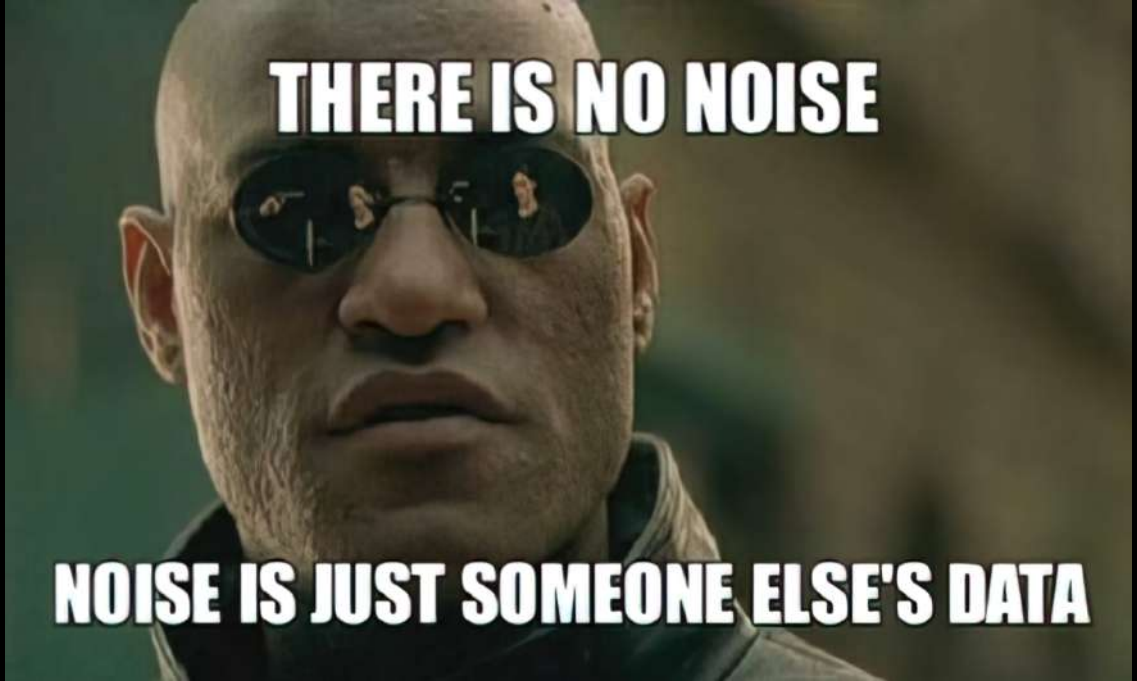
Faulting Hardware from Software and Sustainable Mitigations

Daniel Gruss

2024-04-04

Graz University of Technology


side channel
= obtaining meta-data and
deriving secrets from it
CHANGE MY MIND
imgflip.com

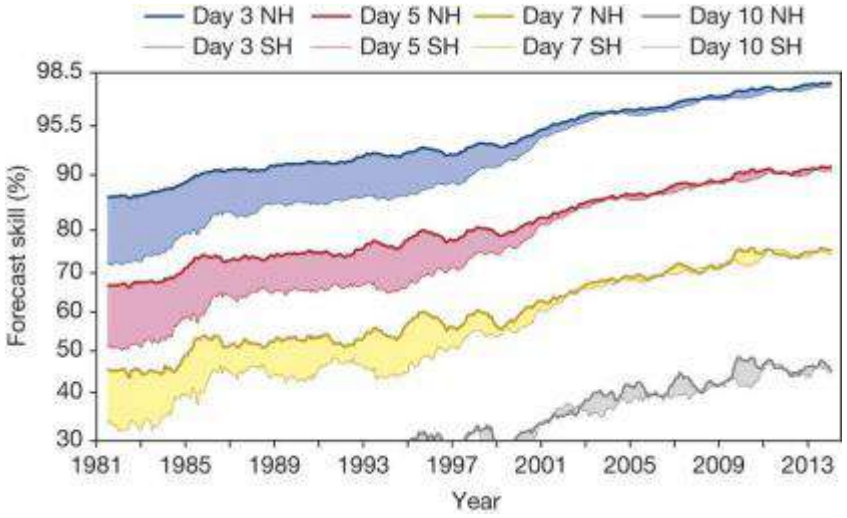

THERE IS NO NOISE
NOISE IS JUST SOMEONE ELSE'S DATA

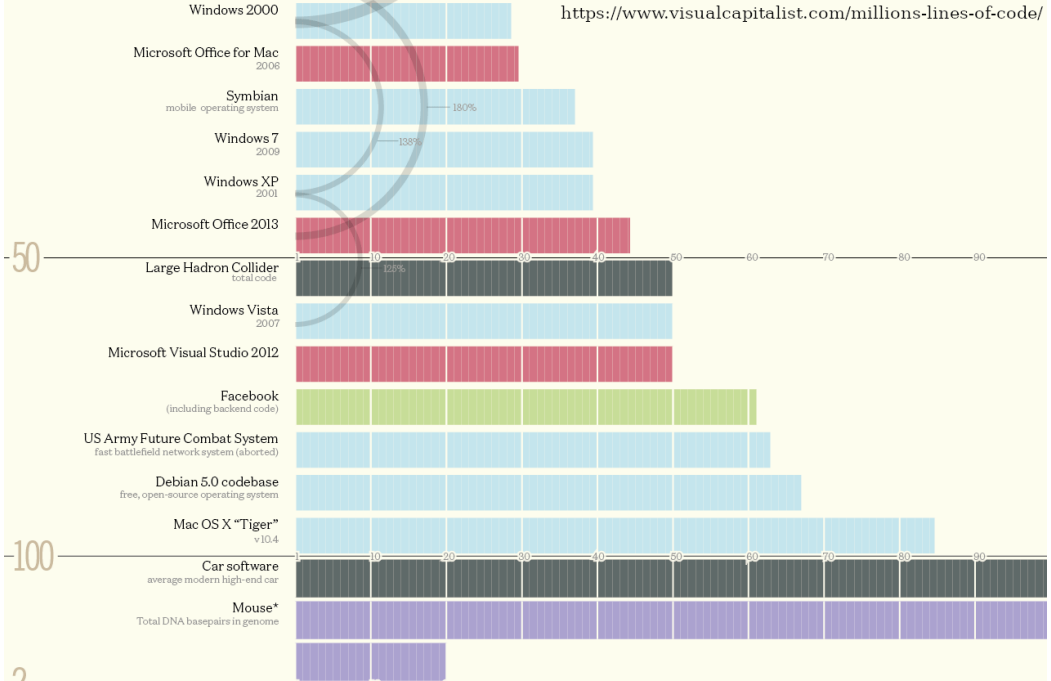
Side Channels are Everywhere


How did this song go again?
Please don't...
Side Channels are everywhere ...
imgflip.com

What about Mitigations?

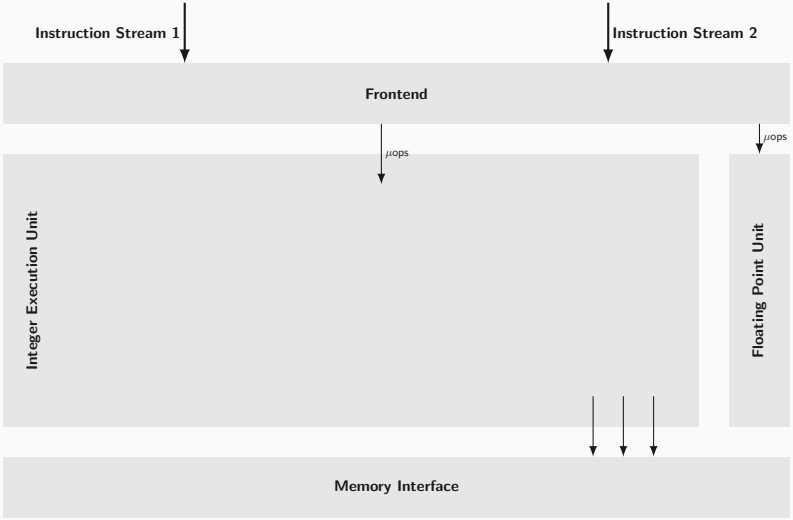
security

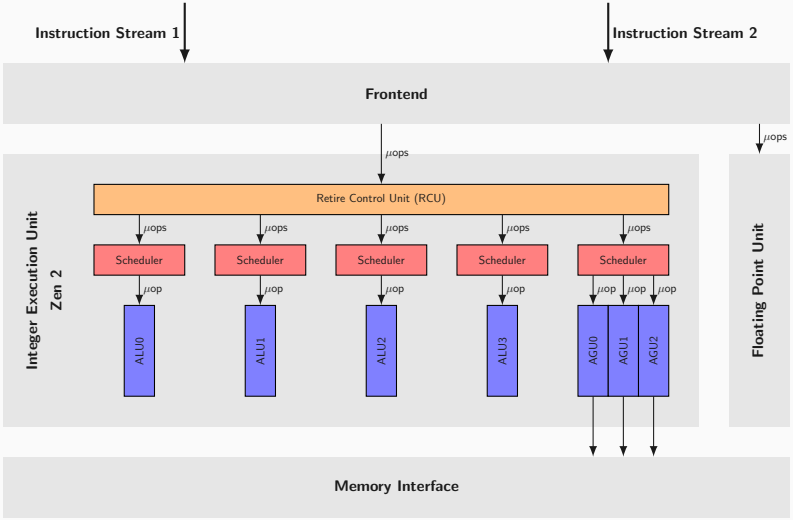

Day 3 NH
Day 5 NH
Day 7 NH
Day 10 NH
Day 3 SH
Day 5 SH
Day 7 SH
Day 10 SH
98.5
95.5
90
80
70
60
50
40
30
Forecast skill (%)
1981
1985
1989
1993
1997
2001
2005
2009
2013
Year

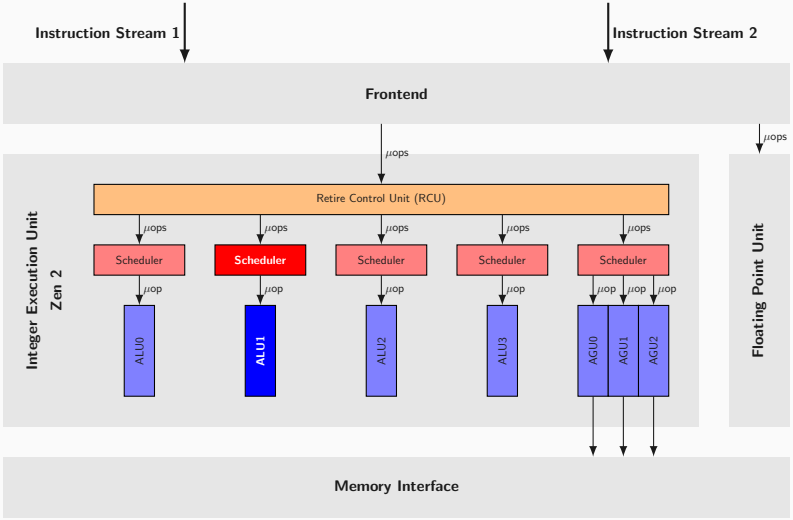

https://www.visualcapitalist.com/millions-lines-of-code/
Windows 2000
Microsoft Office for Mac
2006
Symbian
mobile operating system
180%
Windows 7
2009
138%
Windows XP
2001
Microsoft Office 2013
50
1
10
20
30
40
50
60
70
80
90
Large Hadron Collider
total code
128%
Windows Vista
2007
Microsoft Visual Studio 2012
Facebook
(including backend code)
US Army Future Combat System
fast battlefield network system (aborted)
Debian 5.0 codebase
free, open-source operating system
Mac OS X "Tiger"
v10.4
100
1
10
20
30
40
50
60
70
80
90
Car software
average modern high-end car
Mouse*
Total DNA basepairs in genome
2

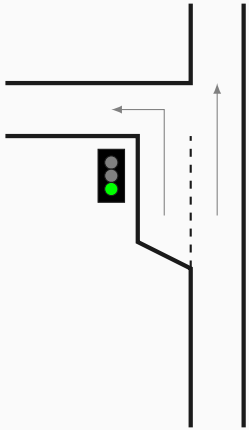
Models of Nature can get Arbitrarily Close to the Truth

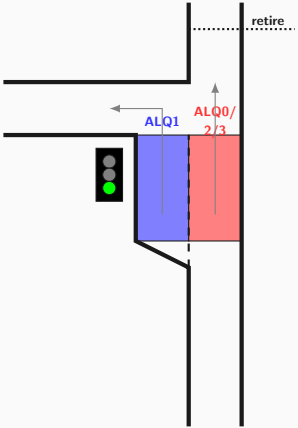
Systems Gain Complexity faster
than our Models can keep up with

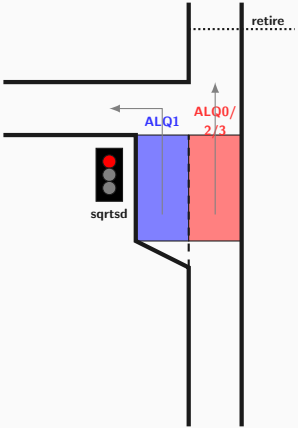

Instruction Stream 1
Instruction Stream 2
Frontend
µops
µops
Integer Execution Unit
Floating Point Unit
Memory Interface

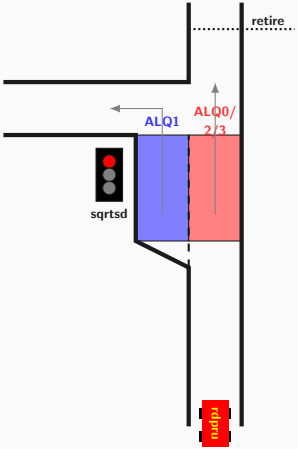

Instruction Stream 1
Instruction Stream 2
Frontend
µops
µops
Retire Control Unit (RCU)
µops
µops
µops
µops
µops
Scheduler
Scheduler
Scheduler
Scheduler
Scheduler
µop
µop
µop
µop
µop
µop
µop
ALU0
ALU1
ALU2
ALU3
AGU0
AGU1
AGU2
Integer Execution Unit
Zen 2
Floating Point Unit
Memory Interface

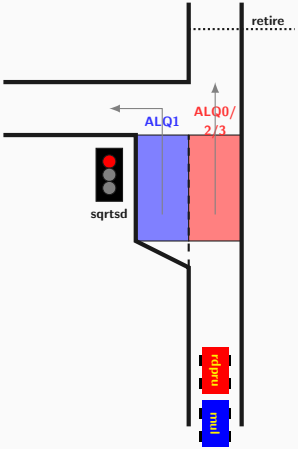

Instruction Stream 1
Instruction Stream 2
Frontend
µops
µops
Retire Control Unit (RCU)
µops
µops
µops
µops
µops
Scheduler
Scheduler
Scheduler
Scheduler
Scheduler
µop
µop
µop
µop
µop
µop
µop
ALU0
ALU1
ALU2
ALU3
AGU0
AGU1
AGU2
Integer Execution Unit
Zen 2
Floating Point Unit
Memory Interface

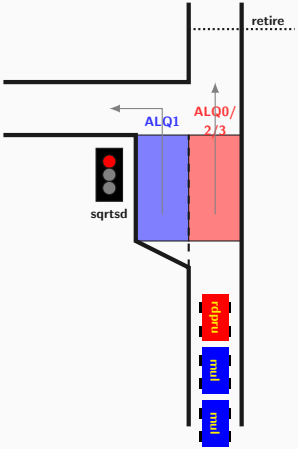


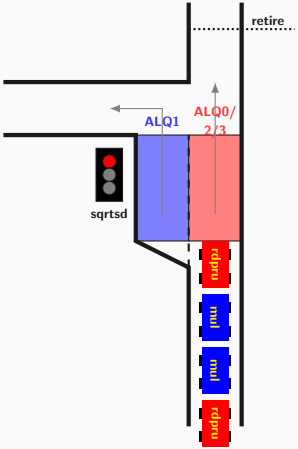

retire
ALQ1
ALQ0/
2/3

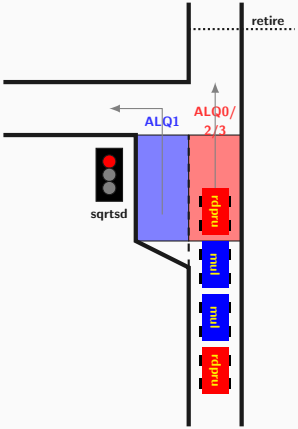

retire
ALQ1
ALQ0/
2/3
sqrtsd

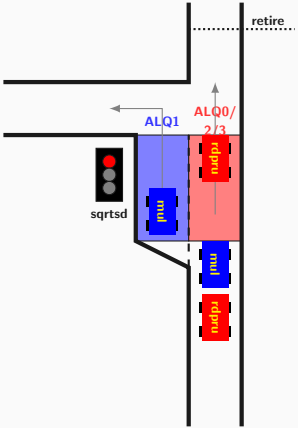

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn

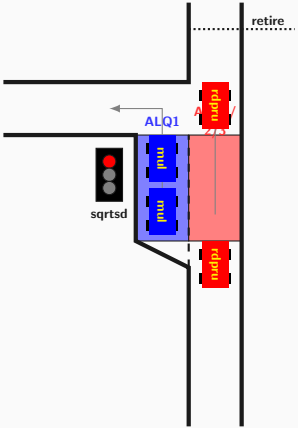

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul

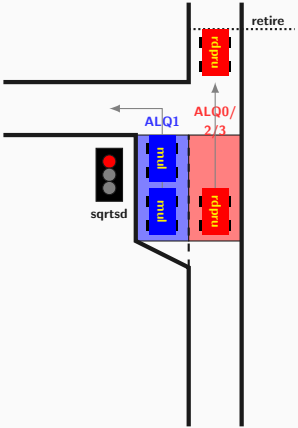

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul
mul

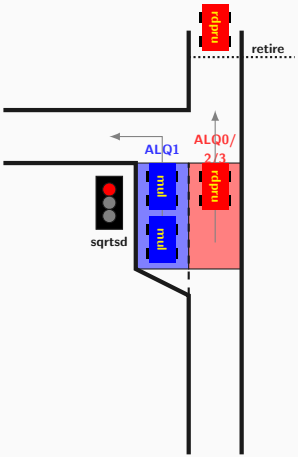

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul
mul
rdpn

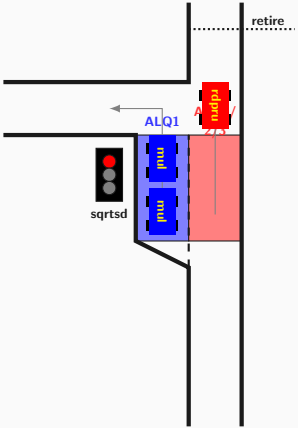

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
rwl
rwl
rdpn

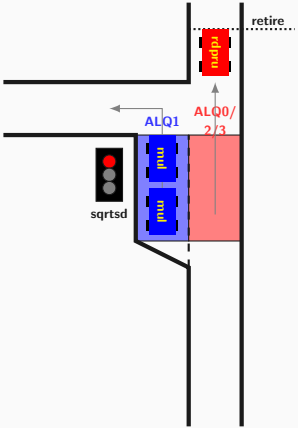

retire
ALQ1
ALQ0/
2/3
rdpn
rdpn
rdpn
mul
mul
sqrtsd

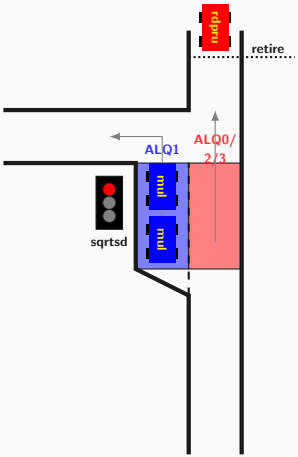

retire
ALQ1
sqrtsd

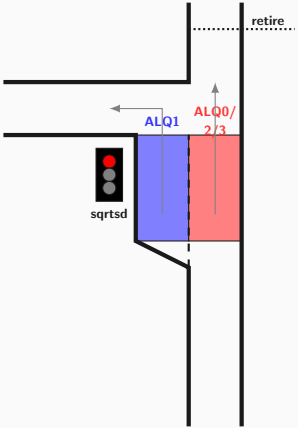

retire
rdpn
ALQ1
ALQ0/
2/3
mul
mul
rdpn
sqrtsd

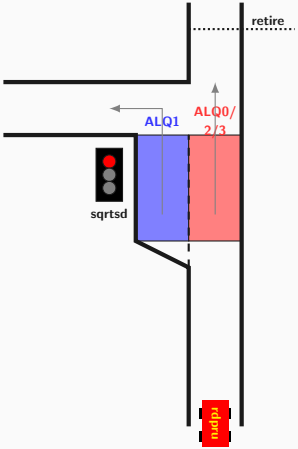

rdpn
retire
ALQ1
ALQ0/
2/3
rdpn
mul
mul
sqrtsd

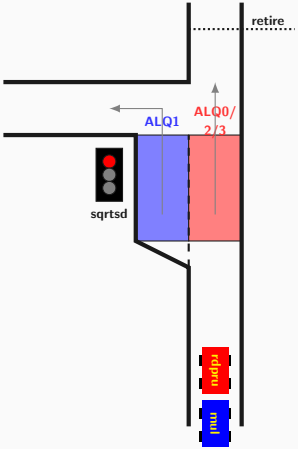

retire
ALQ1
sqrtsd

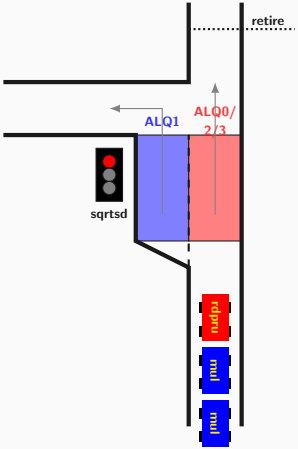

retire
rdprn
ALQ1
ALQ0/
2/3
mwf
mwf
sqrtsd

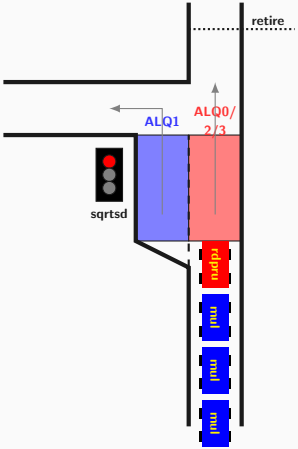

idpm
retire
ALQ1
ALQ0/
2/3
mul
mul
sqrtsd

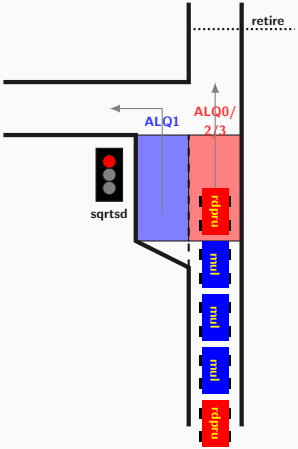

retire
ALQ1
ALQ0/
2/3
sqrtsd

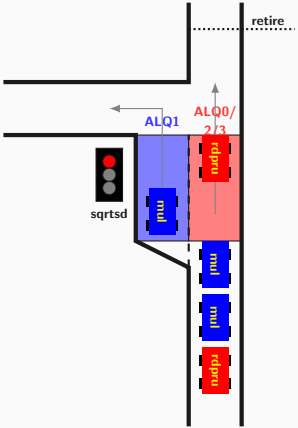

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn

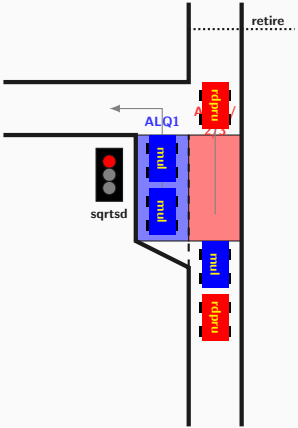

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul

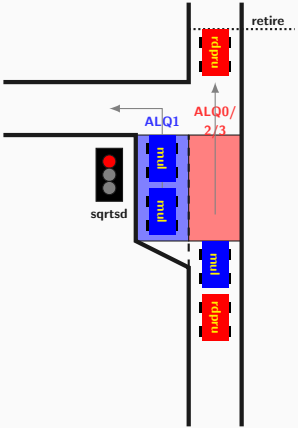

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul
mul

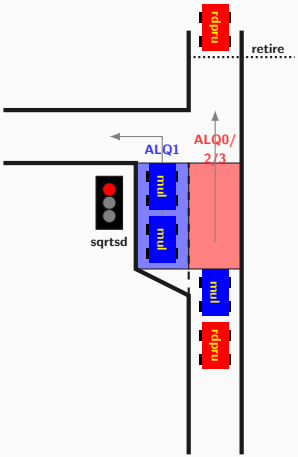

retire
ALQ1
ALQ0/
2/3
sqrtsd
dqrt
mul
mul
mul

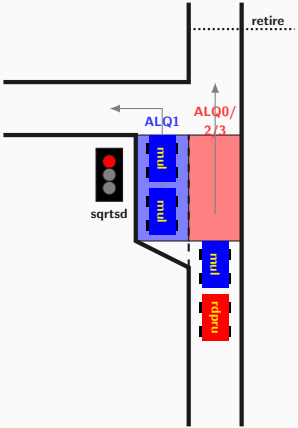

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdqn
mul
mul
mul
rdqn

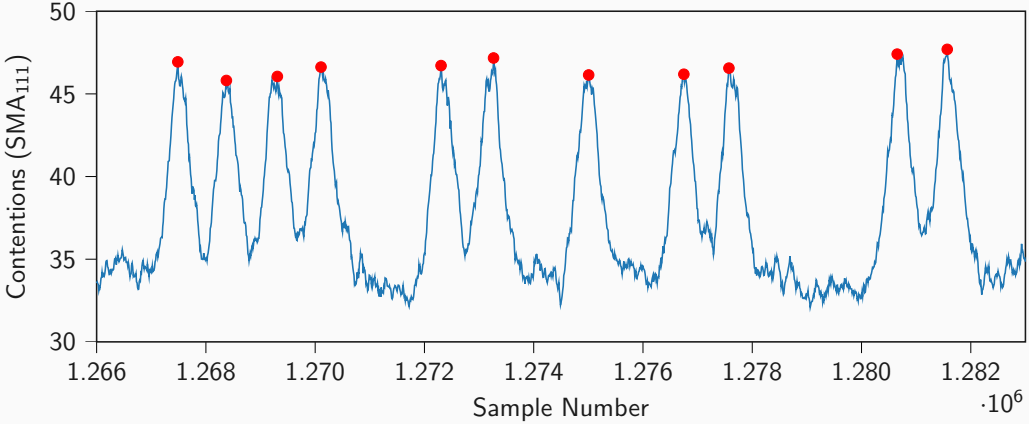

retire
ALQ1
ALQ0/
2/3
rdpn
sqrtsd
mul
mul
mul
rdpn

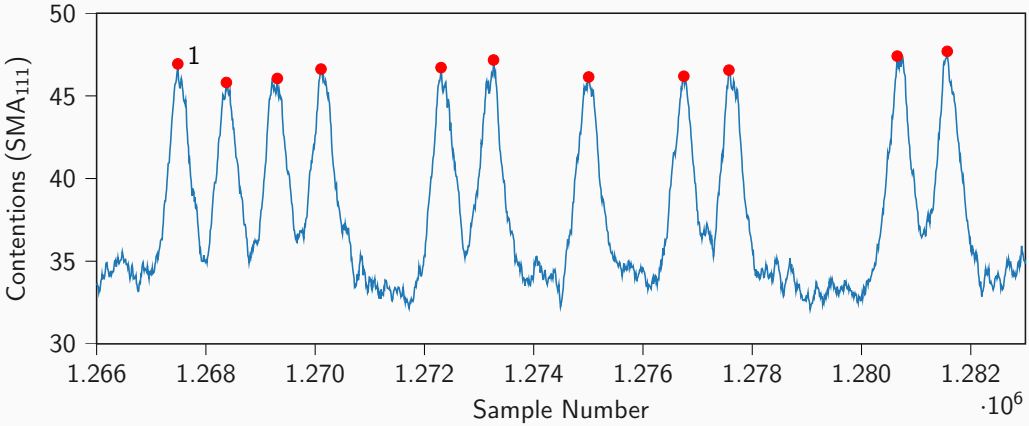

retire
ALQ1
sqrtsd

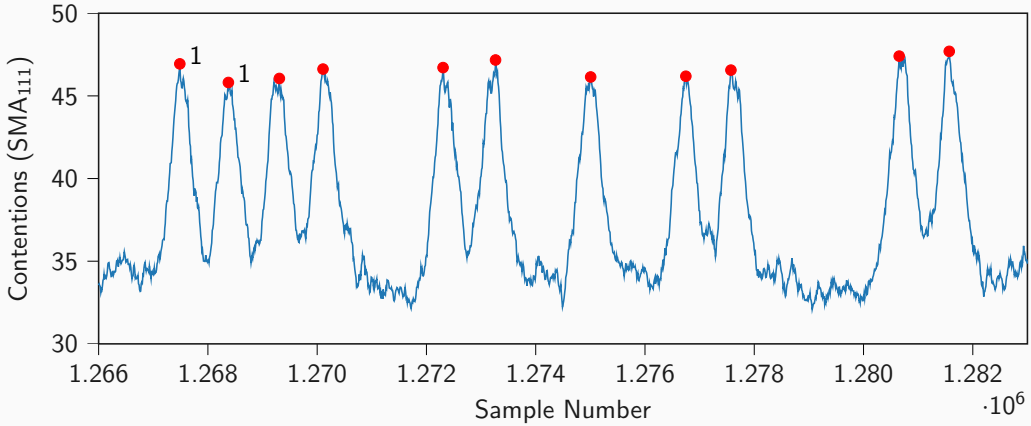

retire
rdpn
ALQ1
ALQ0/
2/3
rwu
rwu
sqrtsd
rwu
rdpn

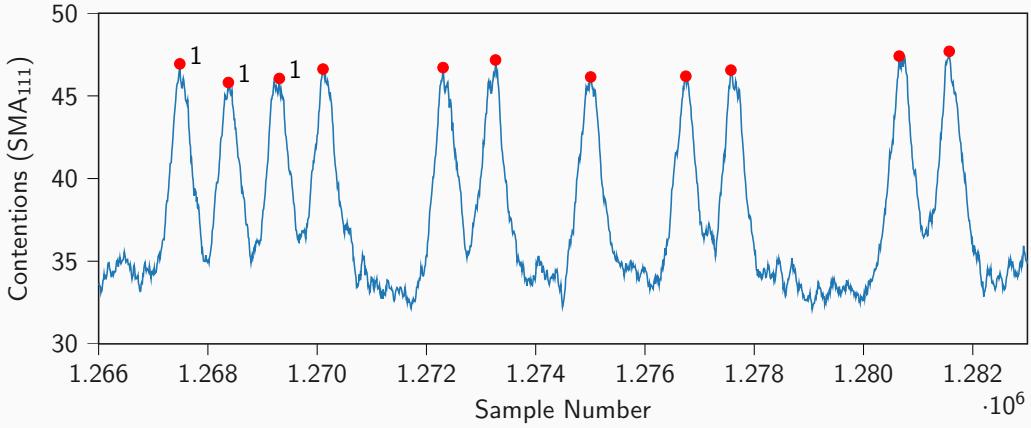

rdpn
retire
ALQ1
ALQ0/
2/3
rwd
rwd
sqrtsd
rwd
rdpn

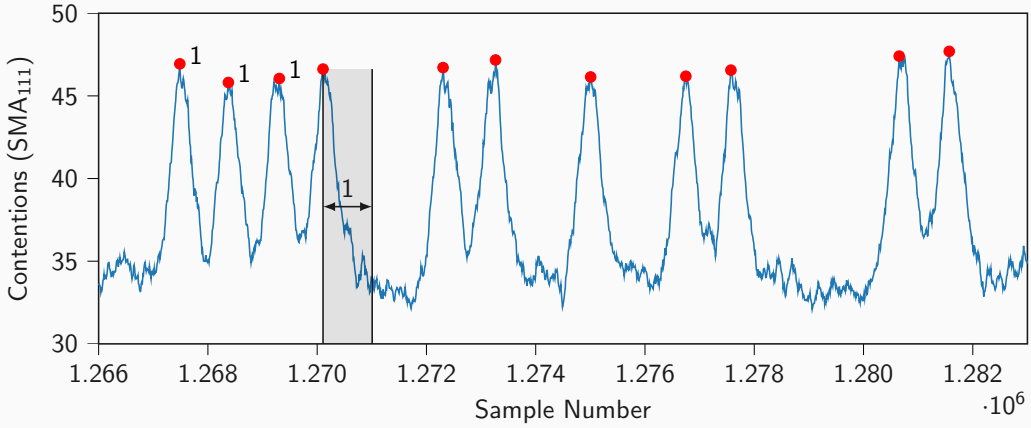

retire
ALQ1
ALQ0/
2/3
sqrtsd
rtdpn

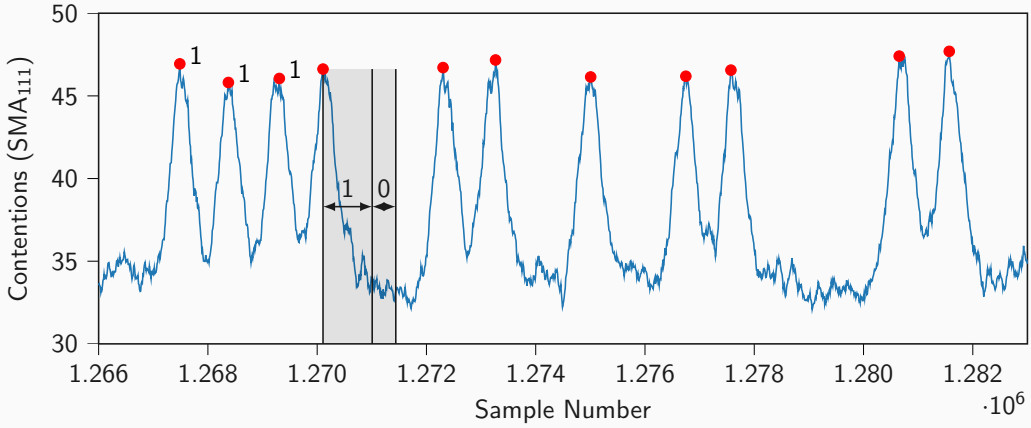

50
45
40
35
30
Contentions (SMA111)
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

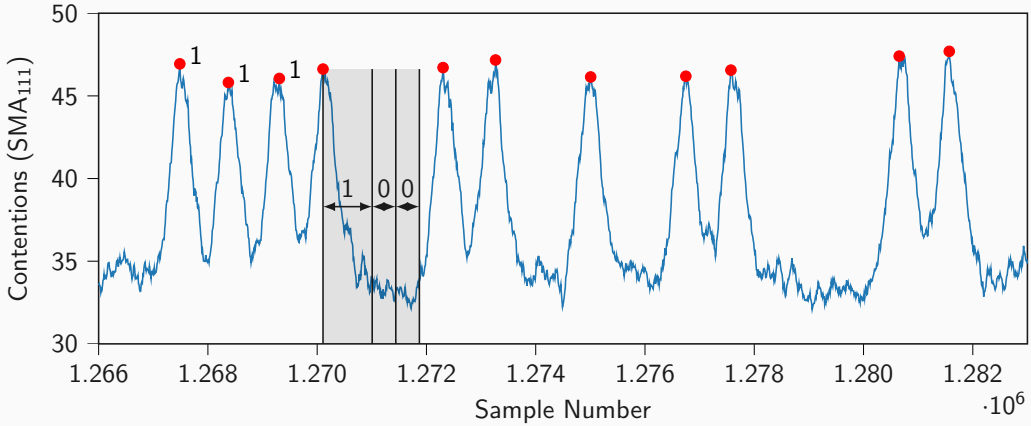

50
45
40
35
30
Contentions (SMA111)
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

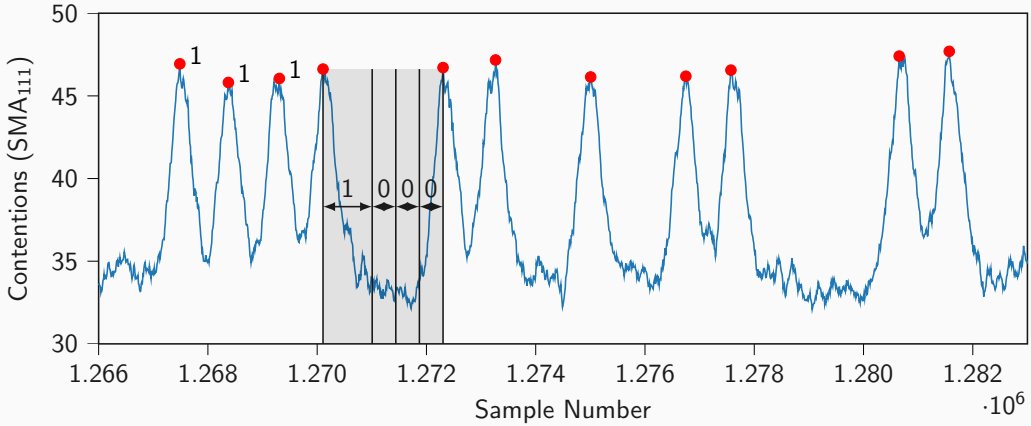

50
45
40
35
30
Contentions (SMA111)
1
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

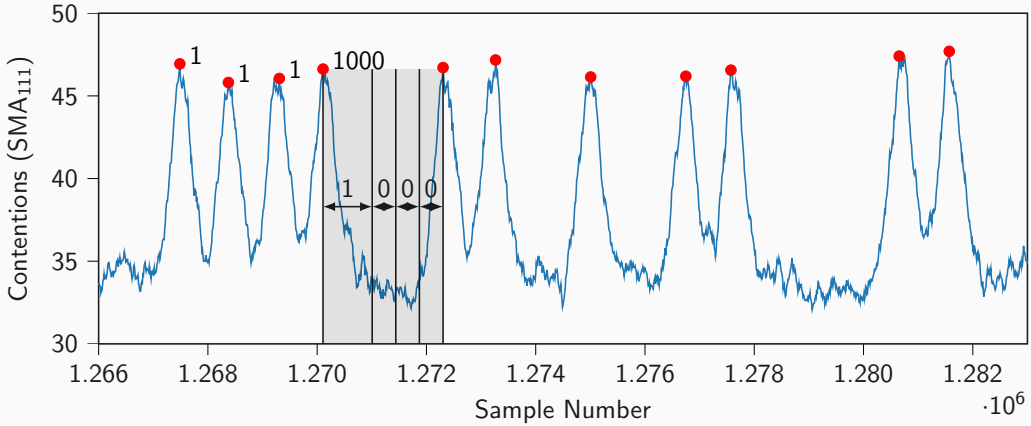

50
45
40
35
30
Contentions (SMA111)
1
1
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

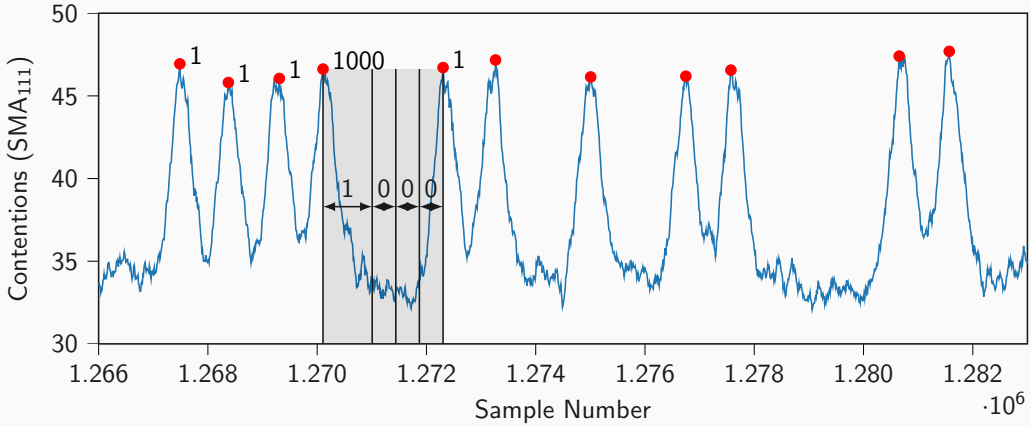

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

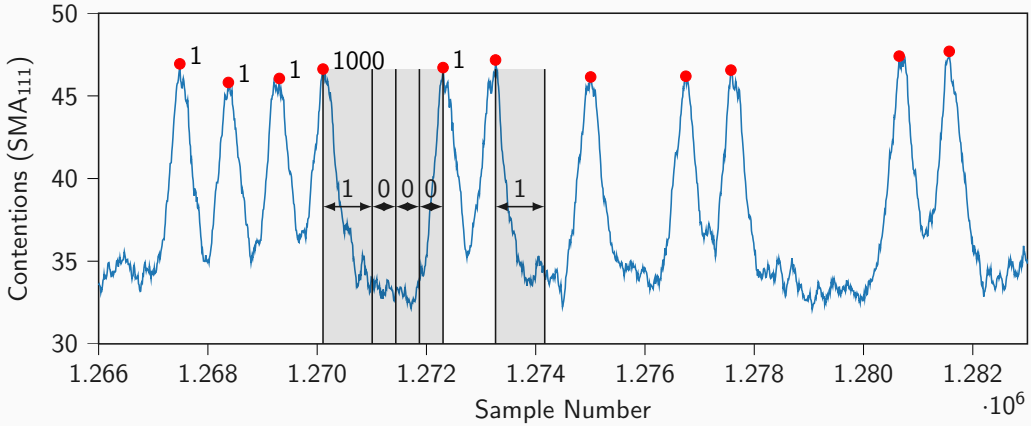

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

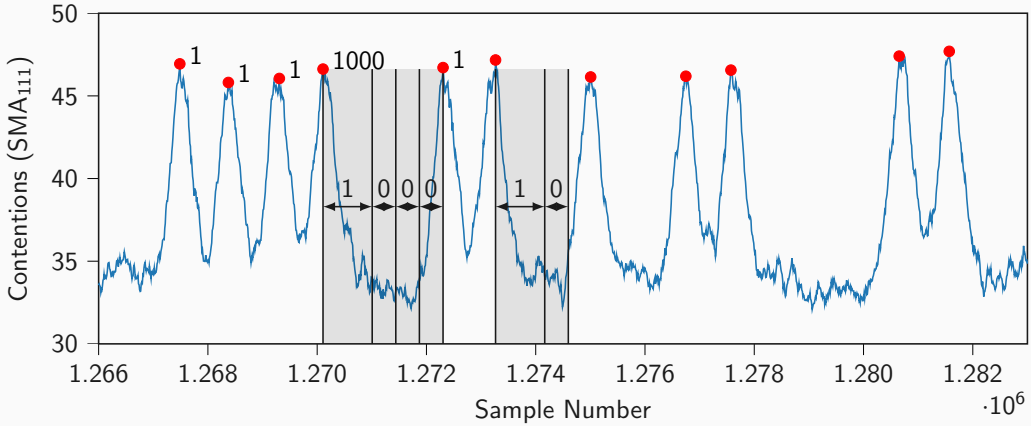

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
0
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

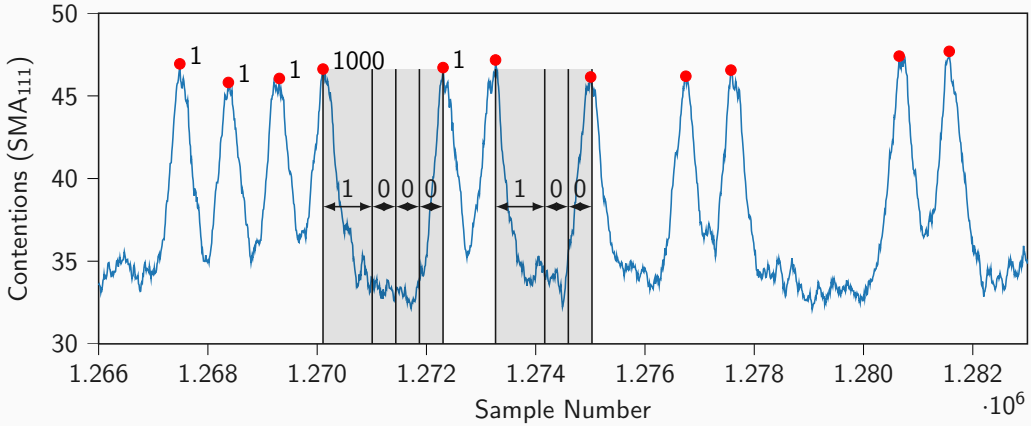

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
0
0
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

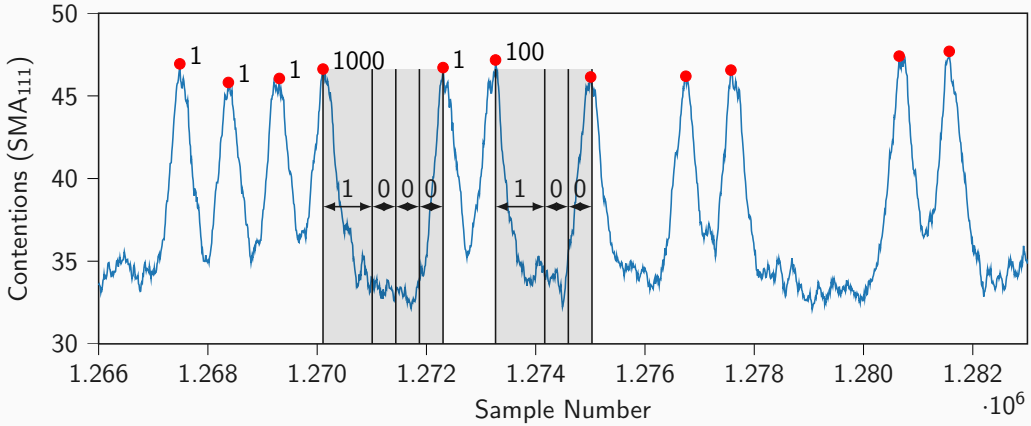

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
0
0
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

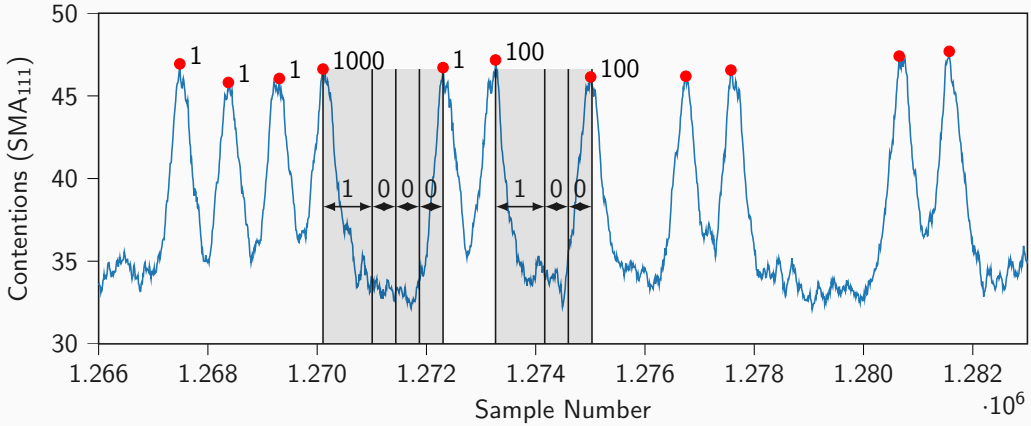

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

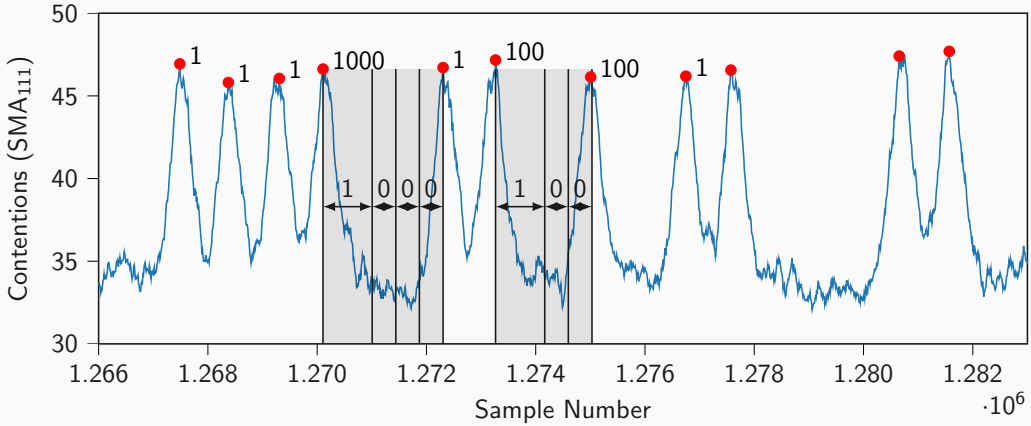

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

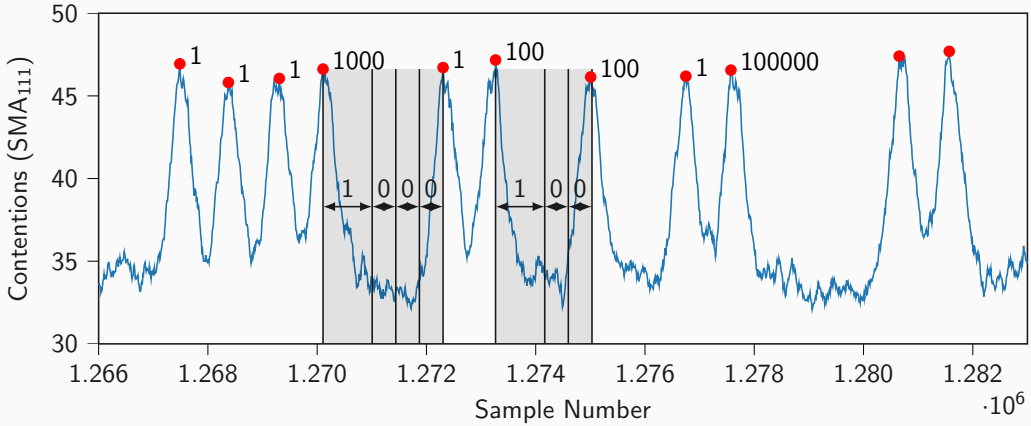

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

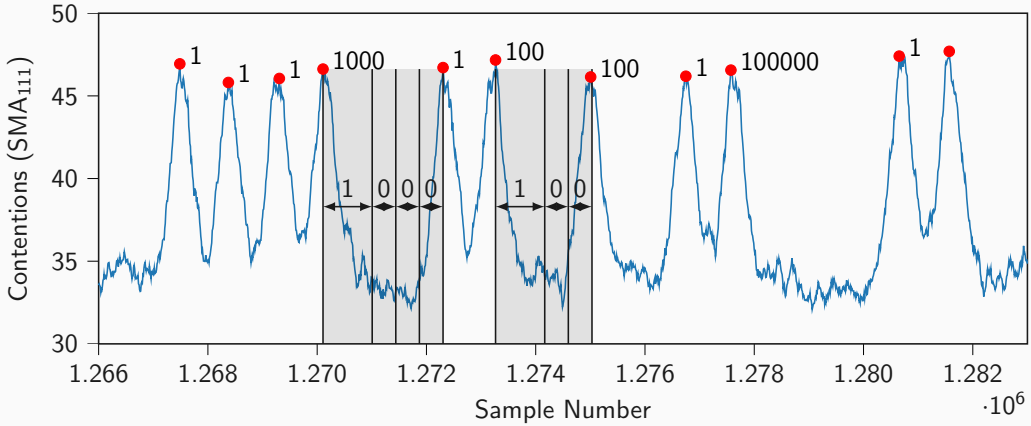

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

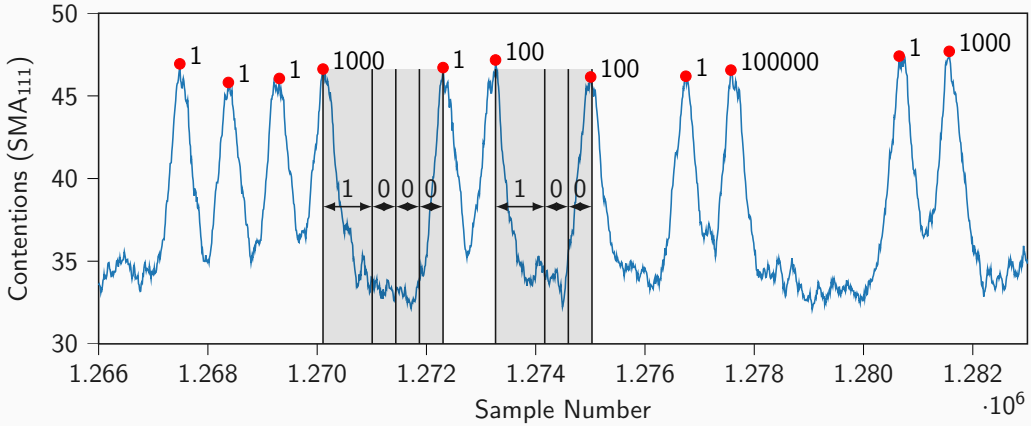

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
100
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

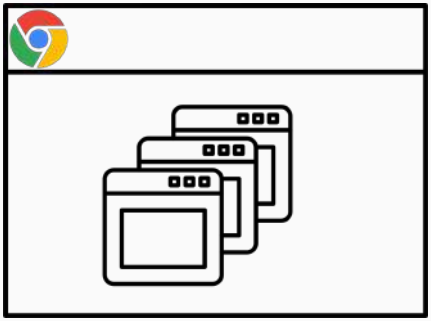

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
100
100
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

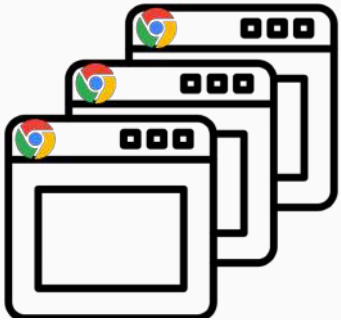

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
100
100
1
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6


Contentions (SMA111)
50
45
40
35
30
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6
1
1
1
1000
1
100
100
1
100000
1 0 0 0
1 0 0


Contentions (SMA111)
50
45
40
35
30
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6
1
1
1
1000
1
100
100
1
100000
1
1 0 0 0
1 0 0


Contentions (SMA111)
50
45
40
35
30
1
1
1
1000
1
100
100
1
100000
1
1000
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6





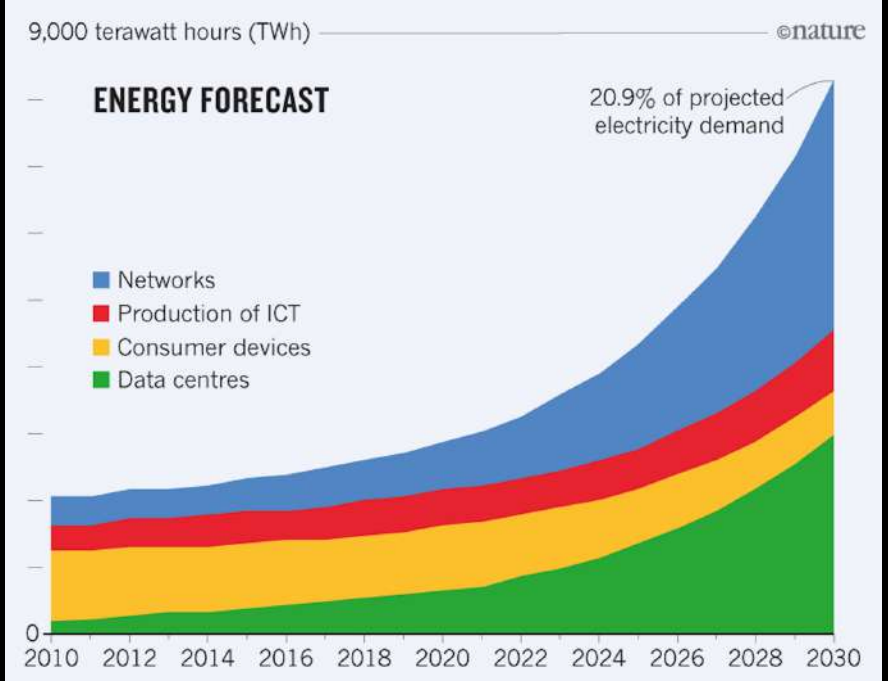

+8.2%


+8.2%


+8.2%


+8.2%


+5%


9,000 terawatt hours (TWh)
©nature
ENERGY FORECAST
20.9% of projected electricity demand
Networks
Production of ICT
Consumer devices
Data centres
0
2010
2012
2014
2016
2018
2020
2022
2024
2026
2028
2030

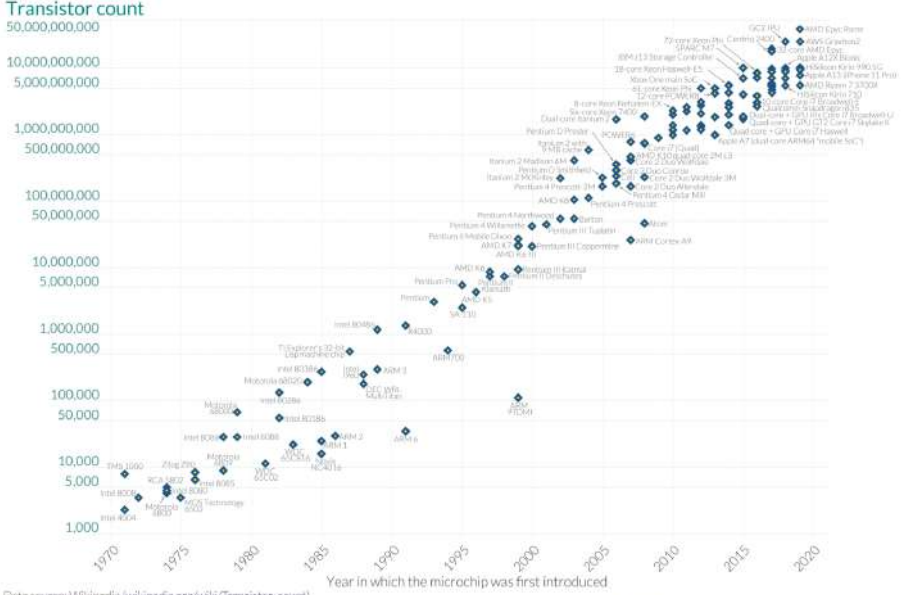
0.09%

0.40%

Moore's Law: The number of transistors on microchips has doubled every two years

Our World in Data

Moore's law describes the empirical regularity that the number of transistors on integrated circuits doubles approximately every two years. This advancement is important for other aspects of technological progress in computing – such as processing speed or the price of computers.



Data source: Wikipedia (wikipedia.org/wiki/Transistor_count)

OurWorldinData.org – Research and data to make progress against the world's largest problems.


THE END IS NEAR
OF MOORE'S LAW

Test - Mozilla Firefox (on lab02)

Test

file:///home/dgruss/rowhammerjs/rowhammer.html

Search

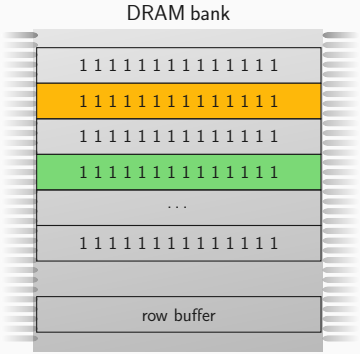
320: 12
330: 9
340: 1
350: 0
360: 1
370: 2
380: 199
390: 76
400: 72
410: 231
420: 572
1250
[!] Found flip (254 != 255) at array index 340021386 when hammering indices 339881984 and 340156416

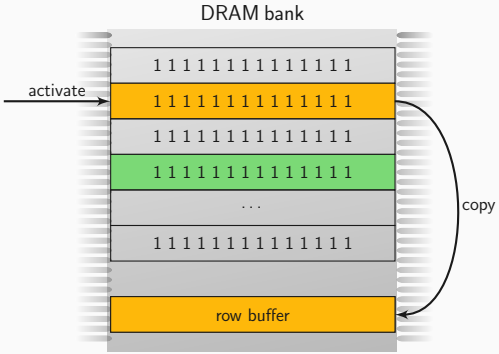
[!] Found flip (239 != 255) at array index 340022176 when hammering indices 339881984 and 340156416

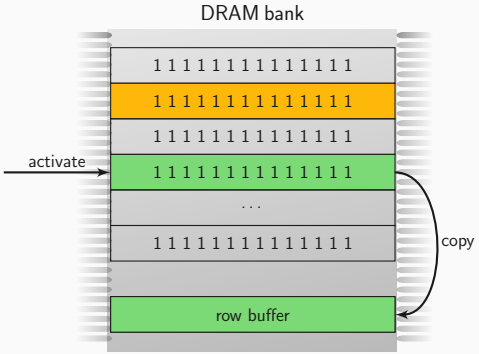
[!] Found flip (191 != 255) at array index 340023138 when hammering indices 339881984 and 340156416

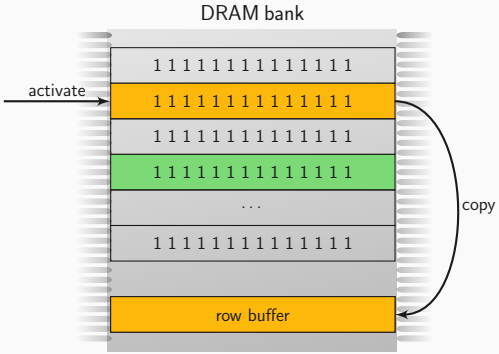
[!] Found flip (254 != 255) at array index 340025146 when hammering indices 339881984 and 340156416

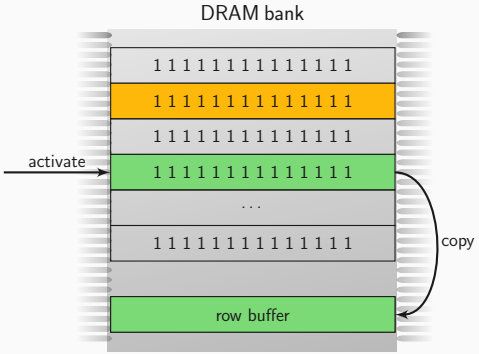
Why is Rowhammer still not solved?

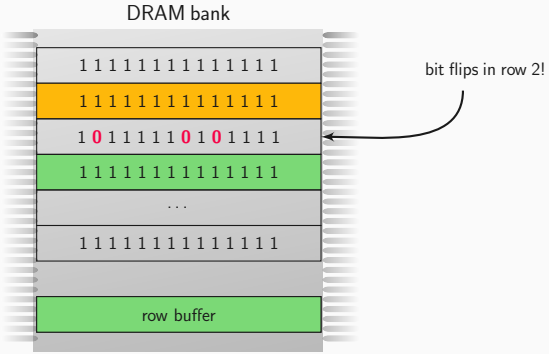

DRAM bank
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
. . .
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
row buffer


DRAM bank
activate
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
. . .
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
copy
row buffer


DRAM bank
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
activate
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
. . .
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
copy
row buffer


DRAM bank
activate
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
. . .
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
copy
row buffer


DRAM bank
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
activate
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
. . .
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
copy
row buffer


DRAM bank
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
1 0 1 1 1 1 1 0 1 0 1 1 1 1
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
. . .
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
row buffer
bit flips in row 2!

What about the defenses?

- ECC?

What about the defenses?

- ECC? doesn't work

What about the defenses?

- ECC? doesn't work
- TRR?

What about the defenses?

- ECC? doesn't work
- TRR? doesn't work either
- We're just creating bad incentives!

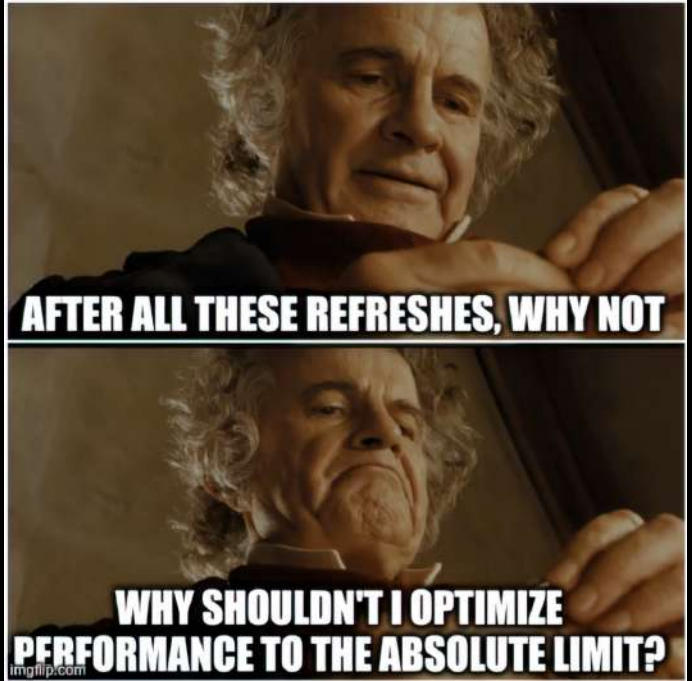
Real-world example

Mobile vendors since 2018: let's add ECC by default

Real-world example

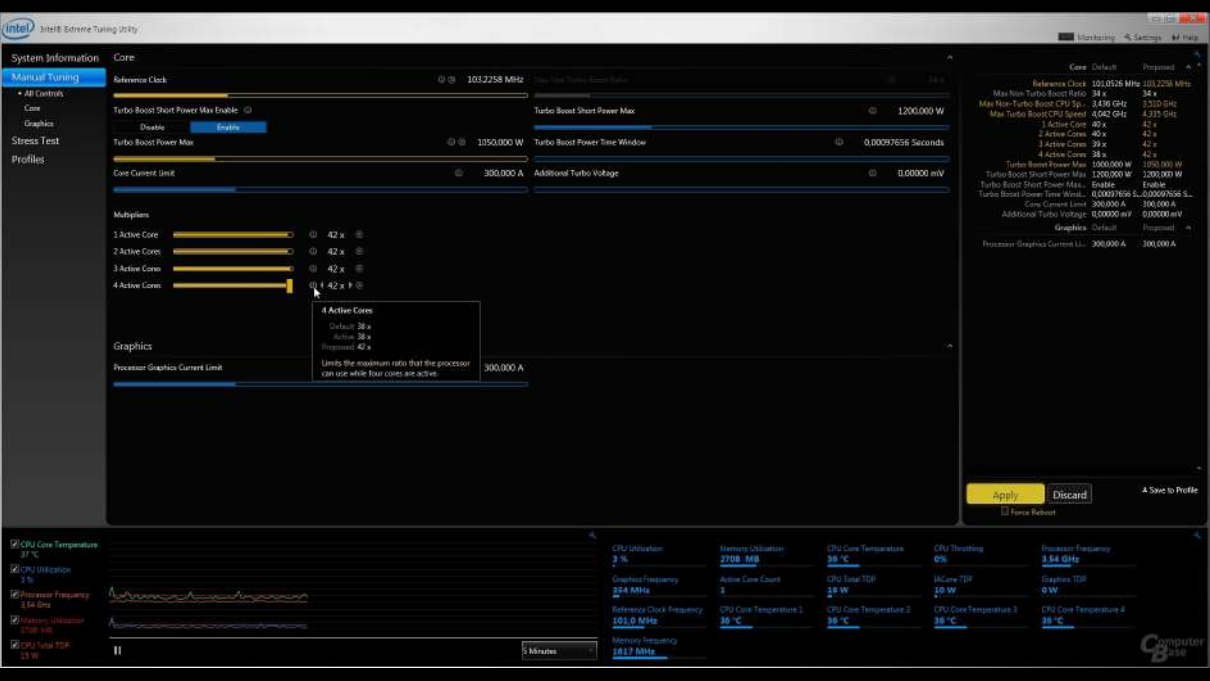
Mobile vendors since 2018: let's add ECC by default

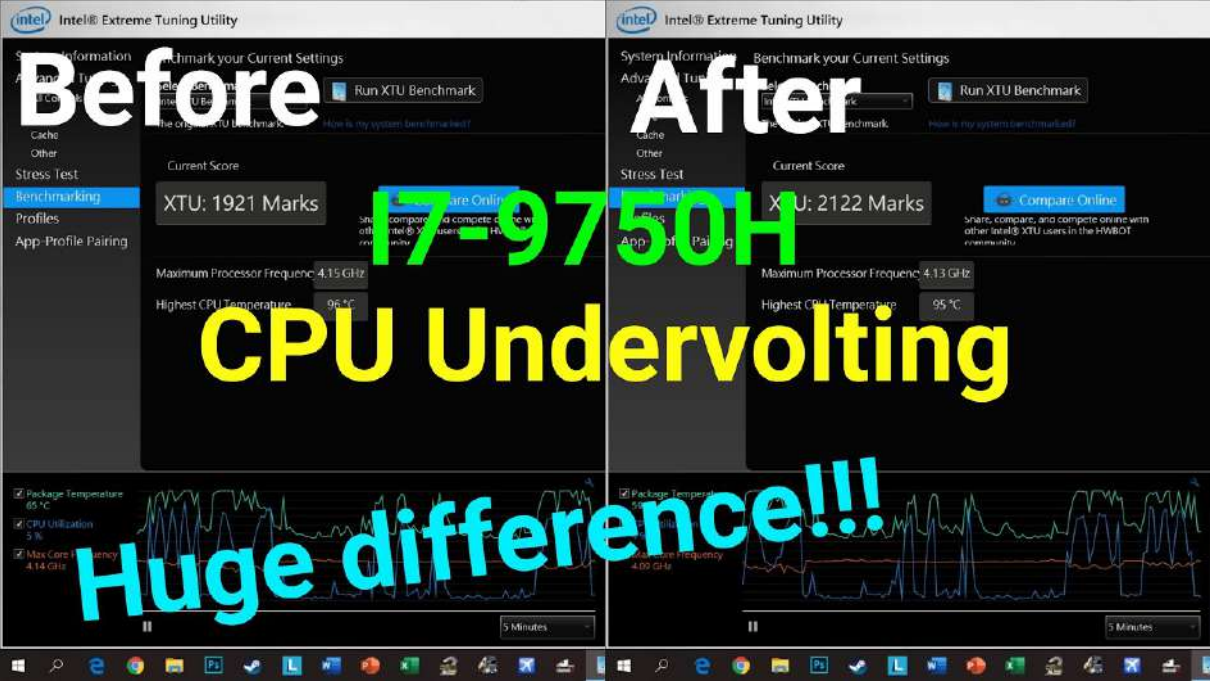
Also vendors: Let's squeeze out the last bit of efficiency for battery runtime

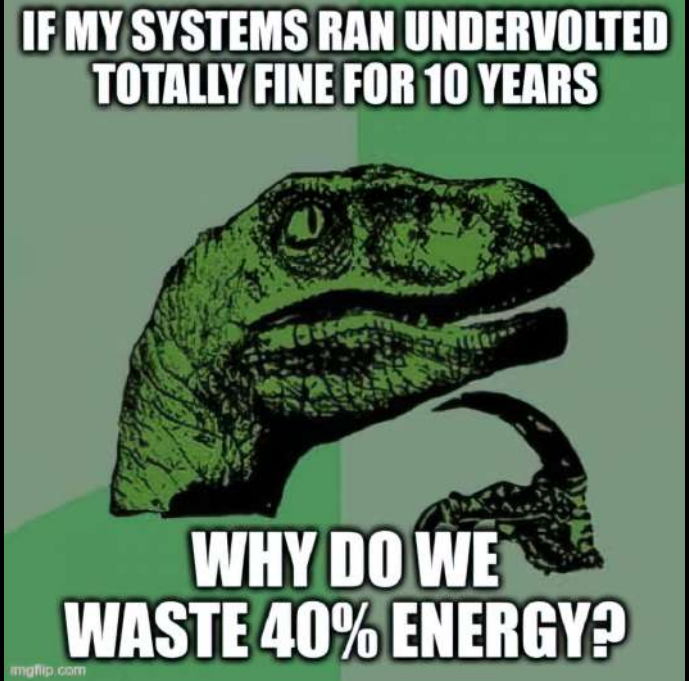

AFTER ALL THESE REFRESHES, WHY NOT
WHY SHOULDN'T I OPTIMIZE
PERFORMANCE TO THE ABSOLUTE LIMIT?
imgflip.com

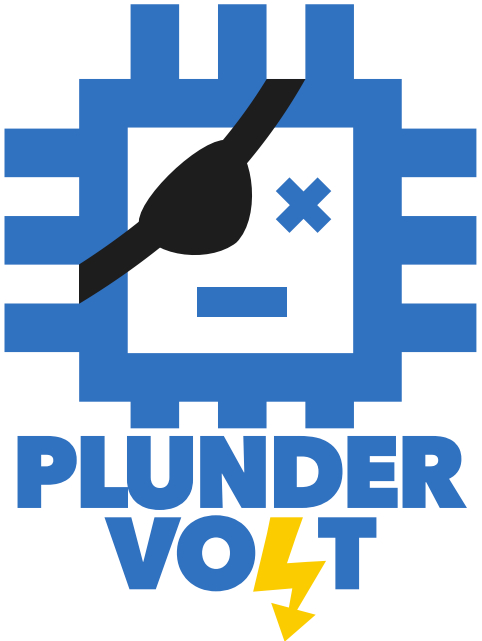
Overclocking

Undervolting


Intel® Extreme Tuning Utility
Monitoring
Settings
Help
System Information
Manual Tuning
• All Controls
Core
Graphics
Stress Test
Profiles
Core
Reference Clock
103.2258 MHz
Turbo Boost Short Power Max Enable
Disable
Enable
Turbo Boost Short Power Max
1200,000 W
Turbo Boost Power Max
1050,000 W
Turbo Boost Power Time Window
0,00097656 Seconds
Core Current Limit
300,000 A
Additional Turbo Voltage
0,00000 mV
Multipliers
1 Active Core
42 x
2 Active Cores
42 x
3 Active Cores
42 x
4 Active Cores
42 x
4 Active Cores
Default 38 x
Active 38 x
Proposed 42 x
Limits the maximum ratio that the processor can use while four cores are active.
Graphics
Processor Graphics Current Limit
300,000 A
Core Default Proposed
Reference Clock 101,0526 MHz 103,2258 MHz
Max Non-Turbo Boost Ratio 34 x 34 x
Max Non-Turbo Boost CPU Sp... 3,436 GHz 3,510 GHz
Max Turbo Boost CPU Speed 4,042 GHz 4,235 GHz
1 Active Core 40 x 42 x
2 Active Cores 40 x 42 x
3 Active Cores 39 x 42 x
4 Active Cores 38 x 42 x
Turbo Boost Power Max 1000,000 W 1050,000 W
Turbo Boost Short Power Max 1200,000 W 1200,000 W
Turbo Boost Short Power Max... Enable Enable
Turbo Boost Power Time Wind... 0,00097656 S... 0,00097656 S...
Core Current Limit 300,000 A 300,000 A
Additional Turbo Voltage 0,00000 mV 0,00000 mV
Graphics Default Proposed
Processor Graphics Current Li... 300,000 A 300,000 A
Apply
Discard
Force Reboot
Save to Profile
CPU Core Temperature
37 °C
CPU Utilization
3 %
Processor Frequency
3.54 GHz
Memory Utilization
2708 MB
CPU Total TDP
10 W
5 Minutes
CPU Utilization
3 %
Memory Utilization
2708 MB
CPU Core Temperature
36 °C
CPU Throttling
0%
Processor Frequency
3.54 GHz
Graphics Frequency
354 MHz
Active Core Count
1
CPU Total TDP
10 W
IACore TDP
10 W
Graphics TDP
0 W
Reference Clock Frequency
101.0 MHz
CPU Core Temperature 1
36 °C
CPU Core Temperature 2
36 °C
CPU Core Temperature 3
36 °C
CPU Core Temperature 4
36 °C
Memory Frequency
1417 MHz

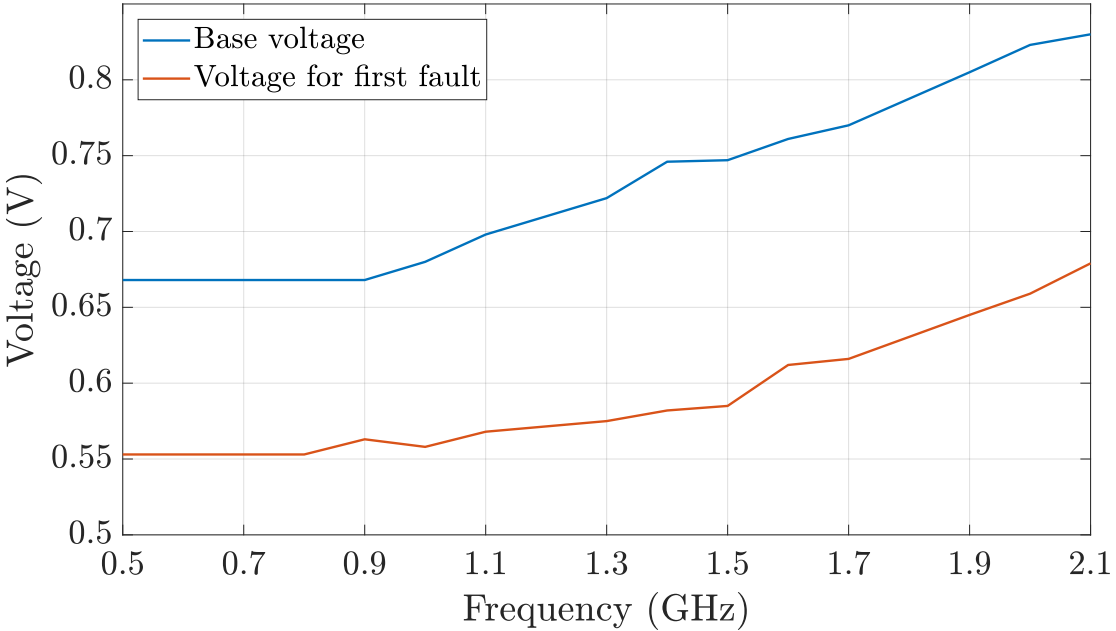

Intel® Extreme Tuning Utility
Before
Run XTU Benchmark
Stress Test
Benchmarking
Profiles
App-Profile Pairing
Current Score
XTU: 1921 Marks
Maximum Processor Frequency 4.15 GHz
Highest CPU Temperature 96 °C
Intel® Extreme Tuning Utility
After
Run XTU Benchmark
Stress Test
Current Score
XTU: 2122 Marks
Compare Online
Maximum Processor Frequency 4.13 GHz
Highest CPU Temperature 95 °C
I7-9750H
CPU Undervolting
Huge difference!!!
5 Minutes
5 Minutes


IF MY SYSTEMS RAN UNDERVOLTED
TOTALLY FINE FOR 10 YEARS
WHY DO WE
WASTE 40% ENERGY?
imgflip.com

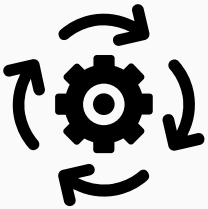

PLUNDER
VOLT

Will it fault?

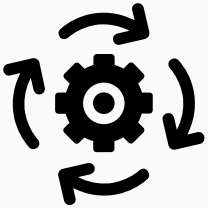
```
uint64_t multiplier = 0x1122334455667788;
uint64_t correct    = 0xdeadbeef * multiplier;
uint64_t var        = 0xdeadbeef * multiplier;

while (var == correct)
{
    var = 0xdeadbeef * multiplier;
}
uint64_t flipped_bits = var ^ correct;
```


Base voltage
Voltage for first fault
Voltage (V)
0.8
0.75
0.7
0.65
0.6
0.55
0.5
0.5
0.7
0.9
1.1
1.3
1.5
1.7
1.9
2.1
Frequency (GHz)

Security for Efficiency?

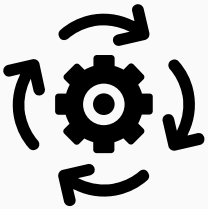


Make bit flips degrade performance **without** impacting security



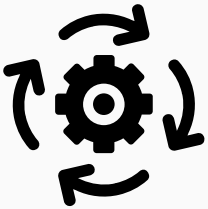
Make bit flips degrade performance **without** impacting security

- Cryptographic MAC



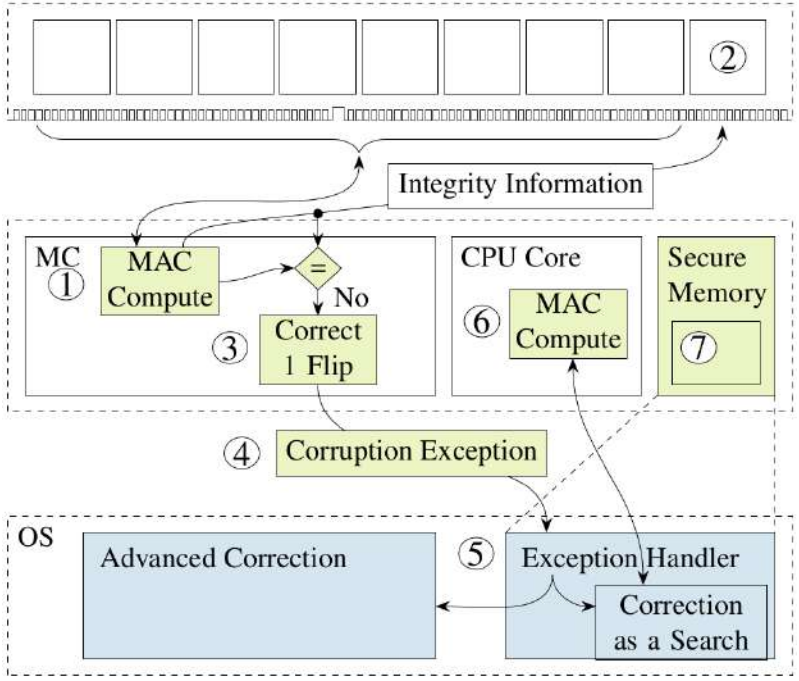
Make bit flips degrade performance **without** impacting security

- Cryptographic MAC
- Detect **any** number of bit flips



Make bit flips degrade performance **without** impacting security

- Cryptographic MAC
- Detect **any** number of bit flips
- Correction by **brute-force** search for correct data

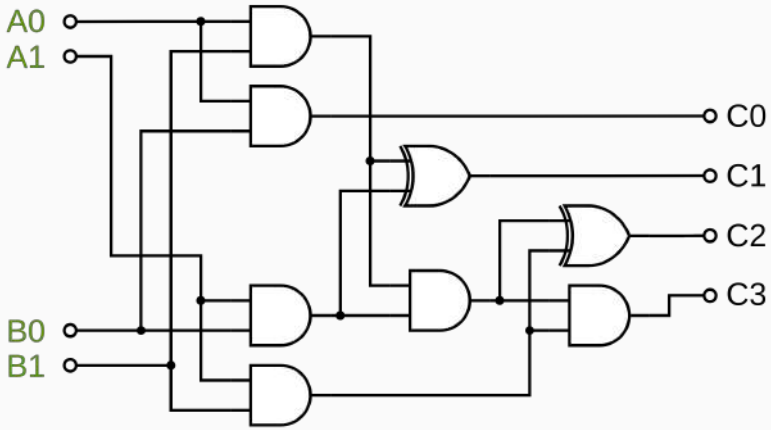

②
Integrity Information
MC
①
MAC
Compute
=
No
③
Correct
1 Flip
CPU Core
⑥
MAC
Compute
Secure
Memory
⑦
④
Corruption Exception
OS
Advanced Correction
⑤
Exception Handler
Correction
as a Search

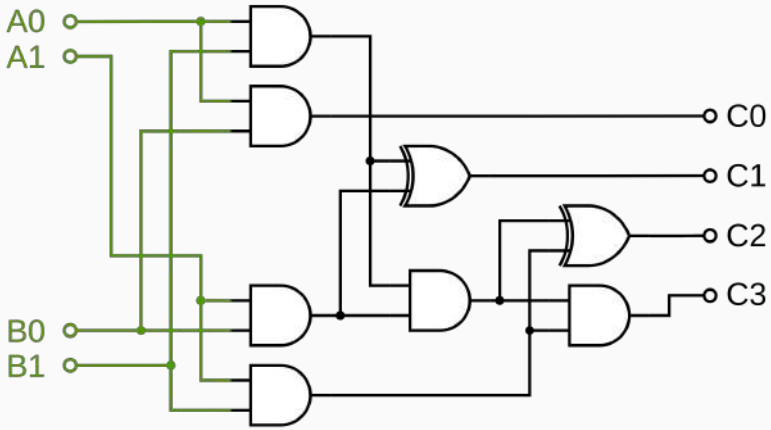
# Errors	# MAC Comp.	Avg Duration
1	17	11 ns
2	771	3.68 µs
3	33 800	124 µs
4	1.51×10^6	6.65 ms
5	6.91×10^7	261 ms
6	3.07×10^9	12.8 s
7	1.21×10^{11}	9.11 min
8	5.72×10^{12}	6.11 h

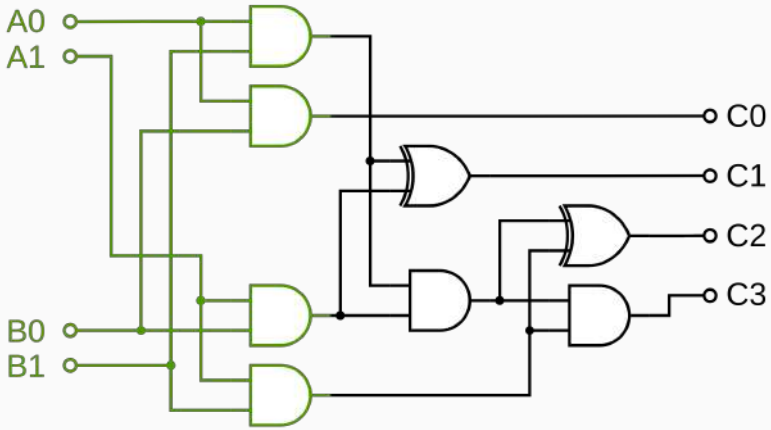
- Silent data corruption less than once per 10^9 billion years

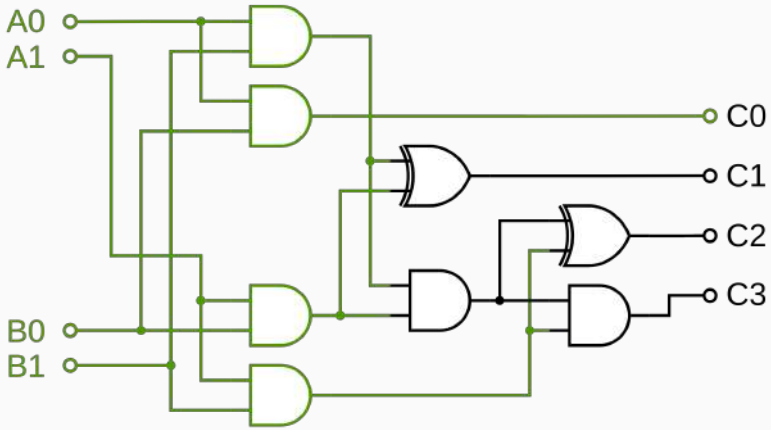
- Silent data corruption less than once per 10^9 billion years
- Second preimage after hammering for one year: $9.75 \cdot 10^{-5}$ %

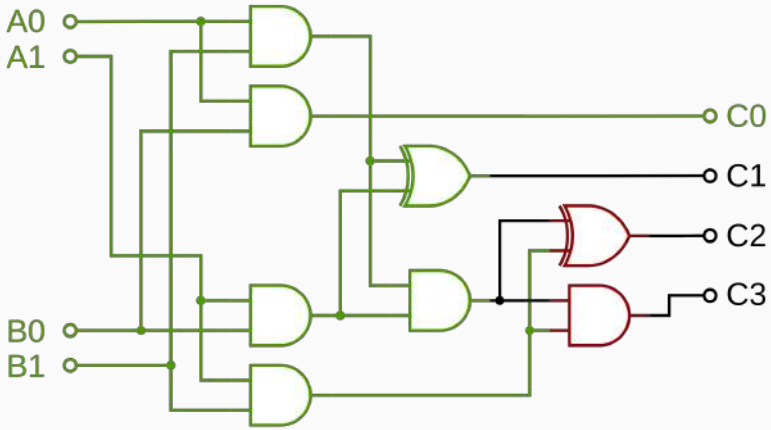
- Silent data corruption less than once per 10^9 billion years
- Second preimage after hammering for one year: $9.75 \cdot 10^{-5}\,\%$
- Erroneous correction of 8-bit errors: $0.0161\,\%$

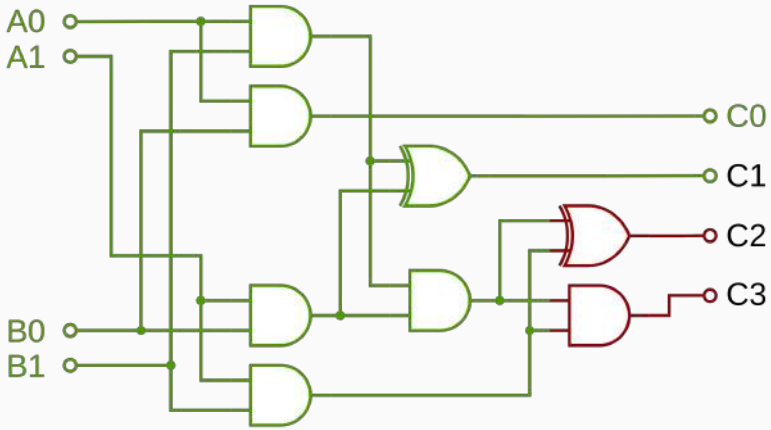

A0
A1
B0
B1
C0
C1
C2
C3

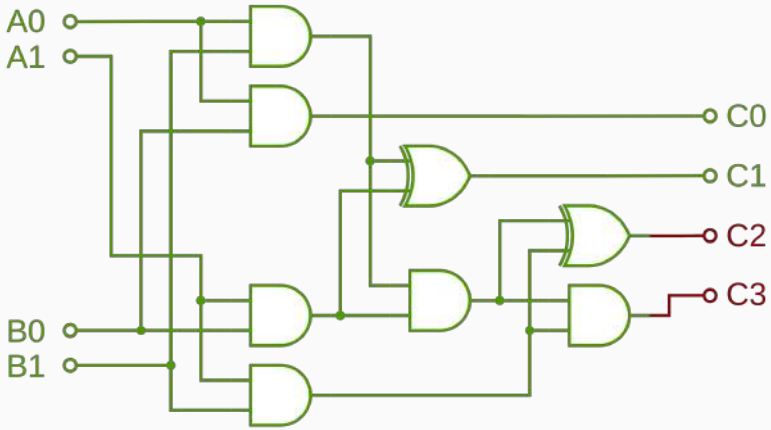

A0
A1
B0
B1
C0
C1
C2
C3

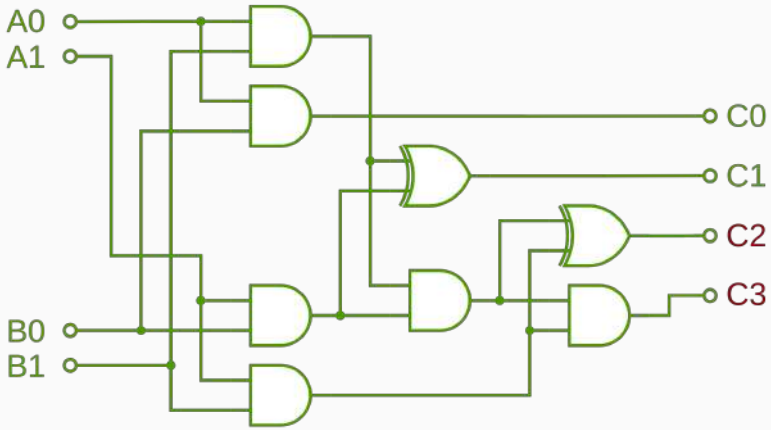

A0
A1
B0
B1
C0
C1
C2
C3

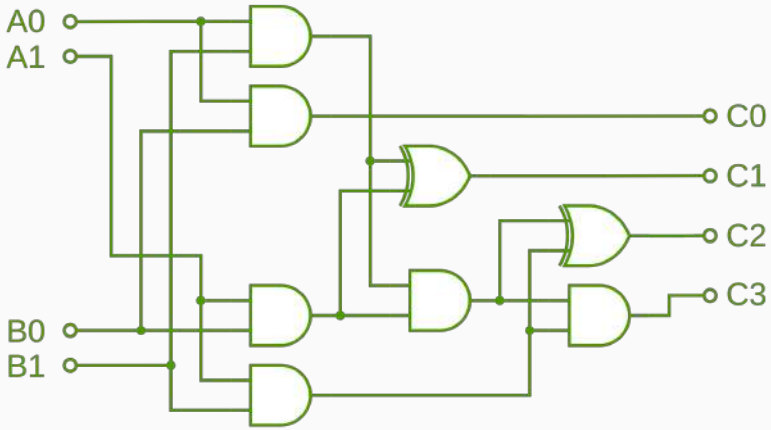

A0
A1
B0
B1
C0
C1
C2
C3


A0
A1
B0
B1
C0
C1
C2
C3

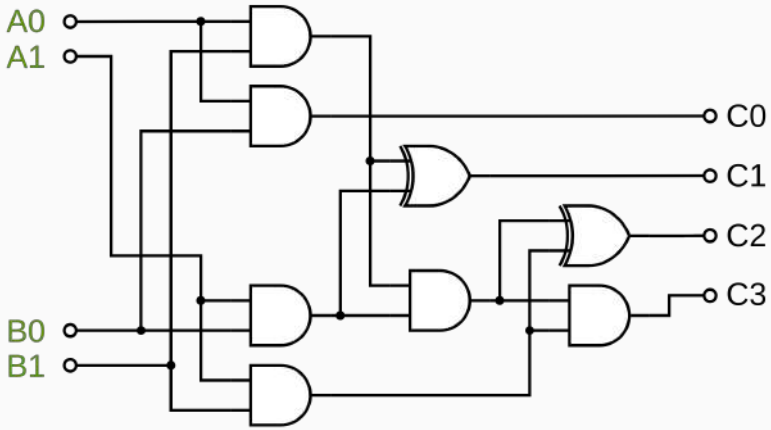

A0
A1
B0
B1
C0
C1
C2
C3


A0
A1
B0
B1
C0
C1
C2
C3

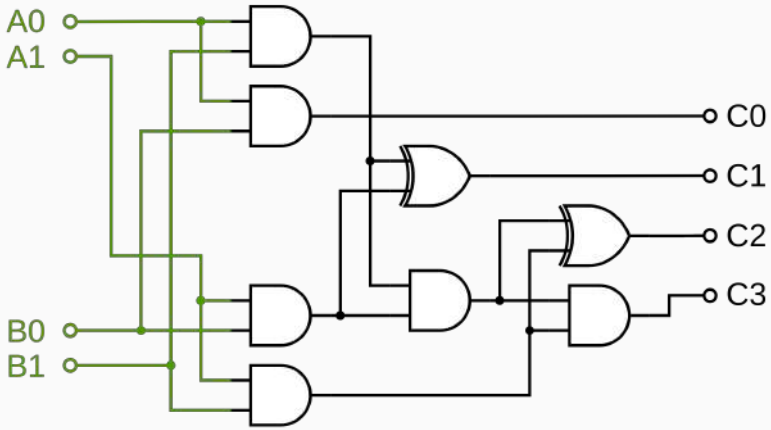

A0
A1
B0
B1
C0
C1
C2
C3

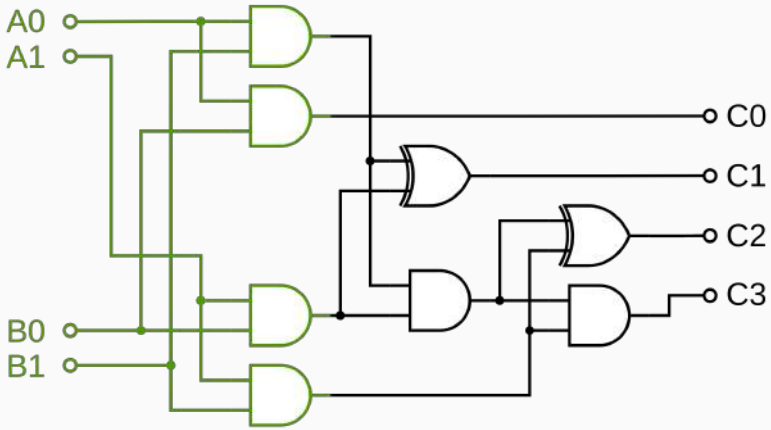

A0
A1
B0
B1
C0
C1
C2
C3

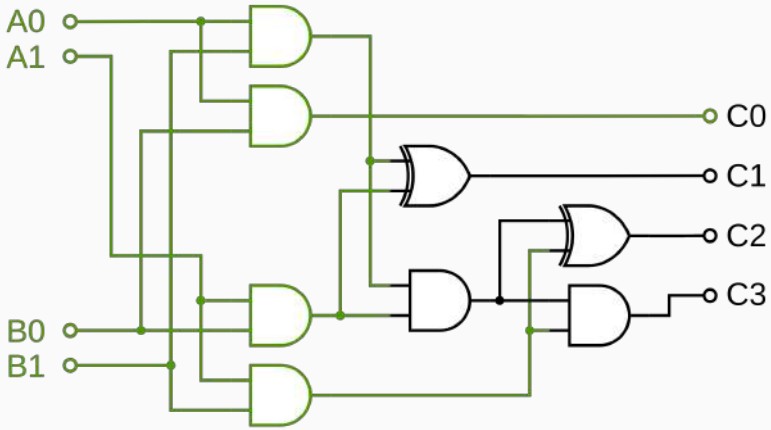
Propagation Delay vs Clock (but now the voltage is too low)

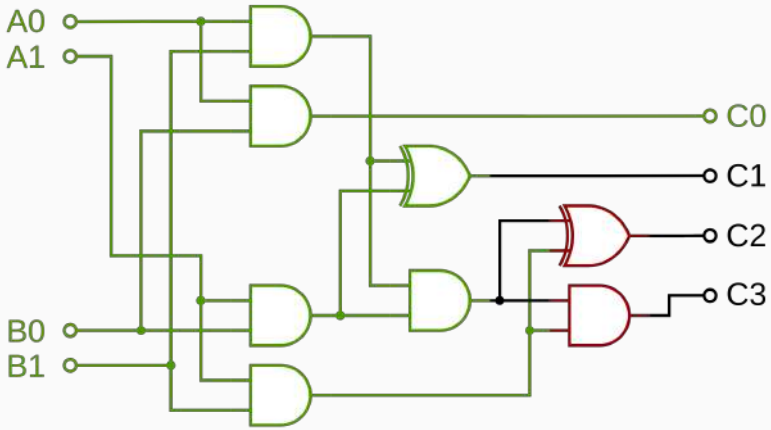


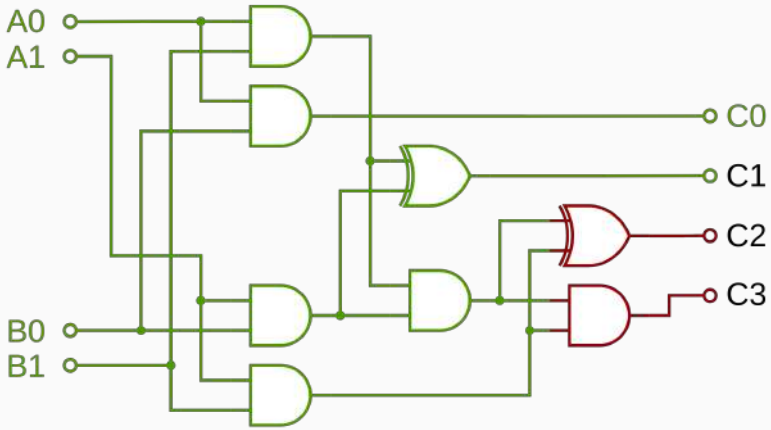
Propagation Delay vs Clock (but now the voltage is too low)



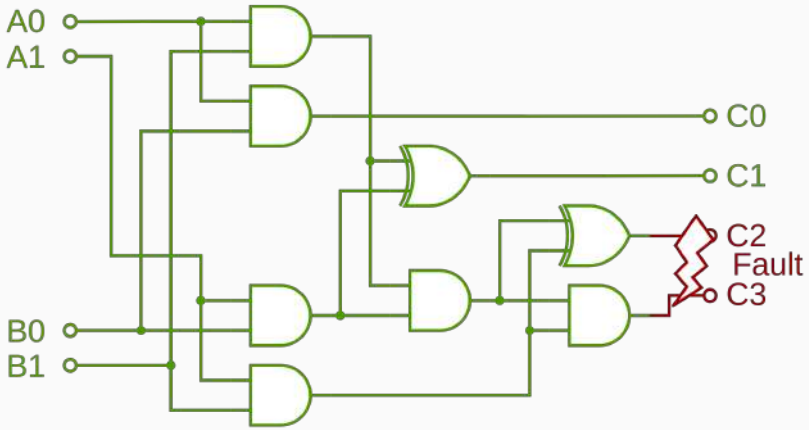

A0
A1
B0
B1
C0
C1
C2
C3


A0
A1
B0
B1
C0
C1
C2
C3


A0
A1
B0
B1
C0
C1
C2
C3

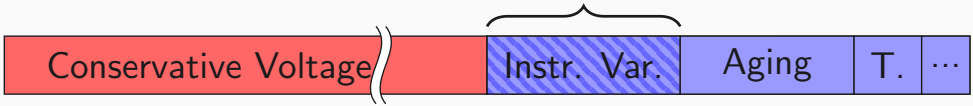

A0
A1
B0
B1
C0
C1
C2
C3

Propagation Delay vs Clock (but now the voltage is too low)



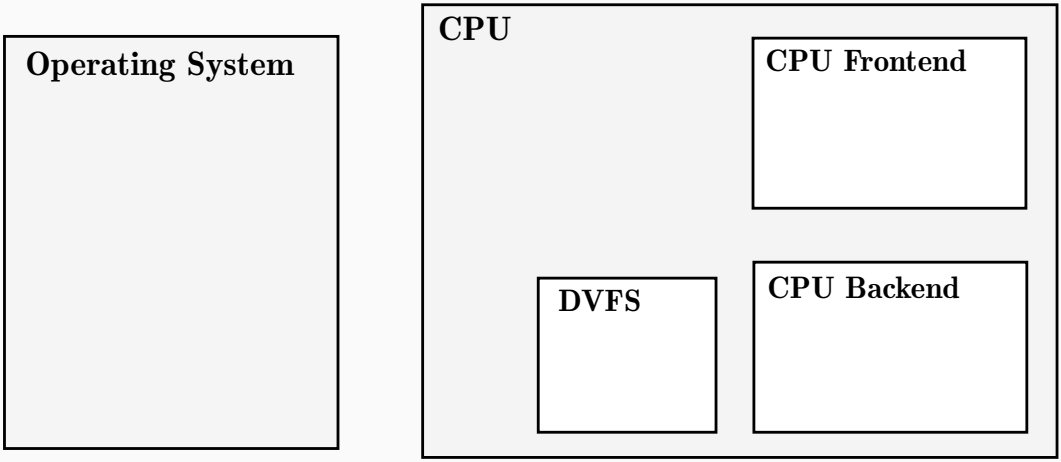

Conservative Voltage
Instr. Var.
Aging
T.
...

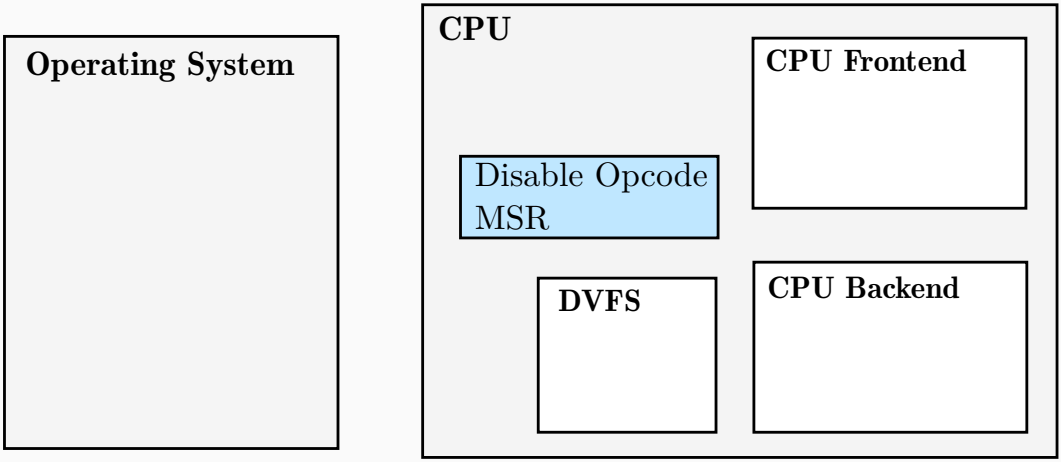
Up to a 150 mV variation in instruction voltage requirement.

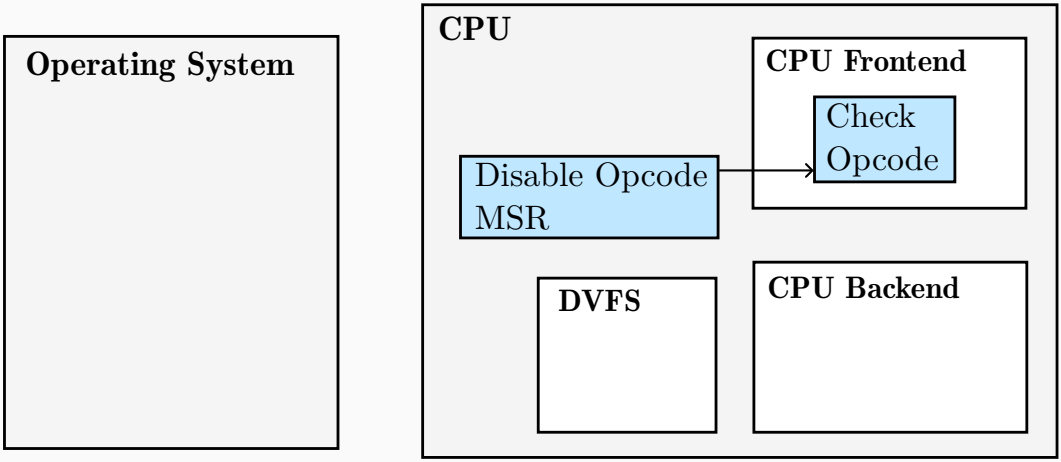


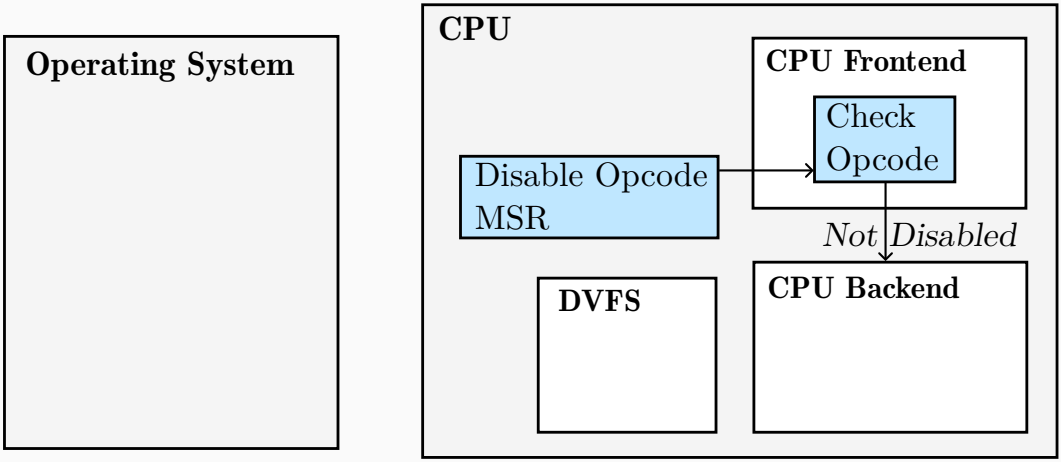
SUIT

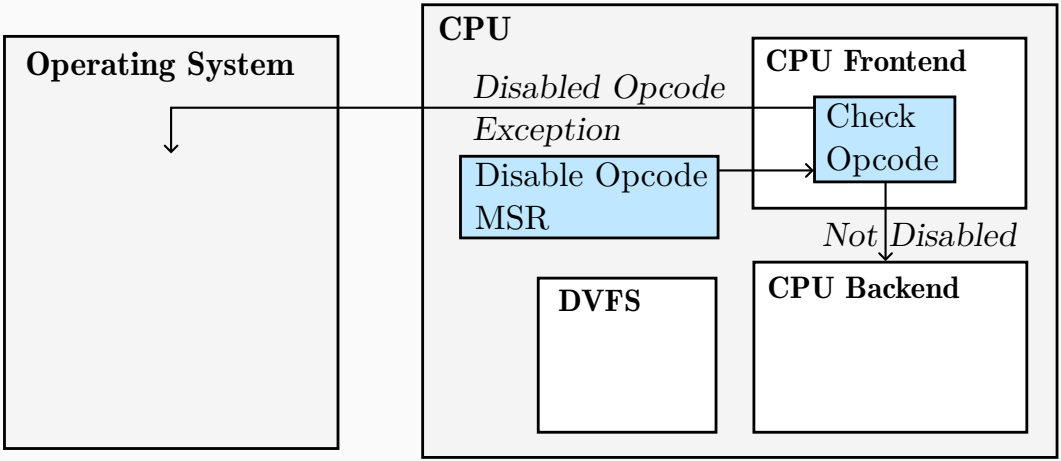
Secure Undervolting with Instruction Traps

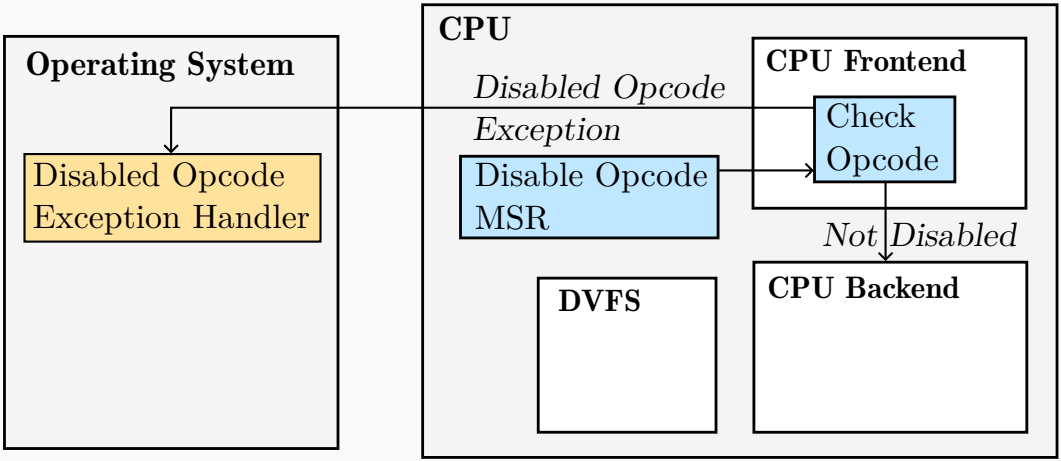

Operating System
CPU
CPU Frontend
DVFS
CPU Backend

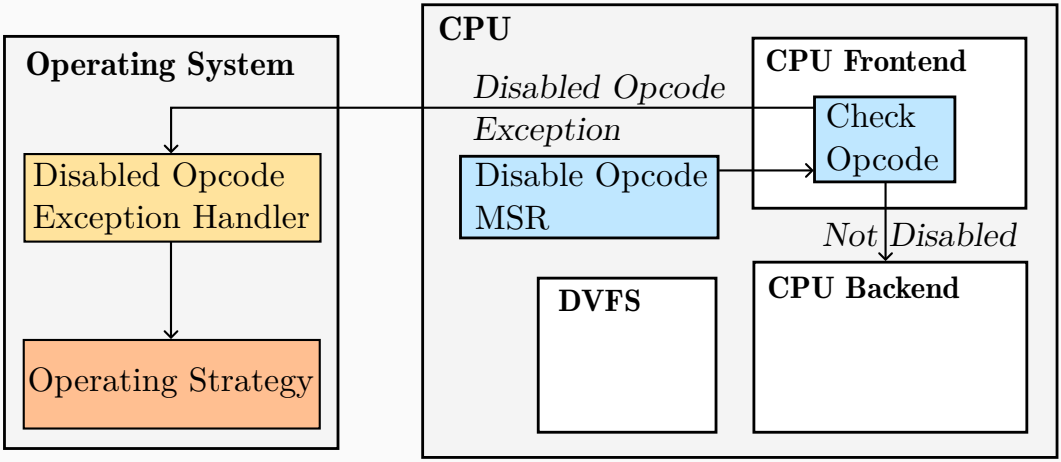

Operating System
CPU
CPU Frontend
Disable Opcode MSR
DVFS
CPU Backend

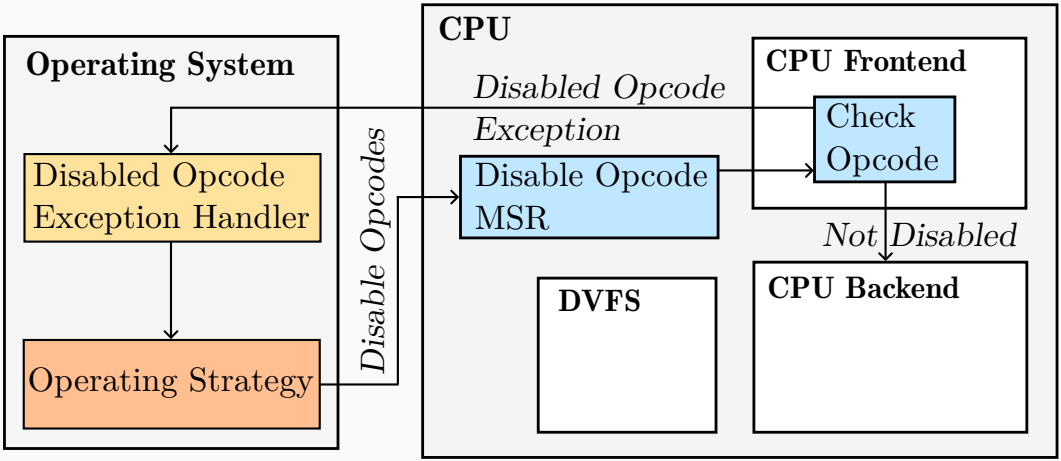

Operating System
CPU
CPU Frontend
Check Opcode
Disable Opcode MSR
DVFS
CPU Backend

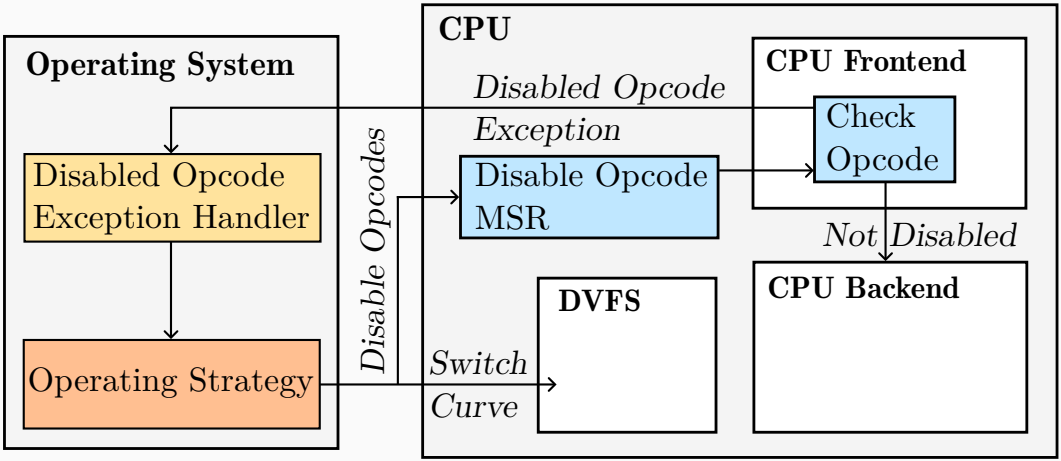

Operating System
CPU
CPU Frontend
Check Opcode
Disable Opcode MSR
Not Disabled
DVFS
CPU Backend

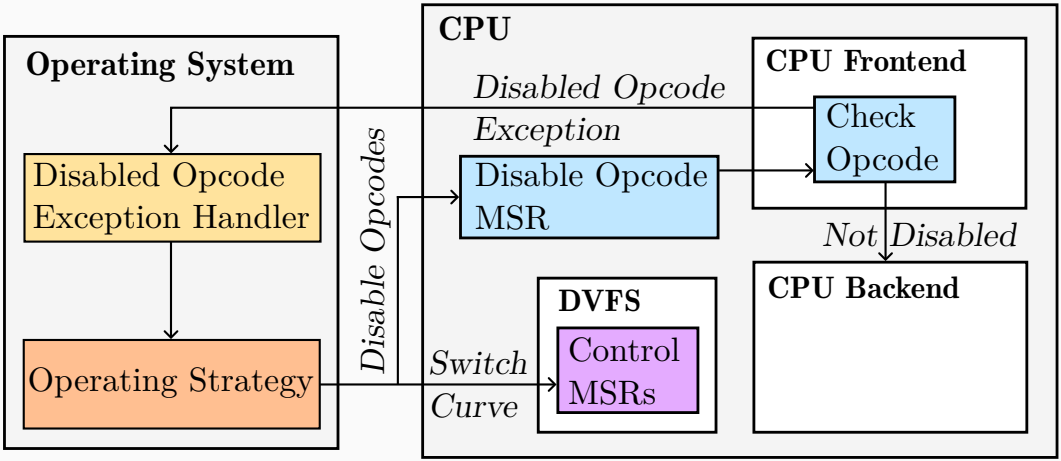

Operating System
CPU
CPU Frontend
Disabled Opcode
Exception
Check
Opcode
Disable Opcode
MSR
Not Disabled
DVFS
CPU Backend

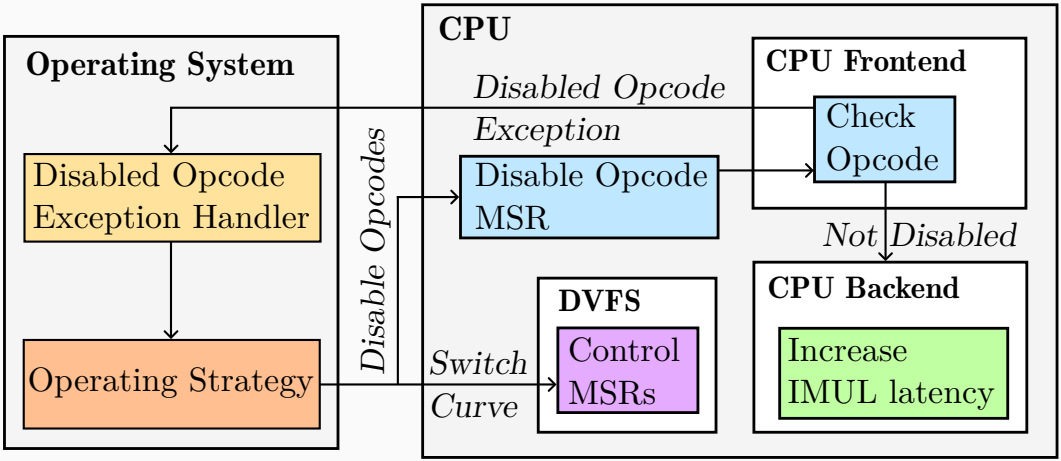

Operating System
Disabled Opcode Exception Handler
CPU
Disabled Opcode Exception
CPU Frontend
Check Opcode
Disable Opcode MSR
Not Disabled
DVFS
CPU Backend

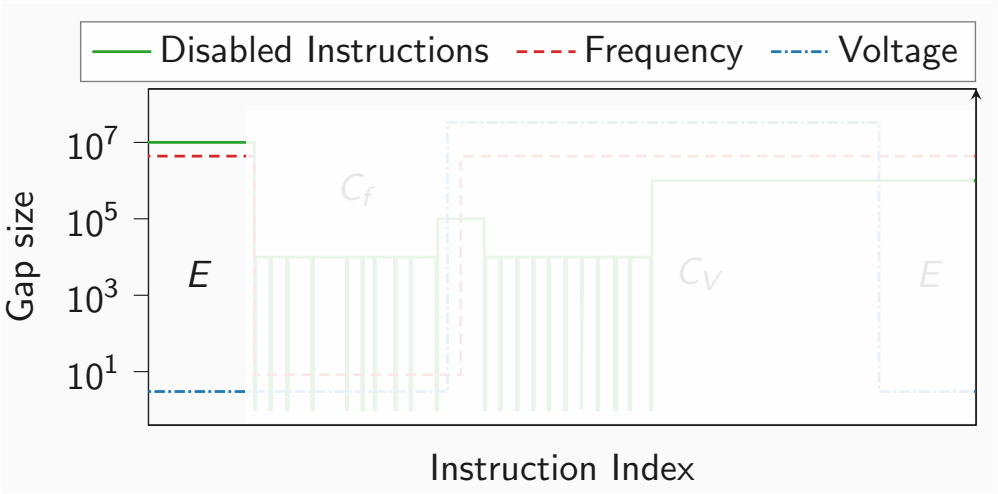

Operating System
Disabled Opcode Exception Handler
Operating Strategy
CPU
Disabled Opcode Exception
CPU Frontend
Check Opcode
Disable Opcode MSR
Not Disabled
DVFS
CPU Backend

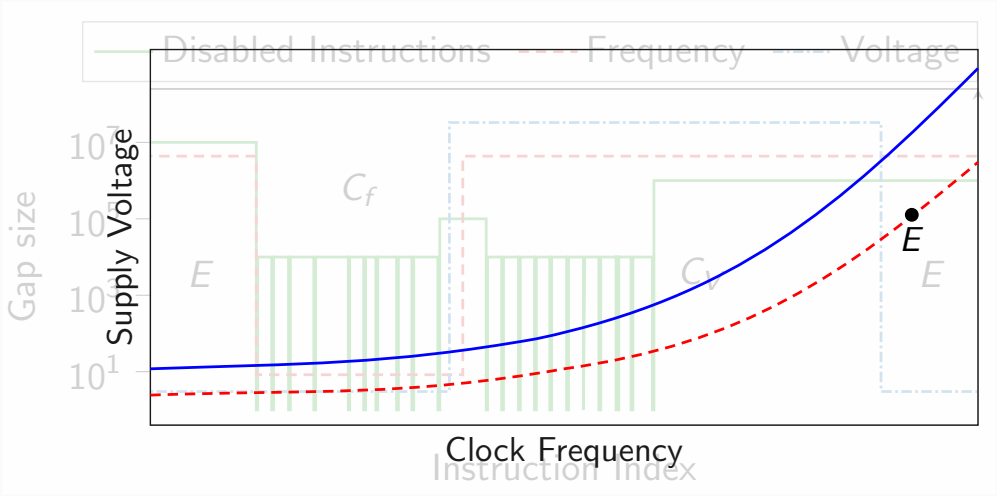

Operating System
Disabled Opcode Exception Handler
Operating Strategy
Disable Opcodes
CPU
Disabled Opcode Exception
Disable Opcode MSR
CPU Frontend
Check Opcode
Not Disabled
DVFS
CPU Backend

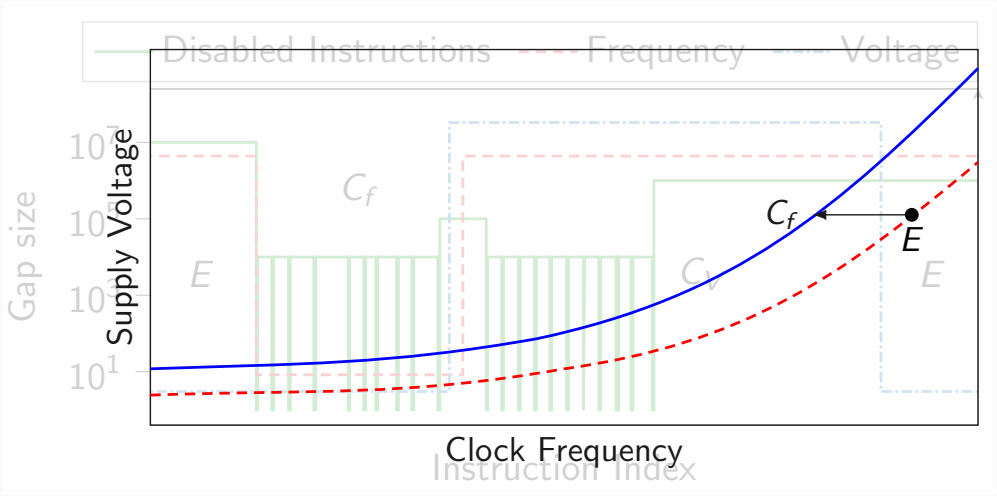

Operating System
Disabled Opcode Exception Handler
Operating Strategy
Disable Opcodes
CPU
Disabled Opcode Exception
Disable Opcode MSR
Switch Curve
DVFS
CPU Frontend
Check Opcode
Not Disabled
CPU Backend

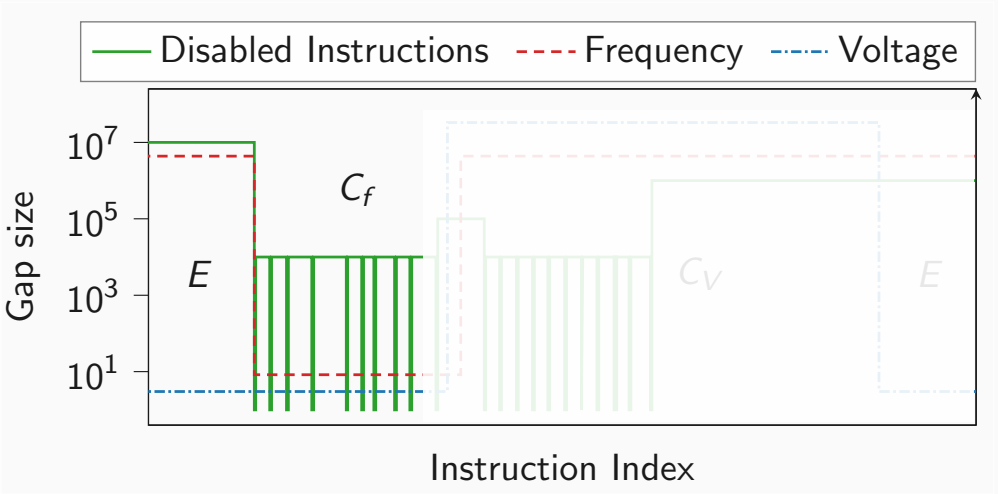

Operating System
Disabled Opcode Exception Handler
Operating Strategy
Disable Opcodes
CPU
Disabled Opcode Exception
Disable Opcode MSR
Switch Curve
DVFS
Control MSRs
CPU Frontend
Check Opcode
Not Disabled
CPU Backend

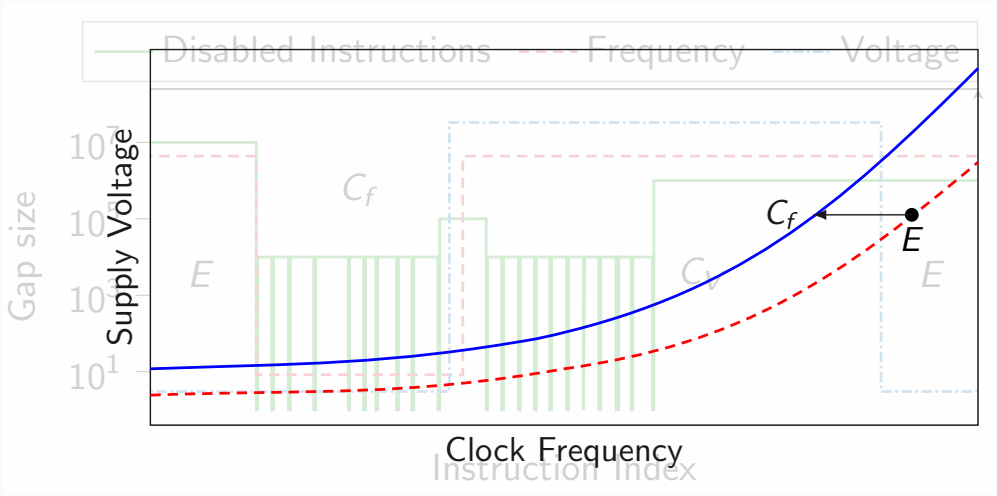

Operating System
Disabled Opcode Exception Handler
Operating Strategy
Disable Opcodes
CPU
Disabled Opcode Exception
Disable Opcode MSR
Switch Curve
DVFS
Control MSRs
CPU Frontend
Check Opcode
Not Disabled
CPU Backend
Increase IMUL latency

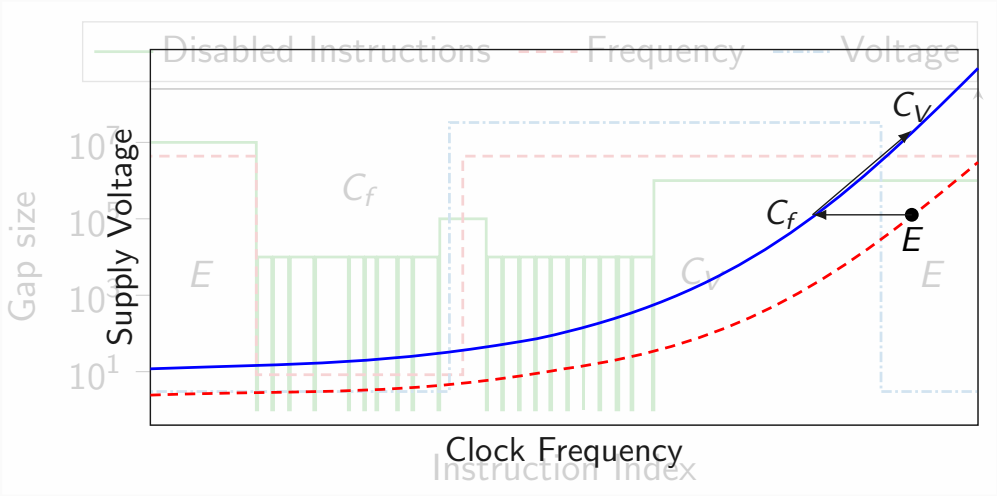

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
E
C_f
C_V
E
Instruction Index

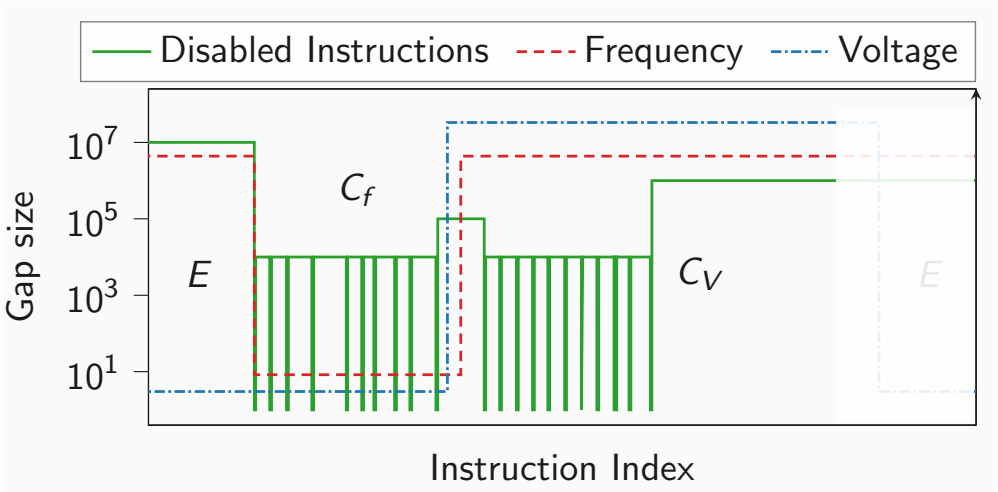

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
Supply Voltage
C_f
E
C_V
E
E
Clock Frequency
Instruction Index

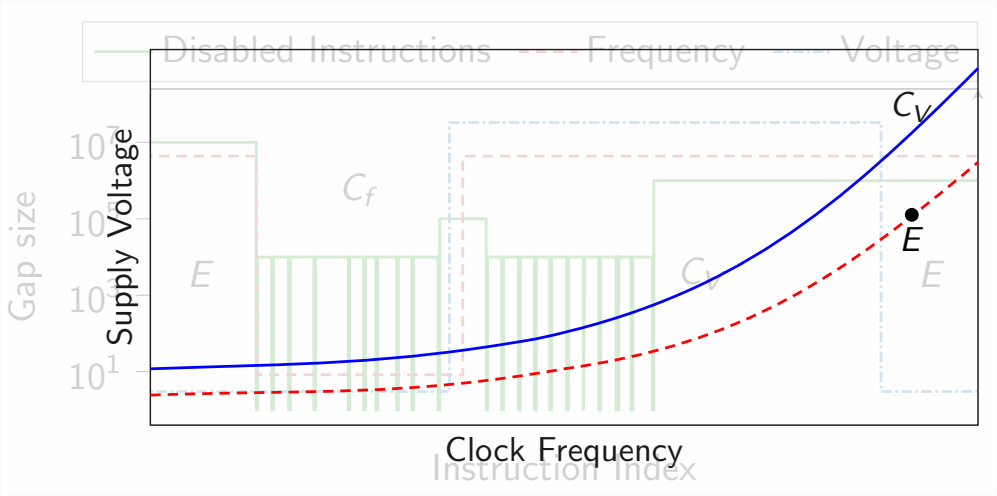

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
Supply Voltage
C_f
E
C_f
E
C_V
E
Clock Frequency
Instruction Index

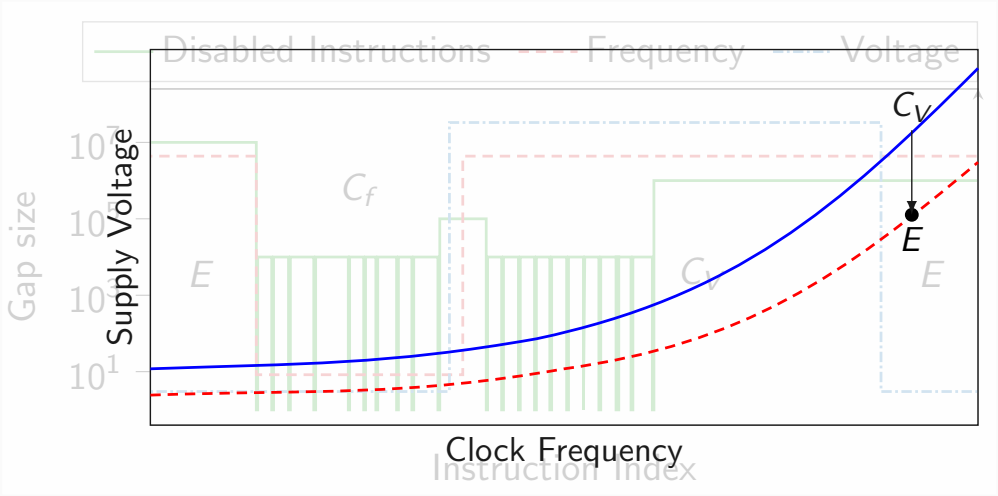

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
E
C_f
C_V
E
Instruction Index

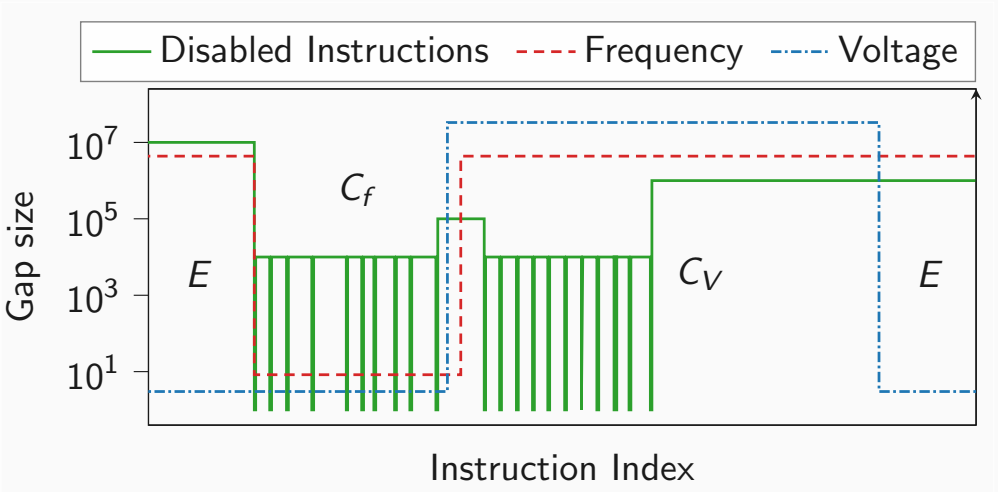

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
Supply Voltage
C_f
E
C_f
E
C_V
E
Clock Frequency
Instruction Index


Disabled Instructions
Frequency
Voltage
Gap size
Supply Voltage
10^7
10^5
10^3
10^1
C_f
E
C_V
C_V
C_f
E
E
Clock Frequency
Instruction Index

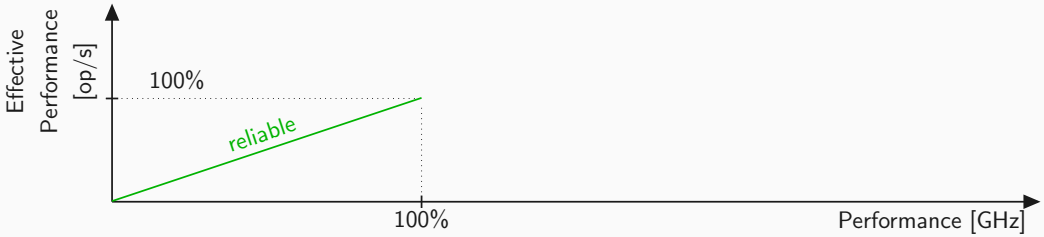

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
E
C_f
C_V
E
Instruction Index

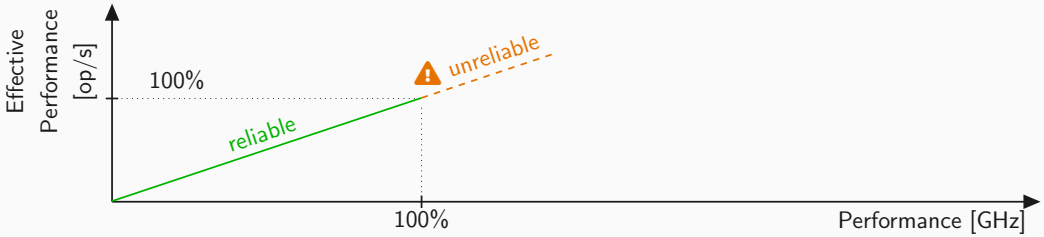

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^4
10^1
Supply Voltage
C_f
E
C_V
C_V
E
E
Clock Frequency
Instruction Index

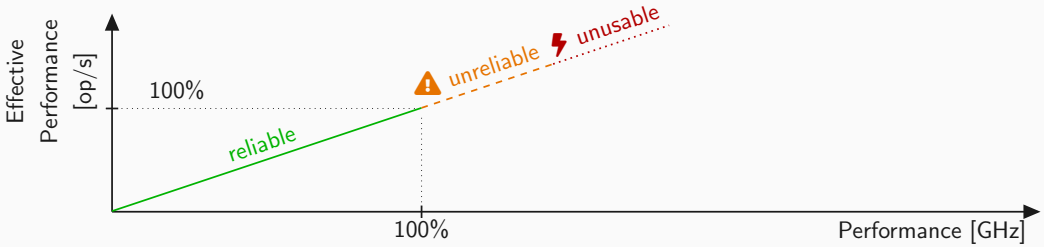

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
Supply Voltage
C_f
E
C_V
E
C_V
E
Clock Frequency
Instruction Index

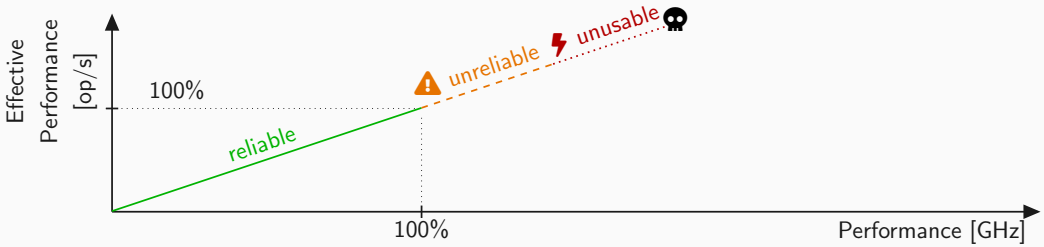

Disabled Instructions
Frequency
Voltage
Gap size
10^7
10^5
10^3
10^1
C_f
E
C_V
E
Instruction Index

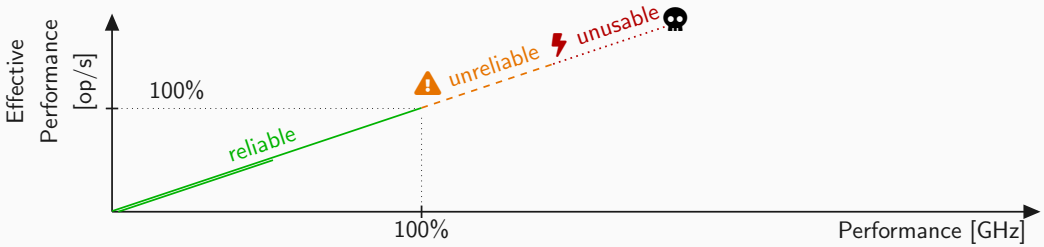
CPU	V_{off}	Score	Power	Freq.	Eff.
i5-1035G1	−70 mV	+6.0 %	−0.1 %	+8.5 %	+6.1 %
	−97 mV	+7.9 %	−0.5 %	+12 %	+8.4 %
i9-9900K	−70 mV	+2.2 %	−7.2 %	+2.6 %	+10 %
	−97 mV	+3.8 %	−16 %	+3.3 %	+23 %
7700X*	−70 mV	+1.4 %	−9.8 %	+1.8 %	+12 %
	−97 mV	+1.9 %	−15 %	+1.8 %	+20 %

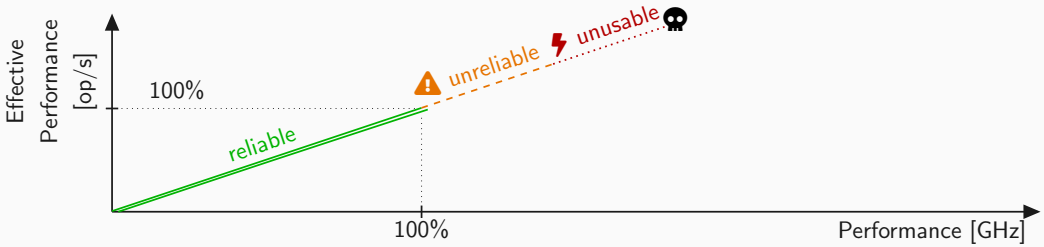

Effective Performance [op/s]
100%
reliable
100%
Performance [GHz]


Effective Performance [op/s]
100%
unreliable
reliable
100%
Performance [GHz]

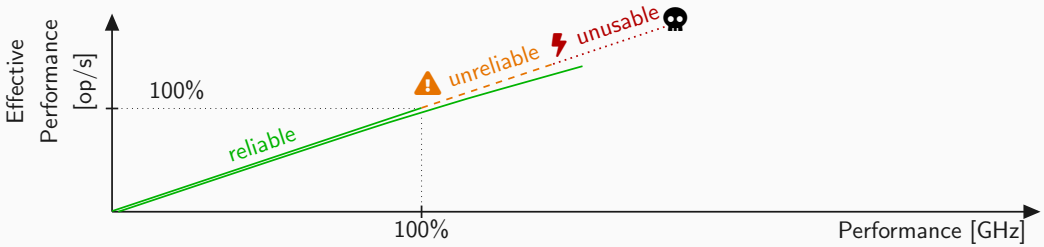

Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]

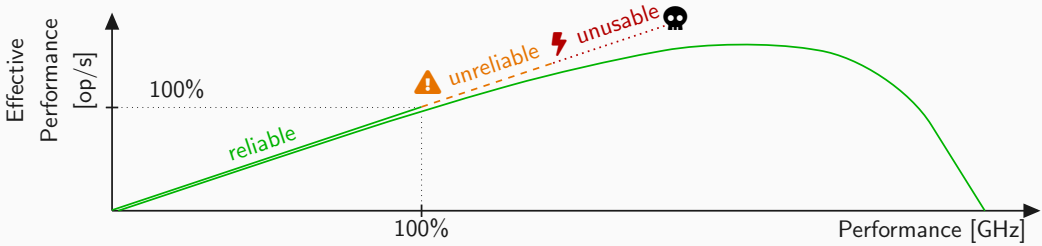

Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]

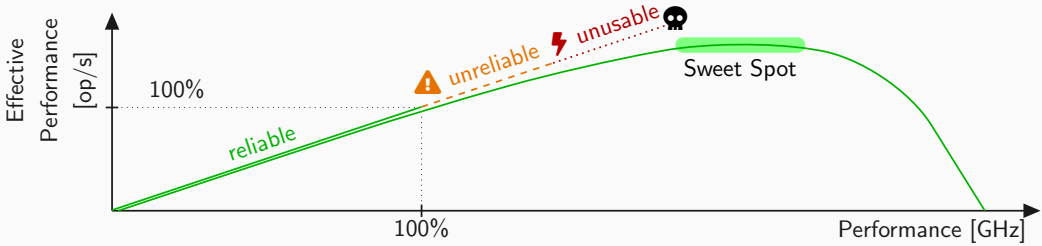

Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]


Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]

How to make Security Sustainable




Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]


Effective Performance [op/s]
100%
reliable
unreliable
unusable
Sweet Spot
100%
Performance [GHz]

Faulting Hardware from Software and Sustainable Mitigations

Daniel Gruss

2024-04-04

Graz University of Technology