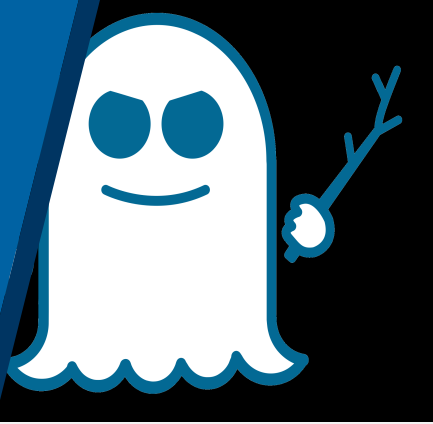
Spectre Attacks: Exploiting Speculative Execution

and why the heck is the computer speculating anyway?



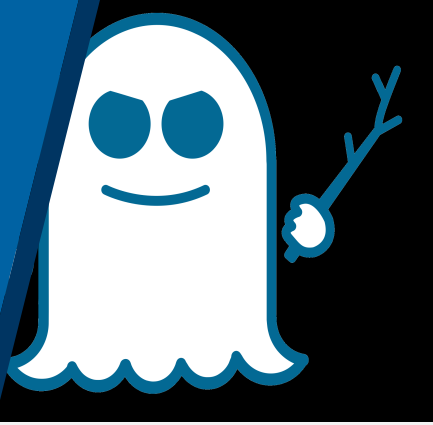
Werner Haas

April 14, 2021

CYBERUS TECHNOLOGY

Spectre Attacks: Exploiting Speculative Execution

and why the heck is the computer speculating anyway?



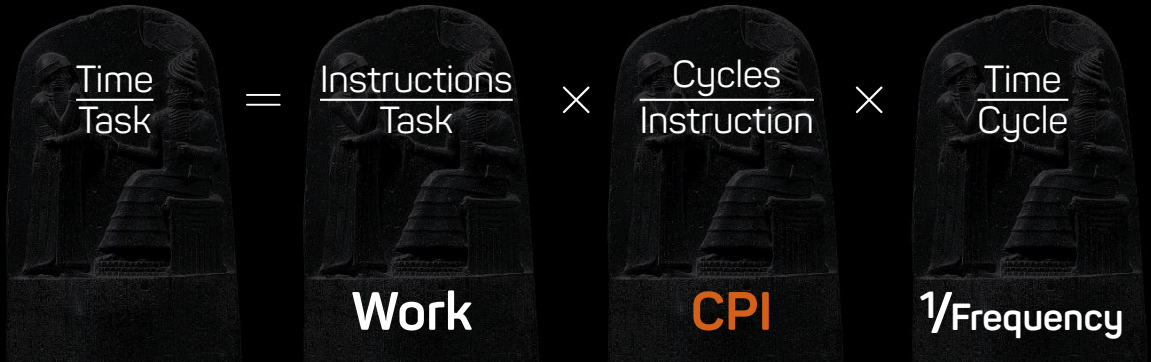
Paul Kocher, Jann Horn, Anders Fogh, Daniel Genkin,
Daniel Gruss, Mike Hamburg, Moritz Lipp, Stefan Mangard,
Thomas Prescher, Michael Schwarz, Yuval Yarom

CYBERUS
TECHNOLOGY

Iron Law of Processor Performance

Iron Law of Processor Performance

Iron Law of Processor Performance

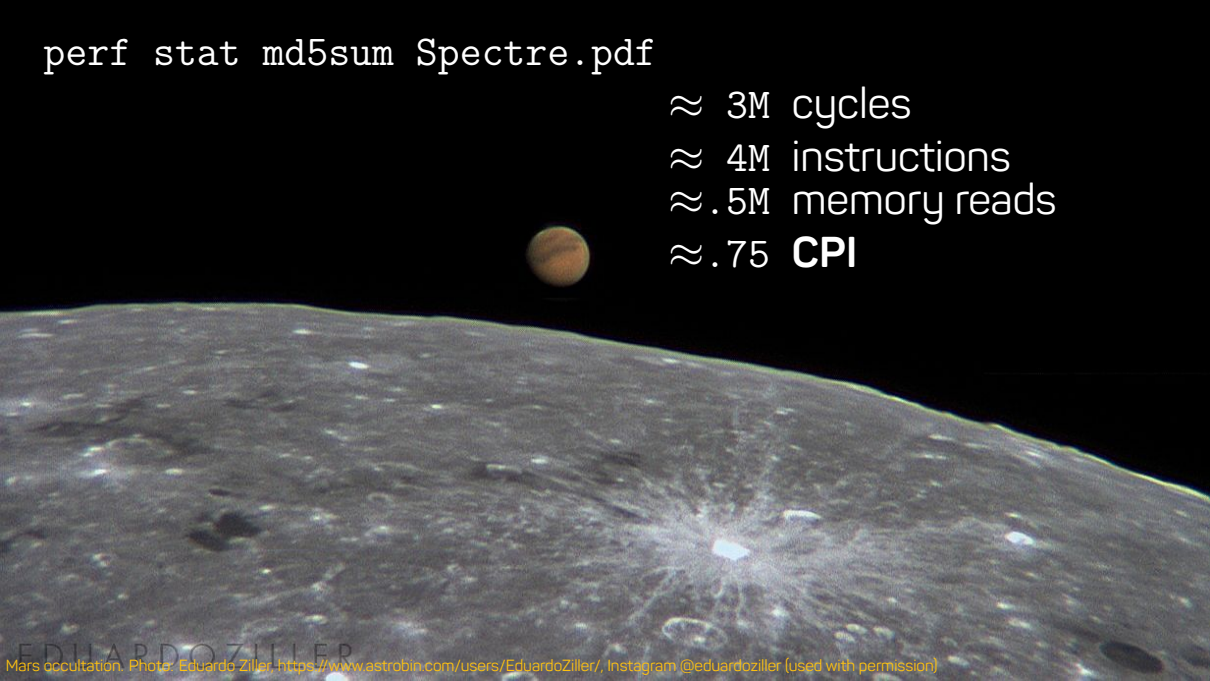


perf stat md5sum Spectre.pdf

Mars occultation. Photo: Eduardo Ziller-https://www.astrobin.com/users/EduardoZiller/, Instagram @eduardoziller (used with permission)

```
perf stat md5sum Spectre.pdf
```

≈ 3M cycles
≈ 4M instructions
≈.5M memory reads
≈.75 **CPI**

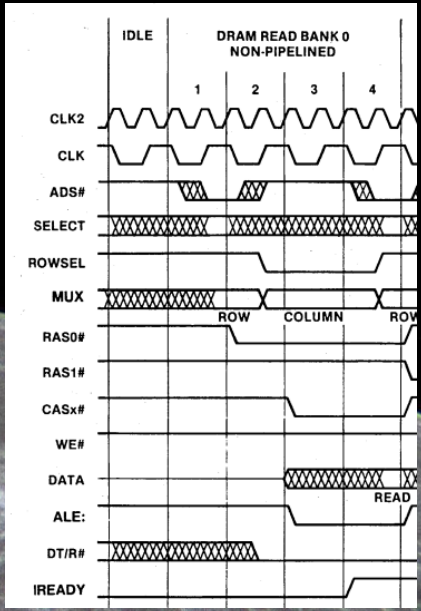


Mars occultation. Photo: Eduardo Ziller-https://www.astrobin.com/users/EduardoZiller/, Instagram @eduardoziller (used with permission)

intel

INTEL386™ DX MICROPROCESSOR

HARDWARE REFERENCE MANUAL

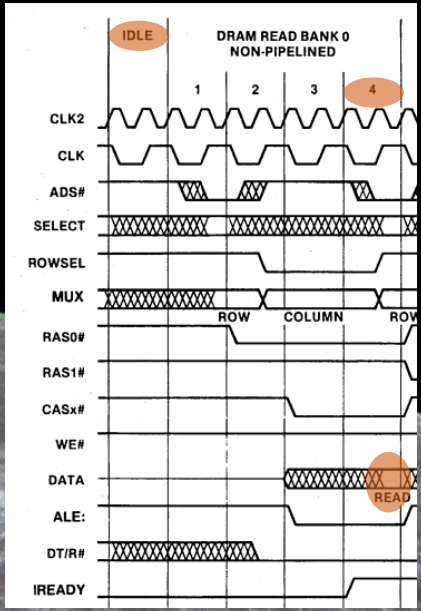


Mars occultation. Photo: Eduardo Ziller- https://www.astrobin.com/users/EduardoZiller/, Instagram @eduardoziller (used with permission)

intel

INTEL386™ DX MICROPROCESSOR

HARDWARE REFERENCE MANUAL



Mars occultation. Photo: Eduardo Ziller- https://www.astrobin.com/users/EduardoZiller/, Instagram @eduardoziller (used with permission)

Technology Evolution

Frequency	20 MHz	→	2 GHz
Instructions	4 M		4 M
Memory reads	.5 M		.5 M
Latency [cycles]	4		
Cycles	3 M		
CPI	0,75		

Hubble sees a smiling lens, Image credit: NASA/ESA

Technology Evolution

Frequency	20 MHz	→	2 GHz
Instructions	4 M		4 M
Memory reads	.5 M		.5 M
Latency [cycles]	4		>100
Cycles	3 M		
CPI	0,75		

Hubble sees a smiling lens, Image credit: NASA/ESA

Technology Evolution

Frequency	20 MHz	→	2 GHz
Instructions	4 M		4 M
Memory reads	.5 M		.5 M
Latency [cycles]	4		>100
Cycles	3 M		>53 M
CPI	0,75		

Hubble sees a smiling lens, Image credit: NASA/ESA

Technology Evolution

Frequency	20 MHz	→	2 GHz
Instructions	4 M		4 M
Memory reads	.5 M		.5 M
Latency [cycles]	4		>100
Cycles	3 M		>53 M
CPI	0,75	→	>13,25

Hubble sees a smiling lens, Image credit: NASA/ESA

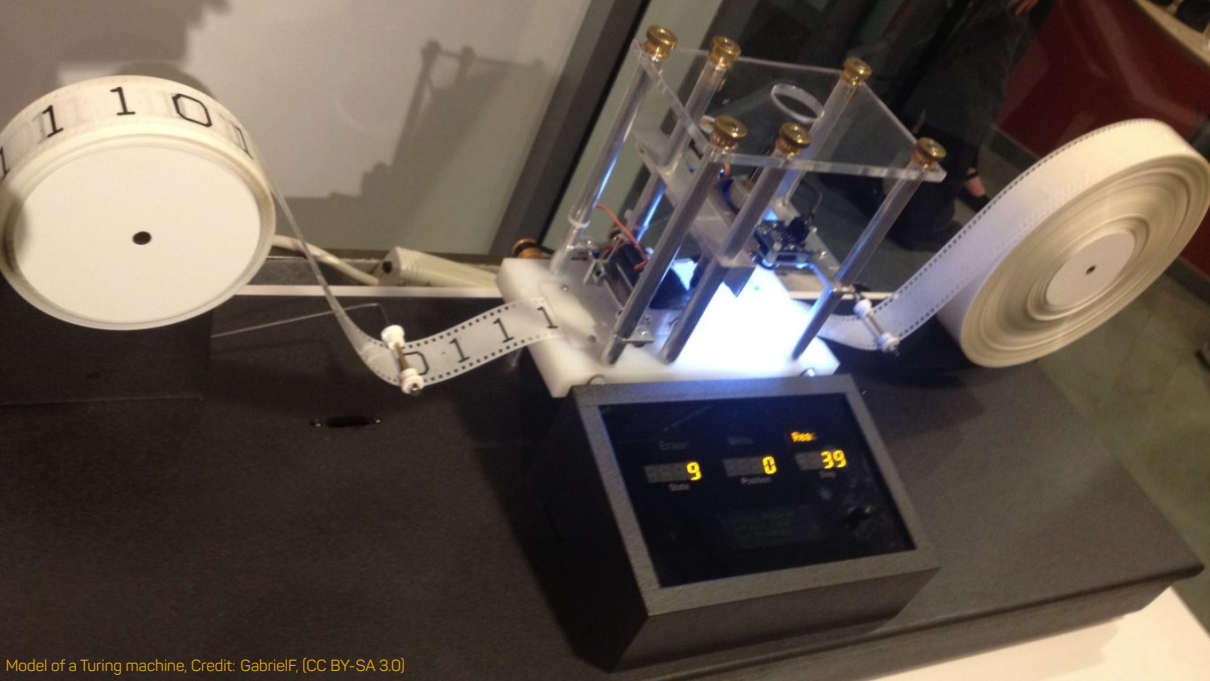
Technology Evolution

Frequency	20 MHz	→	2 GHz	100x
Instructions	4 M		4 M	
Memory reads	.5 M		.5 M	
Latency [cycles]	4		>100	
Cycles	3 M		>53 M	
CPI	0,75	→	>13,25	>17x

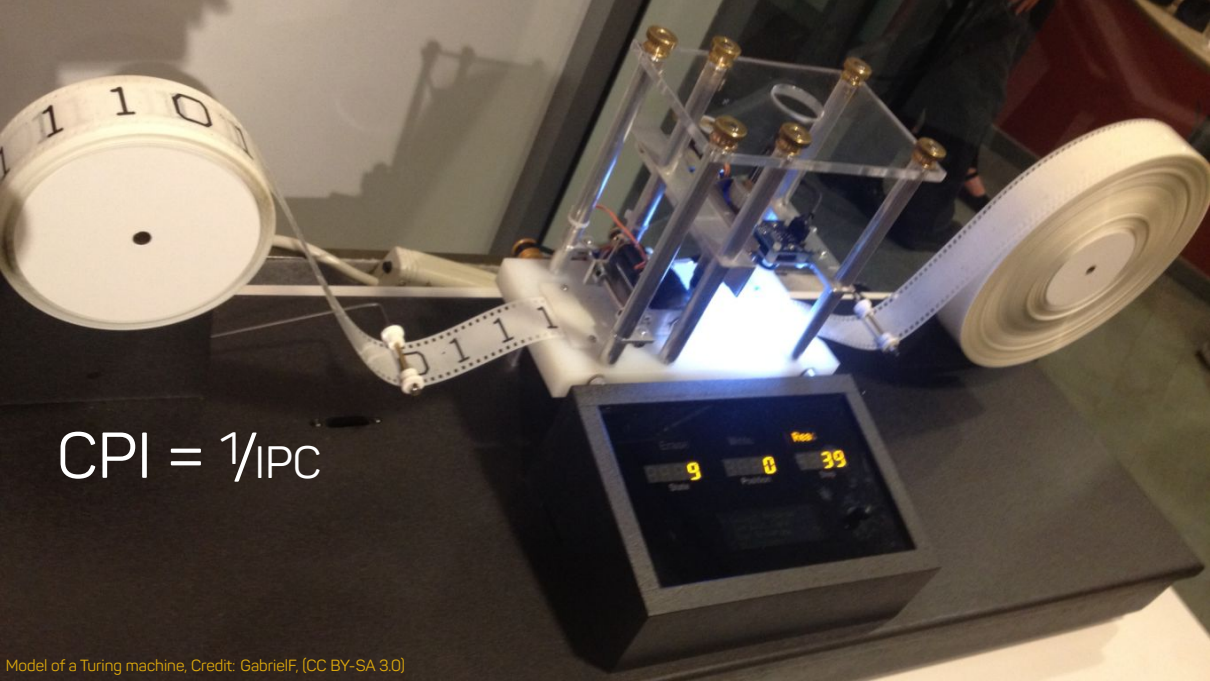
Hubble sees a smiling lens, Image credit: NASA/ESA

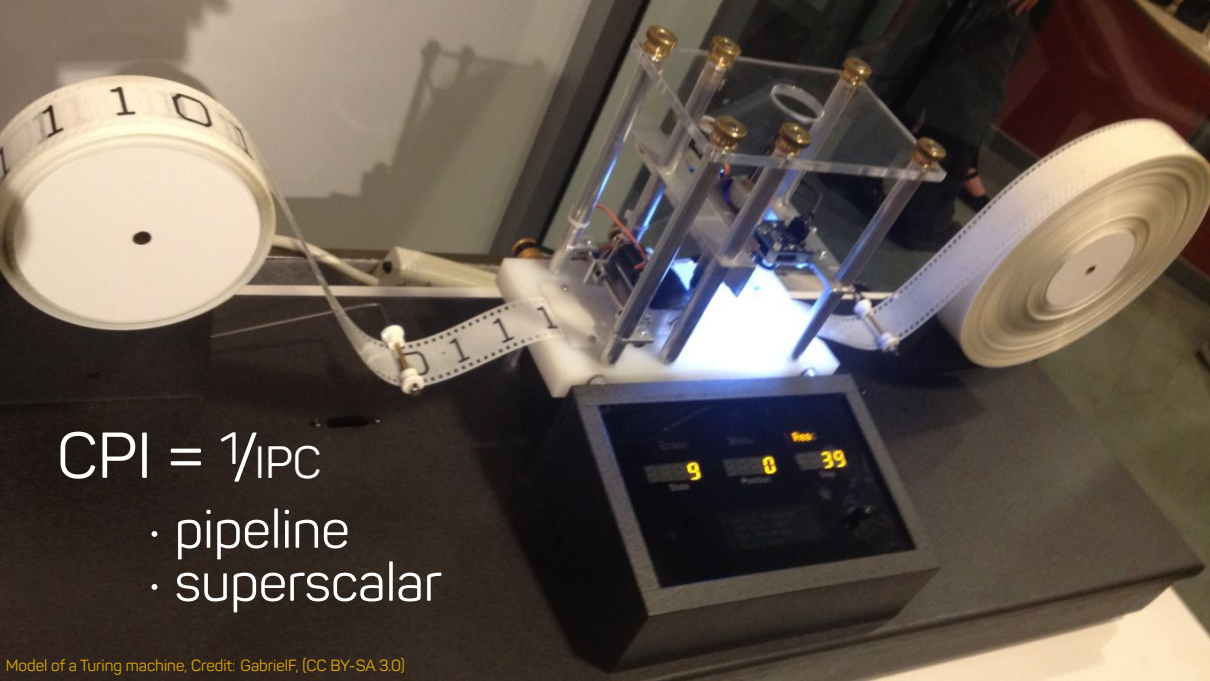
Technology Evolution

Hubble sees a smiling lens, Image credit: NASA/ESA



Model of a Turing machine, Credit: GabrielF, (CC BY-SA 3.0)


CPI = 1/IPC
Model of a Turing machine, Credit: GabrielF, (CC BY-SA 3.0)



CPI = 1/IPC

- pipeline
- superscalar

Model of a Turing machine, Credit: GabrielF, (CC BY-SA 3.0)

```
# Pad with 0s to get 512b chunks
while len(message)%512 != 448:
  message.append(0)
```

Perseverance is Roving on Mars, Image credit: NASA/JPL-Caltech

```
# Pad with 0s to get 512b chunks
while len(message)%512 != 448:
  message.append(0)
```

jump instr.	detection	destination
direct	@decode	calculation

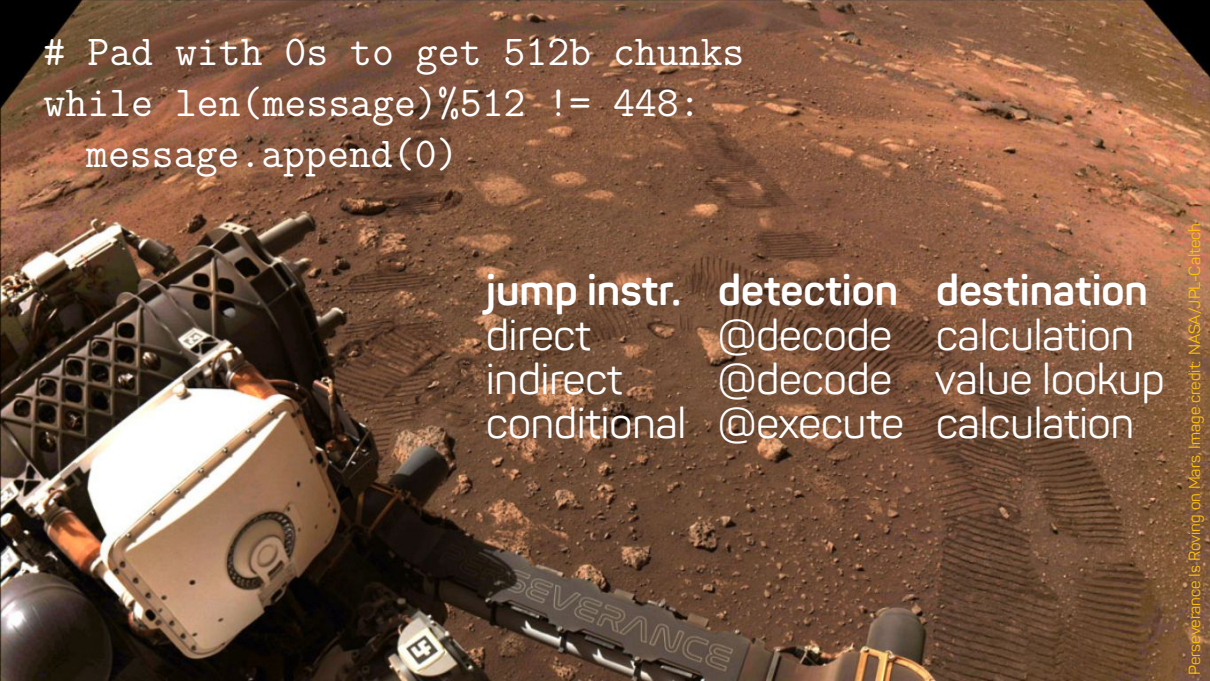
Perseverance is Roving on Mars, Image credit: NASA/JPL-Caltech

```
# Pad with 0s to get 512b chunks
while len(message)%512 != 448:
  message.append(0)
```

jump instr.	detection	destination
direct	@decode	calculation
indirect	@decode	value lookup

Perseverance is Roving on Mars, Image credit: NASA/JPL-Caltech

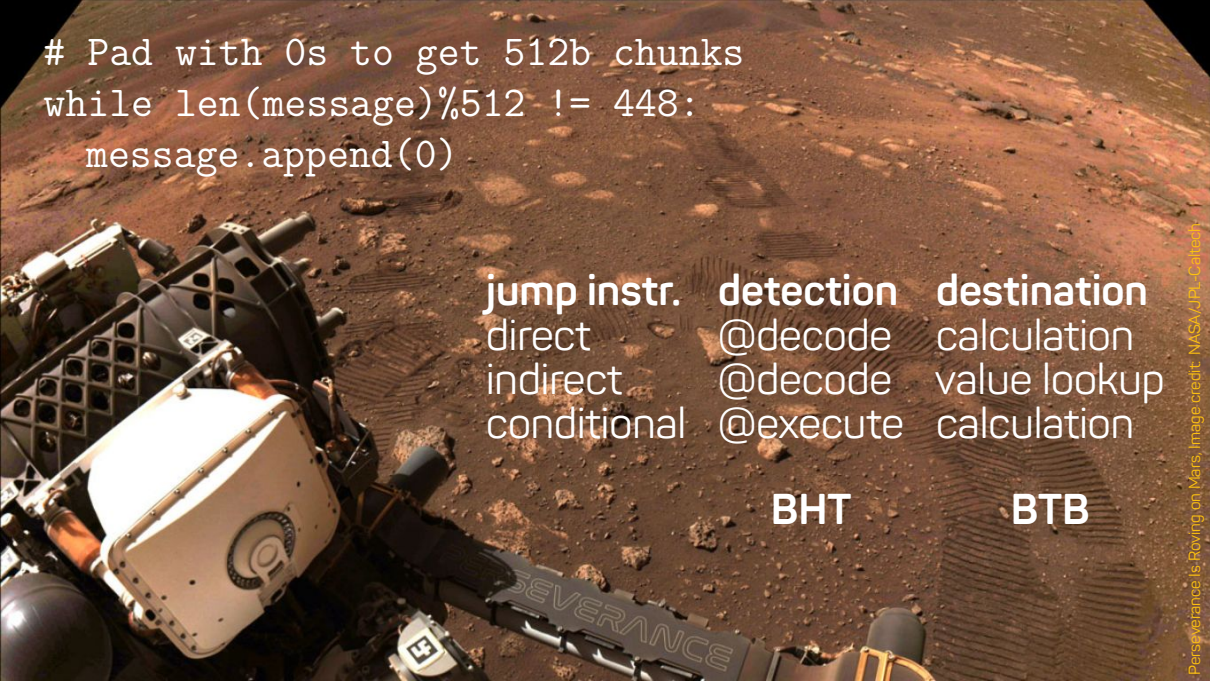
```
# Pad with 0s to get 512b chunks
while len(message)%512 != 448:
  message.append(0)
```



jump instr.	detection	destination
direct	@decode	calculation
indirect	@decode	value lookup
conditional	@execute	calculation

Perseverance is Roving on Mars, Image credit: NASA/JPL-Caltech

```
# Pad with 0s to get 512b chunks
while len(message)%512 != 448:
  message.append(0)
```



jump instr.	detection	destination
direct	@decode	calculation
indirect	@decode	value lookup
conditional	@execute	calculation

BHT **BTB**

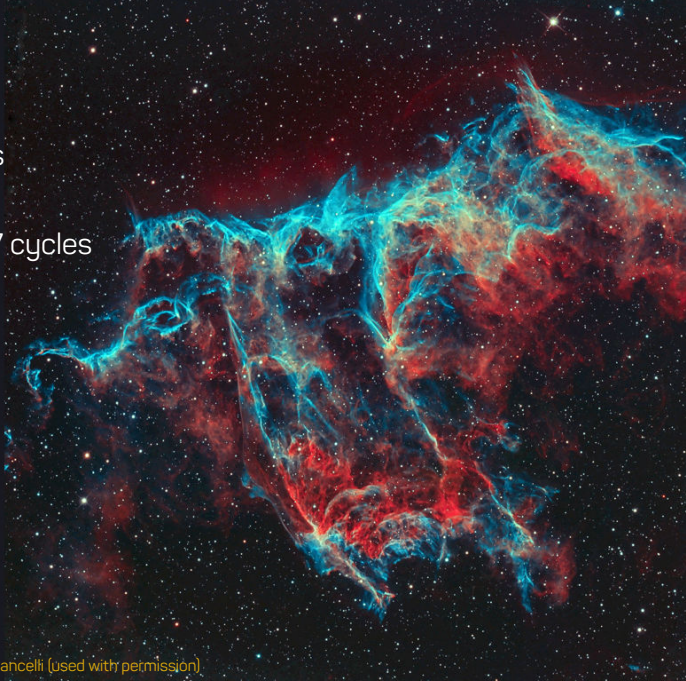
Perseverance is Roving on Mars, Image credit: NASA/JPL-Caltech

Spectre

backyardastronomer.com: Spooky. Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Spectre v1: BHT

- SPEC CPU 2017: ≈ 20% branches
- Intel Ice Lake: 5-way decode
- Branch misprediction penalty ≈ 17 cycles



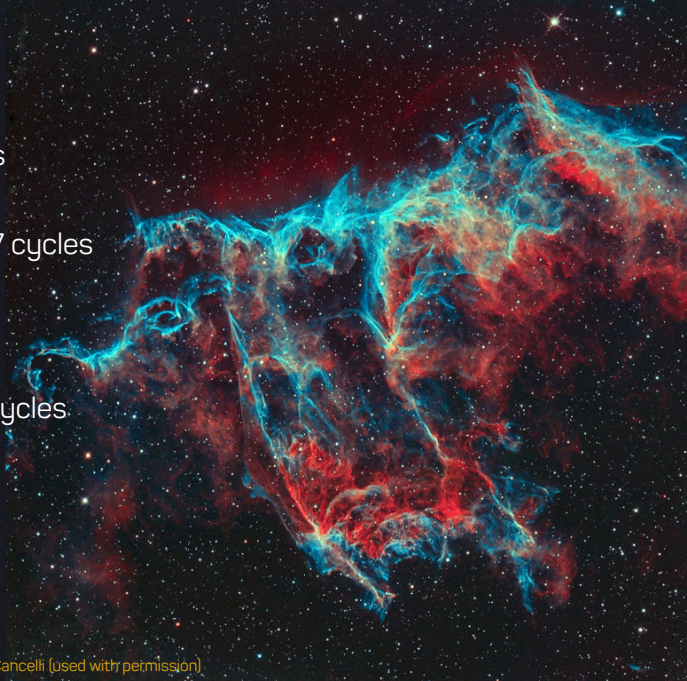
backyardastronomer.com: Spooky. Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Spectre v1: BHT

- SPEC CPU 2017: ≈ 20% branches
- Intel Ice Lake: 5-way decode
- Branch misprediction penalty ≈ 17 cycles

Time to fetch 1000 instructions

- perfect prediction:
  1000 instructions / $^{5}/_{\text{cycle}}$ = 200 cycles



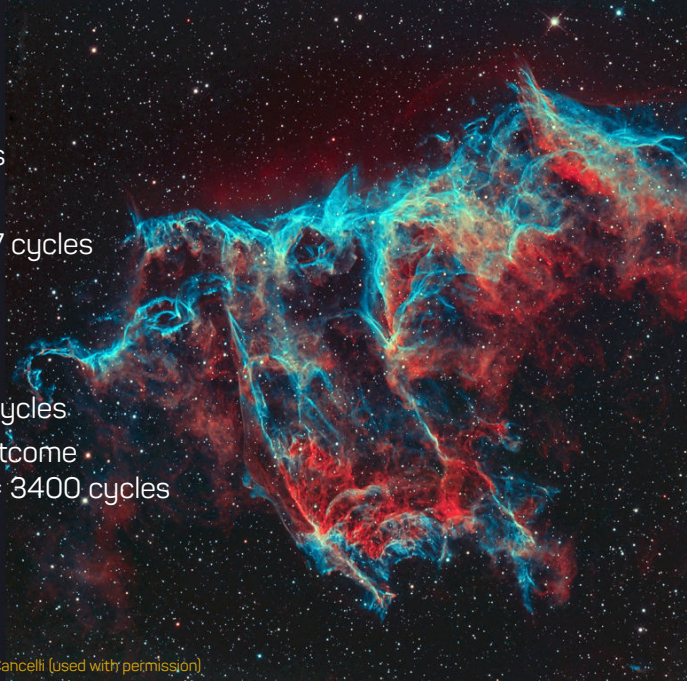
backyardastronomer.com: Spooky. Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Spectre v1: BHT

- SPEC CPU 2017: ≈ 20% branches
- Intel Ice Lake: 5-way decode
- Branch misprediction penalty ≈ 17 cycles

Time to fetch 1000 instructions

- perfect prediction:
  1000 instructions / $^{5}/_{\text{cycle}}$ = 200 cycles
- no speculation: wait for branch outcome
  1000 instructions / 5 · 17 cycles = 3400 cycles



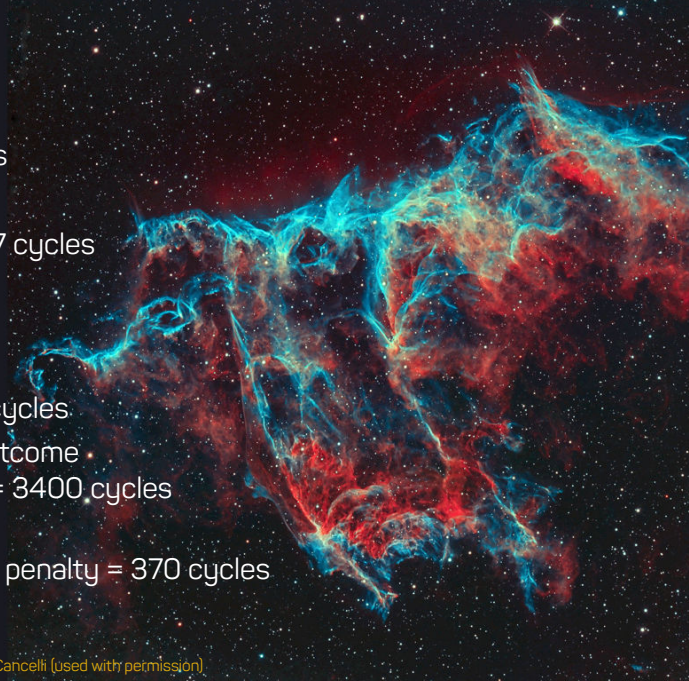
backyardastronomer.com: Spooky, Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Spectre v1: BHT

- SPEC CPU 2017: ≈ 20% branches
- Intel Ice Lake: 5-way decode
- Branch misprediction penalty ≈ 17 cycles

Time to fetch 1000 instructions

- perfect prediction:
  1000 instructions / $^{5}/_{\text{cycle}}$ = 200 cycles
- no speculation: wait for branch outcome
  1000 instructions / 5 · 17 cycles = 3400 cycles
- 99% accuracy:
  200 cycles + 10 misses · 17 cycle penalty = 370 cycles

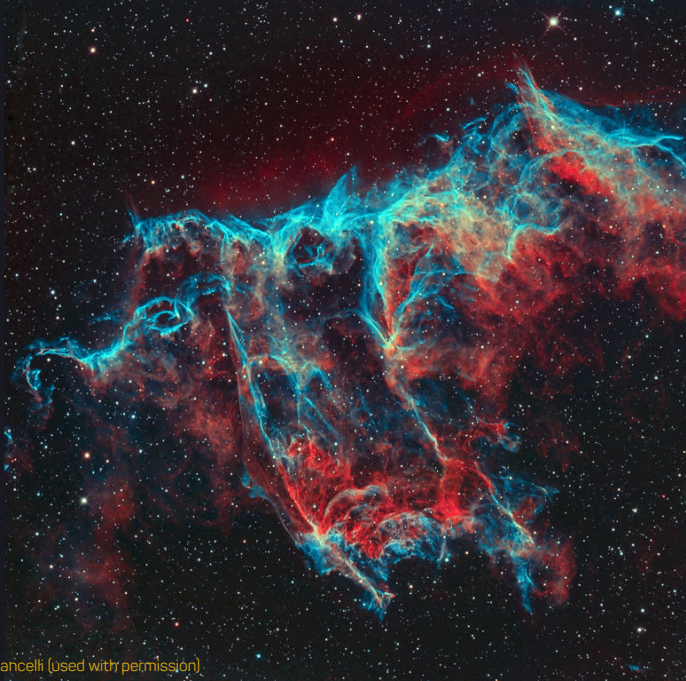


backyardastronomer.com: Spooky, Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Spectre v2: BTB

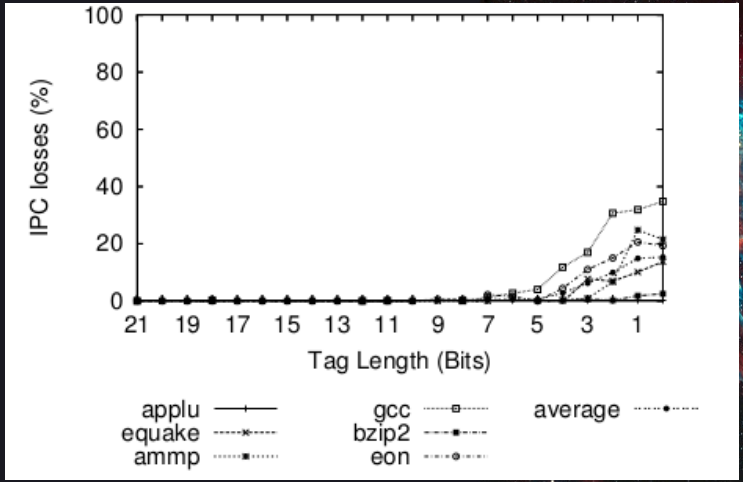
Branch predictor hot spot

- every cycle
- every instruction



backyardastronomer.com: Spooky. Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

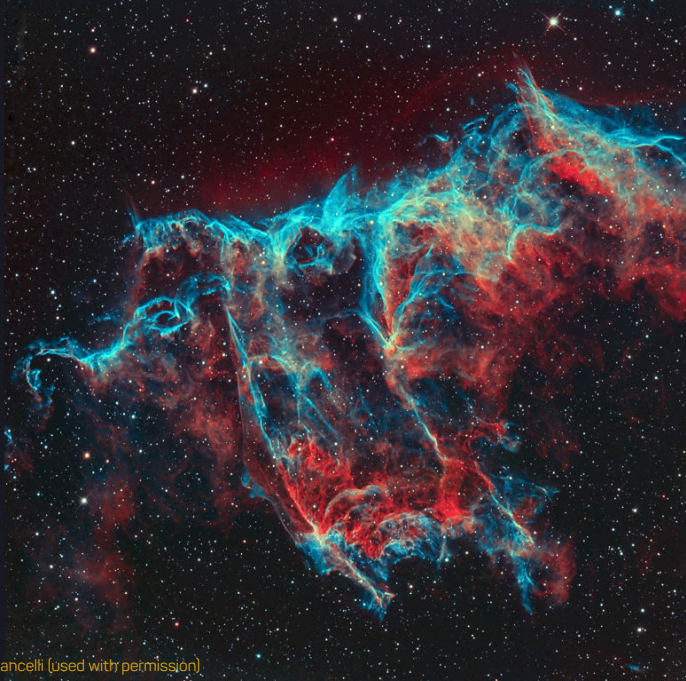
Spectre v2: BTB



Tomas et al.: Reducing the Number of Bits in the BTB to Attack the Branch Predictor Hot-Spot, Euro-Par 2008

backyardastronomer.com: Spooky, Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Spectre

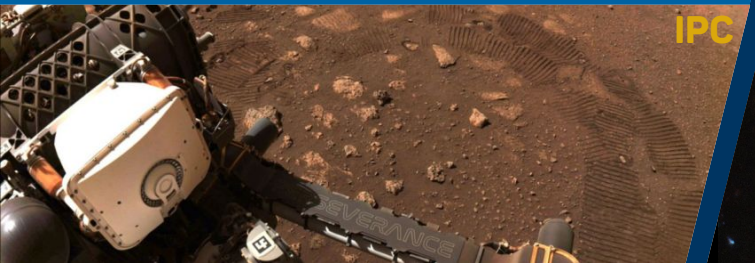


backyardastronomer.com: Spooky. Image credit: Paul Mortfield & Stefano Cancelli (used with permission)

Iron Law

Iron Law

CPI



IPC

Iron Law

CPI

Spectre

Iron Law

IPC

CPI