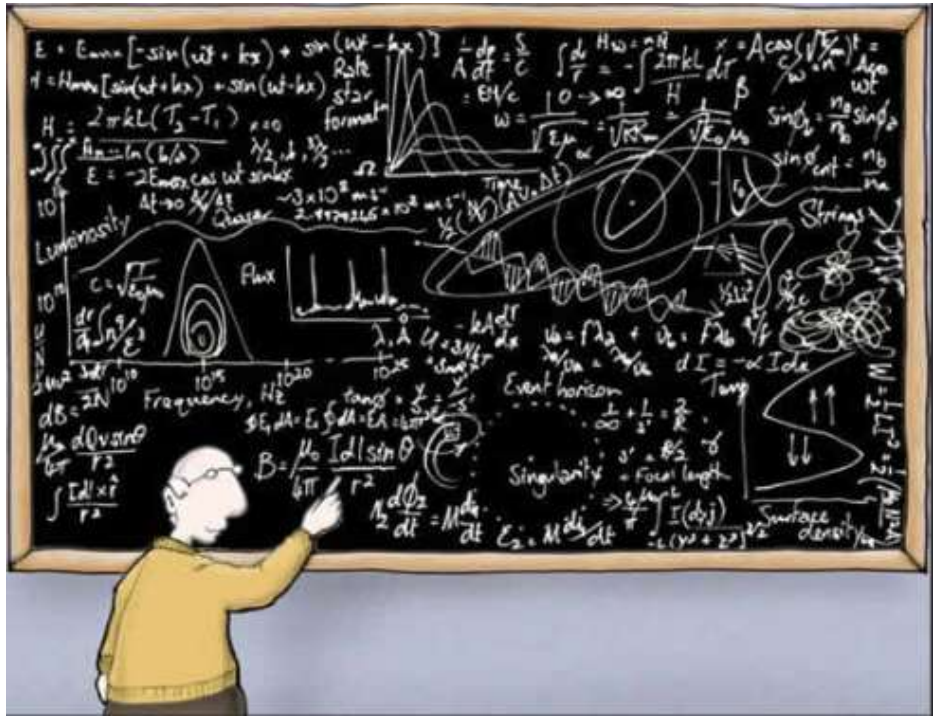
Sur l’application a la microarchitecture des attaques par faute(s) et canaux caches, le tout en 10 mins, tout compris

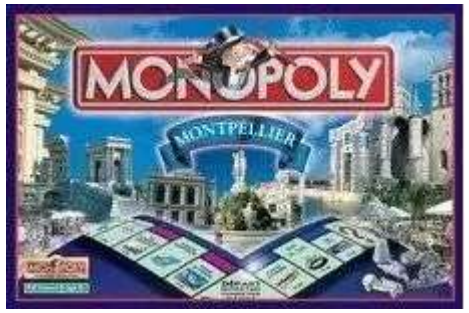


Lendi de la Cyber
Novembre 2022
david@samyde.com

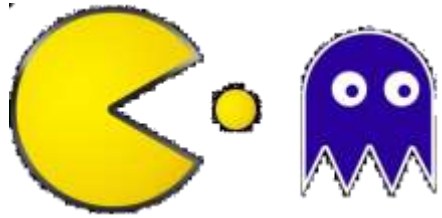
En 600 000 milliseconds, on va parler de :

Cache cache

Attaque(s) par mesure du temps



Prison



PacMan / Spectre

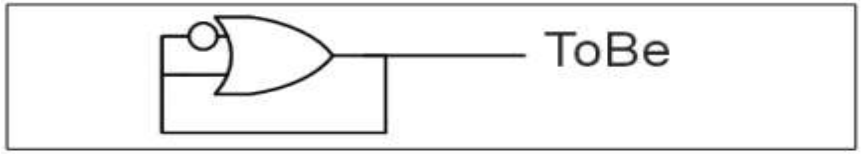


Figure 12 : **Hamlet : ToBe = ToBe or not ToBe**

Horloge

Faute(s)

2B + /2B = FF =255 decimal

Pipe Line

Poisson Volant

R.I.S.C

Microcode

Limitations des attaques physiques materielles …

- “Salut les potos, coucou c’est moi, je le branche ou l’oscillo …?”

- Le centre de donnees est un endroit plus ou moins securise

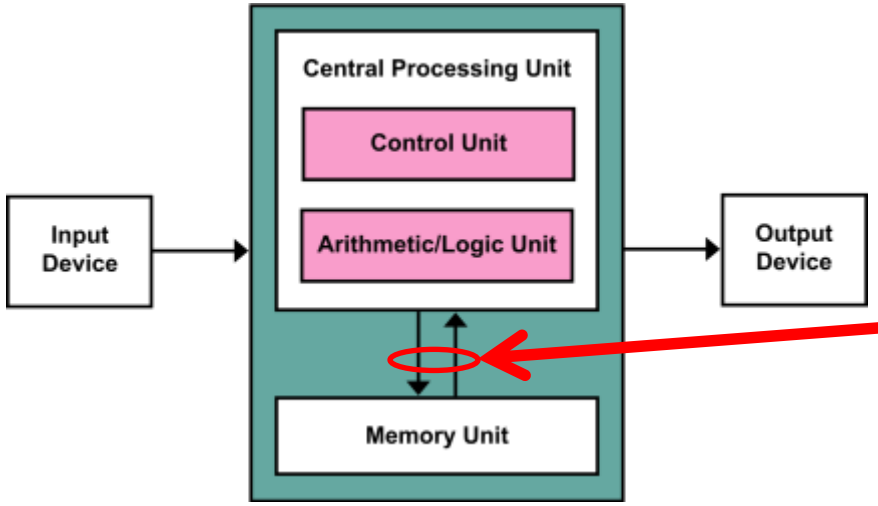
- Methode Spaggiari : Passer par les tuyaux …

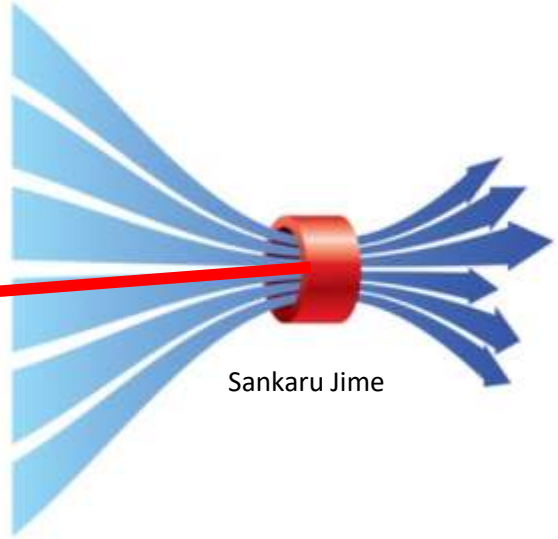
Selon Gerard Berry ...

- Ou :
  - Radio “La tete au carre” emission de radio sur France Inter avec Mathieu Vidard
- Quand :
  - Plusieurs fois par le passe
- Qui:
  - Gerard Berry, Regent de deformatique au college de pataphysique
  - Academicien des sciences, Medaille d’OR CNRS, …, Pr au College de France
- Quoi:
  - “Faire des applications qui marchent vraiment demande de raisonner sur les calculs qu’elles effectuent, à l’aide de modèles mathématiques, comme on raisonne sur des objets physiques.”
  - “L’Ordinateur n’a aucune idee, […] (il est) integralement stupide et totalement obeissant, avec une conscience professionnelle sans faille.”
- Remarque:
  - Il parlait deja de Tic Toc … si,si.

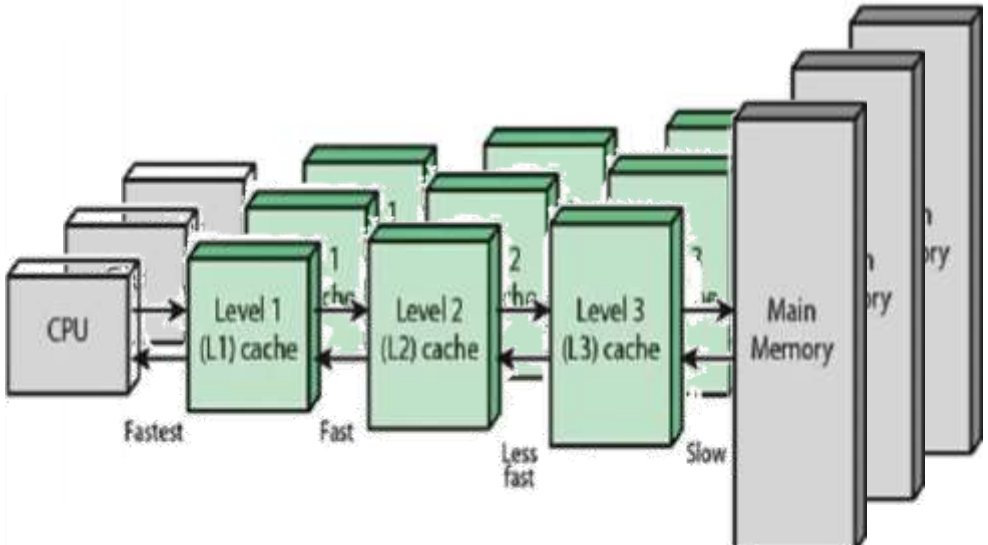
TikTok

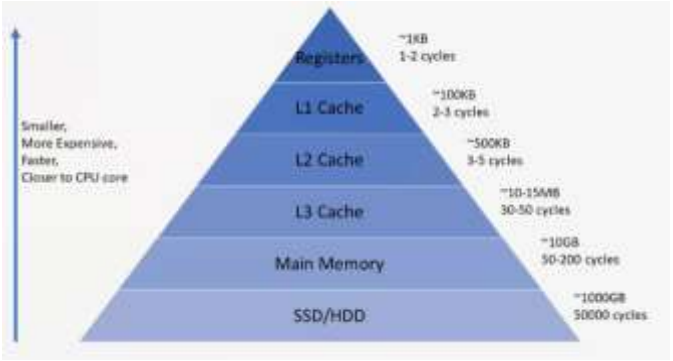
Architecture de Von Neumann et memoire cache





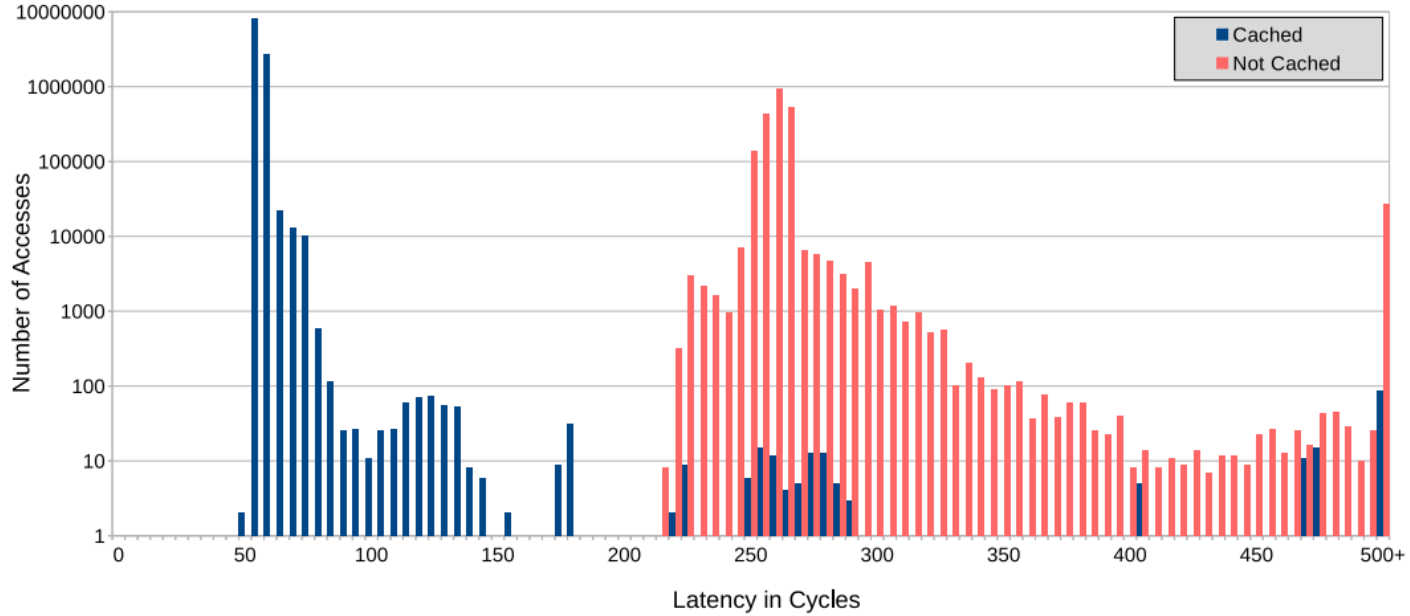
Sankaru Jime

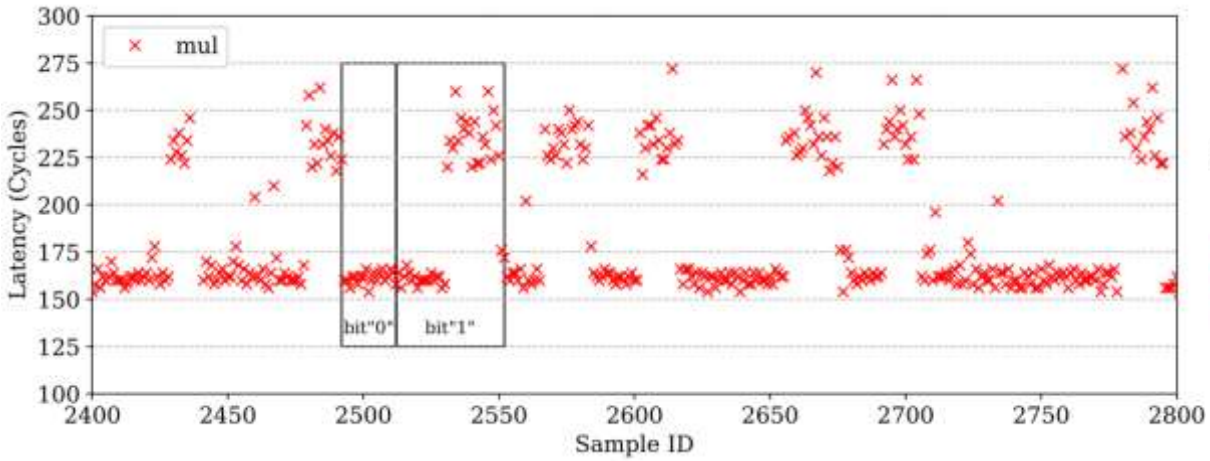




Le temps fait pas …

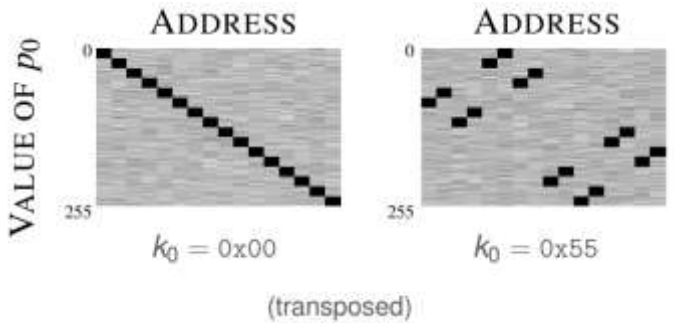
… mais OTAN suspend ton vol





Attack 2: Keylogging

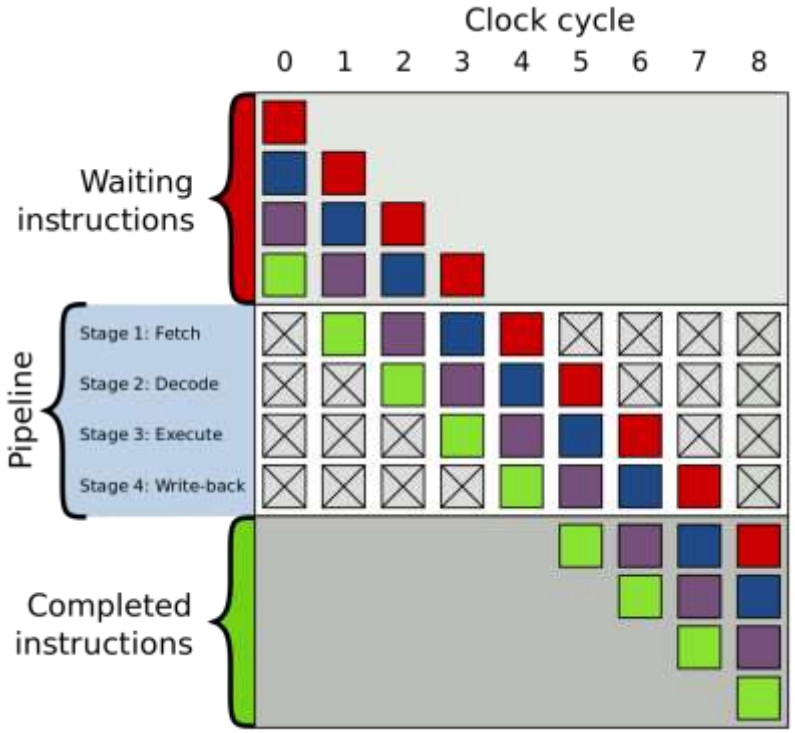
- Linux with GTK: monitor keystrokes of specific keys
- Detect groups of keys
- Some keys distinct

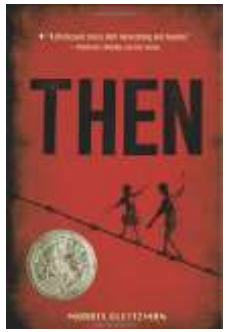


(transposed)

Pipe line, Taylorisation, Swift adaptation

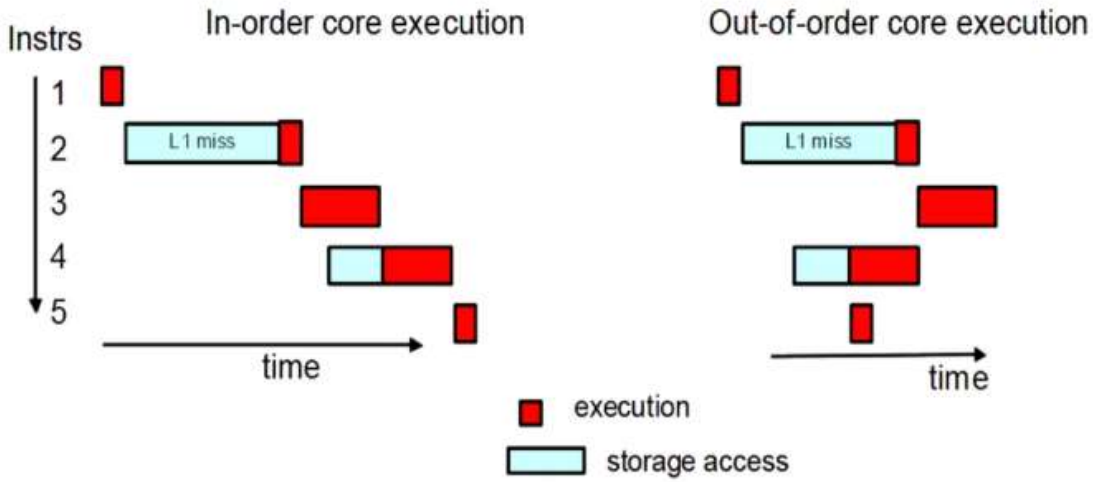
- On va au plus vite …
  - Et parfois on accepte les pertes.

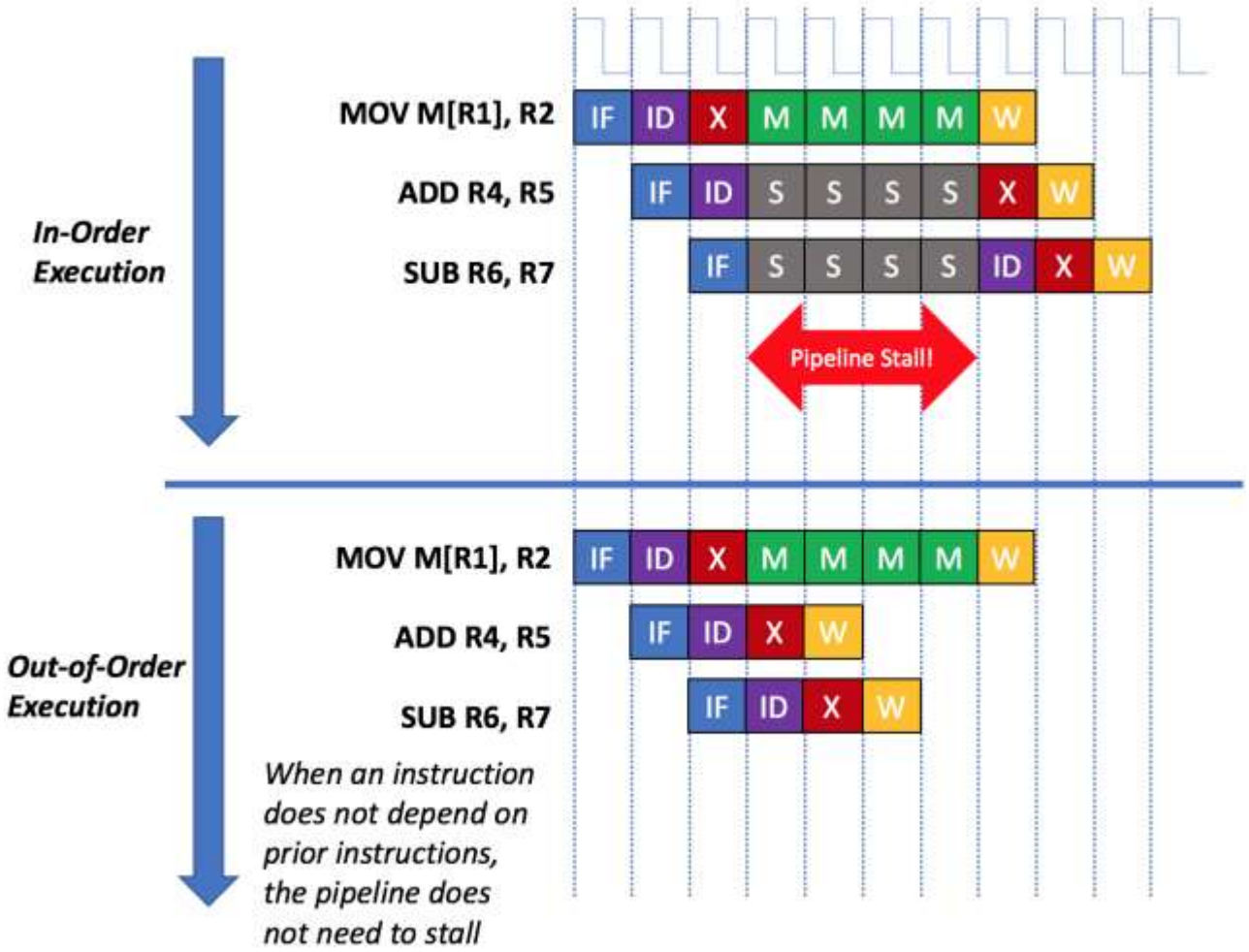





```
for i = n-1 to 0 do
        r = sqr(r)
        r  = r mod n
        if e_i == 1 then
                r = mul(r, b)
                r  = r mod n
        end
end
```

Ordre, Contre-ordre, Desordre





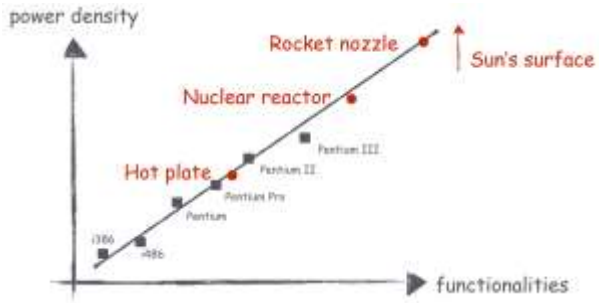
Canaux lateraux

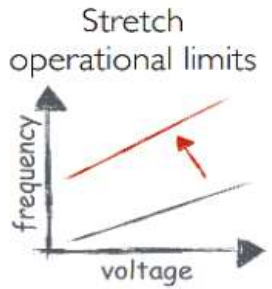
- Attaques par les memoires caches :
  - https://www.daemonology.net/papers/htt.pdf
- Attaque de prediction de branchement :
  - https://eprint.iacr.org/2006/351
- Execution transitoire:
  - https://en.wikipedia.org/wiki/Transient_execution_CPU_vulnerability
- Spectre :
  - https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)
- Meltdown :
  - https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)
- Pacman :
  - https://en.wikipedia.org/wiki/Pacman_(security_vulnerability)
- Microarchitectural Data Sampling :
  - https://en.wikipedia.org/wiki/Microarchitectural_Data_Sampling
- Lazy FP state restore :
  - https://en.wikipedia.org/wiki/Lazy_FP_state_restore
- Foreshadow :
  - https://en.wikipedia.org/wiki/Foreshadow
- RetBleed :
  - https://en.wikipedia.org/wiki/Retbleed

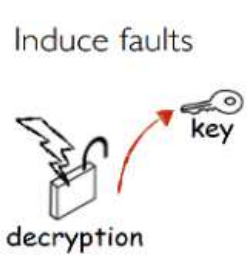
Et les multiples variantes …

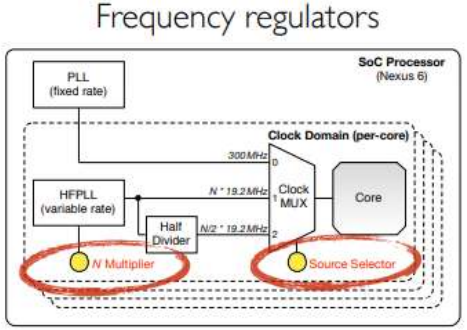
Attaques par faute(s)

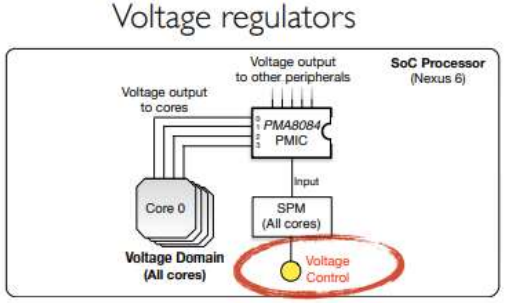
- Clk Screw

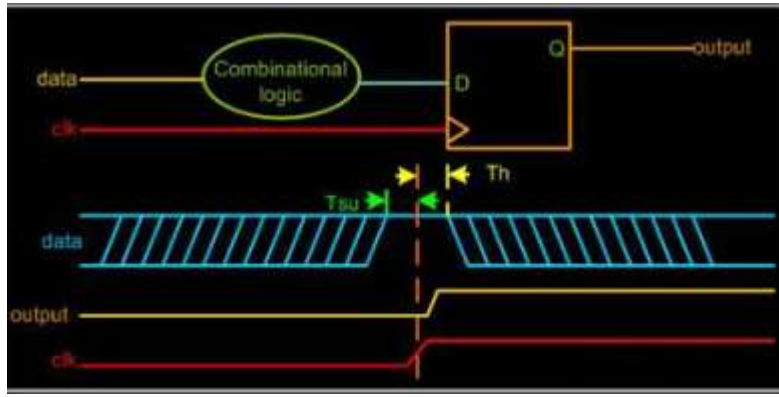












- Row Hammer

- Attaques sur le Microcode
  - [34C3: Hacking Into A CPU's Microcode | Hackaday]

La dernière sorte de parallélisme est le *parallélisme* ***vibratoire***, dans lequel l'information se propage en temps prévisible et borné. C'est par exemple celui qui caractérise la transmission des fronts électriques dans les circuits électroniques. On peut le décliner sous de nombreuses formes, matérielles et logicielles. Il a d'importantes relations avec le parallélisme synchrone : dans un système assez compact, on peut « faire semblant » d'être synchrone en implémentant la fonctionnalité d'une façon vibratoire suffisamment rapide. On allie ainsi la simplicité conceptuelle du synchrone avec l'efficacité des implémentations vibratoires. Par exemple, dans un circuit électronique synchrone, le comportement est conceptuellement défini par un système d'équations booléennes synchrones, dont la solution est calculée dans un temps de l'ordre de la nanoseconde par la propagation des signaux électriques. Une correspondance analogue existe pour les implémentations logicielles des langages synchrones.

Repetez, repetez, repetez, …

28 Wednesday, April 1, 1987 THE HERALD

Plane, fish collide in midair

Associated Press

JUNEAU, Alaska — A midair collision between a jetliner and a fish — that's right, a fish — delayed an Alaska Airlines flight for about an hour while the plane was inspected for damage.

"They found a greasy spot with some scales, but no damage," said Paul Bowers, Juneau airport manager.

And how can a jet hit a fish? It's easy, if the fish is dropped by a bald eagle.

The incident occurred as the Boeing 737 took off Monday from the Juneau airport, the plane's pilot told Bowers. About 400 feet past the runway's end, the jet crossed the flight path of a bald eagle, fish in talons.

"The law of the jungle prevailed," Bowers said. "As the larger bird approached, the smaller bird dropped its prey." The fish hit a small "eyebrow window" at the top of the cockpit, Bowers said.

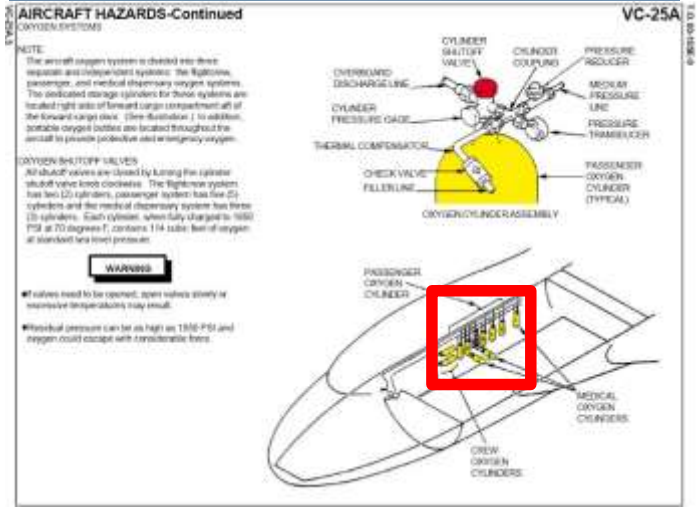
A mechanic was dispatched to the plane's next stop in Yakutat, 200 miles to the northwest, said Jerry Kvasnikoff, Alaska Airlines customer service manager in Juneau.

The eagle apparently escaped injury. The fish, species unknown, is presumed dead.

"This time of year, if I had to guess, it might have been a cod," Kvasnikoff said. "You never know what an eagle will get into."

Kvasnikoff and Bowers said this was the first airplane-fish collision they had heard of, but they said jets occasionally collide with other forms of Alaska wildlife.

"Over the years, we've had planes hit various critters — moose, deer, every kind of bird. But that's a first for a fish," Kvasnikoff said.



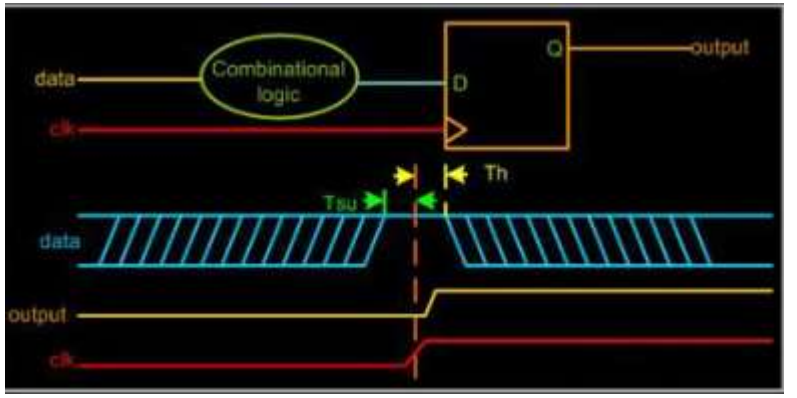
- https://cryptome.org/eyeball/af1-rescue/af1-rescue.htm
- Web site exposes Air Force One defenses, by Paul J. Caffera, on Saturday, April 8, 2006
- “[...] a government document containing specific information about the anti-missile defenses on Air Force One and detailed interior maps of the two planes -- including the location of Secret Service agents within the planes -- was posted on the Web site of an Air Force base.
- The document also shows the location where a terrorist armed with a high-caliber sniper rifle could detonate the tanks that supply oxygen to Air Force One's medical facility.”
- As of Friday, the document was still posted online. The Secret Service refused to comment on the document's release.
- "It is not a good thing" for that information to be in the public domain, said Lt. Col Bruce Alexander, director of public affairs for the Air Mobility Command's 89th Airlift Wing, Andrews Air Force Base, which operates the presidential air transport fleet. "We are concerned with how it got there and how we can get it out. This affects operational security."

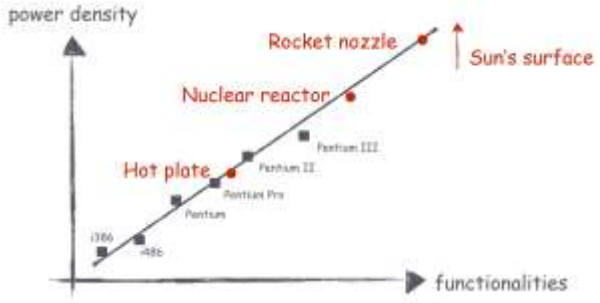
Un jour sans fin …

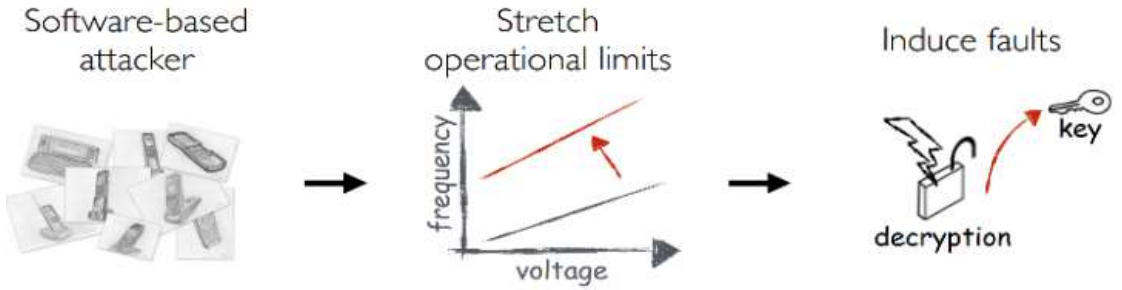
- Software est generalement non destructif
- Grand nombre de tentatives grace au RESET ou a la REPETITION
- Synchronization est le parametre clef (Pun intended)

CLKSCREW

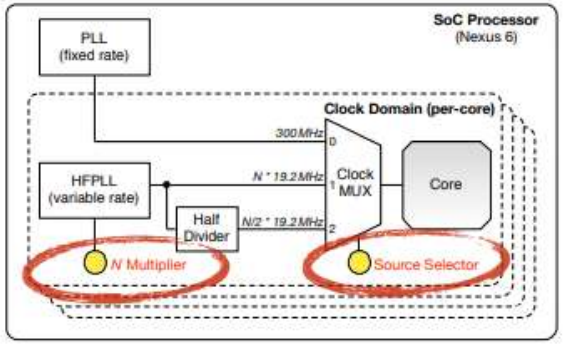
- Gestion de l’energie



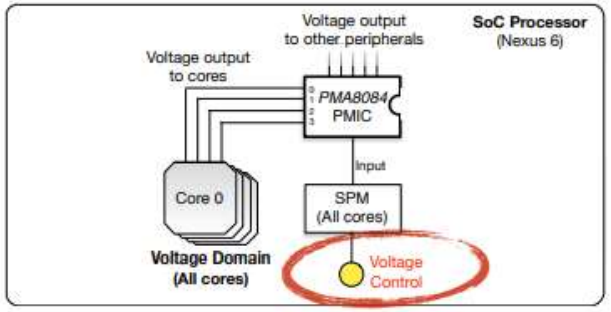


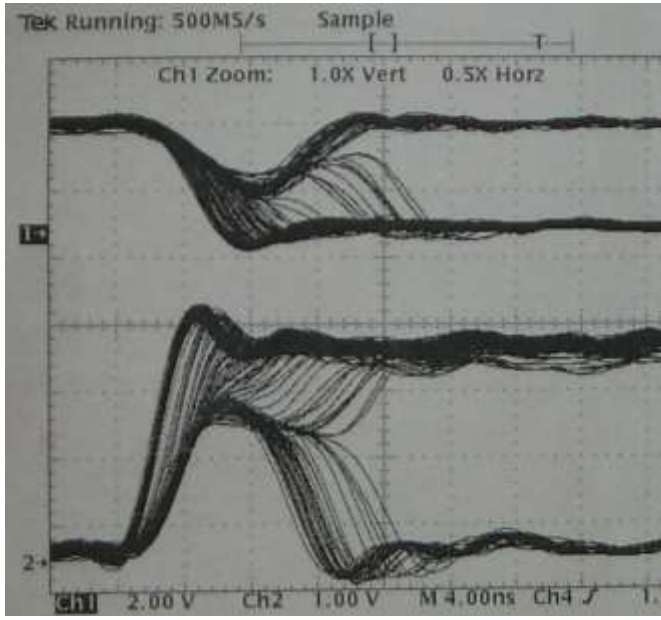


Frequency regulators



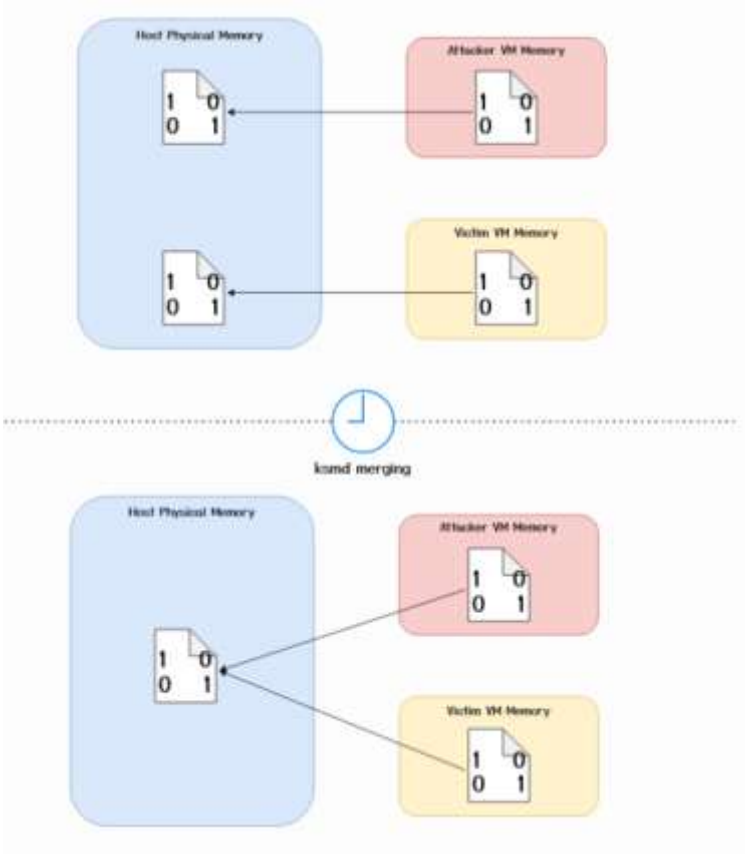
Voltage regulators

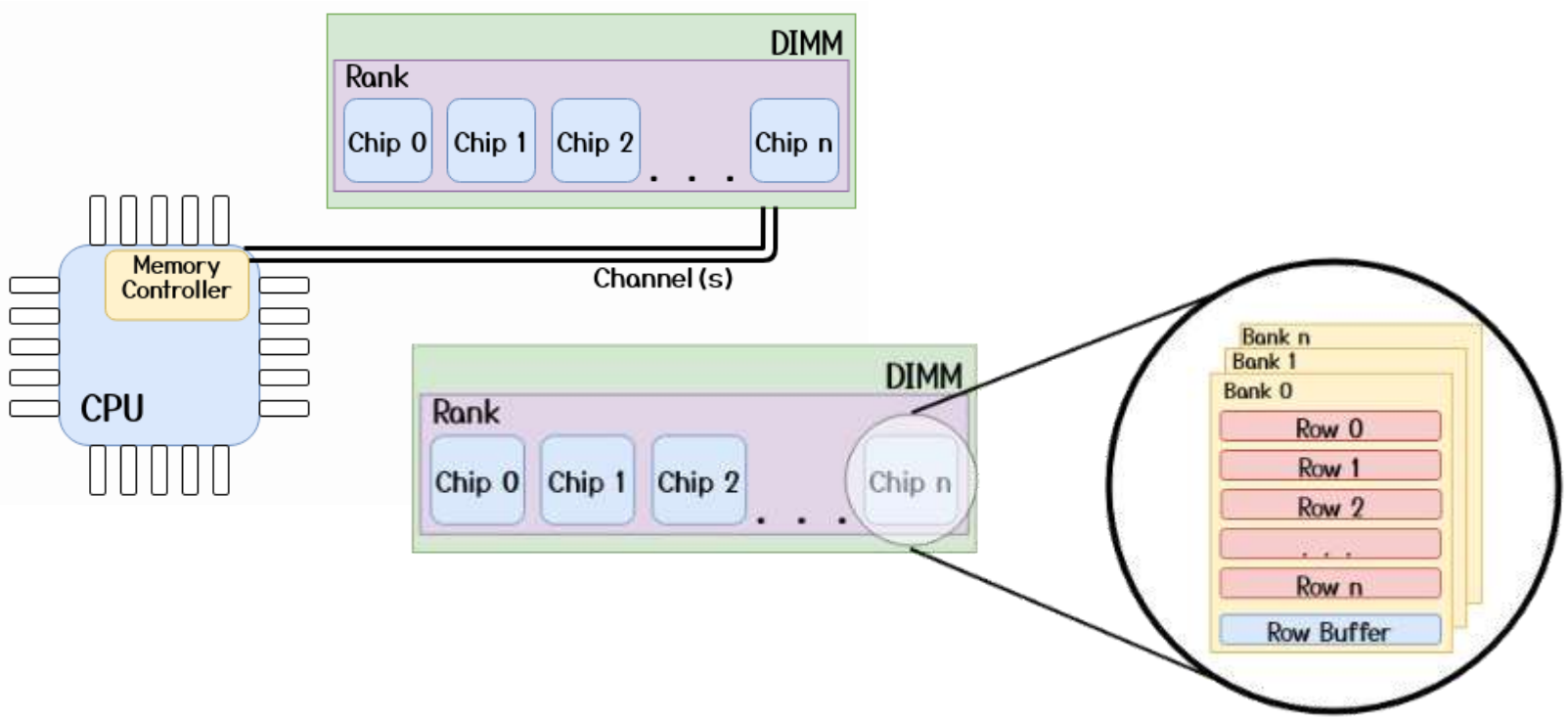


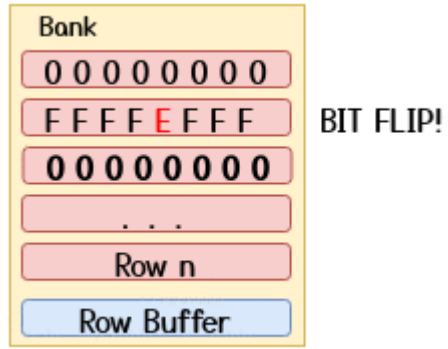


Row Hammer

- https://github.com/google/rowhammer-test







Quelques demos disponibles en ligne

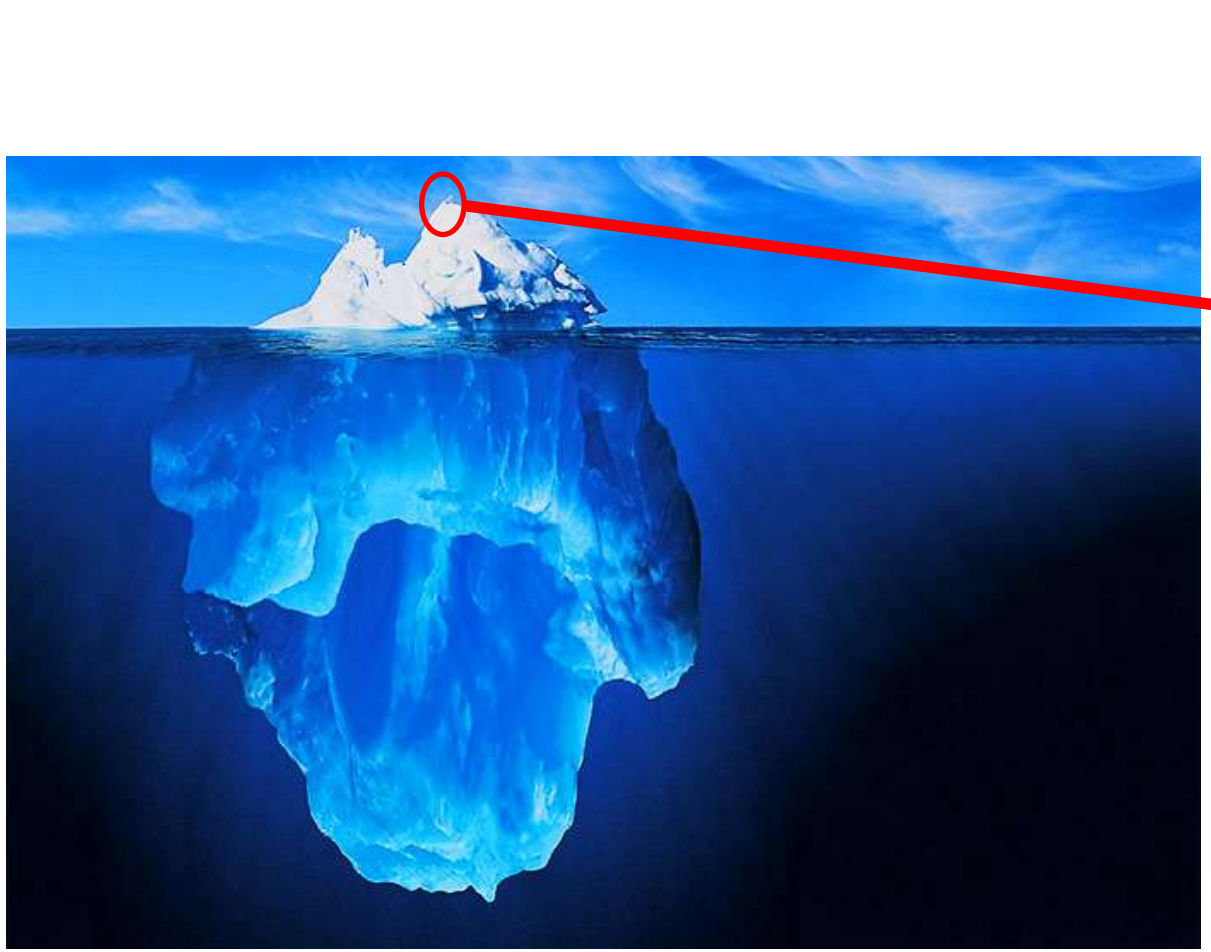
... et le source code

- Row Hammer applique a Android:
  - Drammer on Android 6.0.1 – YouTube
  - Source code
- Spectre:
  - Spectre (leaky.page)
  - Demonstration reussie
- Meltdown:
  - En action et dans ses oeuvres
  - En action dans ses oeuvres

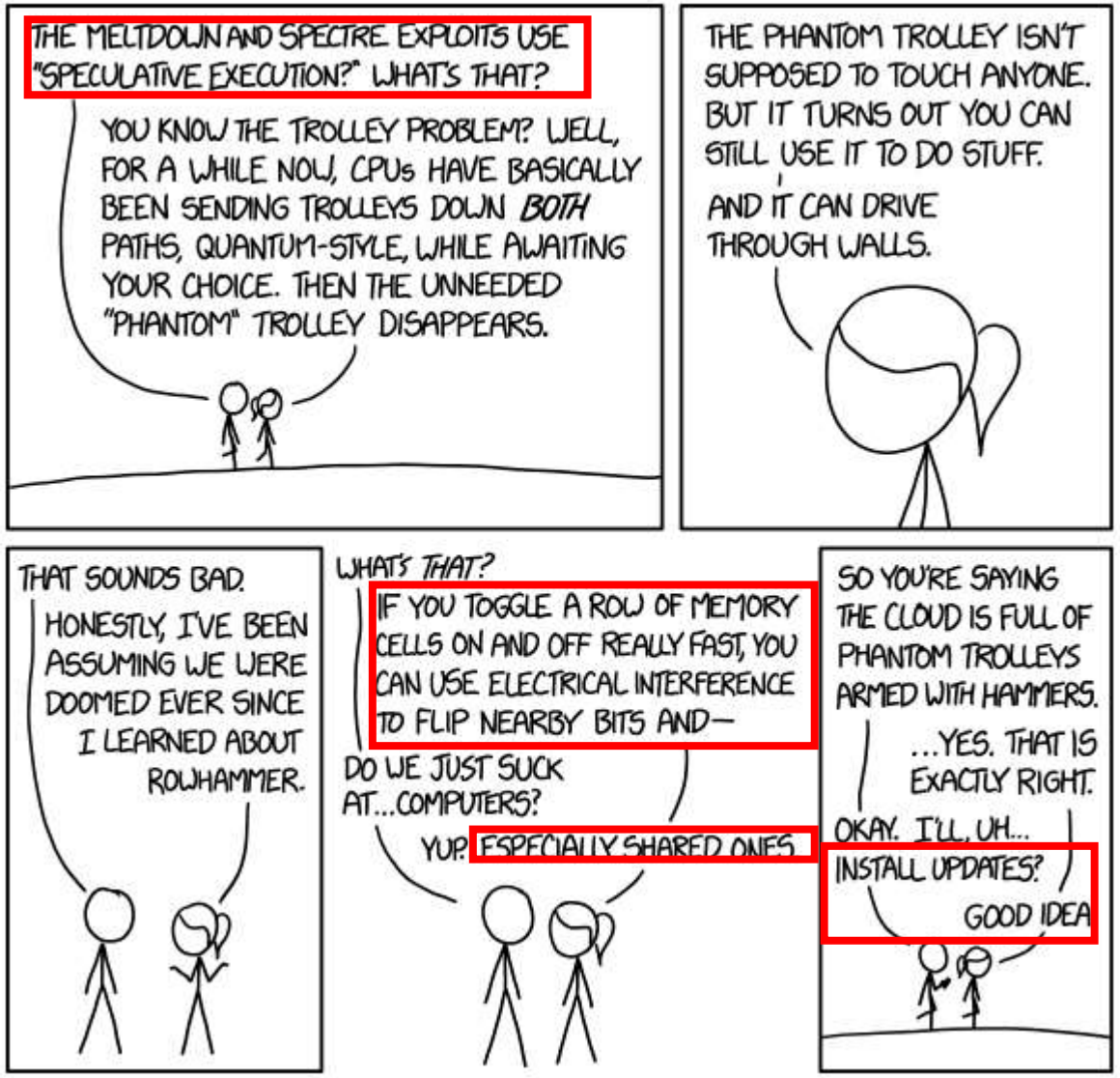
*ffleurer le sommet de l’iceberg

{a, e , de, …}

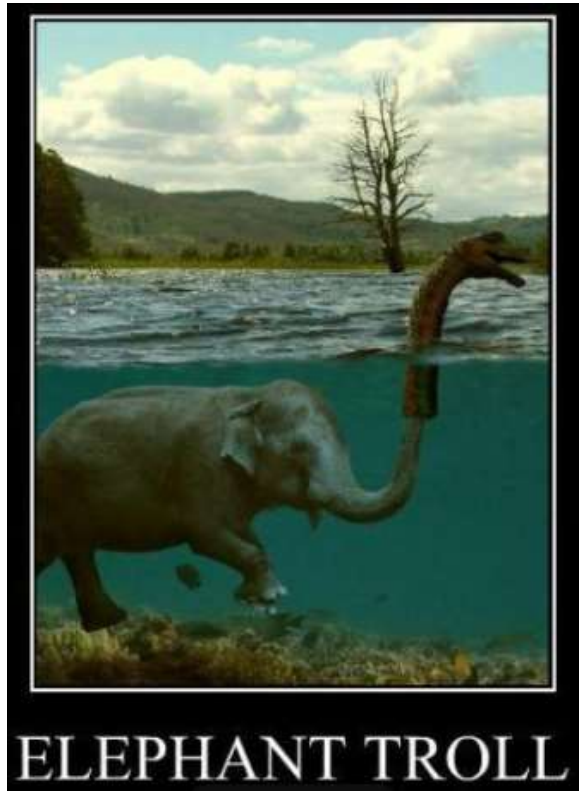
- Toute ressemblance serait … gratuite



Conclusion / Questions?



- GAFAM Inside
- Intel Outside



References 1/2

- Quelques liens a explorer :
  - - Cheap side channel attacks : https://www.youtube.com/watch?v=6VSPzSRR4Uk
  - - Power analysis on GPU : http://www1.ece.neu.edu/~saoni/files/Chao_ICCD_2015.pdf
  - - Paper for Spectre : https://spectreattack.com/spectre.pdf
  - - Paper for meltdown : https://meltdownattack.com/meltdown.pdf
  - - Spectre wikipedia: https://en.wikipedia.org/wiki/Spectre_(security_vulnerability)
  - - Meltdown wikipedia : https://en.wikipedia.org/wiki/Meltdown_(security_vulnerability)
  - - Meltdown from Google Project Zero : https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html
  - - New York Times : https://www.nytimes.com/2018/01/03/business/computer-flaws.html#:~:text=The%20two%20problems%2C%20called%20Meltdown,so%2Dcalled%20cloud%20computer%20networks.
  - - Spectre demo : https://leaky.page/
  - - Code source for demo : https://github.com/google/security-research-pocs/tree/master/spectre.js
  - - Demo Spectre JavaScript : https://www.youtube.com/watch?v=V_9cQP60ZGI
  - - Fantastic timers : https://pure.tugraz.at/ws/portalfiles/portal/17611474/fantastictimers.pdf

References 2/2

- Informatique et sciences numériques : https://www.college-de-france.fr/media/gerard-berry/UPL7123112924601846267_R0910_Berry.pdf
- Out of order execution : https://en.wikipedia.org/wiki/Out-of-order_execution
- RISC architecture :
- https://en.wikipedia.org/wiki/Reduced_instruction_set_computer
- “La tete au carre” France Inter Jeudi 13 novembre 2014
- https://www.radiofrance.fr/franceinter/podcasts/la-tete-au-carre/l-informatique-avec-gerard-berry-3127859
- Timing channels in cryptography by C.Rebeiro, D.Mukhopadhay and S.Bhattacharya (ISBN:9783319123691)
- http://csg.csail.mit.edu/6.888Yan/slides/4-Practical-Cache-Attack.pdf
- https://www.usenix.org/sites/default/files/conference/protected-files/sec15_slides_gruss.pdf
- https://fengweiz.github.io/18fa-csc6991/slides/clkscrew-alokparna.pdf
- https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/tang
- Anatomy of a CPU | TechSpot :https://www.techspot.com/article/2000-anatomy-cpu/
- Fr.Misc.Cryptologie, https://fr.misc.cryptologie.narkive.com/En4bjHJc/article-de-misc-sur-l-attaque-par-prediction-de-branchement