Finding, Patching, and Promoting Security Research

... and what about Sustainability?

Daniel Gruss

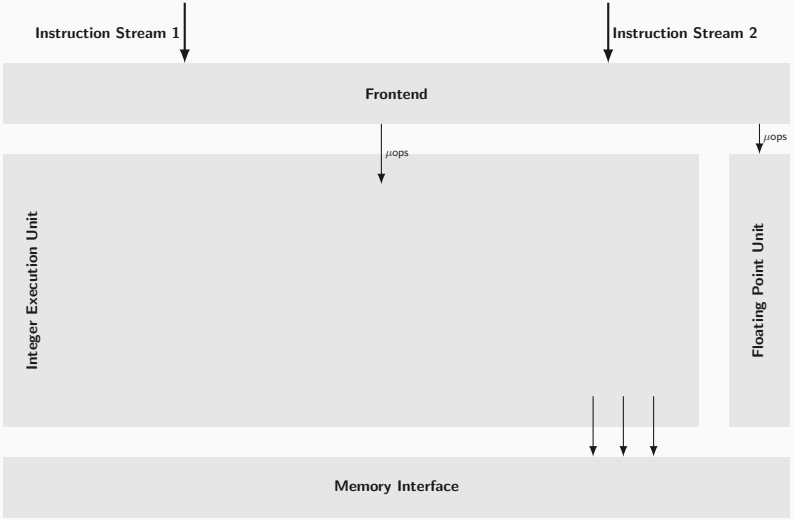
2024-04-17

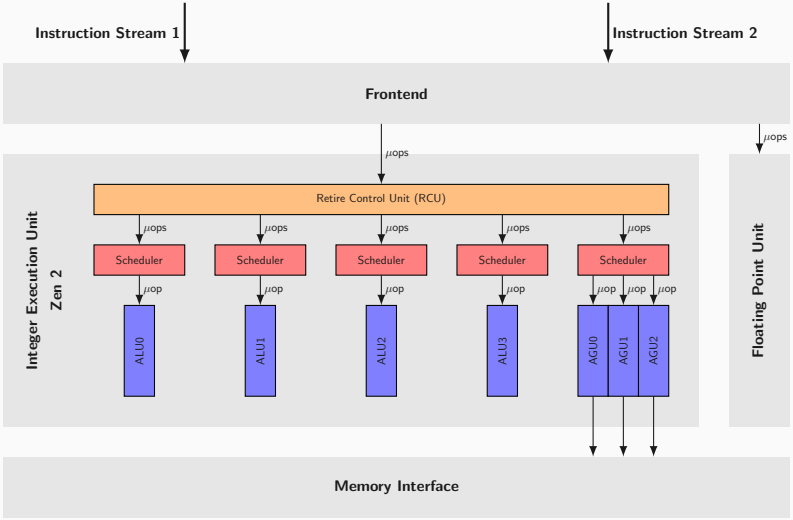
Graz University of Technology

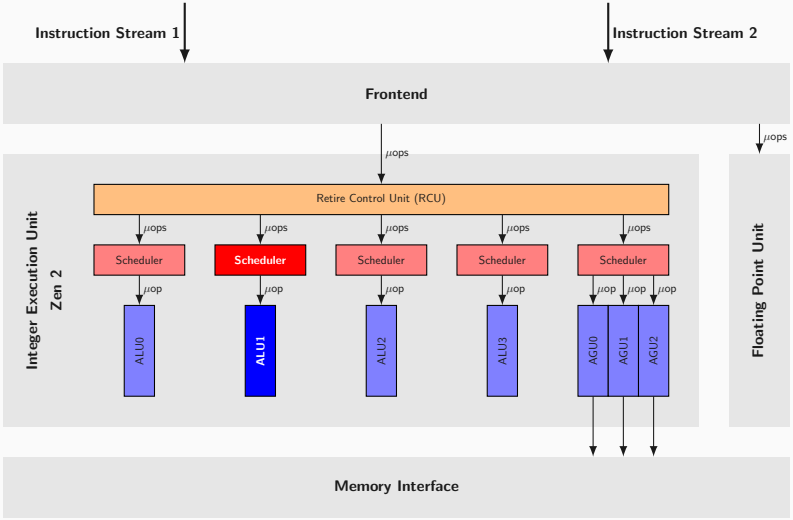
How to find ...

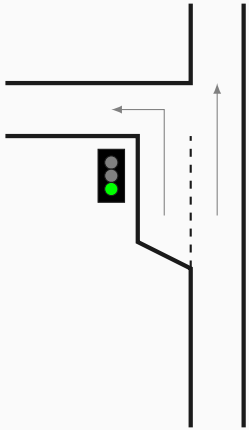
How to find ... side channels?

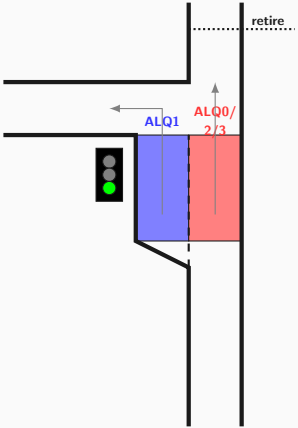
Side Channels are Everywhere

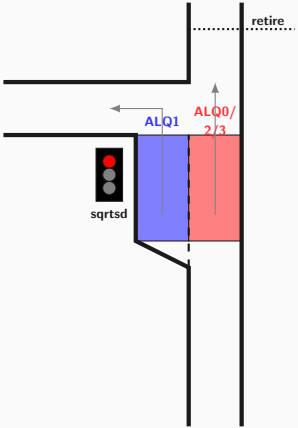

Instruction Stream 1
Instruction Stream 2
Frontend
µops
µops
Integer Execution Unit
Floating Point Unit
Memory Interface

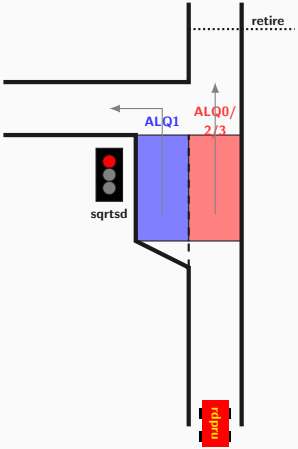

Instruction Stream 1
Instruction Stream 2
Frontend
µops
µops
Retire Control Unit (RCU)
µops
µops
µops
µops
µops
Scheduler
Scheduler
Scheduler
Scheduler
Scheduler
µop
µop
µop
µop
µop
µop
µop
ALU0
ALU1
ALU2
ALU3
AGU0
AGU1
AGU2
Integer Execution Unit
Zen 2
Floating Point Unit
Memory Interface

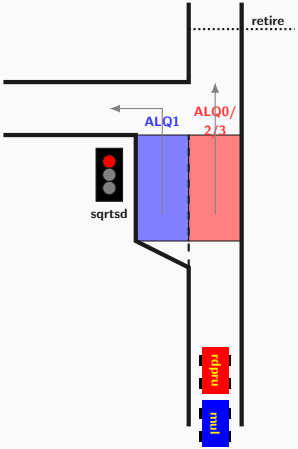

Instruction Stream 1
Instruction Stream 2
Frontend
µops
µops
Retire Control Unit (RCU)
µops
µops
µops
µops
µops
Scheduler
Scheduler
Scheduler
Scheduler
Scheduler
µop
µop
µop
µop
µop
µop
µop
ALU0
ALU1
ALU2
ALU3
AGU0
AGU1
AGU2
Integer Execution Unit
Zen 2
Floating Point Unit
Memory Interface

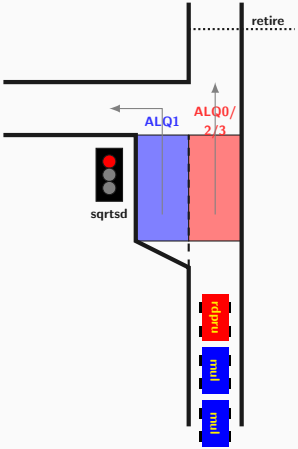


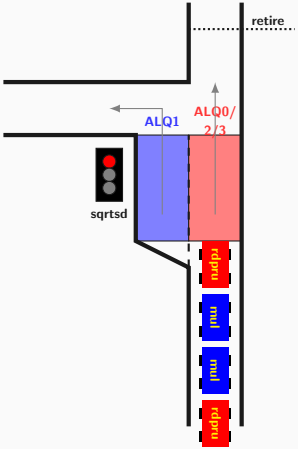

retire
ALQ1
ALQ0/
2/3

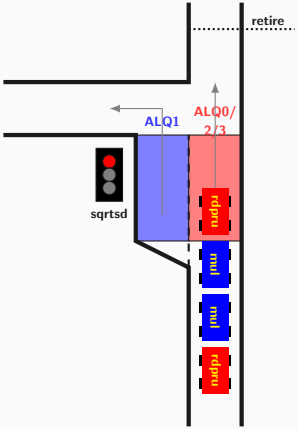

retire
ALQ1
ALQ0/
2/3
sqrtsd

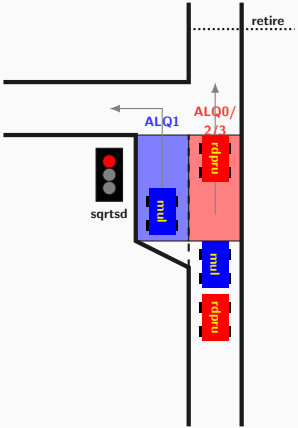

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn

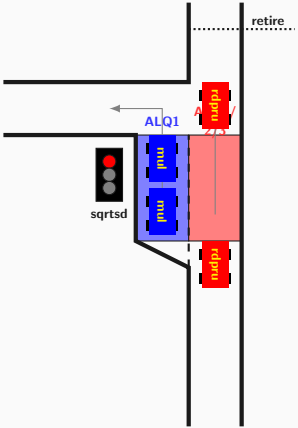

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul

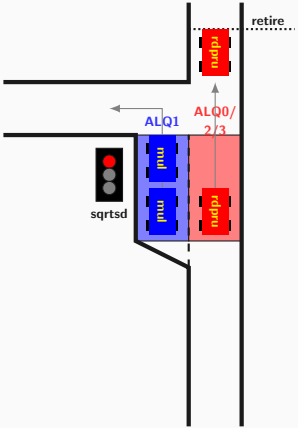

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul
mul

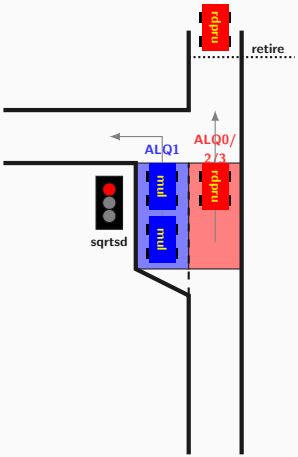

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul
mul
rdpn

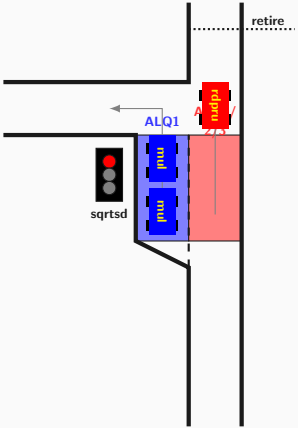

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
rwl
rwl
rdpn

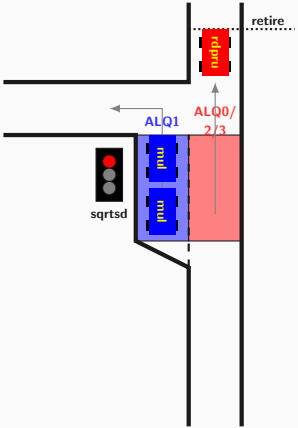

retire
ALQ1
ALQ0/
2/3
rdpn
rdpn
rdpn
mul
mul
sqrtsd

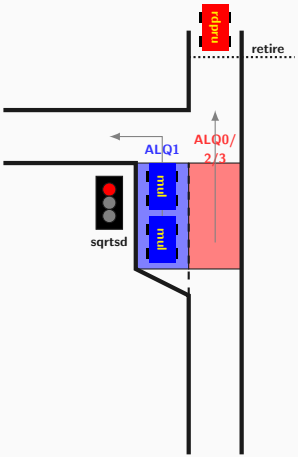

retire
ALQ1
sqrtsd

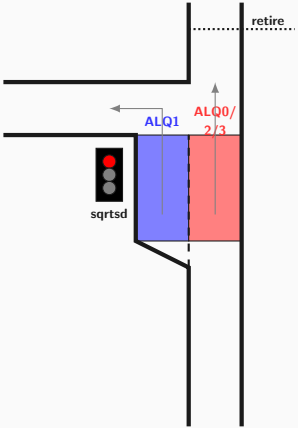

retire
rdpn
ALQ1
ALQ0/
2/3
mul
mul
rdpn
sqrtsd

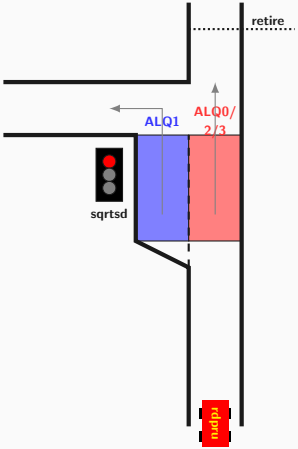

rdpn
retire
ALQ1
ALQ0/
2/3
rdpn
mul
mul
sqrtsd

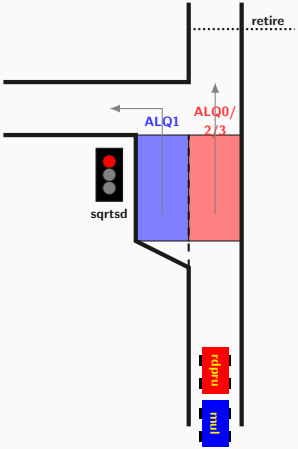

retire
ALQ1
sqrtsd

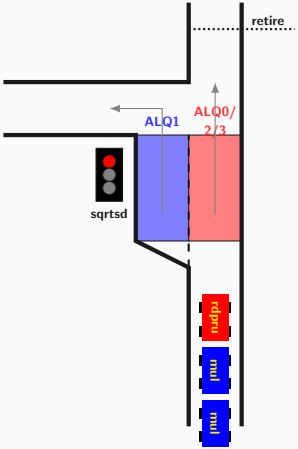

retire
rdprn
ALQ1
ALQ0/
2/3
mwf
mwf
sqrtsd

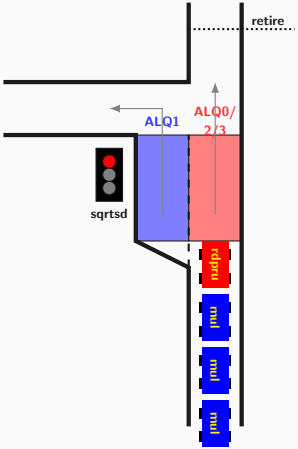

idpm
retire
ALQ1
ALQ0/
2/3
mul
mul
sqrtsd

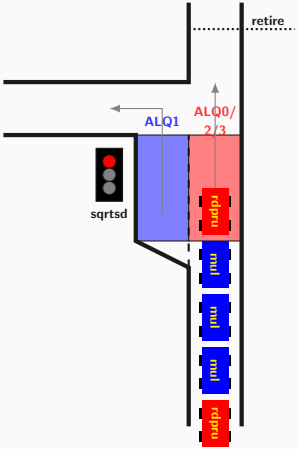

retire
ALQ1
ALQ0/
2/3
sqrtsd

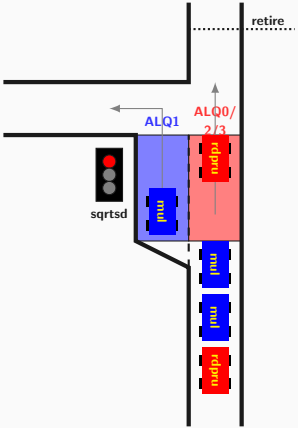

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn

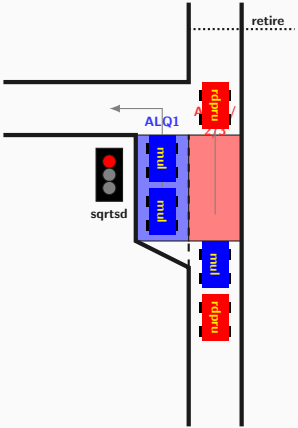

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul

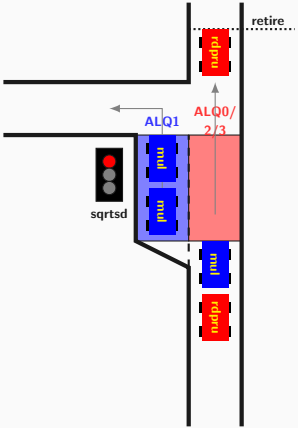

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdpn
mul
mul

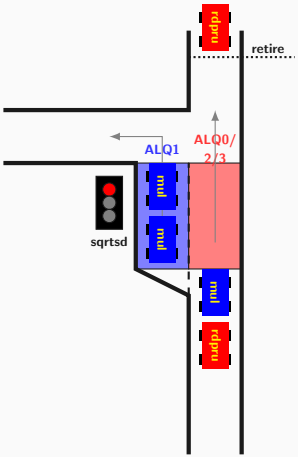

retire
ALQ1
ALQ0/
2/3
sqrtsd
dqrt
mul
mul
mul

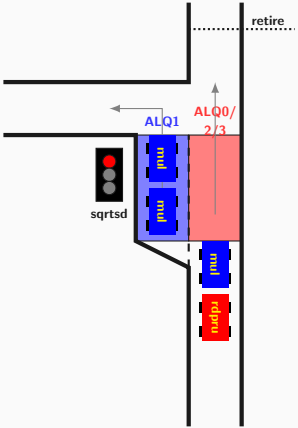

retire
ALQ1
ALQ0/
2/3
sqrtsd
rdqn
mul
mul
mul
rdqn

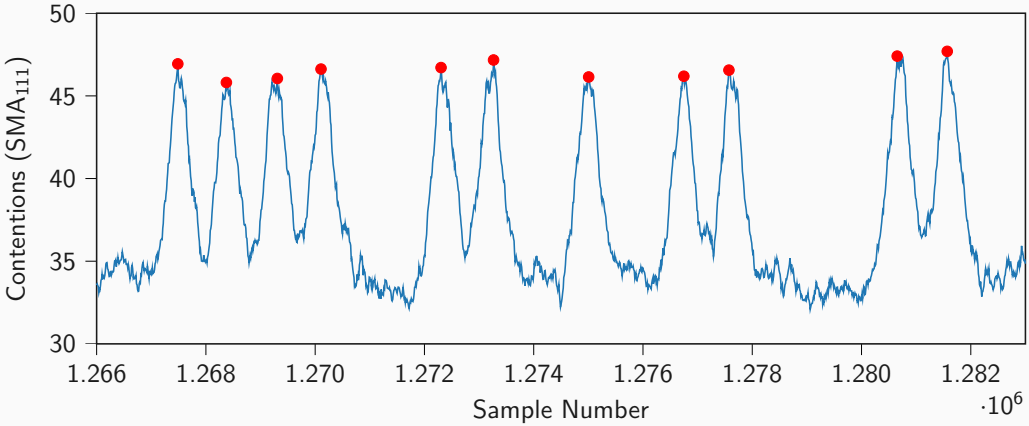

retire
ALQ1
ALQ0/
2/3
rdpn
sqrtsd
mul
mul
mul
rdpn

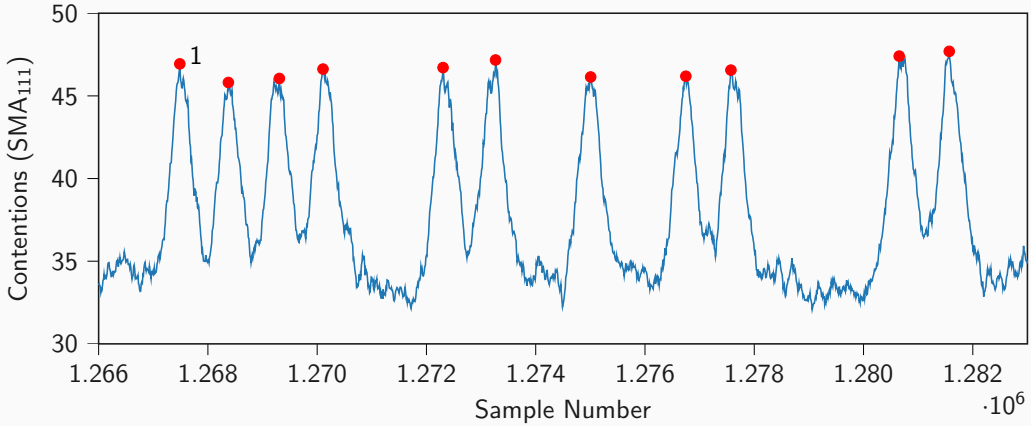

retire
ALQ1
sqrtsd

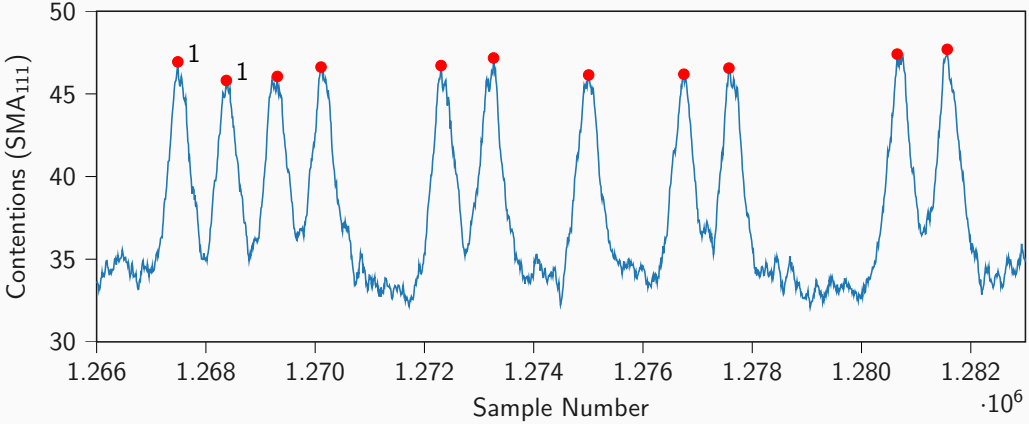

retire
rdpn
ALQ1
ALQ0/
2/3
rwu
rwu
sqrtsd
rwu
rdpn

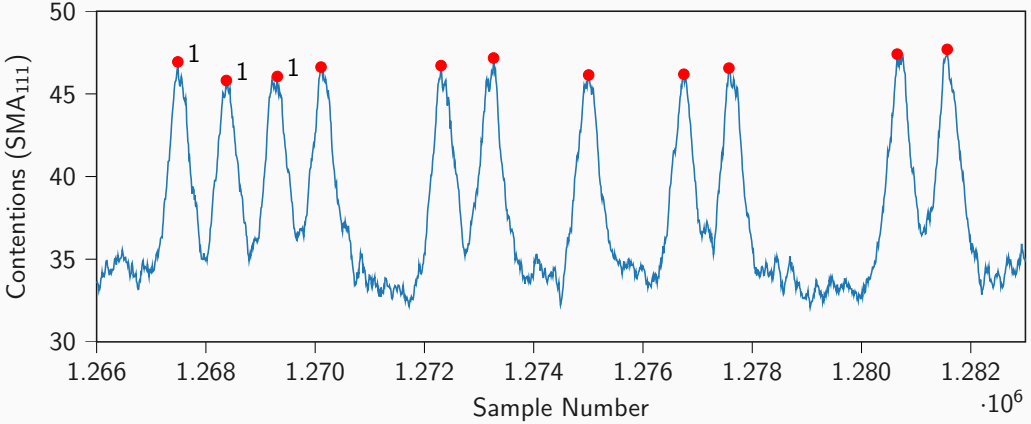

rdpn
retire
ALQ1
ALQ0/
2/3
rwd
rwd
sqrtsd
rwd
rdpn

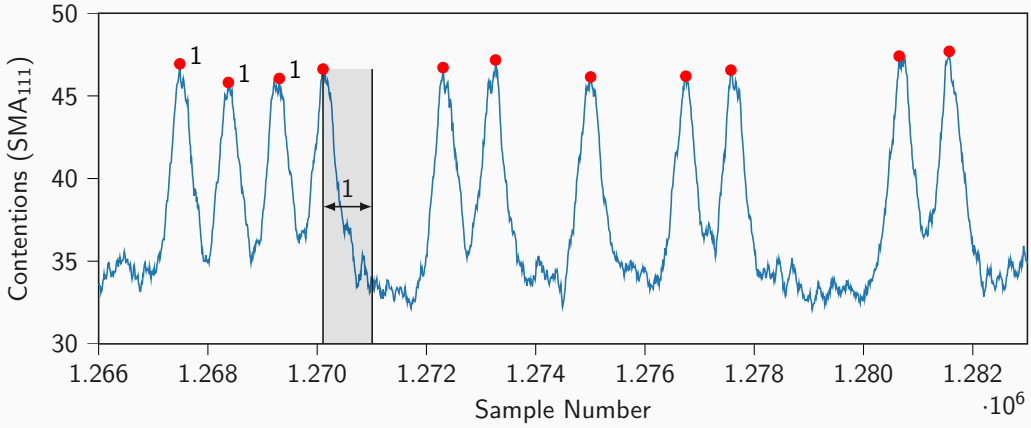

retire
ALQ1
ALQ0/
2/3
sqrtsd
rtdpn

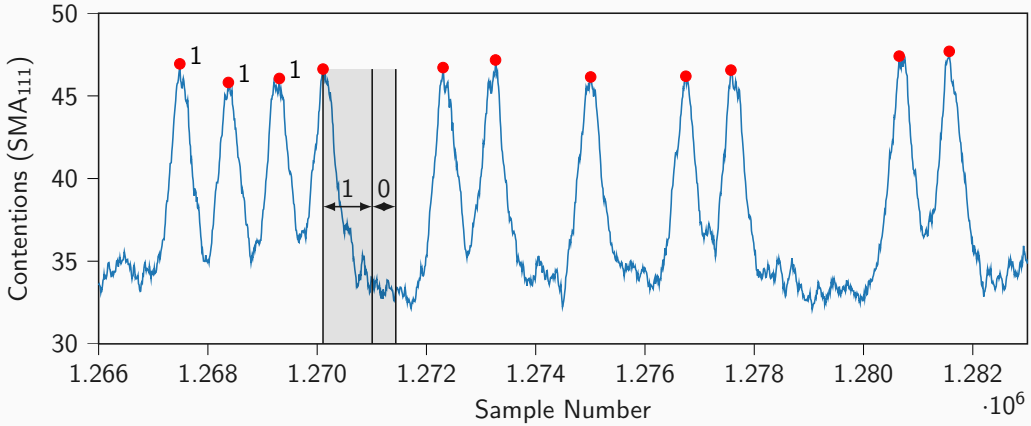

50
45
40
35
30
Contentions (SMA111)
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

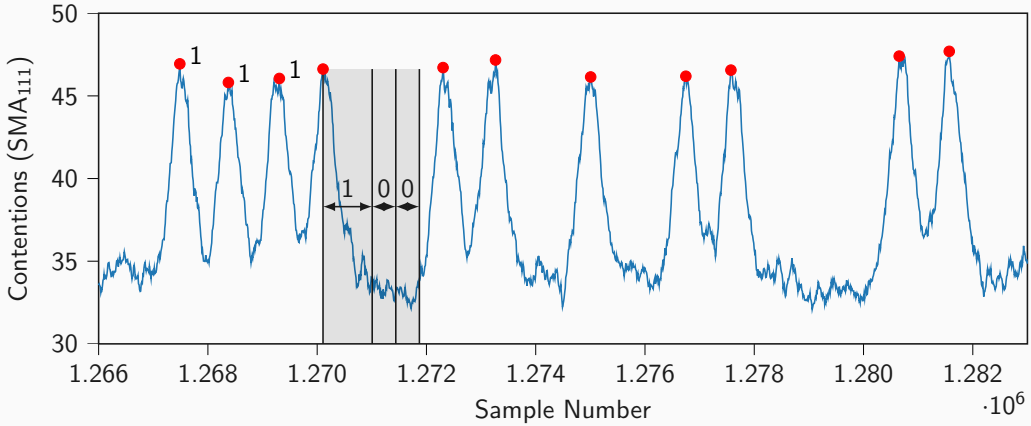

50
45
40
35
30
Contentions (SMA111)
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

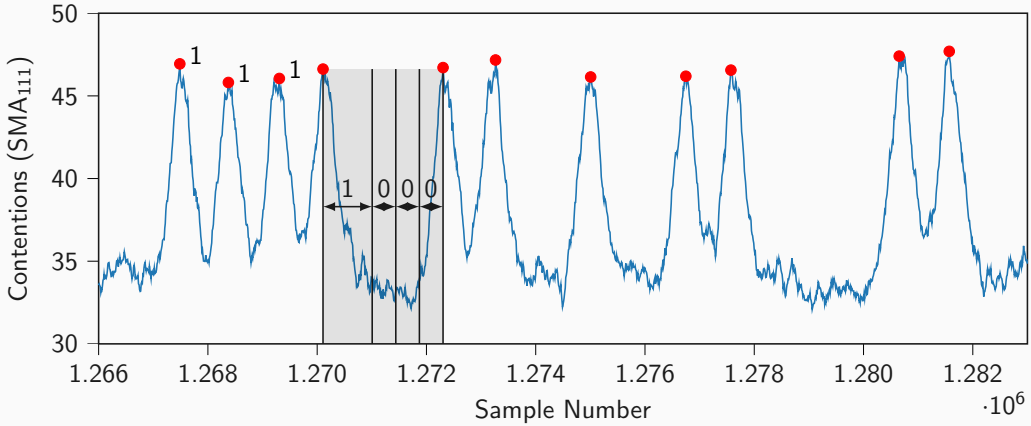

50
45
40
35
30
Contentions (SMA111)
1
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

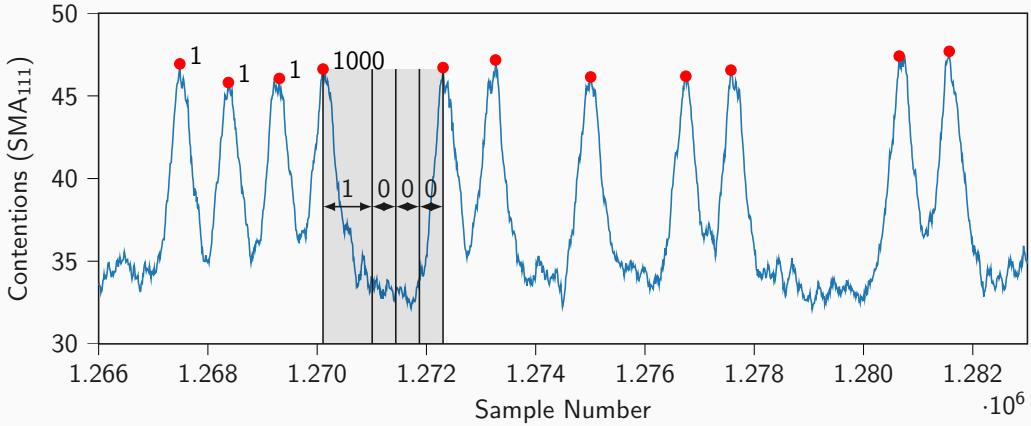

50
45
40
35
30
Contentions (SMA111)
1
1
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

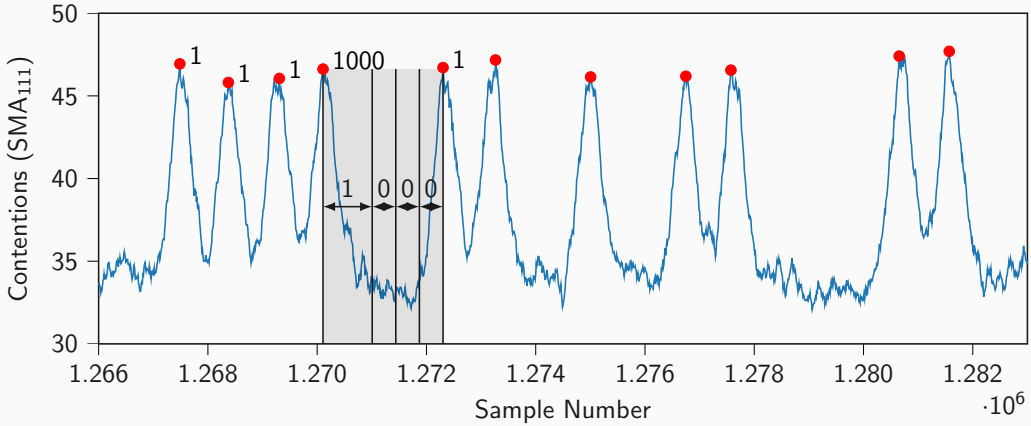

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

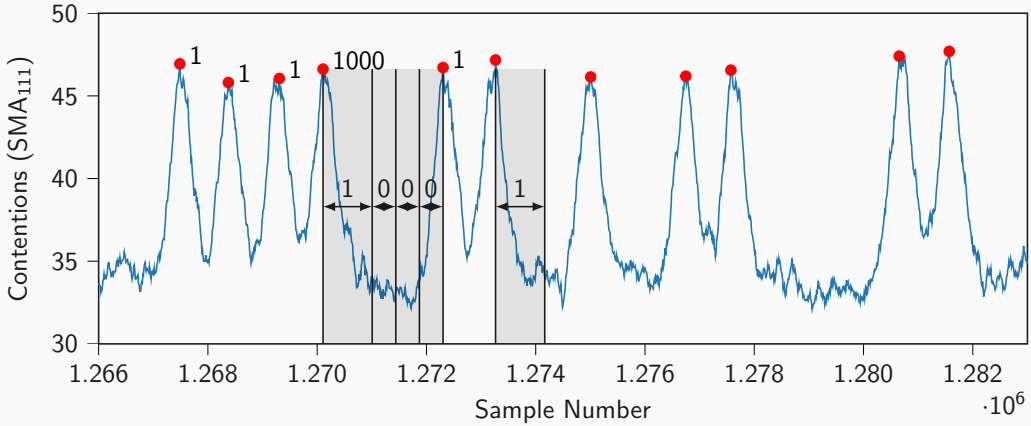

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

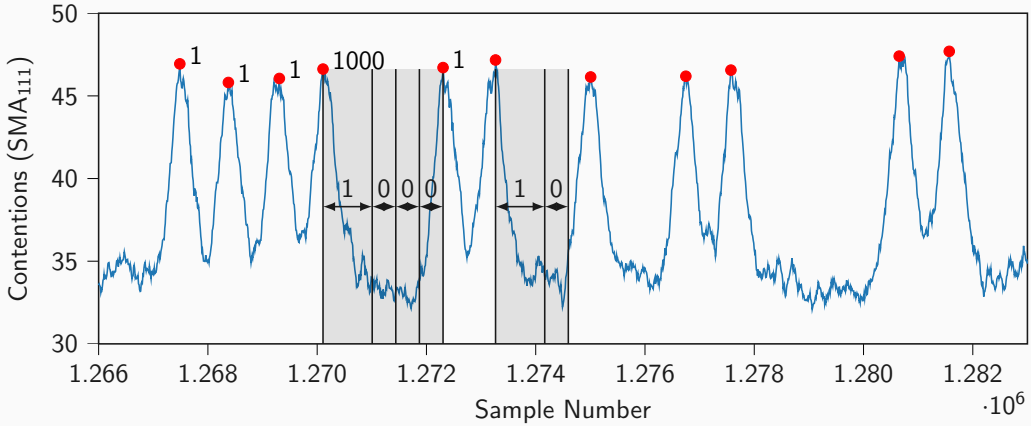

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
0
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

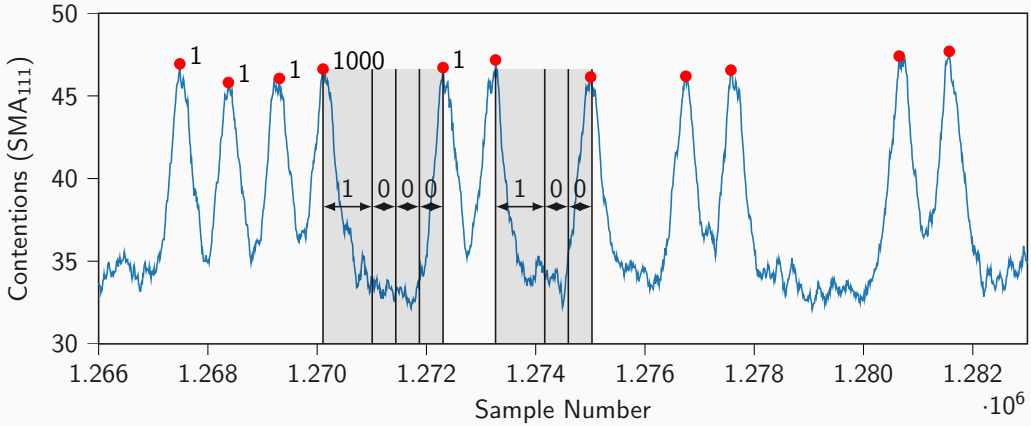

50
45
40
35
30
Contentions (SMA111)
1
1
1
1
0
0
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

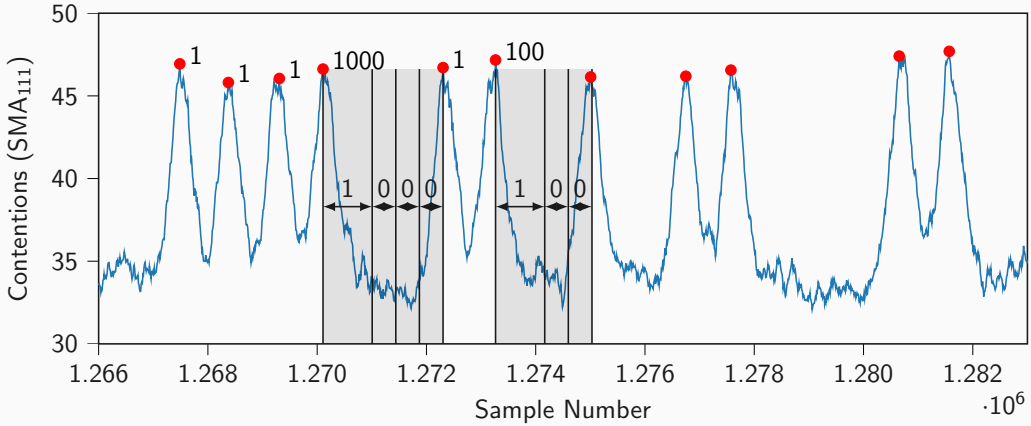

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
0
0
0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

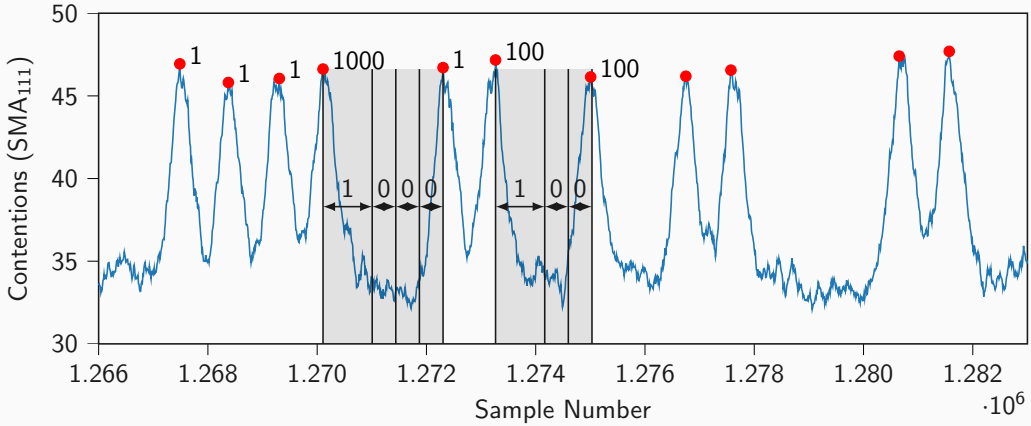

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

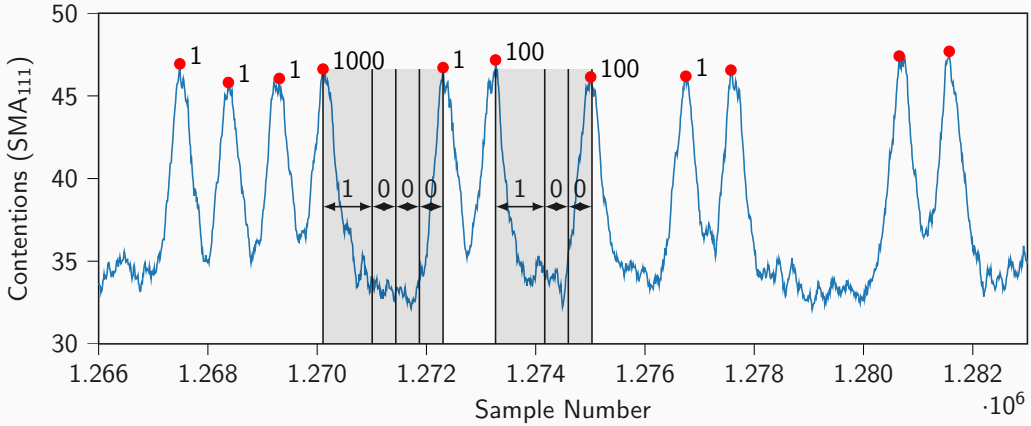

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

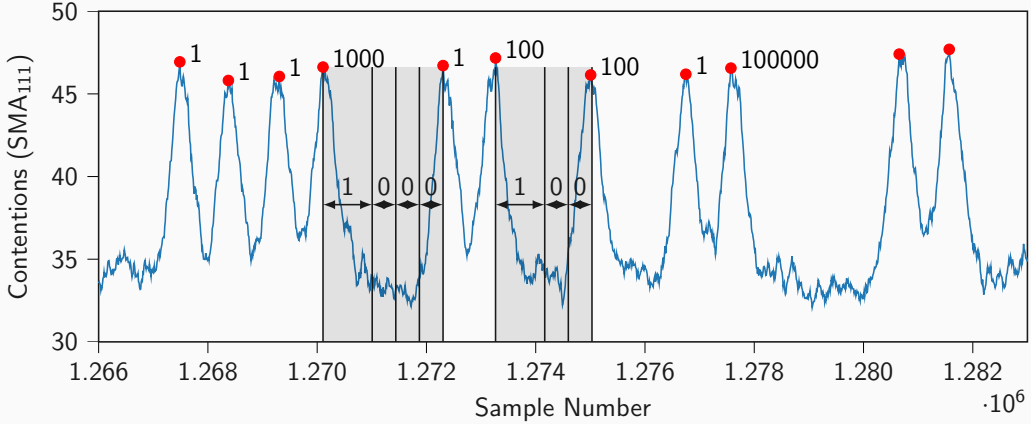

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

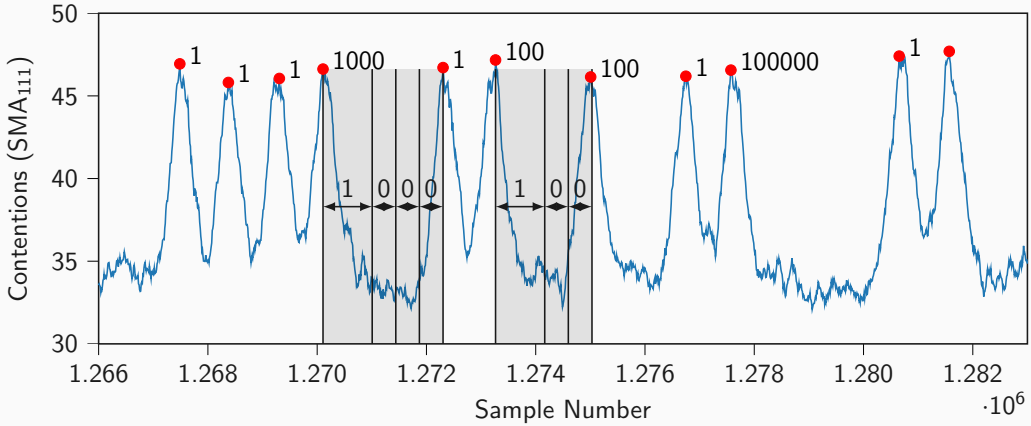

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

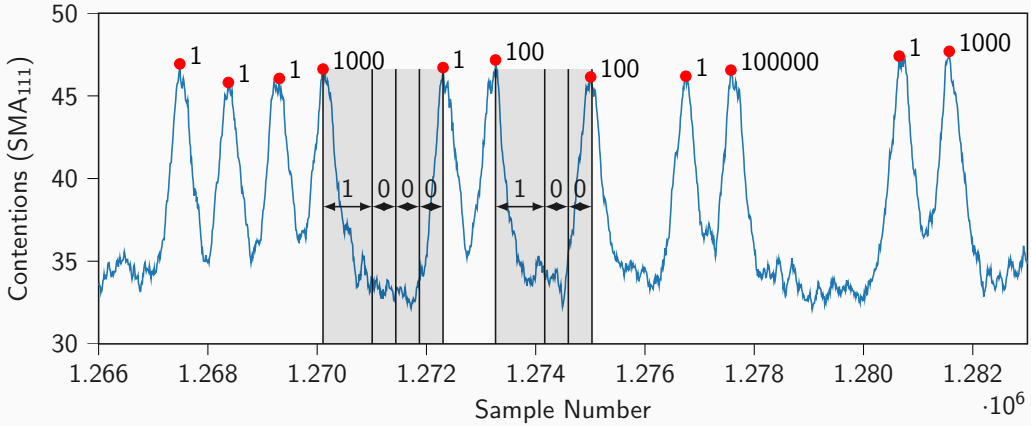

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
100
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

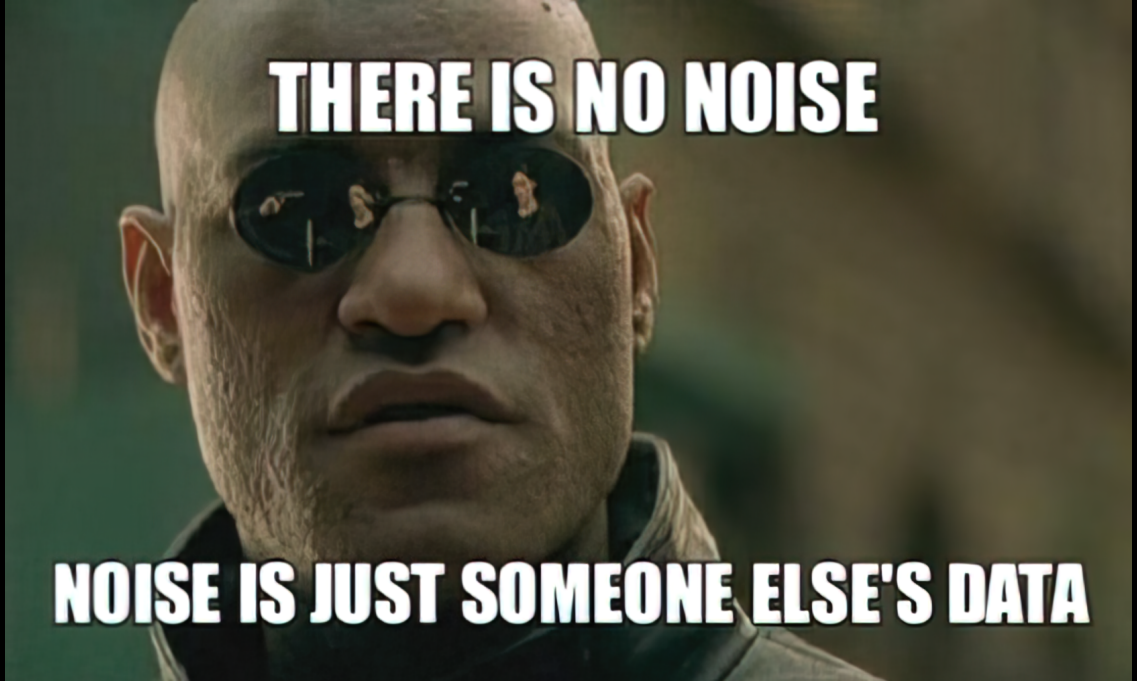

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
100
100
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6


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

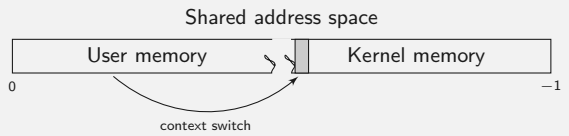

Contentions (SMA111)
50
45
40
35
30
1
1
1
1000
1
100
100
1
100000
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6

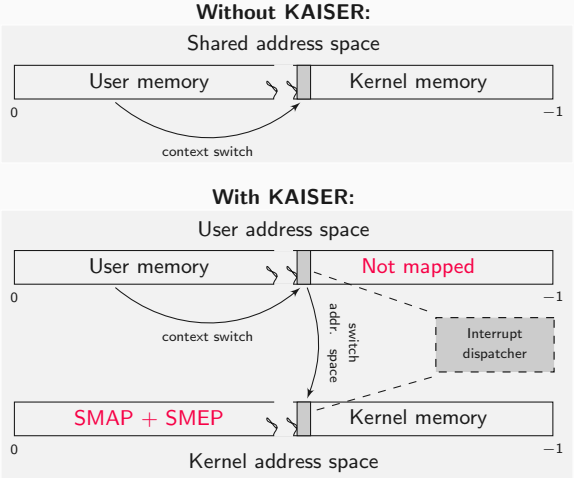

50
45
40
35
30
Contentions (SMA111)
1
1
1
1000
1
100
100
1
100000
1
1 0 0 0
1 0 0
1.266
1.268
1.270
1.272
1.274
1.276
1.278
1.280
1.282
Sample Number
·10^6


Contentions (SMA111)
50
45
40
35
30
1
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

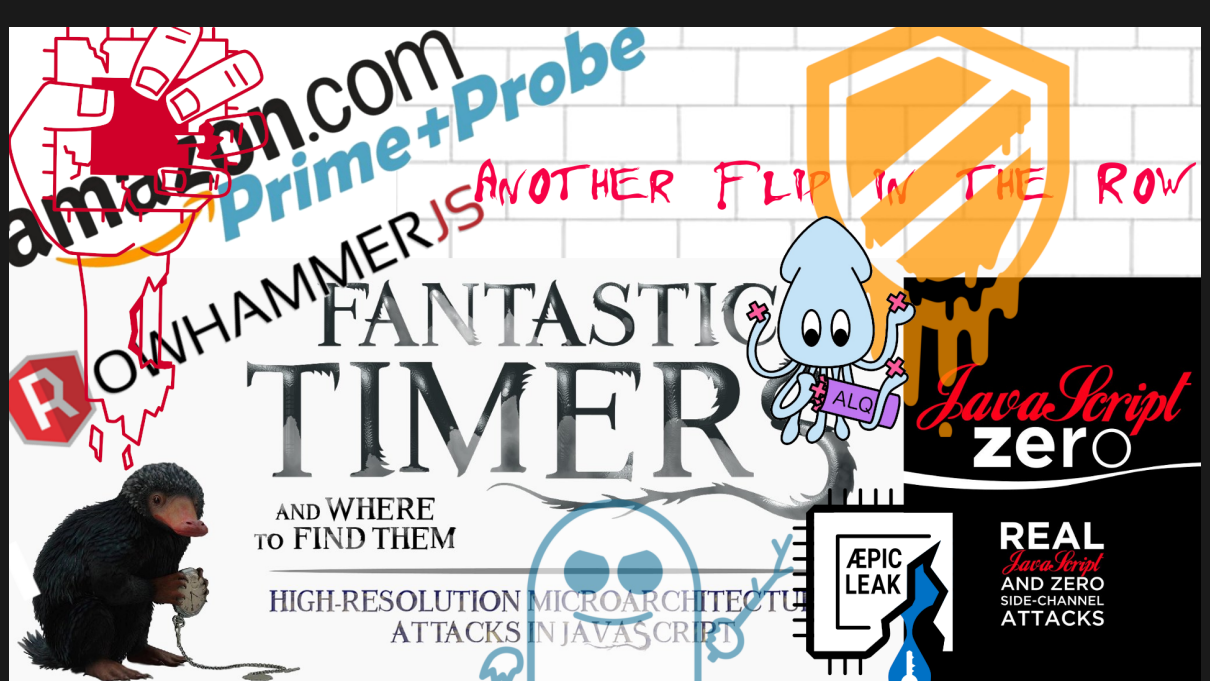

THERE IS NO NOISE
NOISE IS JUST SOMEONE ELSE'S DATA

Without KAISER:




Without KAISER:
Shared address space
User memory
Kernel memory
0
−1
context switch
With KAISER:
User address space
User memory
Not mapped
0
−1
context switch
addr. space switch
Interrupt dispatcher
SMAP + SMEP
Kernel memory
0
−1
Kernel address space

Vulnerability Marketing?


amazon.com
Prime+Probe
ROWHAMMERJS
ANOTHER FLIP IN THE ROW
FANTASTIC
TIMERS
AND WHERE
TO FIND THEM
HIGH-RESOLUTION MICROARCHITECTU
ATTACKS IN JAVASCRIPT
ALO
JavaScript
zero
ÆPIC
LEAK
REAL
JavaScript
AND ZERO
SIDE-CHANNEL
ATTACKS

Marketing...

- Why do you have a website?

- Why do you have a website?$\rightarrow$ Inform journalists and the general public

Marketing...

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names?

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names? → what was CVE-2017-5754 again?

Marketing...

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names? → what was CVE-2017-5754 again?
  - People will throw things together that don't belong together

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names? → what was CVE-2017-5754 again?
  - People will throw things together that don't belong together

  → Names enable unambiguous communication

Marketing...

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names? → what was CVE-2017-5754 again?
  - People will throw things together that don't belong together

  → Names enable unambiguous communication
- Why do you need a logo?

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names? → what was CVE-2017-5754 again?
  - People will throw things together that don't belong together

  → Names enable unambiguous communication
- Why do you need a logo?
  - Otherwise: media makes their own

- Why do you have a website?→ Inform journalists and the general public
  - Otherwise: completely misleading presentation of your work in the media

  → defend yourself against misleading presentations!
- Why do you have fancy names? → what was CVE-2017-5754 again?
  - People will throw things together that don't belong together

  → Names enable unambiguous communication
- Why do you need a logo?
  - Otherwise: media makes their own → no control over how inappropriate these are

Let's Keep it to Ourselves: Don't Disclose Vulnerabilities

by Gus Uht on Jan 31, 2019 | Tags: Opinion, Security

With the complexity of current hardware and software systems arising from billions of transistors and millions of lines of code, it is unlikely that any system will ever be bug-free or vulnerability-free. There are effectively an infinite number of unknown vulnerabilities: "Every day, the AV-TEST Institute registers over 350,000 new malicious programs (malware) and potentially unwanted applications (PUA)." What then is the point of actively 'discovering' new vulnerabilities and disclosing them? They are effectively being invented and empower black hats to wreak havoc without making systems safer. It is a race to the bottom. At the same time it can unnecessarily ratchet up the public's anxieties.

Pros and Cons: Many arguments for full disclosure have been made over the years, e.g.: *Schneier: Full Disclosure of Security Vulnerabilities a 'Damned Good Idea'*, *Hardware Security* and references therein, and *Reflections on trusting SGX*. However, they all seem to miss the basic point: if you don't want to be blown up, you don't tell the world how to make and use a bomb. Better yet, don't even tell the world that such a thing as a 'bomb' exists. Just knowing that something can be done is enough to drive others to successful re-invention.

Even with responsible disclosure it may be the case that a fix cannot be made quickly, but the vulnerability inventor decides to fully disclose it anyway, as in the case of Spectre. In this case users will be exposed for possibly a long

CONTRIBUTE

Editor: Brandon Lucia

Associate Editor: Christina Delimitrou

Contribute to Computer Architecture Today

RECENT BLOG POSTS

The Brain-Computer Interfacing Landscape for Computer Architects

Extending Dataflow Techniques from Dense to Sparse Accelerators

Architecture 2.0 Workshop: How Machine Learning Will Redefine Computer Architecture and Systems

Tuning the Symphony of Heterogeneous Memory Systems

Think Twice Before… Using Machine Learning to Manage Cloud Resources

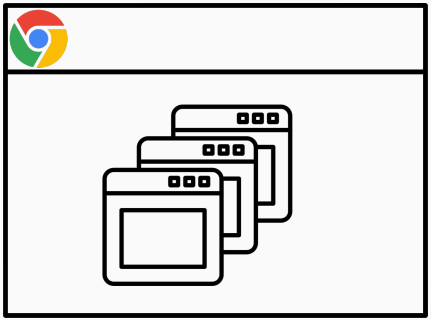
ARCHIVES

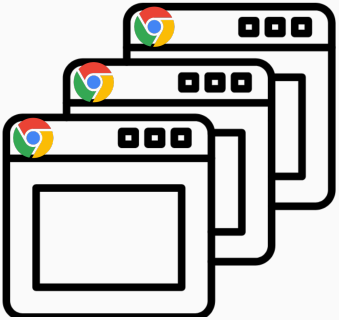
January 2024 (1)

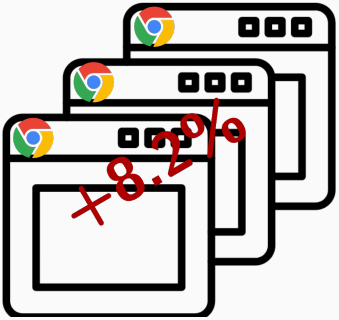

IGNORANCE IS BLISS

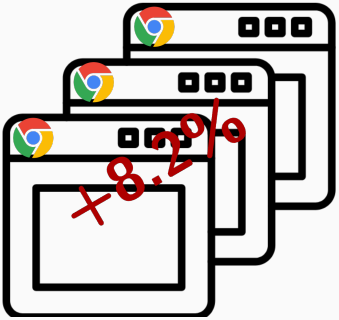
What is the value of security?

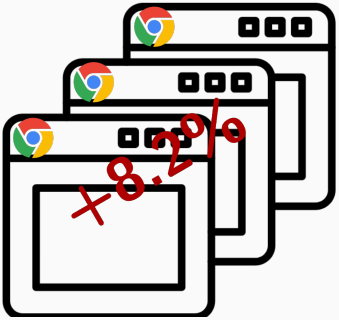
What is the cost of security?

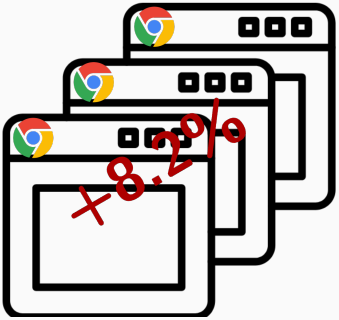




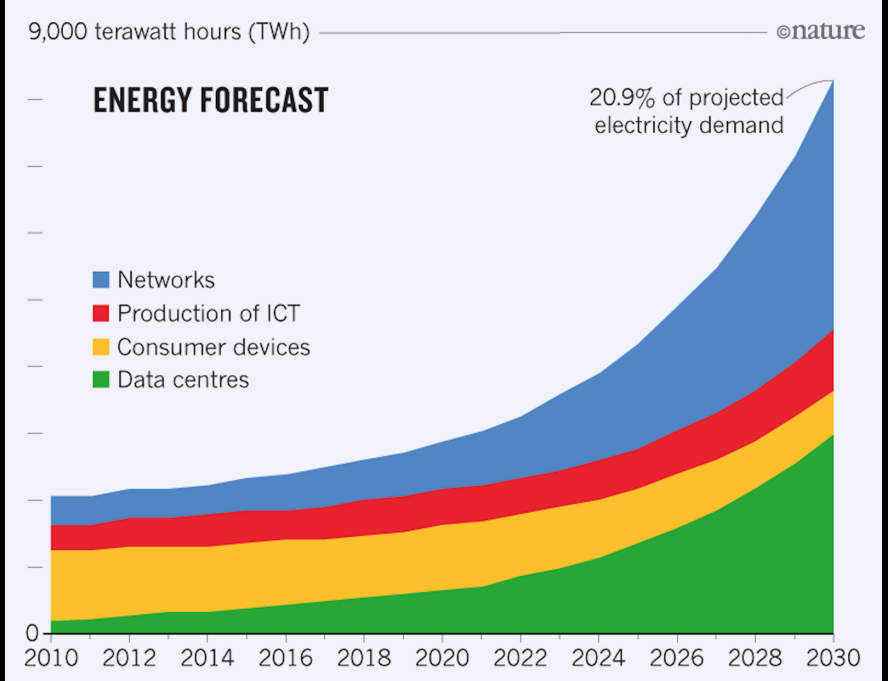

+8.2%


+8.2%


+8.2%

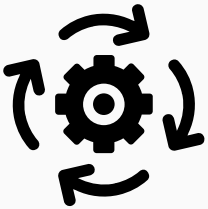

+8.2%


+5%

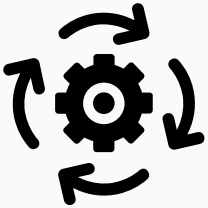

9,000 terawatt hours (TWh)
©nature
ENERGY FORECAST
20.9% of projected electricity demand
Networks
Production of ICT
Consumer devices
Data centres
0
2010
2012
2014
2016
2018
2020
2022
2024
2026
2028
2030

0.09%

0.40%

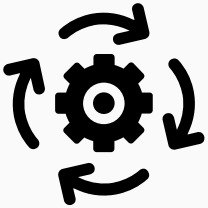


Make bit flips degrade performance **without** impacting security



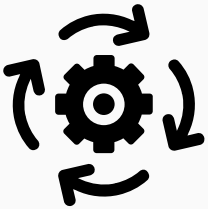
Make bit flips degrade performance **without** impacting security

- Cryptographic MAC



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

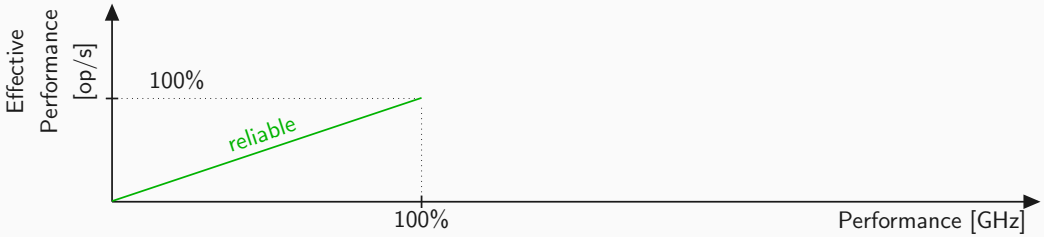
- Cryptographic MAC
- Detect **any** number of bit flips

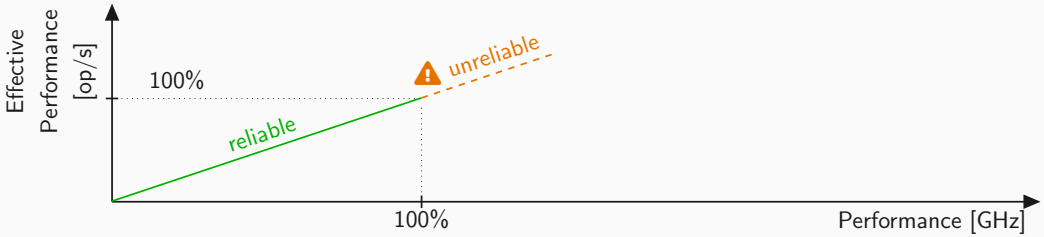


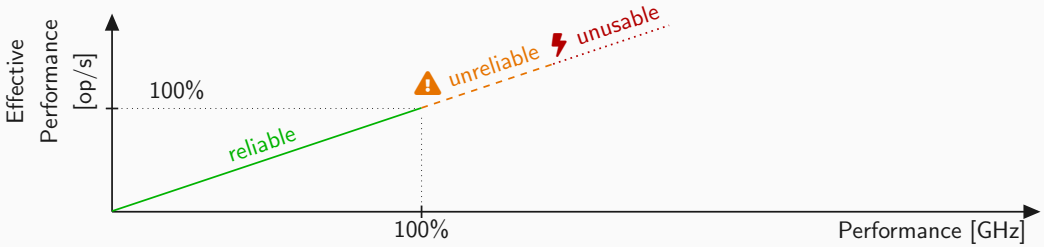
Make bit flips degrade performance **without** impacting security

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

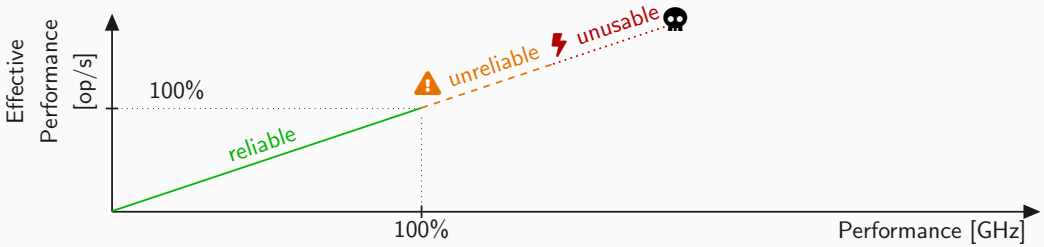
# Errors	# MAC Comp.	Avg Duration
1	17	11 ns
2	771	3.68 µs
3	33 800	124 µs
4	1.51×10^6	6.65 ms
5	6.91×10^7	261 ms
6	3.07×10^9	12.8 s
7	1.21×10^{11}	9.11 min
8	5.72×10^{12}	6.11 h


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

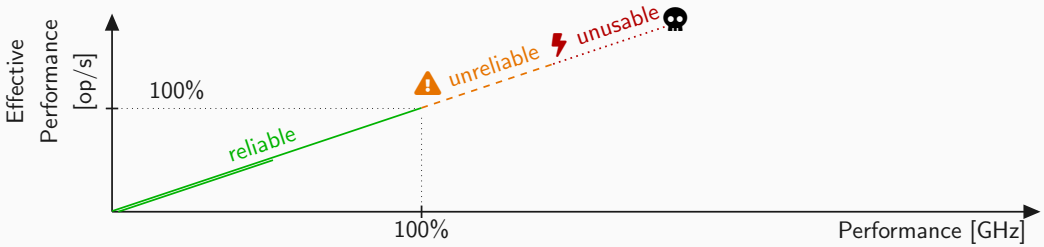

Effective Performance [op/s]
100%
unreliable
reliable
100%
Performance [GHz]

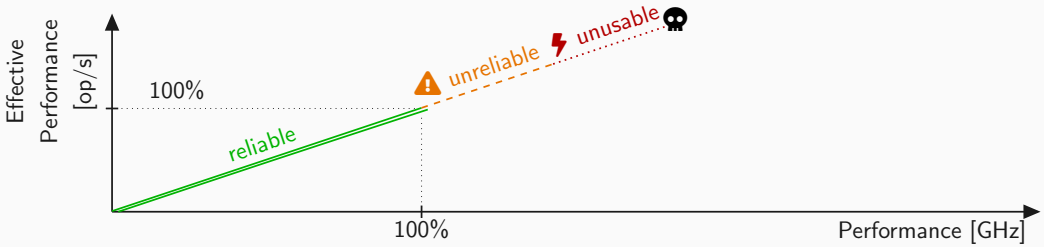

Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]

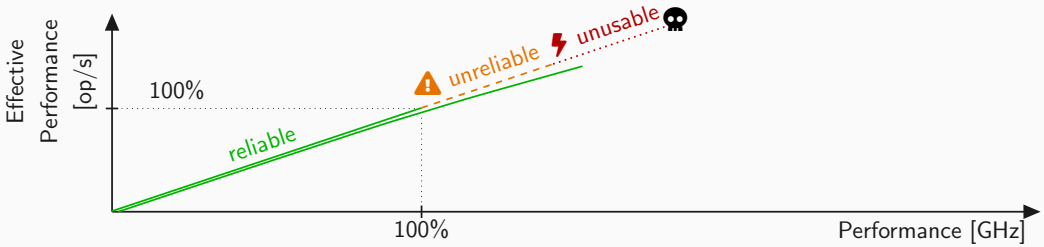
How to make Security Sustainable



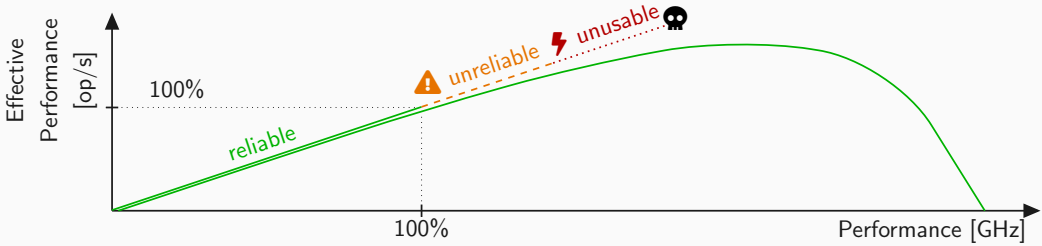
How to make Security Sustainable

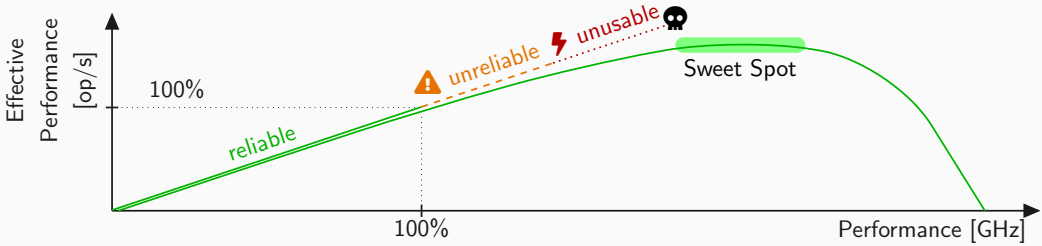



Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Performance [GHz]


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

How to make Security Sustainable




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

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 %

Finding, Patching, and Promoting Security Research

... and what about Sustainability?

Daniel Gruss

2024-04-17

Graz University of Technology