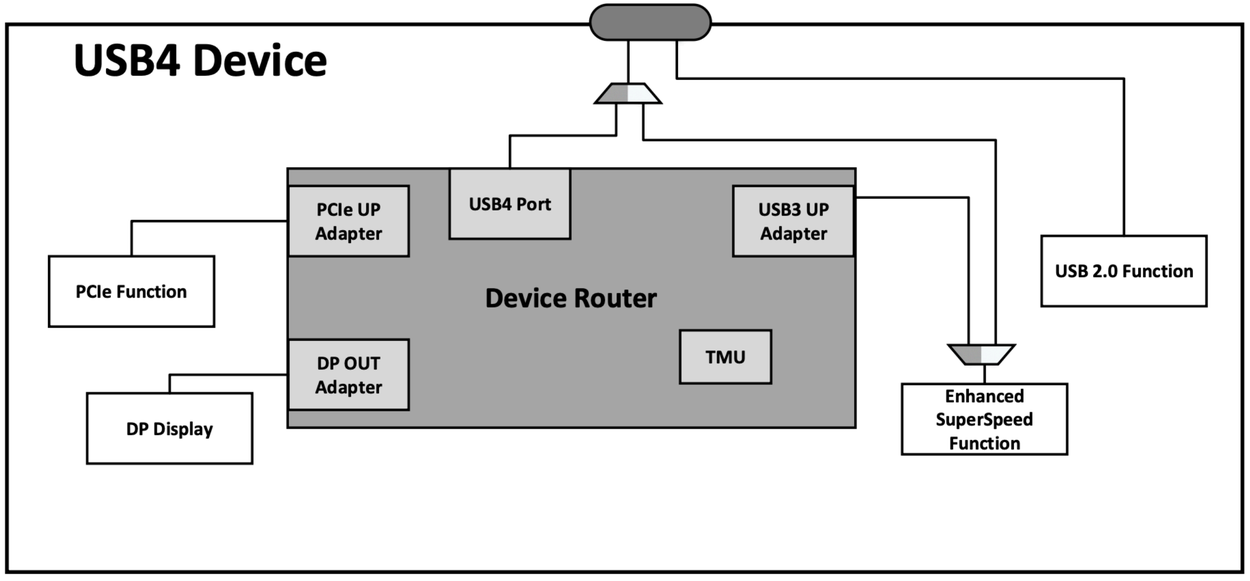


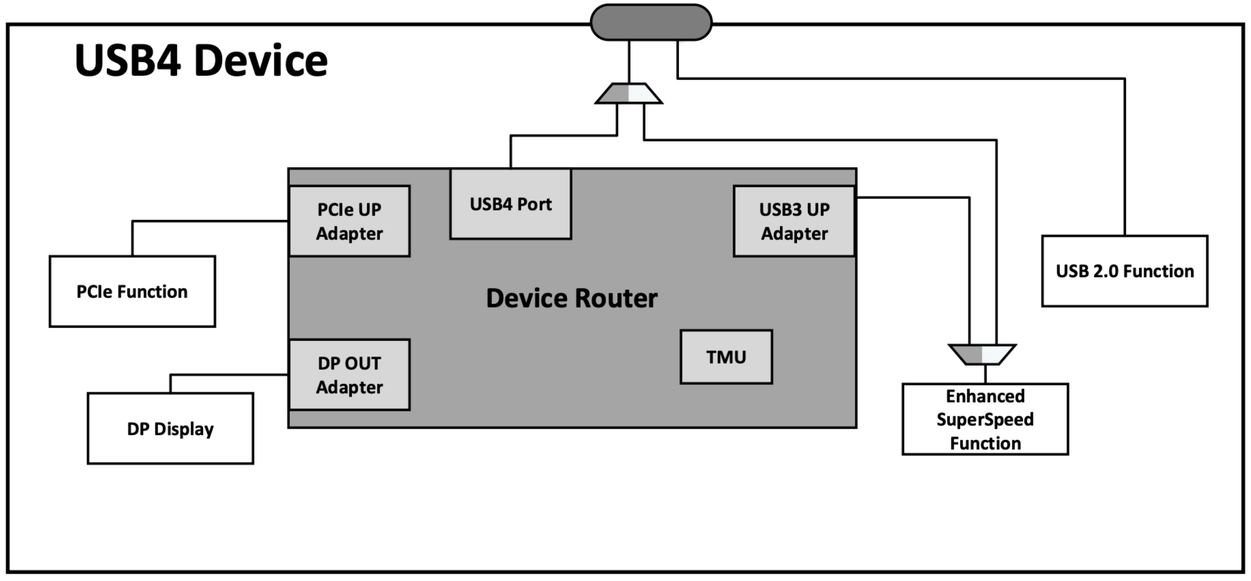
USB4™ DisplayPort™ Considerations

- This presentation focuses only on USB4 DP requirements. Other requirements are covered in earlier presentations and the USB4 specification.
- There are three USB product types of interest for DisplayPort
- USB4 Host, USB4 Hub and USB4 Device
  - USB4 Hosts and Hubs must support DP Protocol Tunneling, with support optional for USB4 Devices




USB4 Host
DP Source
Host I/F Adapter
Enhanced SuperSpeed Host
DP IN Adapter
TMU
PCIe Controller
Host Router
USB 2.0 Host
PCIe DN Adapter
USB3 DN Adapter
PCIe DN Adapter
USB4 Port
USB4 Port
USB3 DN Adapter


USB4 Device
PCIe UP Adapter
USB4 Port
USB3 UP Adapter
PCIe Function
USB 2.0 Function
Device Router
TMU
DP OUT Adapter
DP Display
Enhanced SuperSpeed Function


USB4 Device
PCIe UP Adapter
USB4 Port
USB3 UP Adapter
PCIe Function
USB 2.0 Function
Device Router
TMU
DP OUT Adapter
DP Display
Enhanced SuperSpeed Function

USB4 versus Thunderbolt

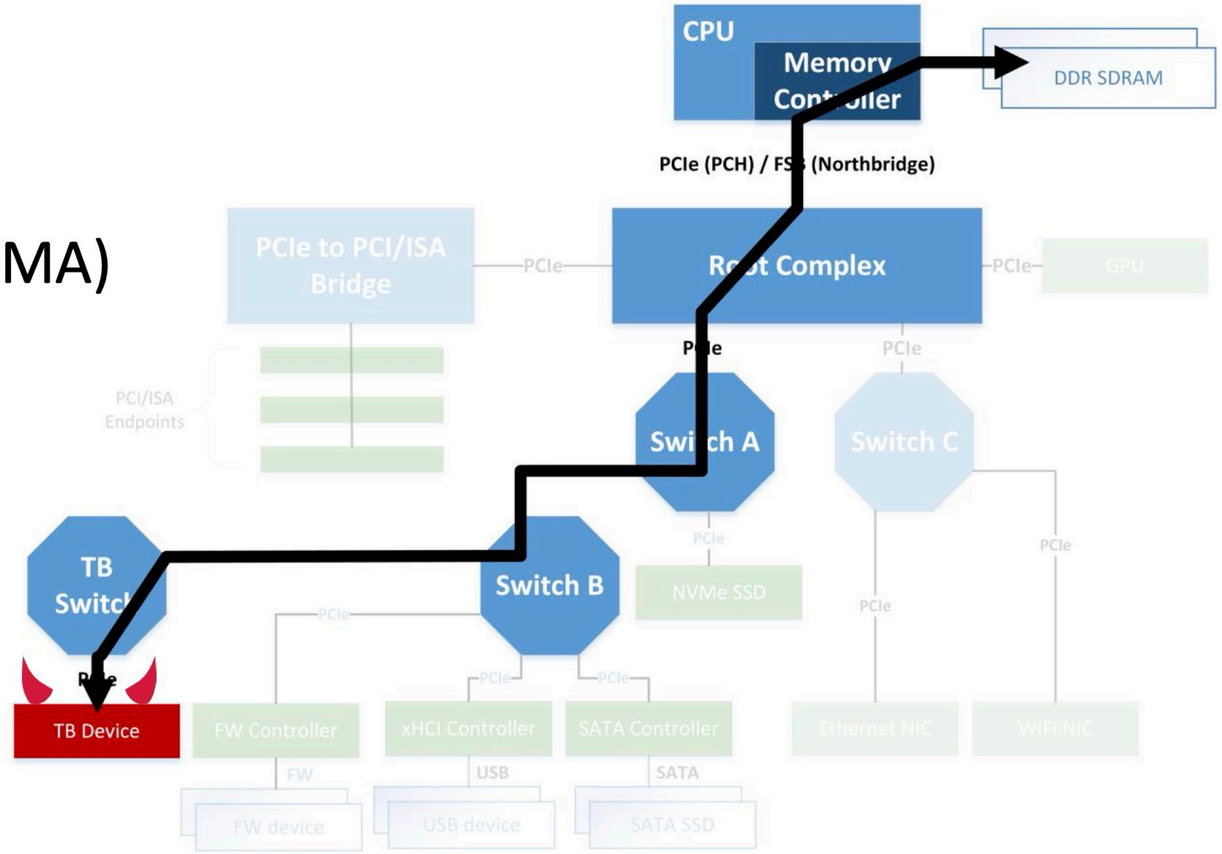
- As an attack vector, both can give the attacker **PCI Express access**
- They are, however, **different utilizations** of the USB Type-C interface
- Their activation sequence via USB PD on the CC line differs
- They may not be both supported by the same port - check the computer manual
- When striving to get PCIe access, we shall try both ways
  - as one may be blocked/not available, while the other one could be there

USB Type-C plus PCIe/DMA Attack Vector

- Part #1
  - getting through the USB-C PD controller and TB host controller combo
  - for instance, *Thunderspy* by Björn Ruytenberg, https://thunderspy.io/
- Part #2
  - lateral movement in PCI Express bus environment
  - for instance, *PCILeech* by Ulf Frisk, https://github.com/ufrisk/pcileech
  - also relevant, *Thunderclap: Exploring Vulnerabilities in Operating System IOMMU Protection via DMA from Untrustworthy Peripherals* by A. Theodore Markettos et al.
  - https://thunderclap.io/wp-content/uploads/2024/01/thunderclap-paper-ndss2019.pdf

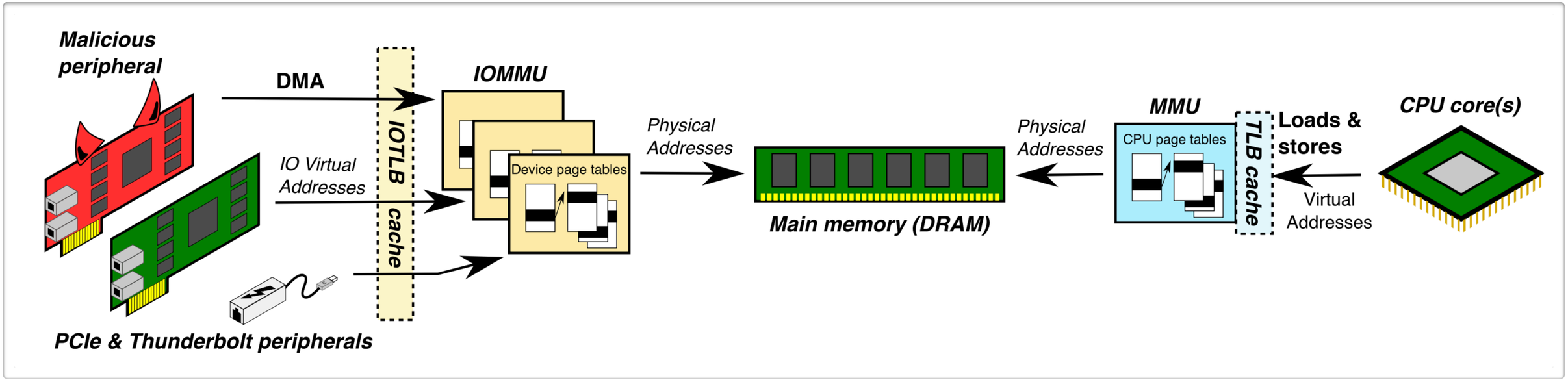
DMA attacks

- **Thunderbolt 1**: no protection against physical attacks
- Plug in malicious device
  → Unrestricted R/W memory access (DMA)
- Access data from encrypted drives
- Persistent access possible, by e.g. installing rootkit



-- Ruytenberg, 2020

IOMMU in Action



-- https://thunderclap.io/

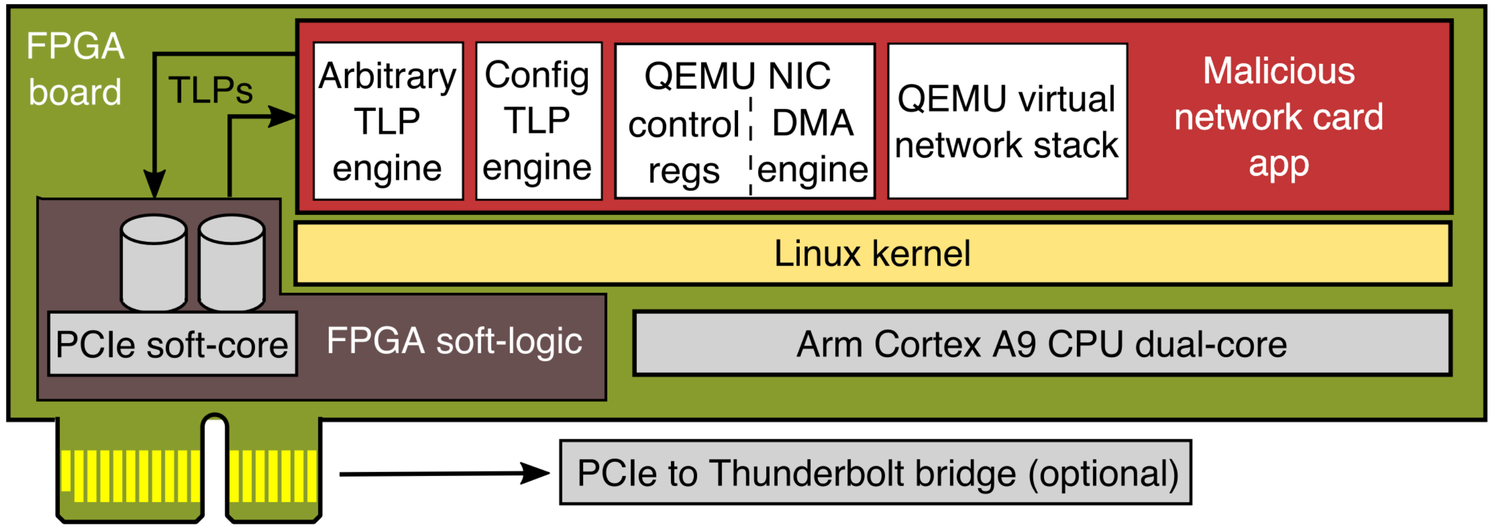


Fig. 4: Implementation of fully-functional network card using a QEMU device model running on FPGA

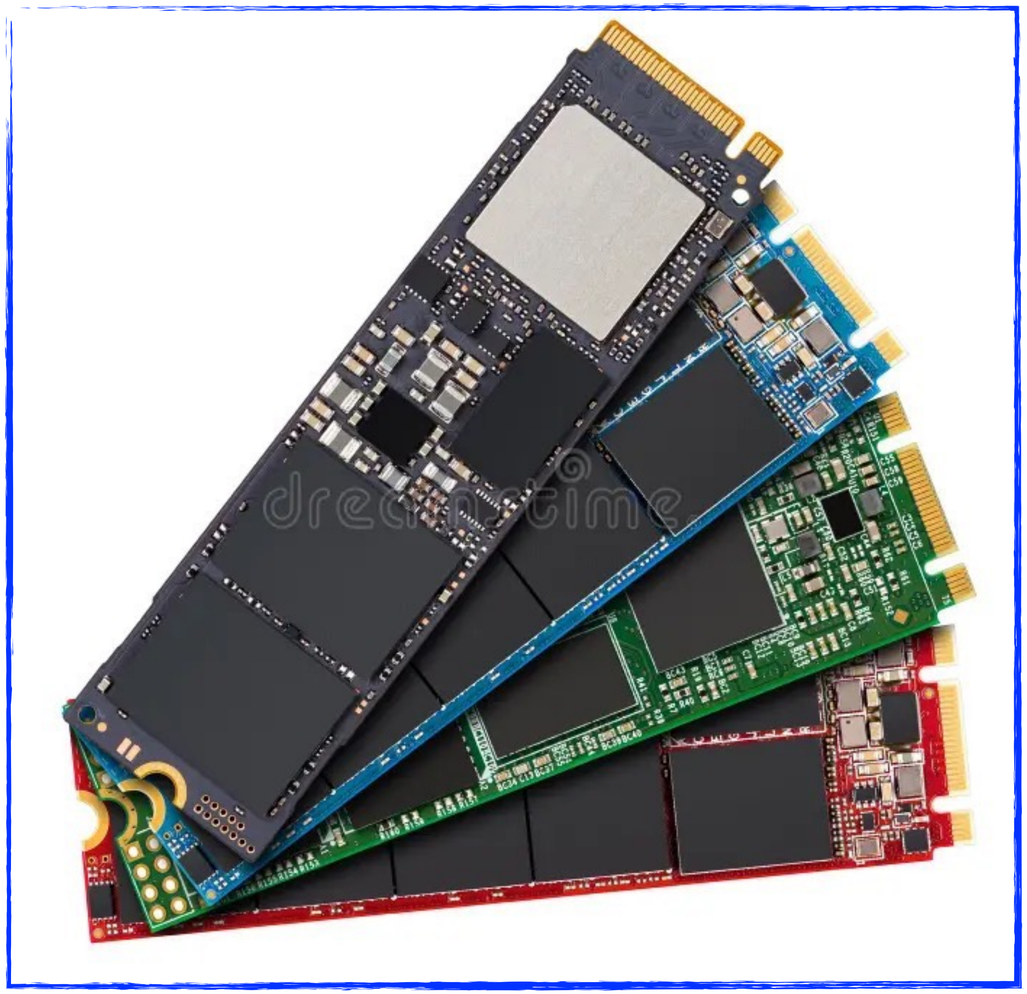
-- https://thunderclap.io/

NVMe Solid State Drive

- NVMe (Non-Volatile Memory Express) is SSD standard incorporating disk controller and disk host adapter into one device connecting directly to PCI Express system bus

  - does not require PCIe to SATA host adapter

  - usually uses M.2 connector factor regarded as yet-another PCIe plug here



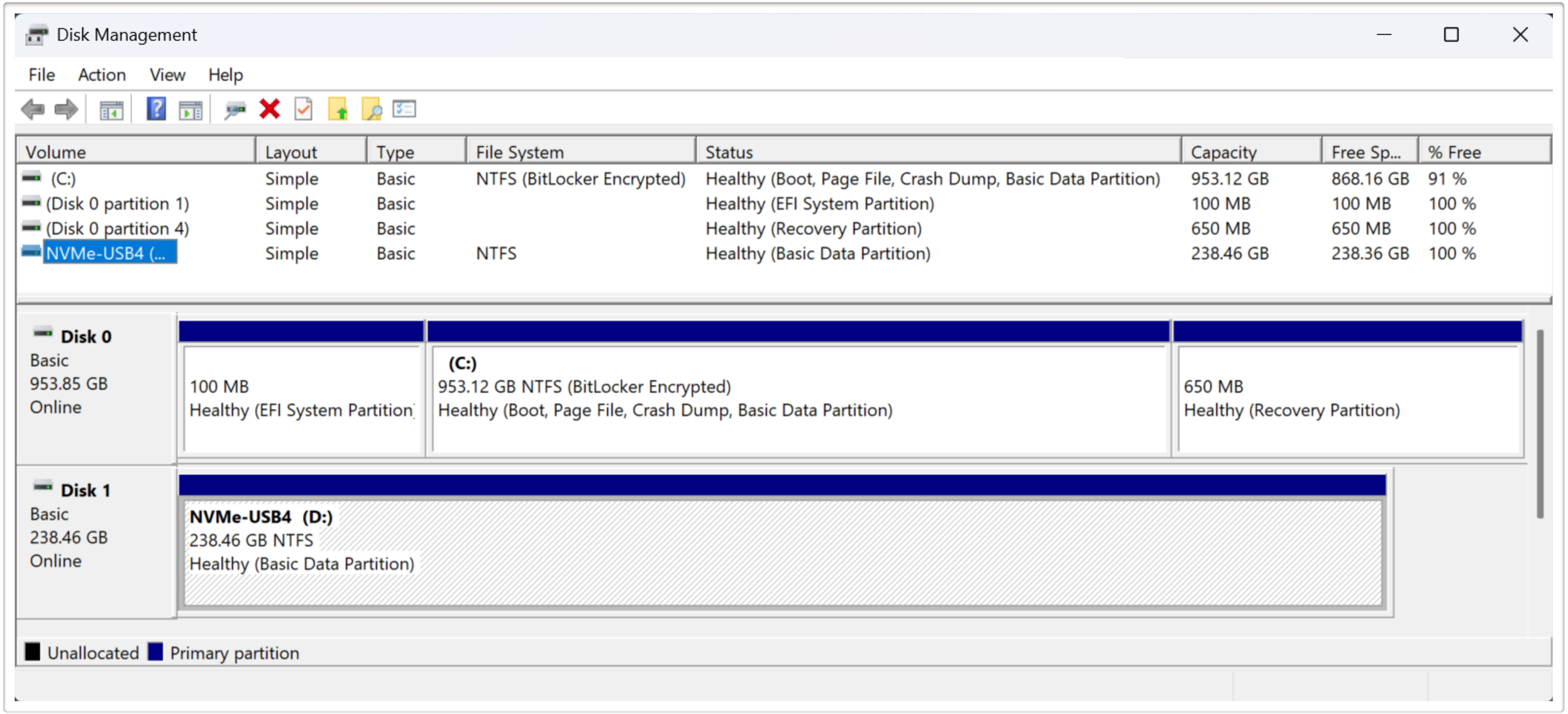
Thunderbolt / USB4 to NVMe

- In fact, having PCIe adapter immediately implies having NVMe, as this is just a question of a connector format
  - CEM (Card ElectroMechanical connector - i.e. PCIe classic) versus M.2
- Can be used as a security policy bypass in case of USB Mass Storage device class being actively blocked
  - from the USB Type-C viewpoint, this is not a USB peripheral, as it runs through the PCIe channel instead
  - so, it may be totally invisible for a plain USB filtering SW

HyperDrive USB4 NVMe Case

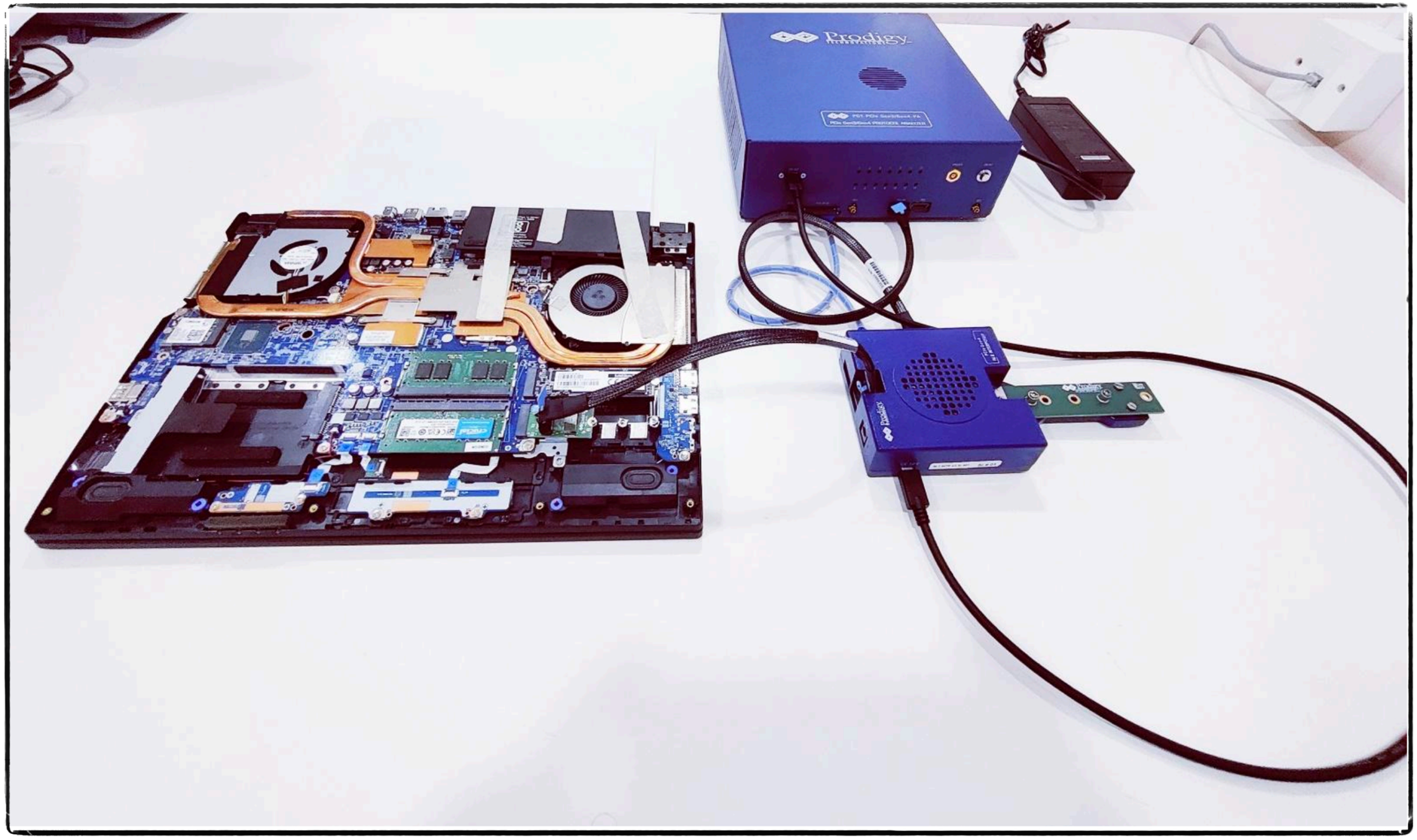
NVMe SSD inserted in the case

USB Type-C providing PCIe access via USB4



note BitLocker did not automatically cover the external NVMe

-- MS Windows 11 Professional

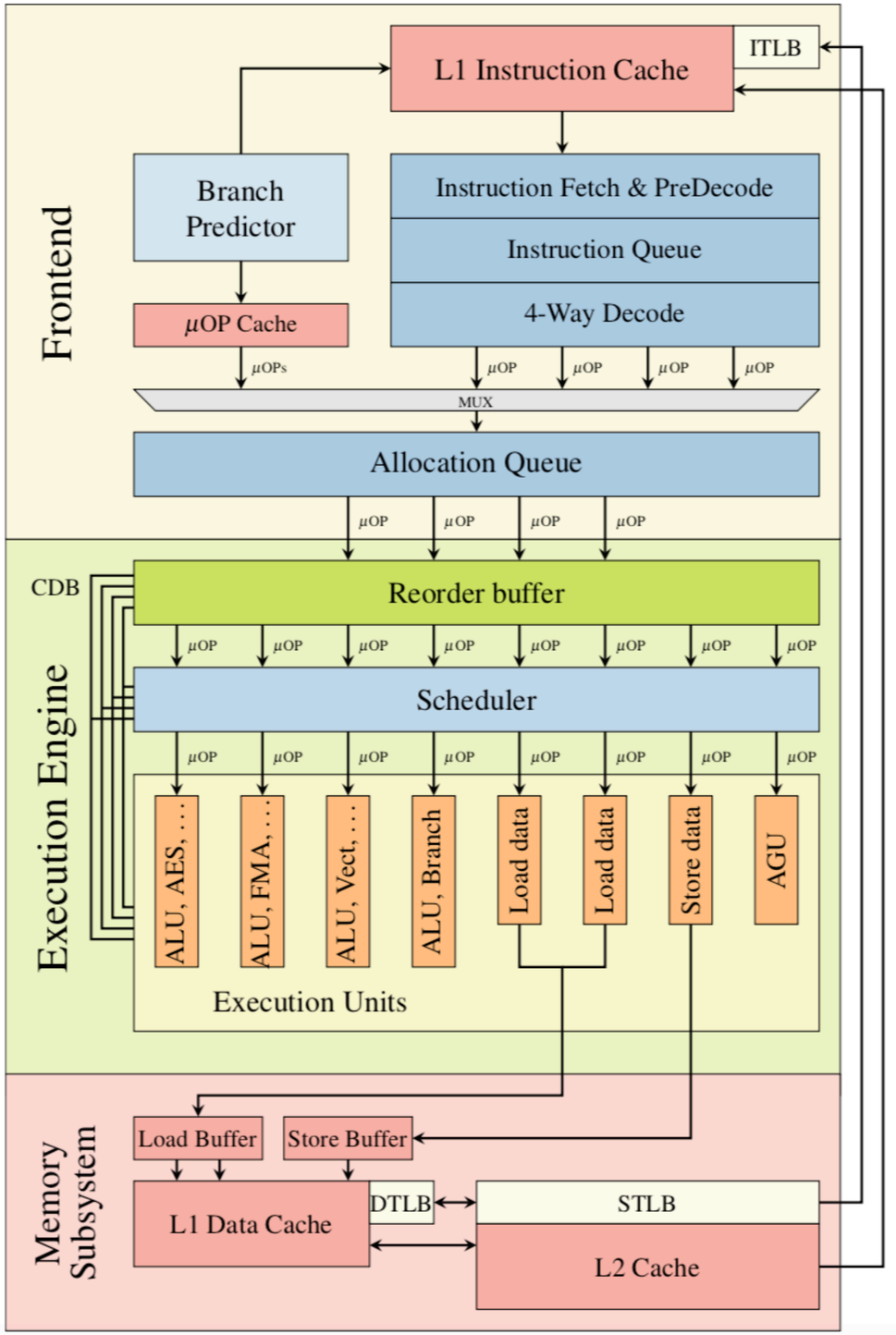


Prodigy Technovations PCIe Protocol Analyzer

CPU: Microarchitecture Vulnerabilities

Intel Skylake Microarchitecture (single core)

- Predicted instruction flow decoded into µOPs
- Out-of-order and speculative execution of µOPs by individual units
- Architecture main state vs. transient microarchitecture state
- Plenty of shared resources inducing side and covert channels
  - these are leaking the microarchitecture state, so making the effects of the transient execution observable



“From a security perspective, speculative execution involves executing a program in possibly incorrect ways.”

–Spectre Attack Paper

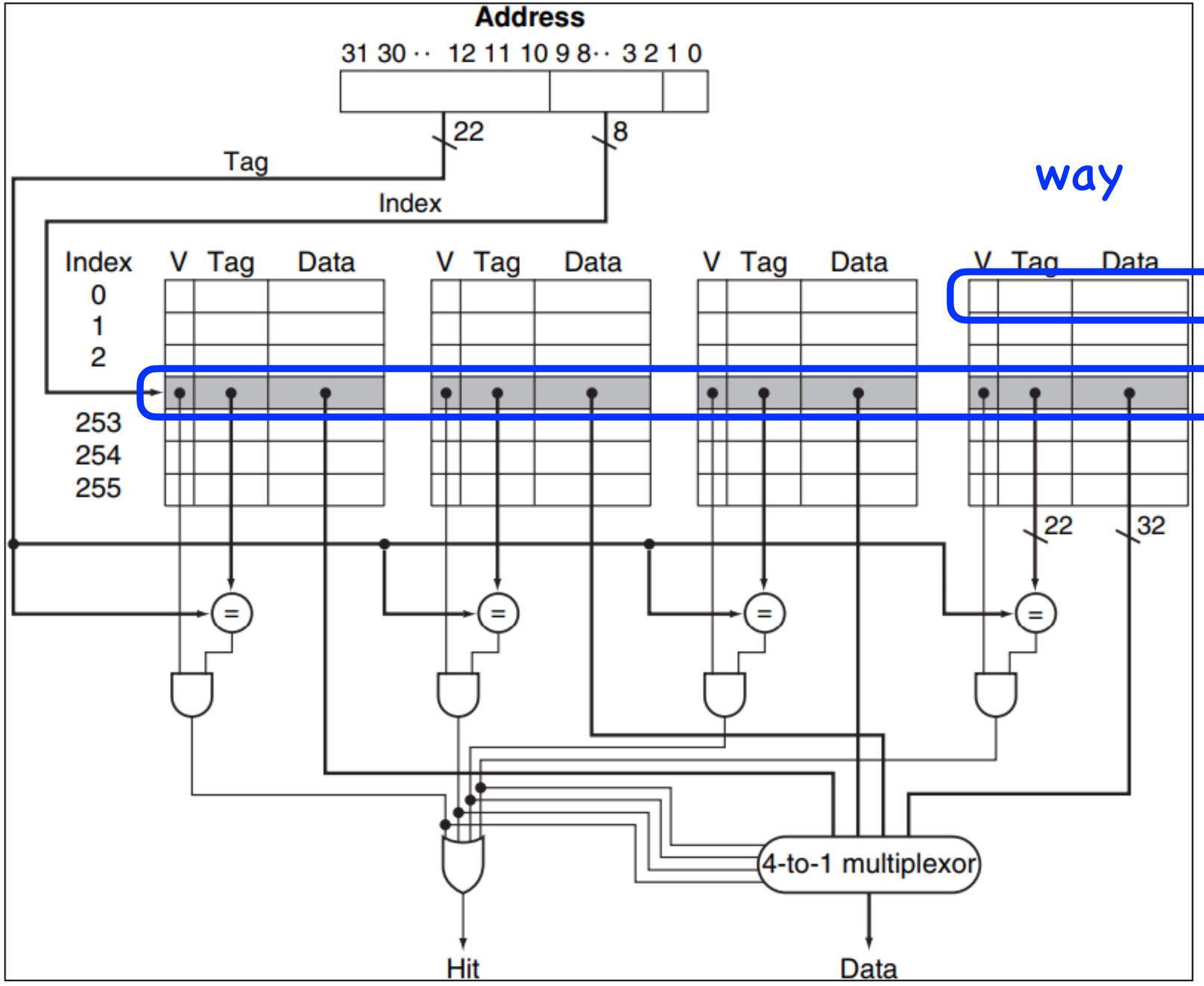
Meltdown

```
1 ; rcx = kernel address
2 ; rbx = probe array
3 retry:
4 mov al, byte [rcx]
5 shl rax, 0xc
6 jz retry
7 mov rbx, qword [rbx + rax]
```

Channel invocation from the attacker's process

-- https://meltdownattack.com/

4-way set associative cache 32b example



line size = 32 b

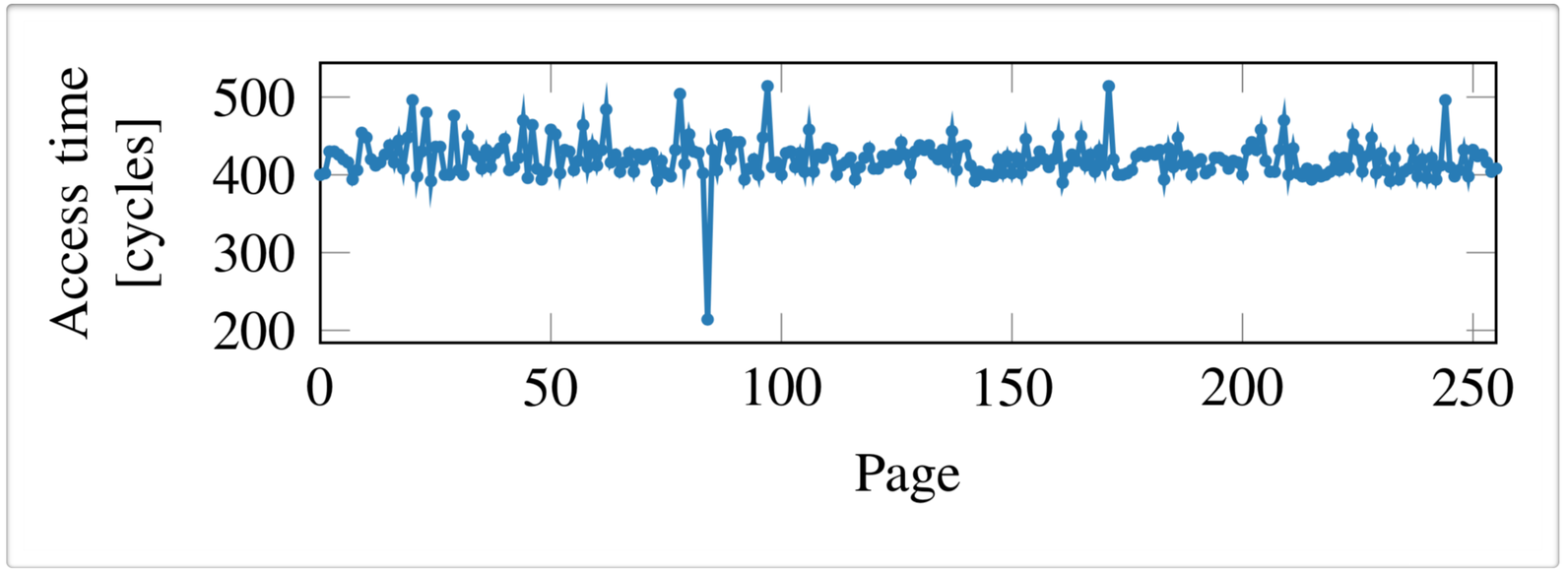
way

line

set of lines

Index ~ set no.

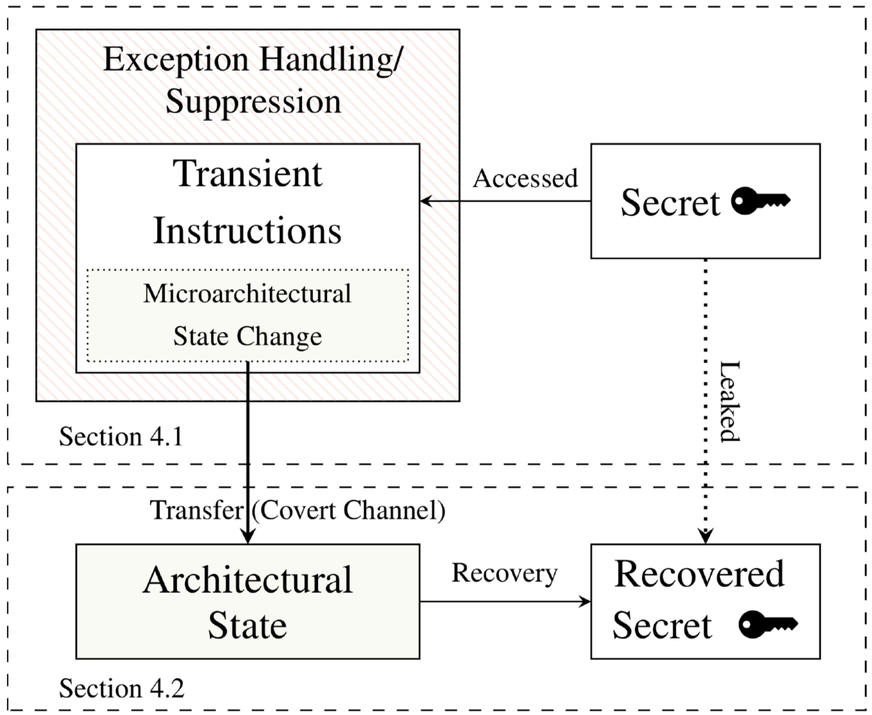
Channel Reception



-- https://meltdownattack.com/

Meltdown Covert/Side Channel

- Allows accessing privileged memory regions from an unprivileged process
  - this actually may include the complete image of the whole physical memory



-- https://meltdownattack.com/

User Space to Another User Space Access via Kernel Maps

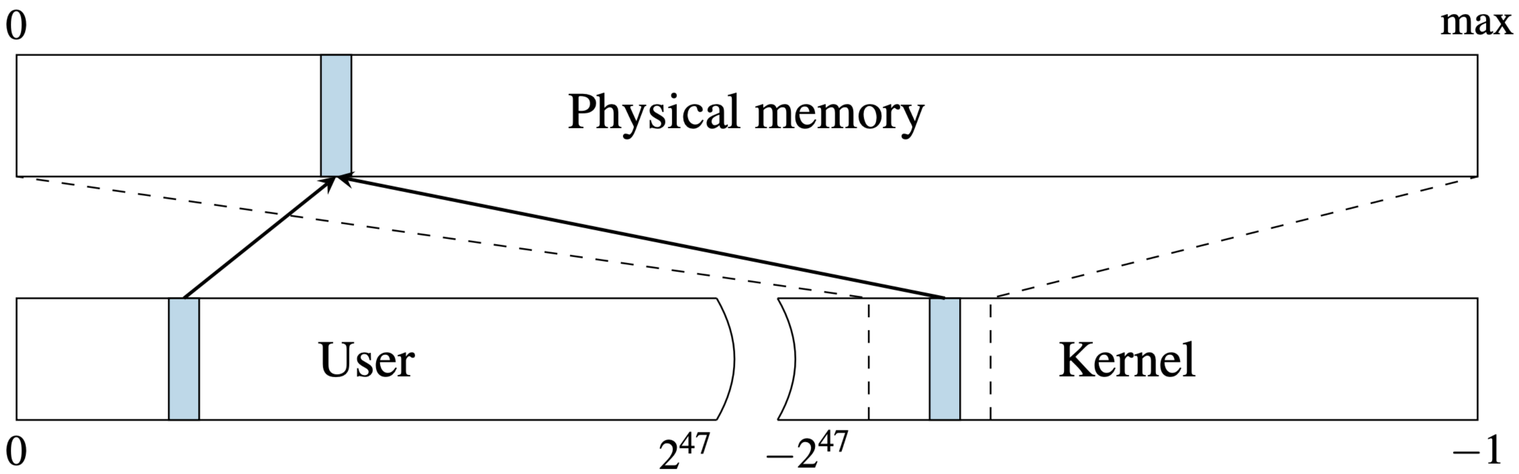


Figure 2: The physical memory is directly mapped in the kernel at a certain offset. A physical address (blue) which is mapped accessible to the user space is also mapped in the kernel space through the direct mapping.

-- https://meltdownattack.com/

Canonical Addressing of x86-64 in IA32e Mode

- Let us assume **48-bit canonical** version for 4-level paging
  - bits 63:47 of the linear (virtual) address are identical and sign-extension of the most significant bit
- **0xFFFF 8** is considered a kernel-space address prefix
- As we are on 64-bit architecture, modulo 2^{64} generally applies

Noting that $$\sum_{i=47}^{63} 2^i \equiv \sum_{i=47}^{63} 2^i - 2^{64} = -2^{47} \pmod{2^{64}}$$

we can consider the kernel-space address interval as $-2^{47} \ldots -1$ with low to high order preserved

-- *Intel 64 and IA-32 Architectures Software Developer's Manual Volume 3: System Programming Guide*, Intel Corp, March 2025

Spectre

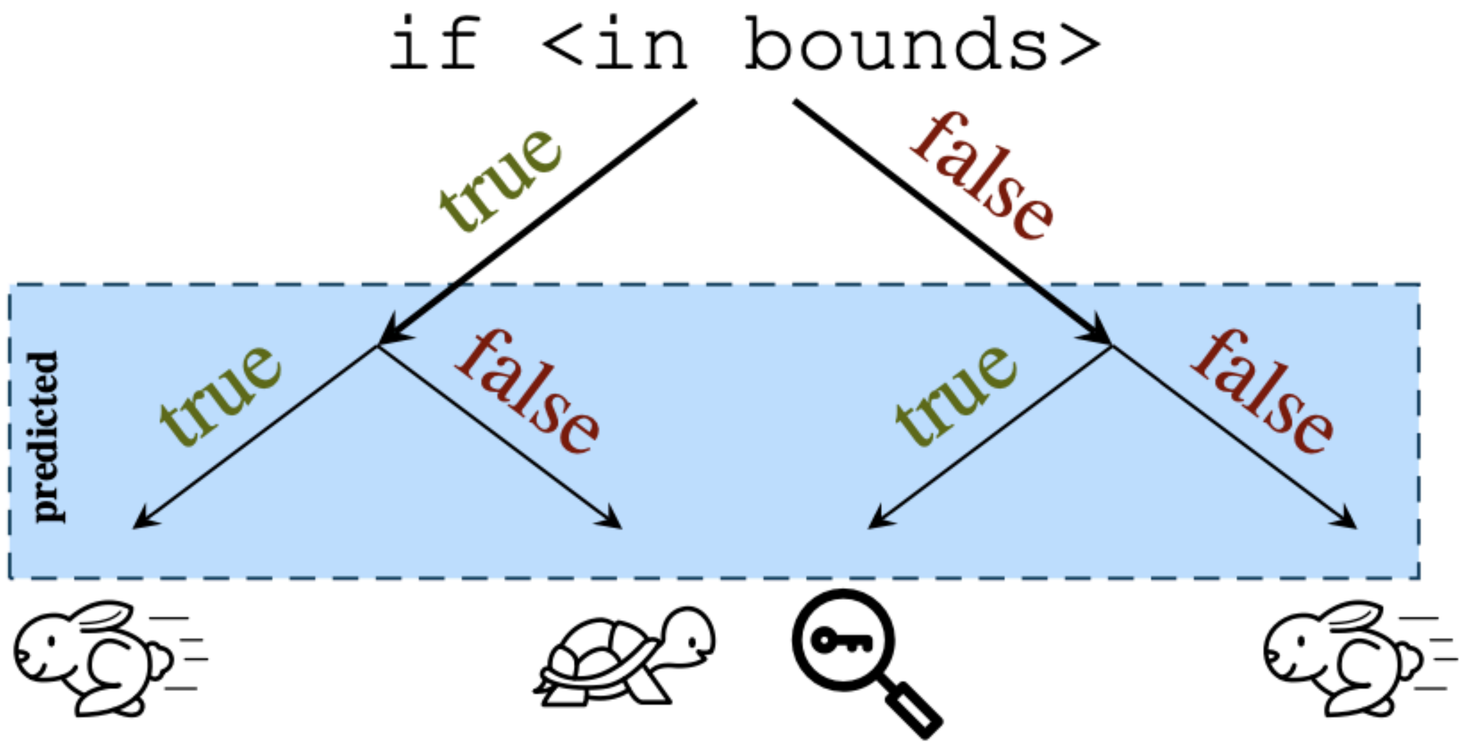
- Targets the memory of a victim process from another (possibly user-space) process
  - also possible within the same process - e.g. JavaScript sandbox escape
- Abuses a latent transmitting gadget already present in the victim process

```
if (x < array1_size)
    y = array2[array1[x] * 4096];
```

Spectre Variant 1 - conditional branch misprediction

-- https://spectreattack.com/

```
if (x < array1_size)
    y = array2[array1[x] * 4096];
```

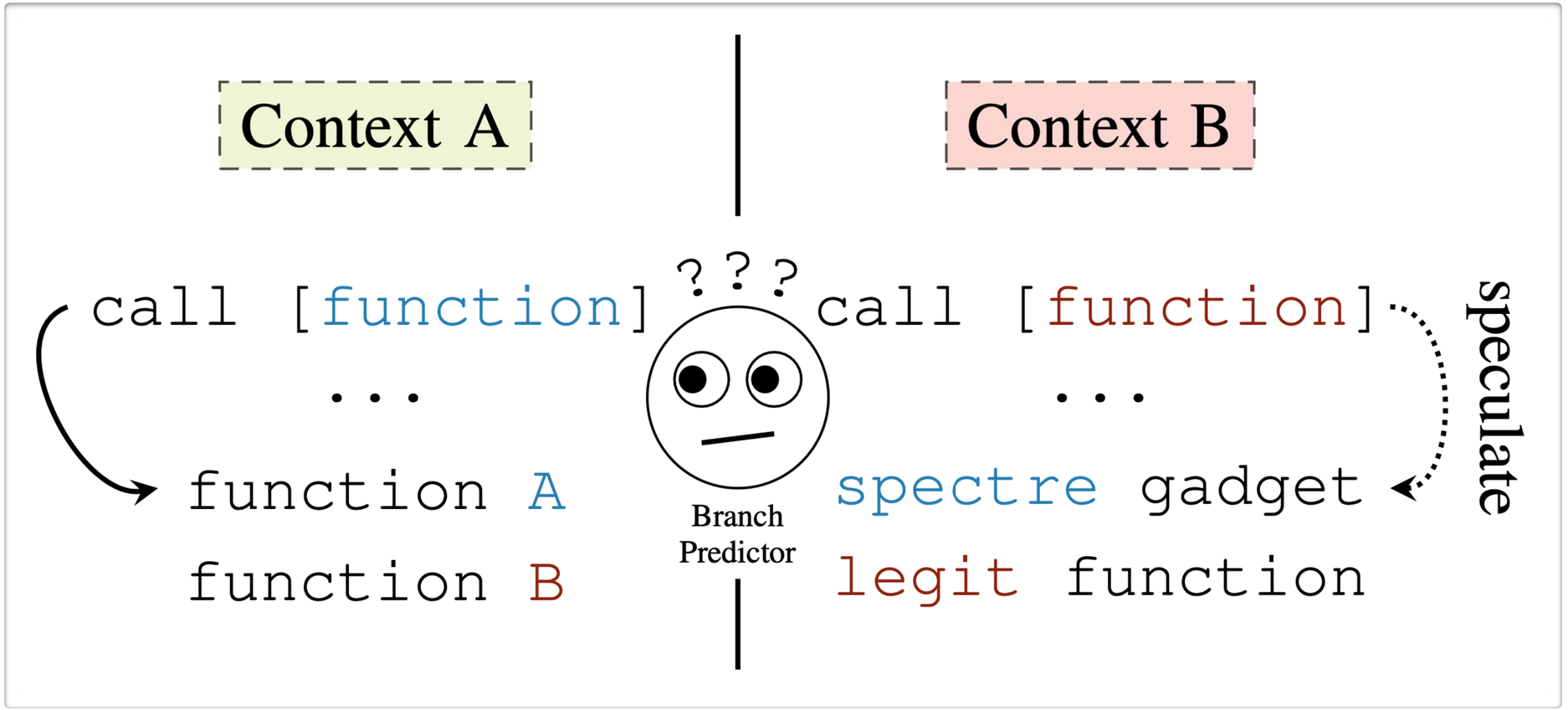


actual value

predicted value

-- https://spectreattack.com/

Spectre - Variant 2



Indirect branch target misprediction

-- https://spectreattack.com/

Return-Oriented Programming (ROP) Similarities

- The attacker relies on the code that is already existing in the attacked process memory map - such a code is called ***gadget***

  - also similar to LOLBIN mentioned with Powershell above

- In Spectre Variant 2, the gadget is invoked via indirect jump, having a similar role to stack-driven returns in ROP here

  - notably, the gadget does not have to terminate cleanly, since this all happens in a transient microarchitecture context

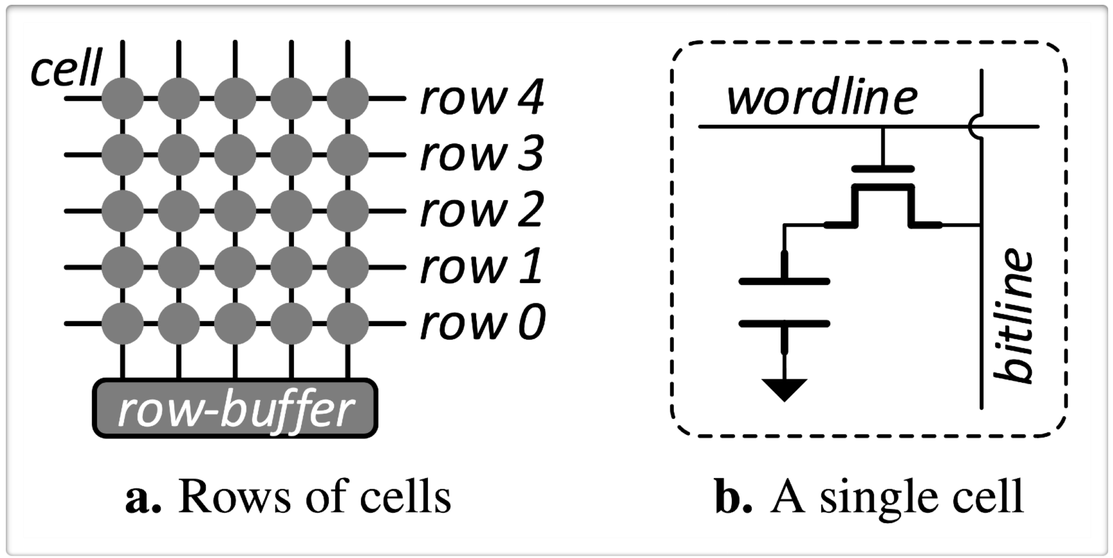
Spectre Variant 2 Gadget Example

```
adc  edi,dword ptr [ebx+edx+13BE13BDh]
adc  dl,byte ptr [edi]
```

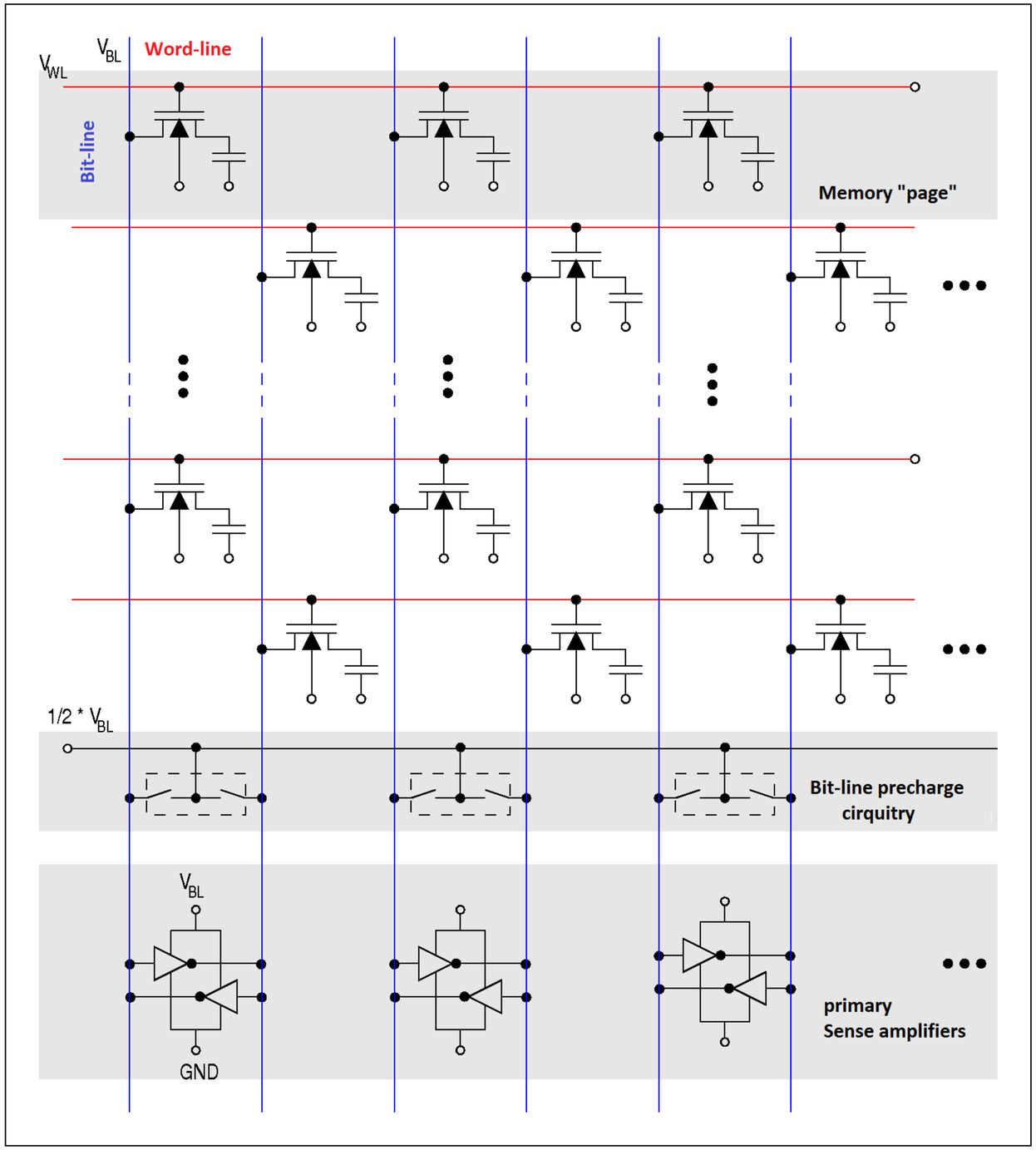
- Found in `ntdll.dll` on both Windows 8 and Windows 10
- Assumes the attacker can control `edi` and `ebx`, while knowing `edx`
  - the assumption has to hold **before the indirect branch occurs** that in turn leads to the gadget invocation
  - so, the attacker has to **find both the susceptible branch together with the useful gadget** in the victim *context* memory map
- Setting `ebx = m - edx - 0x13BE13DB` selects the memory location *m* whose content is to be transmitted by the cache side channel by fetching the `edi` address in the second `adc` instruction

-- https://spectreattack.com/

DRAM: Fault Induction, a.k.a. Row Hammering



-- [Kim et al., 2014]



-- https://en.wikipedia.org/wiki/Dynamic_random-access_memory

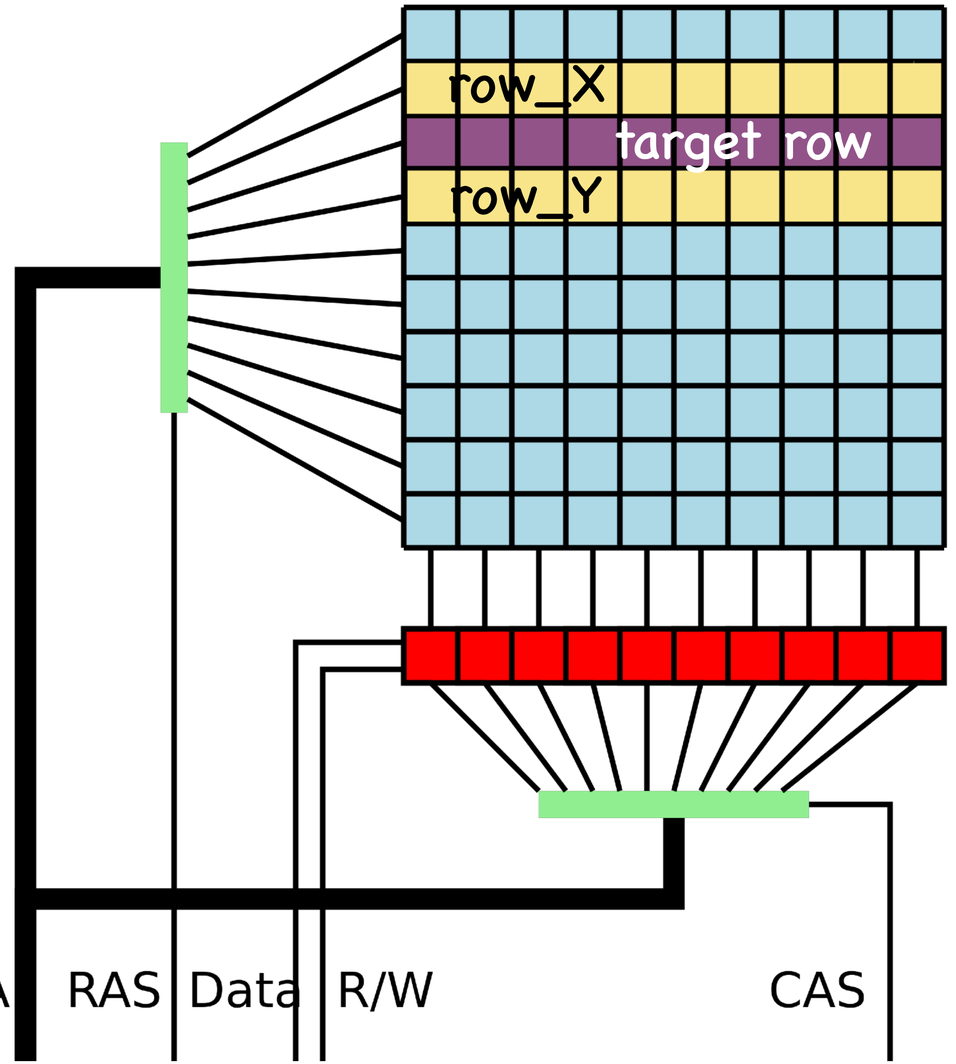
“When a wordline’s voltage is toggled repeatedly, some cells in nearby rows leak charge at a much faster rate.”

– Kim et al., 2014

Row Hammer Principle Illustrated

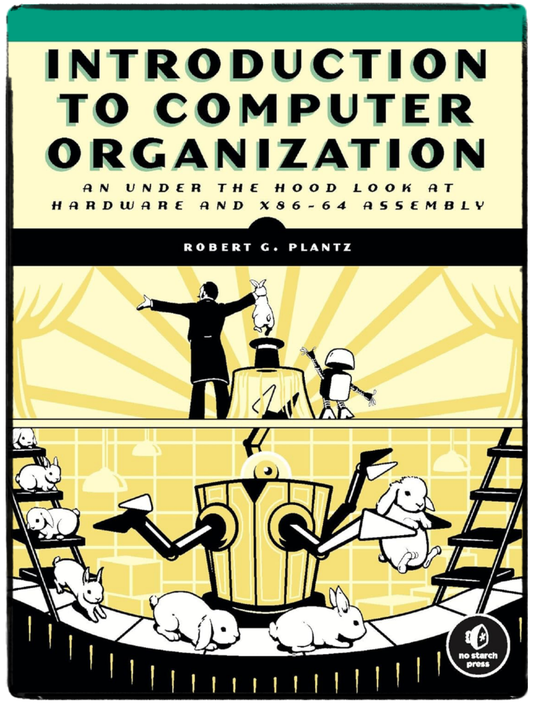
```
row_hammer:
      mov EAX, [ADDR_X]
      mov EBX, [ADDR_Y]
      clflush [ADDR_X]
      clflush [ADDR_Y]
      mfence
      jmp row_hammer
```

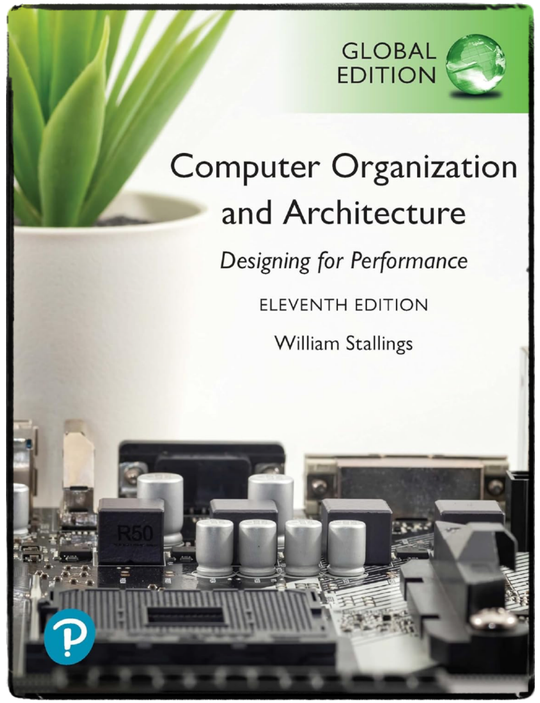
-- [Kim et al., 2014]

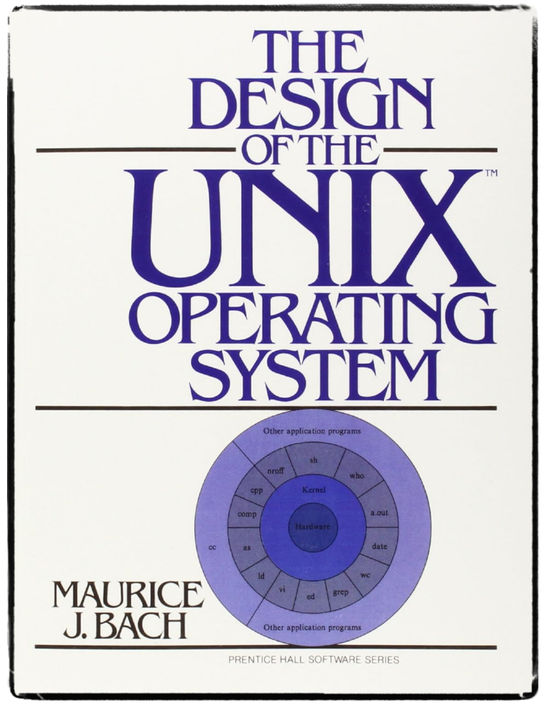


-- https://en.wikipedia.org/wiki/Row_hammer

Shall we recommend some intro books for you now...







- plus then any title on UNIX / Linux *system programming* that you are comfortable with

- distinguish ***system*** vs ***kernel*** programming as well as computer ***architecture*** vs ***organization***

Thank you for your attention

Co-funded by the European Union
Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Cybersecurity Competence Centre. Neither the European Union nor the European Cybersecurity Competence Centre can be held responsible for them

Supported by ECCC
The project funded under Grant Agreement No. 101158662 is supported by the European Cybersecurity Competence Centre

History (year-month-day format)

- 2026-03-10, version 1.0 released