ROWHAMMERJS

ROOT privileges for web apps!

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

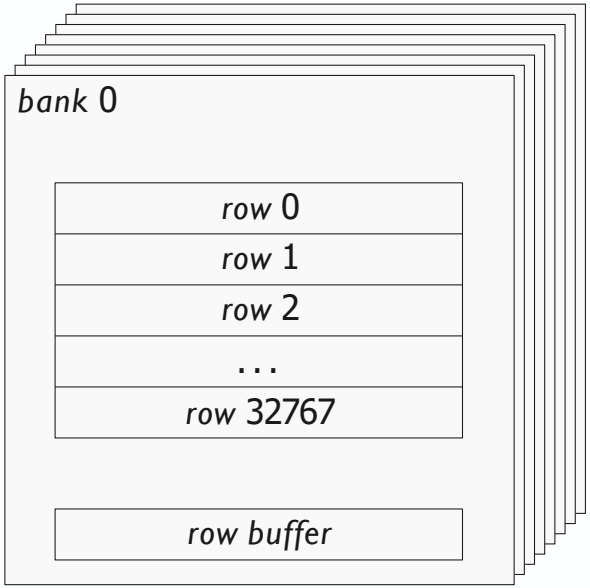
[!] Found flip (239 != 255) at array index 340022176 when hammering indices 339881984 and 340156416

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

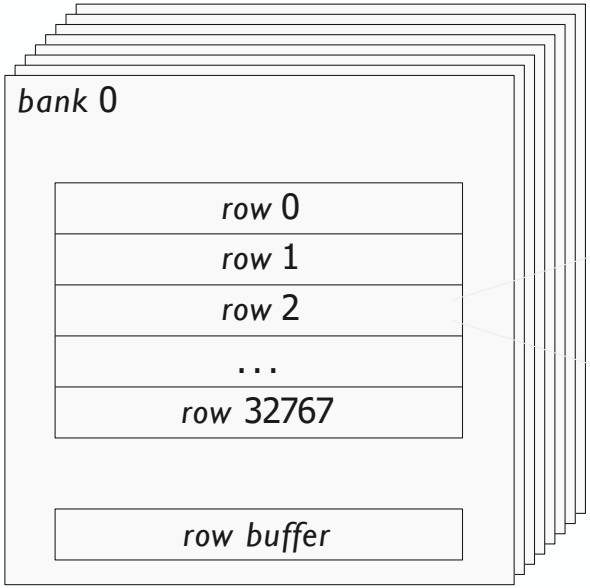
[!] Found flip (254 != 255) at array index 340025146 when hammering indices 339881984 and 340156416

DRAM organisation

chip

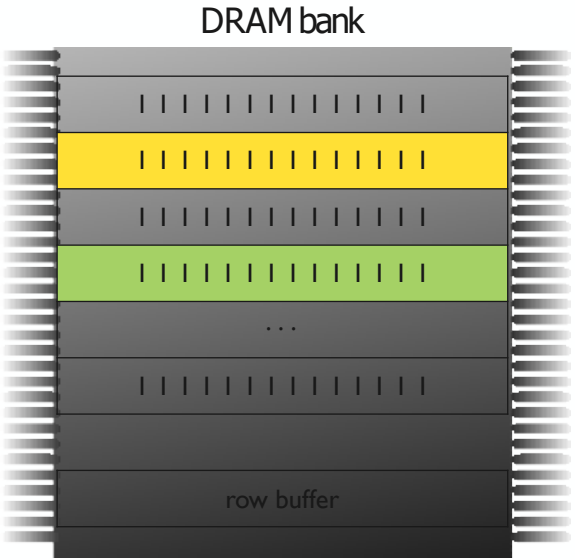


DRAM organisation



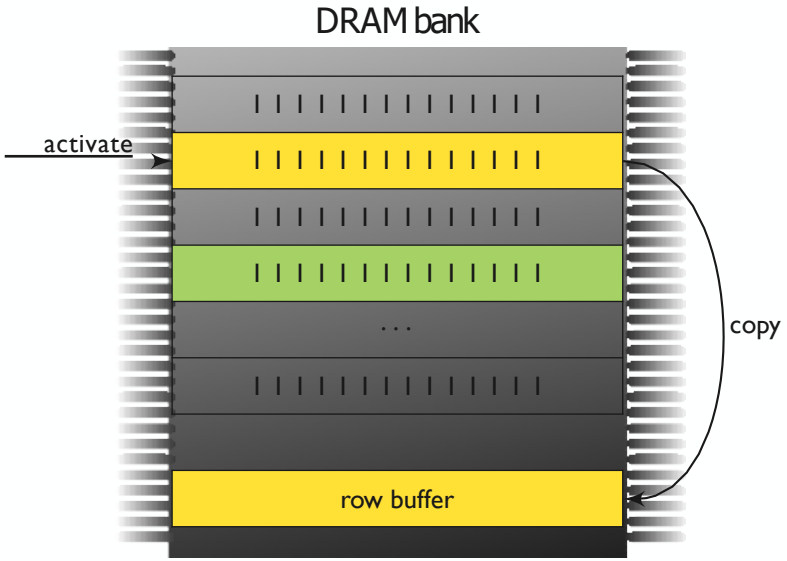
64k cells
1 capacitor,
1 transitor each

Rowhammer



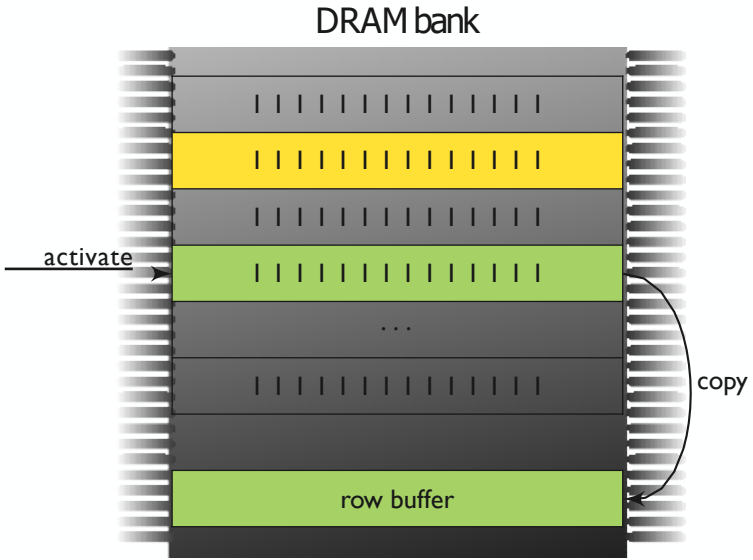
- Cells leak → need refresh
- Max. refresh interval to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



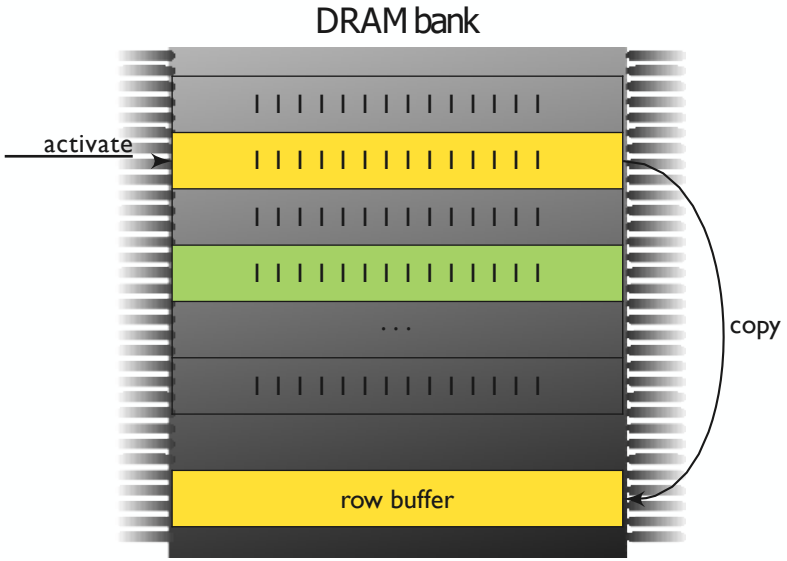
- Cells leak → need refresh
- Max. refresh interval to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



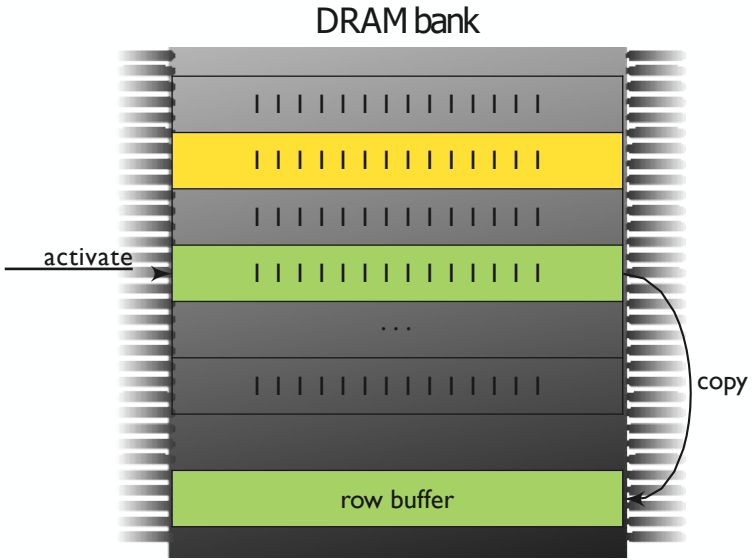
- Cells leak → need refresh
- Max. refresh interval to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



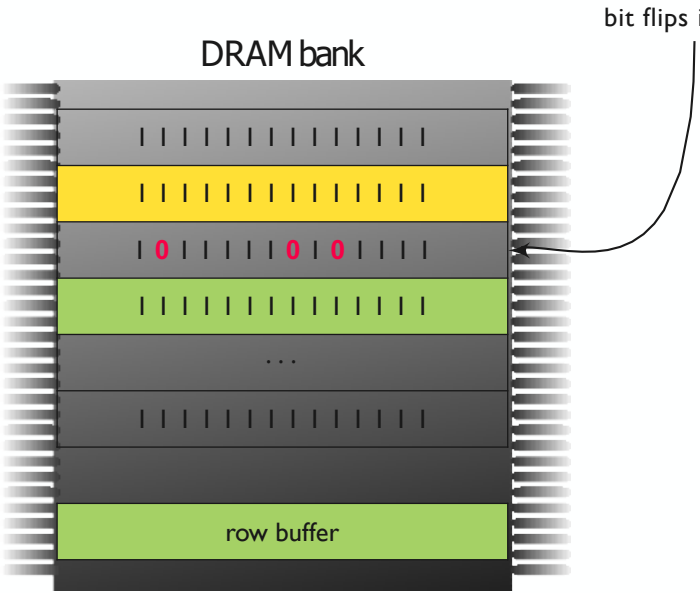
- Cells leak → need refresh
- Max. refresh interval to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



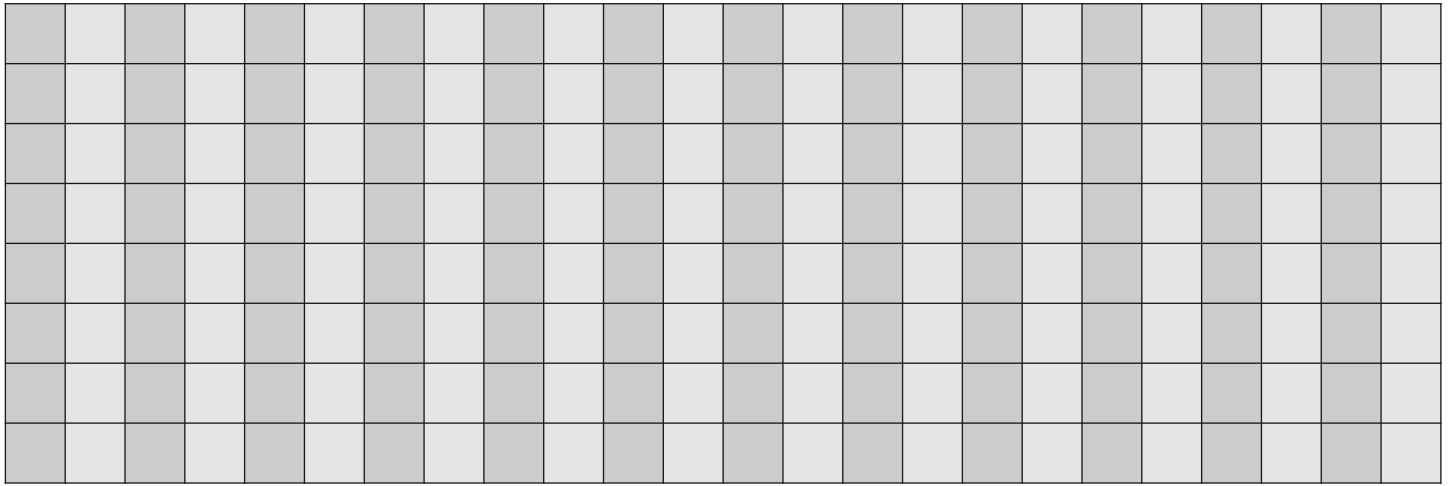
- Cells leak → need refresh
- Max. refresh interval to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Rowhammer



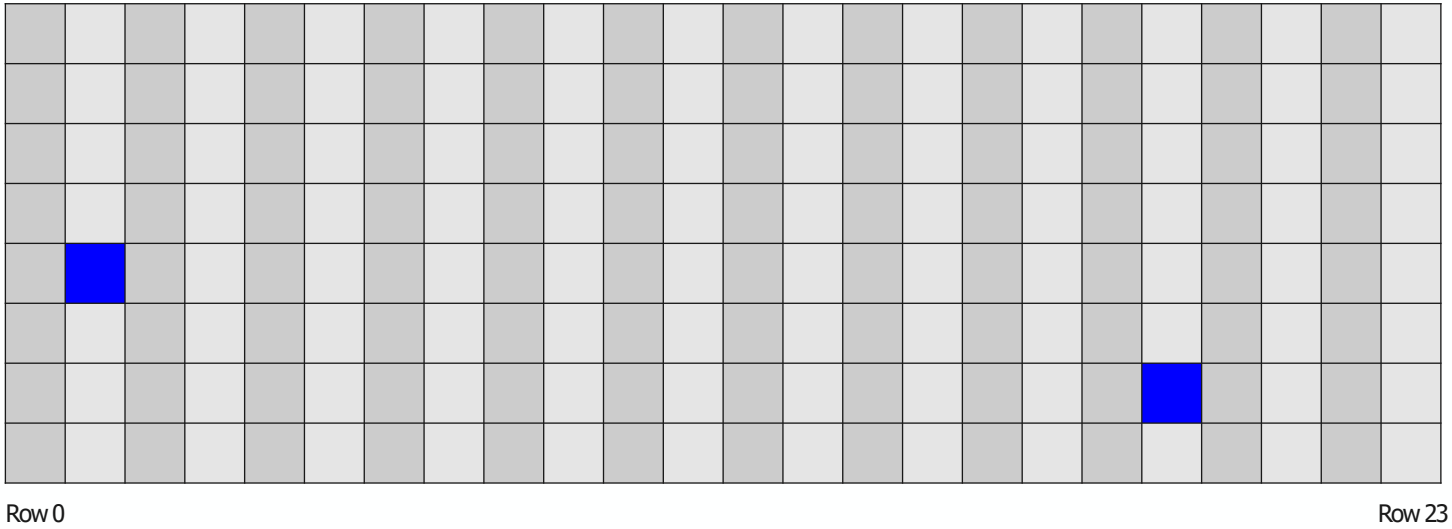
- Cells leak → need refresh
- Max. refresh interval to guarantee data integrity
- Cells leak faster upon proximate accesses → Rowhammer

Search for page with flip



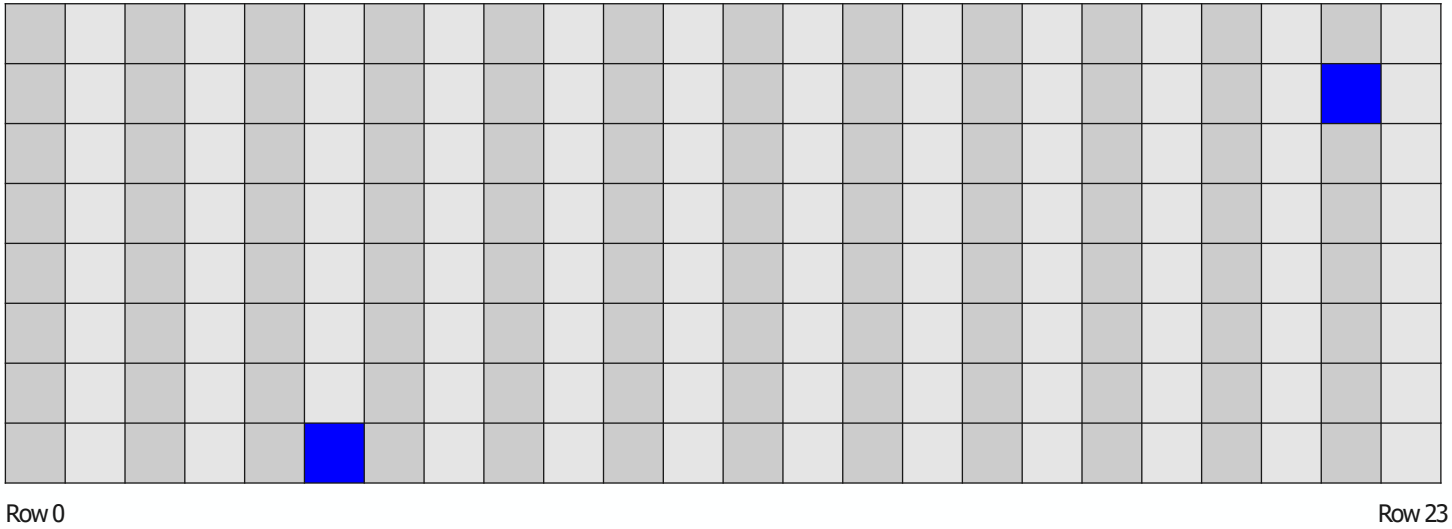
Hammering memory locations in different rows

Search for page with flip



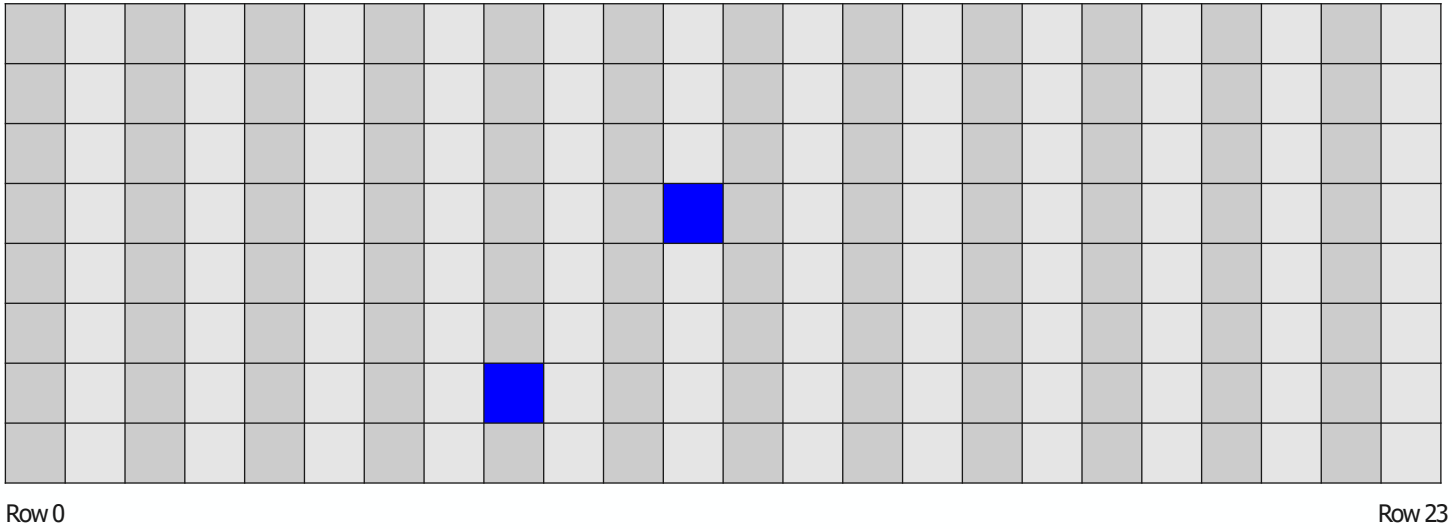
Hammering memory locations in different rows

Search for page with flip



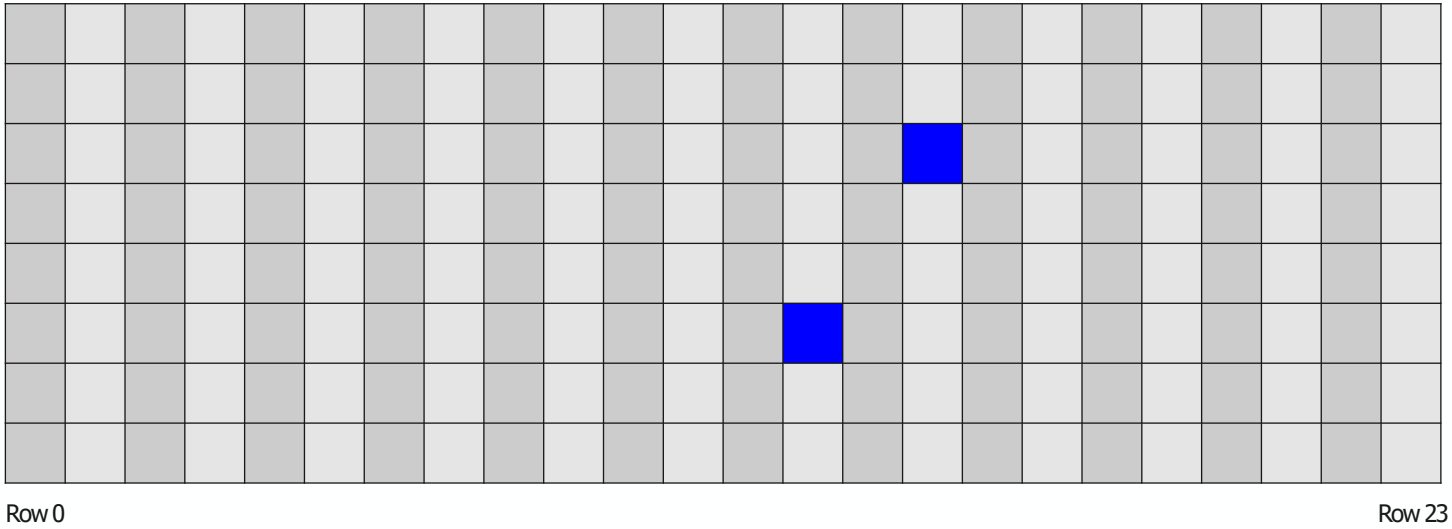
Hammering memory locations in different rows

Search for page with flip



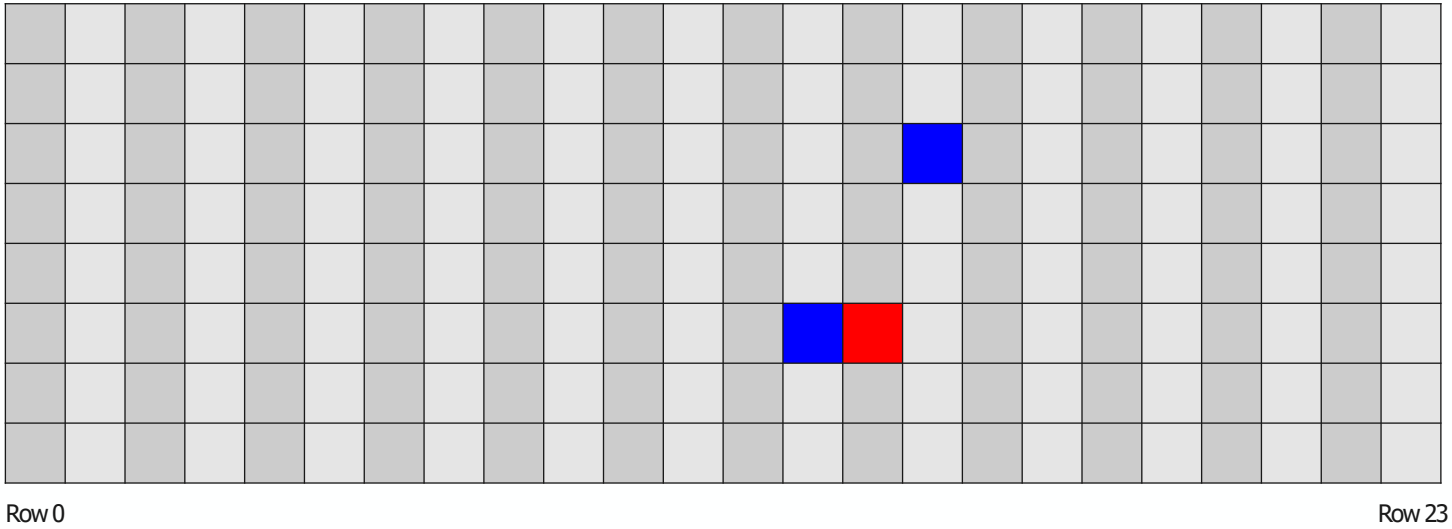
Hammering memory locations in different rows

Search for page with flip



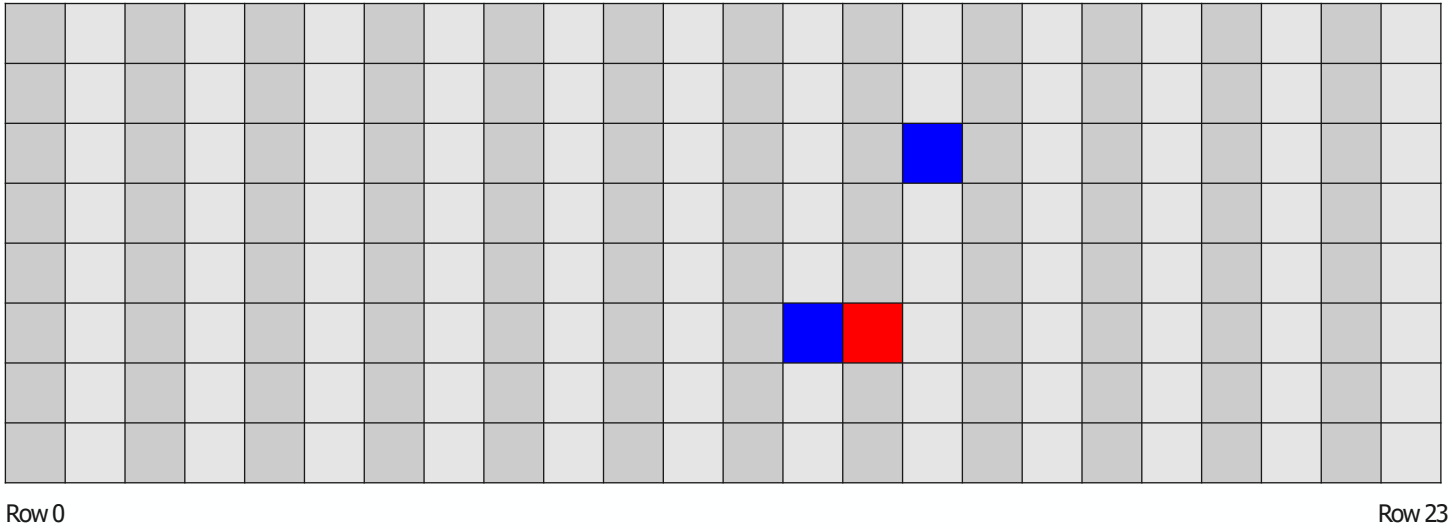
Hammering memory locations in different rows

Search for page with flip



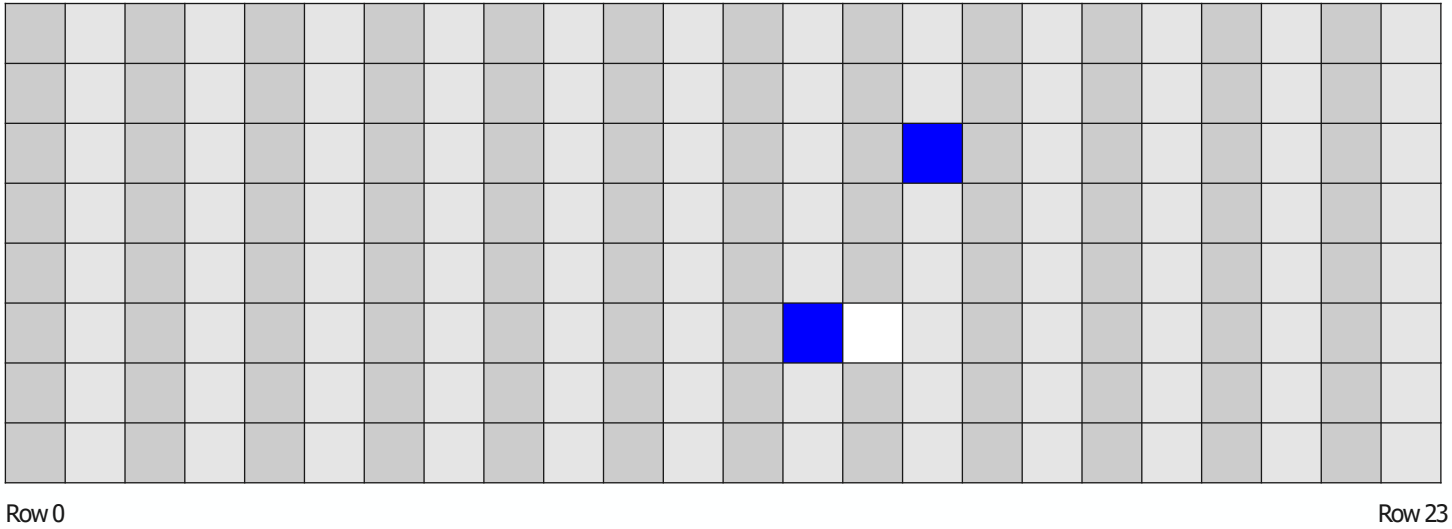
Hammering memory locations in different rows

Search for page with flip



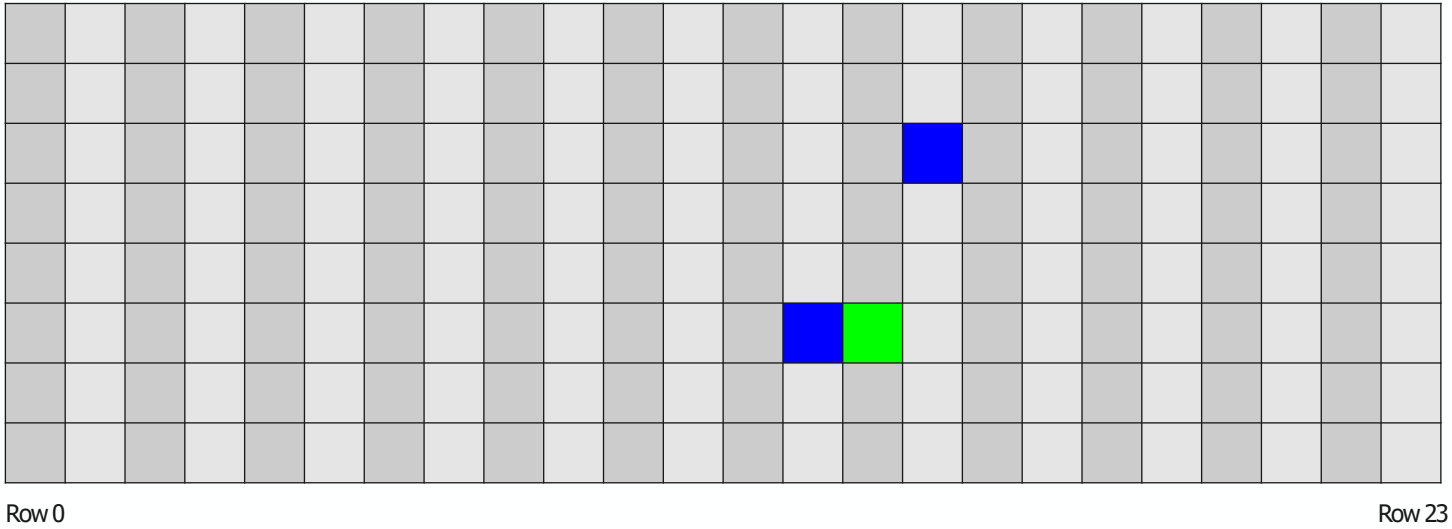
Hammering memory locations in different rows

Search for page with flip



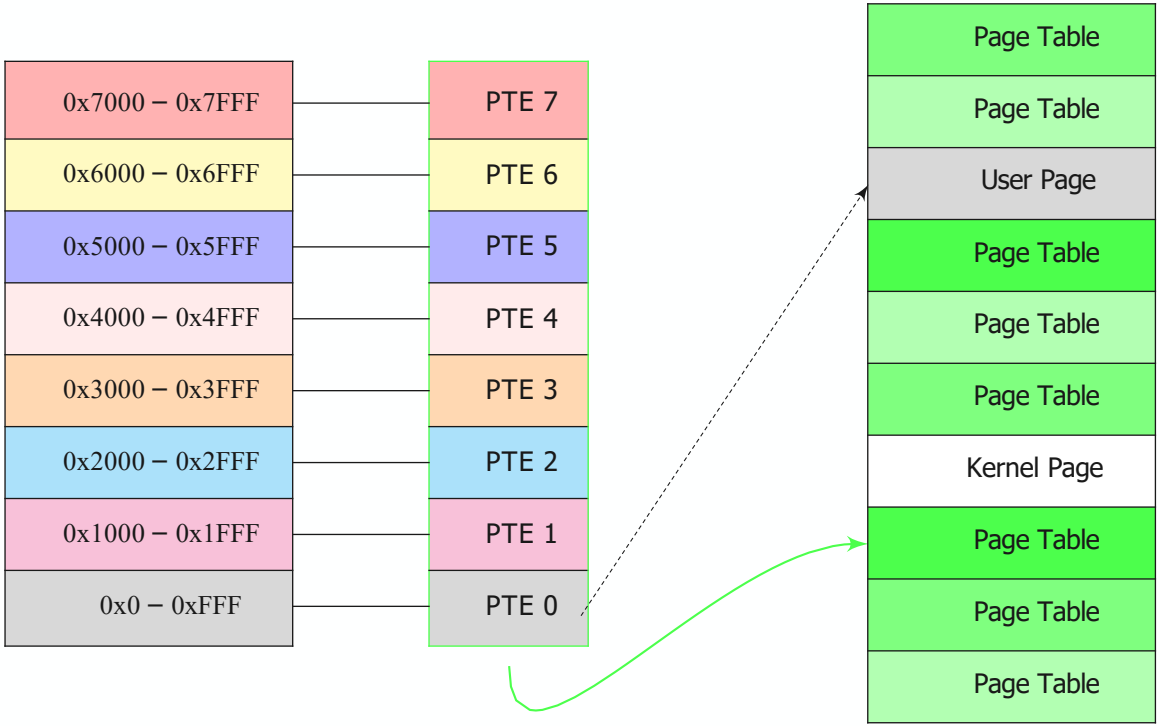
Hammering memory locations in different rows

Search for page with flip

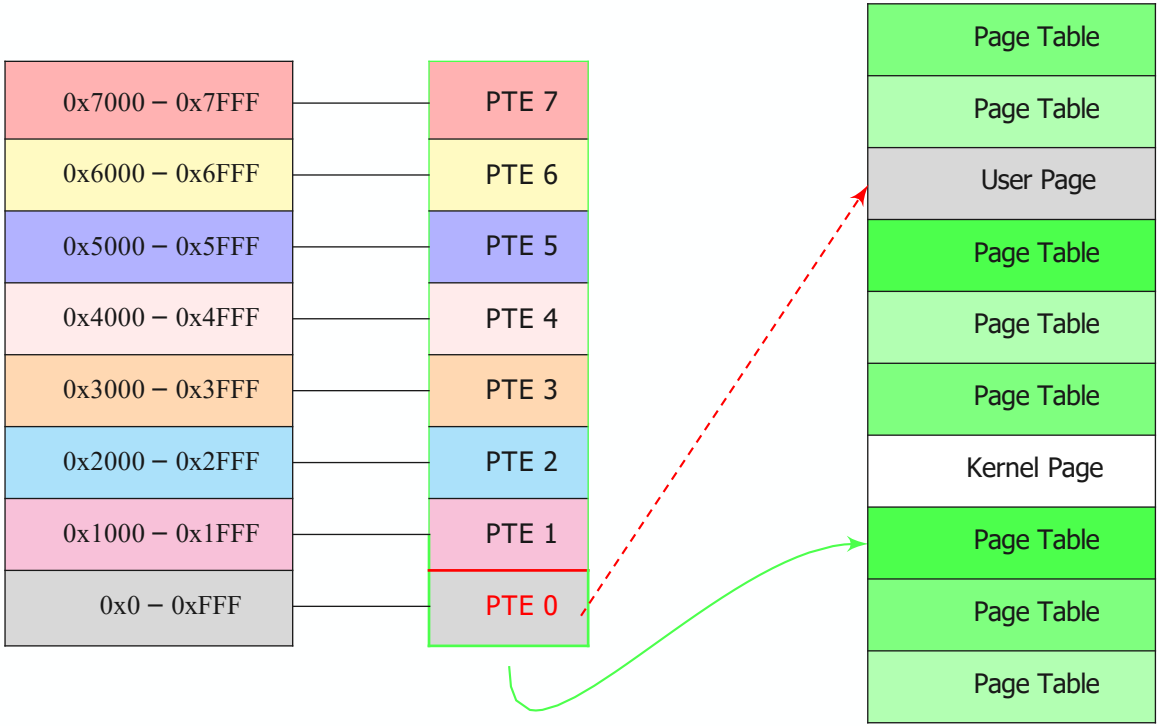


Hammering memory locations in different rows

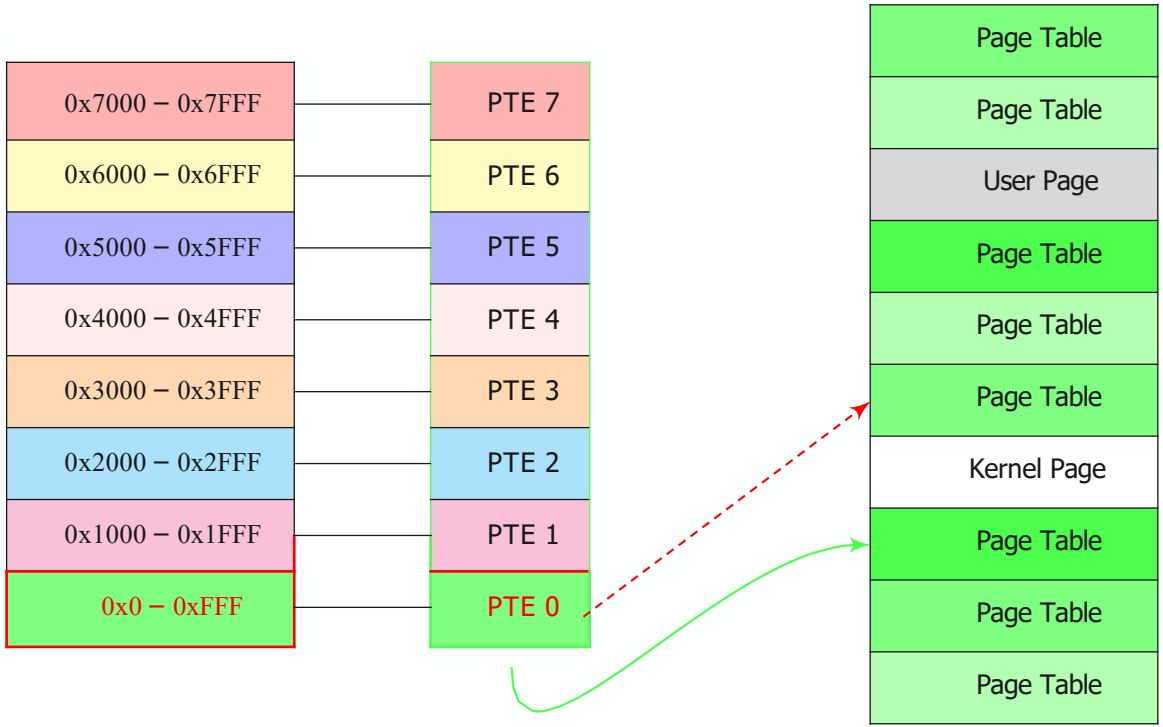
Page Table Example



Page Table Example



Page Table Example



Code Page Example

Code Page Example

Code Page Example

Code Page Example

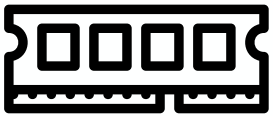
Code Page Example

Code Page Example

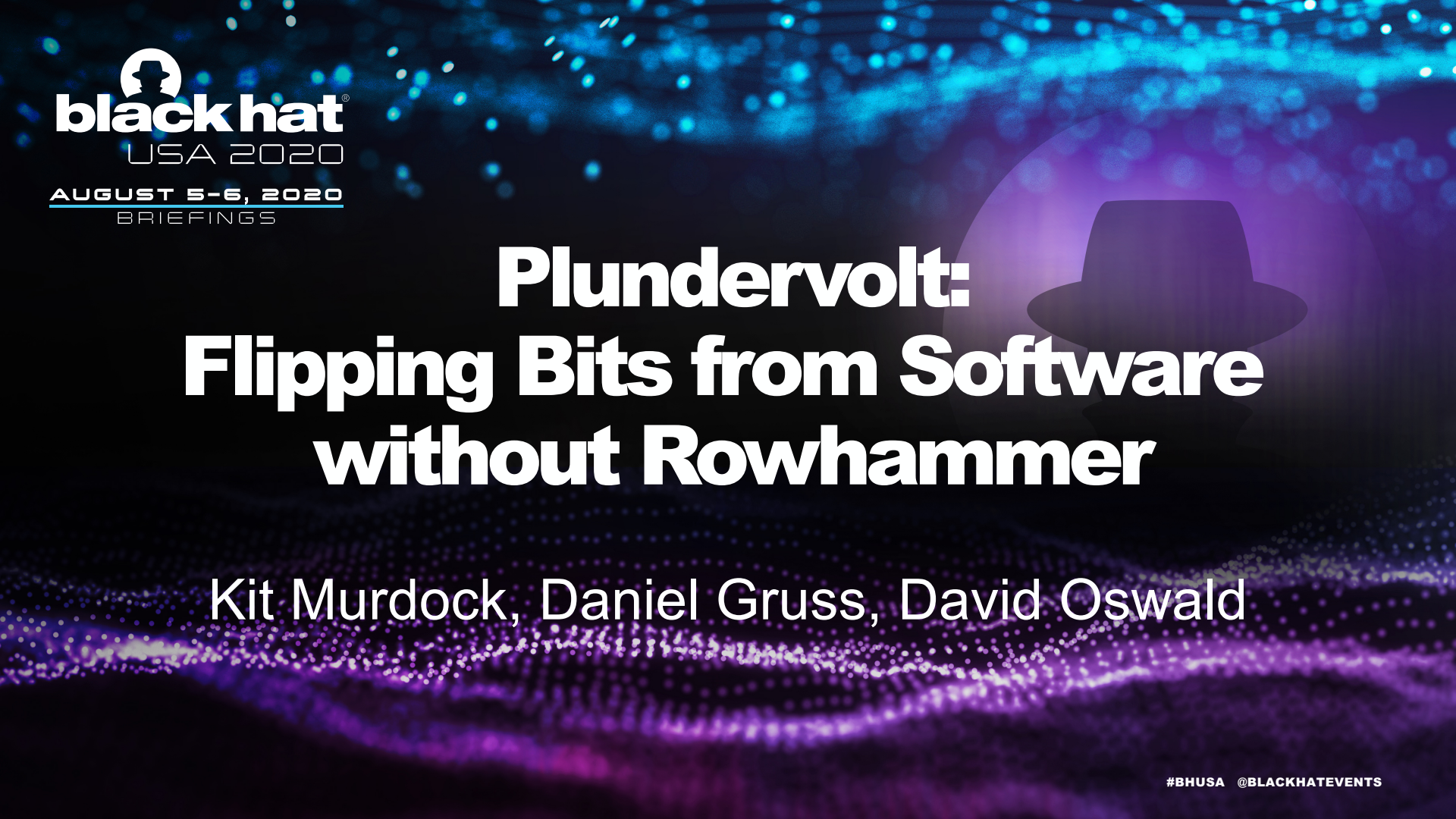
Code Page Example

Code Page Example

Rowhammer

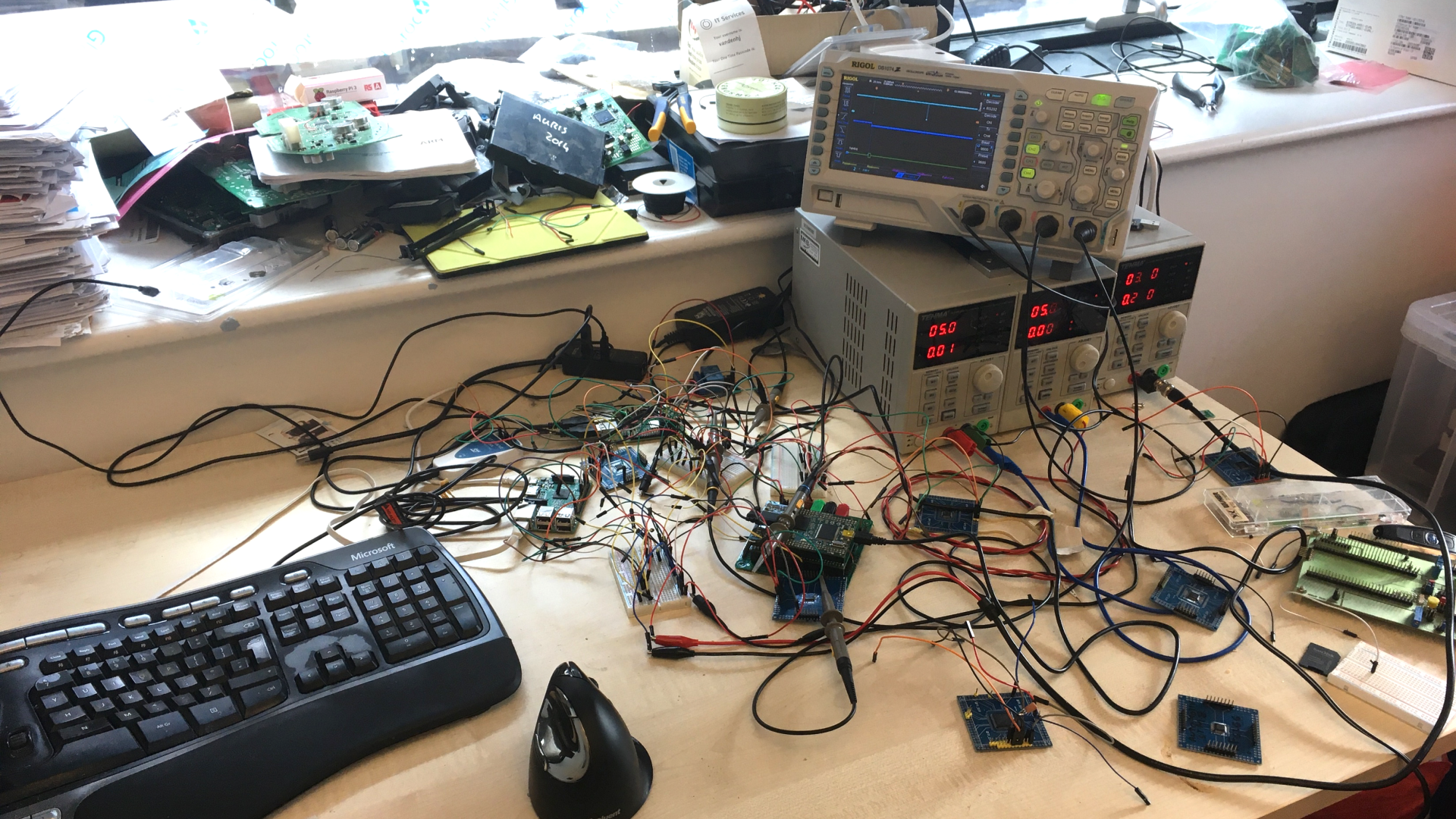


- DDR3 affected
- DDR4 affected
- Even ECC affected despite error correction!
  - Can SGX’s integrity protection prevent Rowhammer?

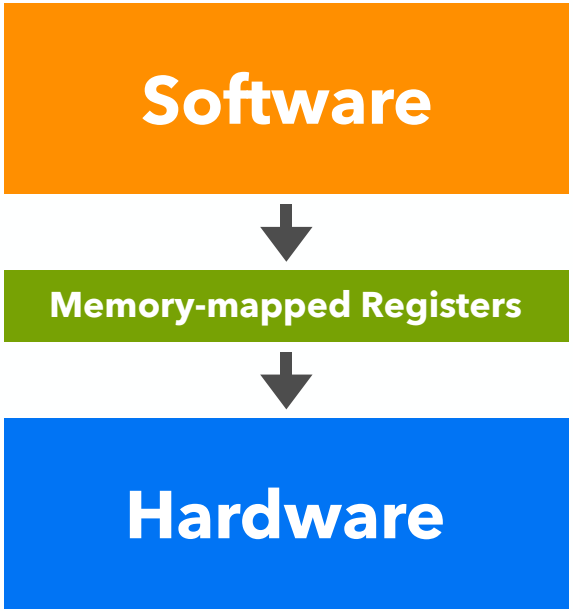


Plundervolt: Flipping Bits from Software without Rowhammer

Kit Murdock, Daniel Gruss, David Oswald


RIGOL
Microsoft

Memory Mapped Registers



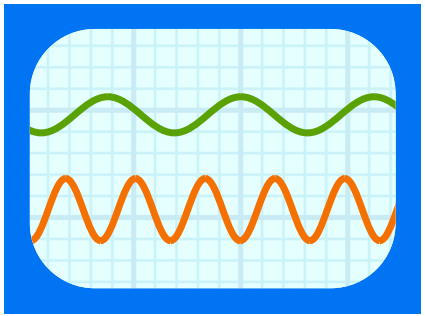
DVFS

Adrian Tang et al. "CLKSCREW: exposing the perils of security-oblivious energy management"

In: USENIX Security Symposium 2017

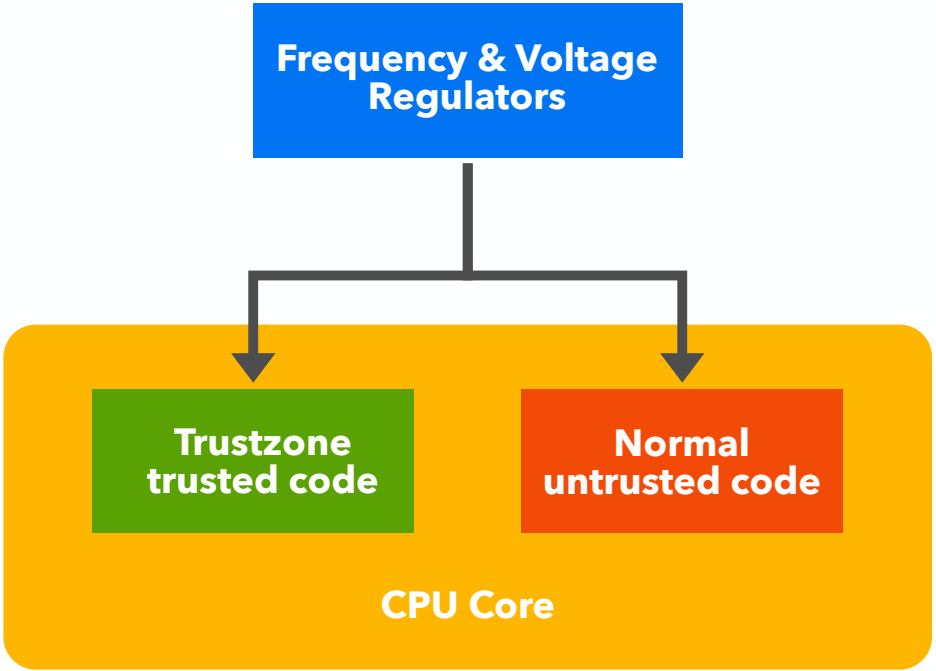
CLKscrew attack


```
add.w    (a0)+,d1
cmp.l    a0,d0
bcc.s    loop
movea.l  #$18E,a1
cmp.w    (a1),d1
bne.w    WrongChecksum
```



2 + 2 = 5

Trustzone v normal world



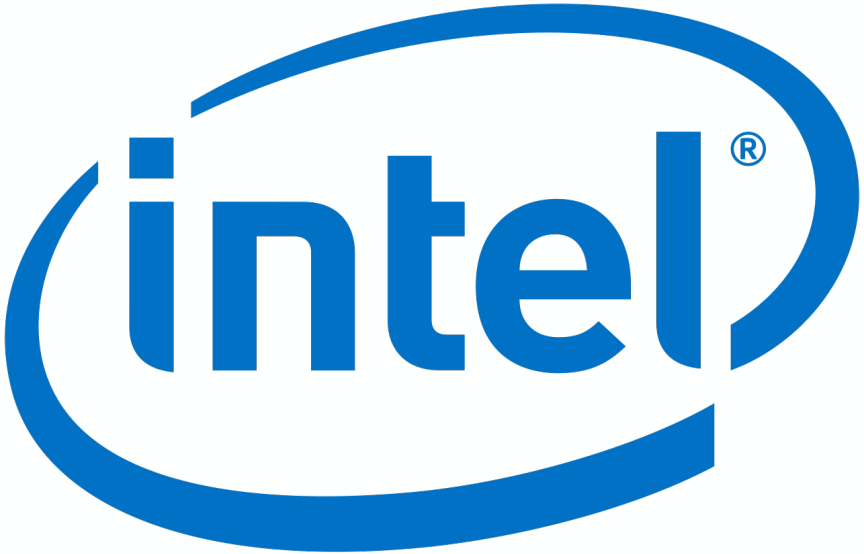
- Infer secret AES key that was stored within Trustzone
- Trick Trustzone into loading a self-signed app

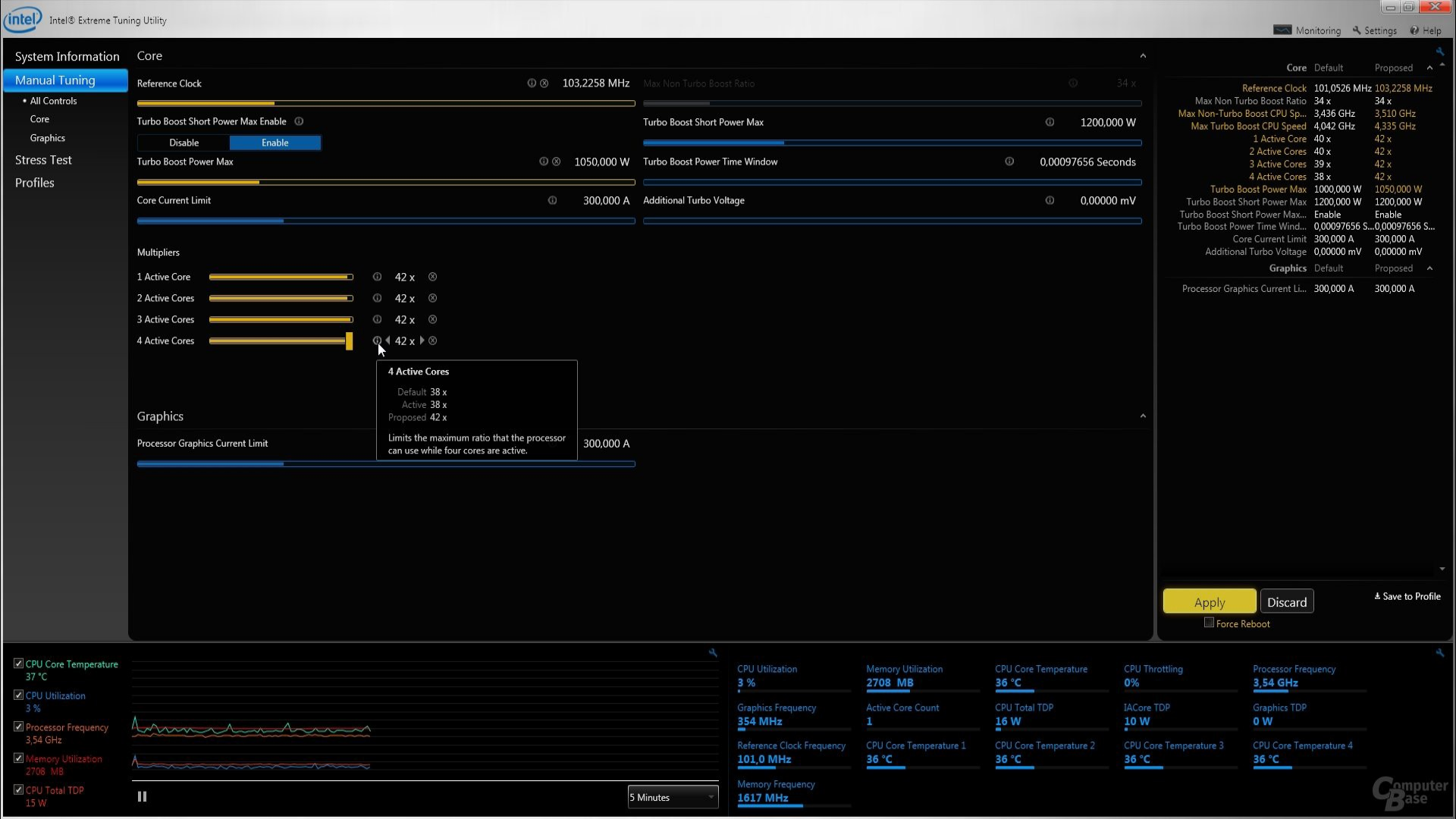
Pengfei Qiu et al. "VoltJockey: Breaching TrustZone by Software-Controlled Voltage Manipulation over Multi-core Frequencies"

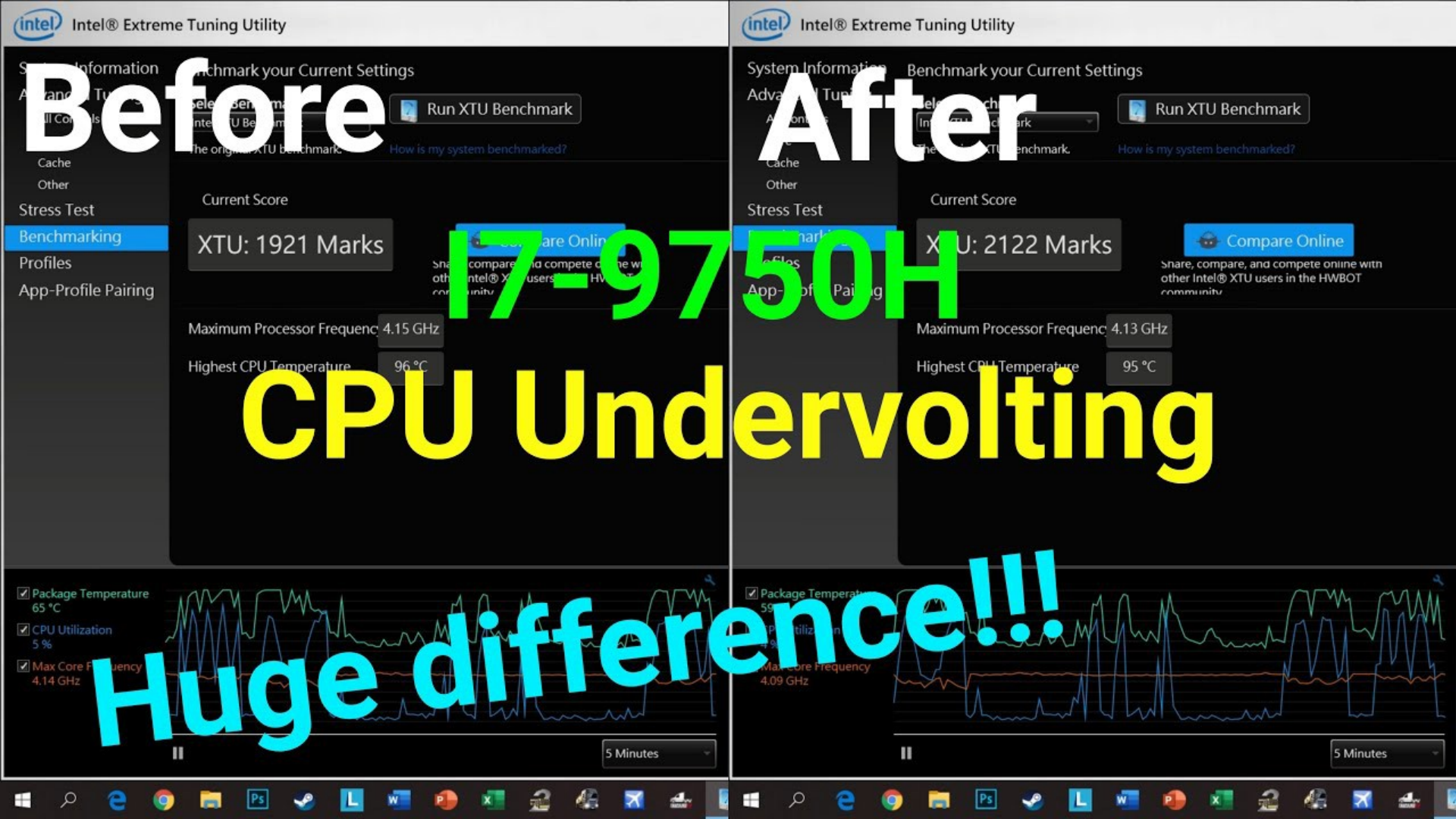
In: CCS 2019

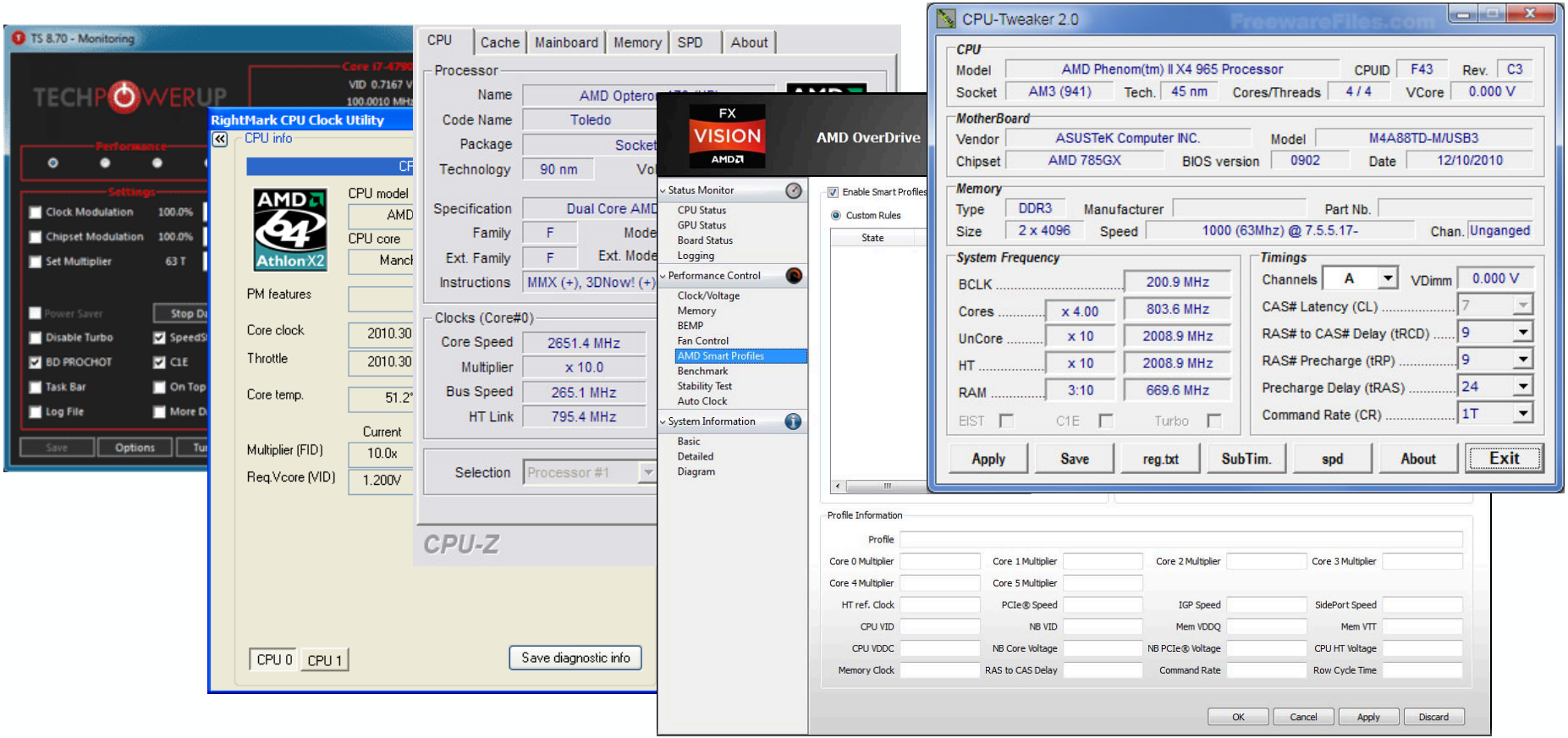
ARM

What about Intel?



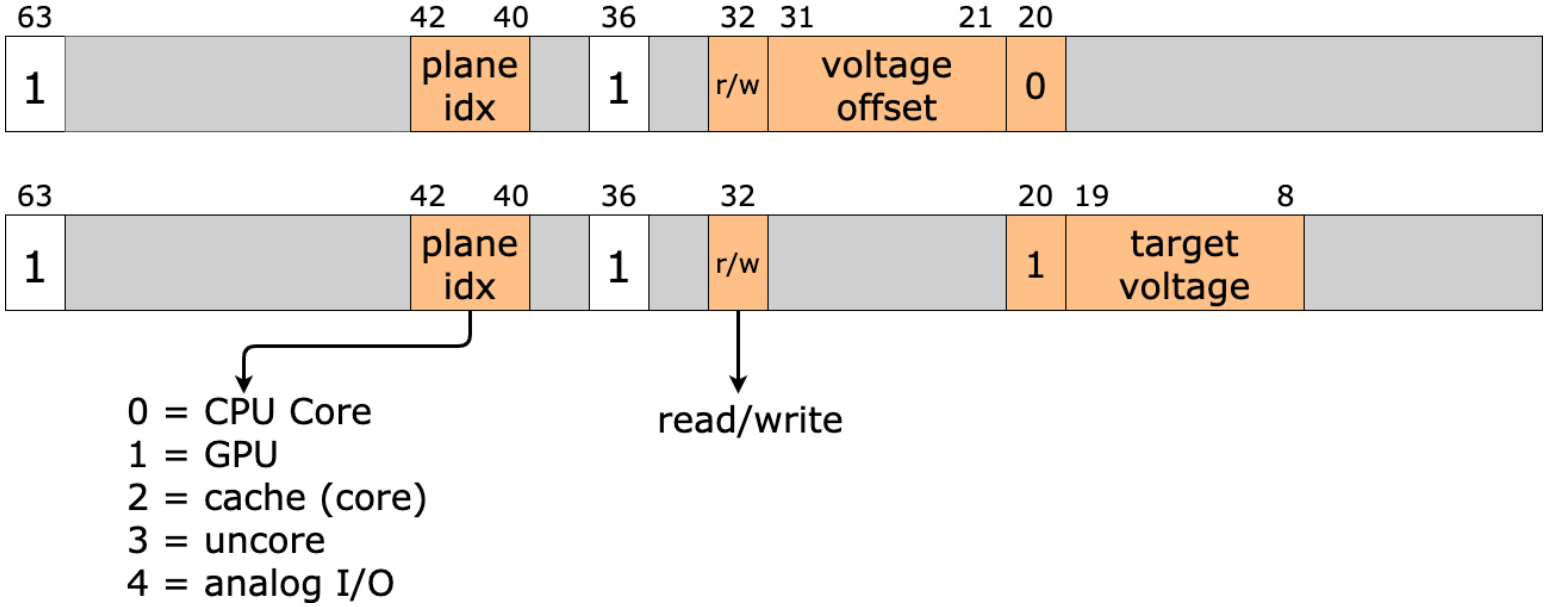

Intel® Extreme Tuning Utility
Monitoring
Settings
Help
System Information
Manual Tuning
• All Controls
Core
Graphics
Stress Test
Profiles
Core
Reference Clock
103,2258 MHz
Max Non Turbo Boost Ratio
34 x
Turbo Boost Short Power Max Enable
Disable
Enable
Turbo Boost Short Power Max
1200,000 W
Turbo Boost 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 4,335 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
Save to Profile
Force Reboot
CPU Core Temperature 37 °C
CPU Utilization 3 %
Processor Frequency 3,54 GHz
Memory Utilization 2708 MB
CPU Total TDP 15 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 16 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 1617 MHz


Before
After
i7-9750H
CPU Undervolting
Huge difference!!!
Intel® Extreme Tuning Utility
Benchmark your Current Settings
Run XTU Benchmark
How is my system benchmarked?
Cache
Other
Stress Test
Benchmarking
Profiles
App-Profile Pairing
Current Score
XTU: 1921 Marks
Maximum Processor Frequenc 4.15 GHz
Highest CPU Temperature 96 °C
Compare Online
Share, compare, and compete online with other Intel® XTU users in the HWBOT community
Package Temperature 65 °C
CPU Utilization 5 %
Max Core Frequency 4.14 GHz
5 Minutes
XTU: 2122 Marks
Maximum Processor Frequenc 4.13 GHz
Highest CPU Temperature 95 °C
Package Temperature
Max Core Frequency 4.09 GHz
5 Minutes


TS 8.70 - Monitoring
TECHPOWERUP
Performance
Settings
Clock Modulation 100.0%
Chipset Modulation 100.0%
Set Multiplier 63 T
Power Saver
Disable Turbo
BD PROCHOT
Task Bar
Log File
Stop Du
SpeedSt
C1E
On Top
Save
Options
RightMark CPU Clock Utility
CPU info
AMD 64 AthlonX2
CPU model
CPU core
PM features
Core clock 2010.30
Throttle 2010.30
Core temp. 51.2°
Current
Multiplier (FID) 10.0x
Req.Vcore (VID) 1.200V
CPU 0
CPU 1
Save diagnostic info
CPU
Cache
Mainboard
Memory
SPD
About
Processor
Name
Code Name Toledo
Package
Technology 90 nm
Specification Dual Core AMD
Family F
Ext. Family F
Instructions MMX (+), 3DNow! (+)
Clocks (Core#0)
Core Speed 2651.4 MHz
Multiplier x 10.0
Bus Speed 265.1 MHz
HT Link 795.4 MHz
Selection Processor #1
CPU-Z
FX VISION
AMD OverDrive
Status Monitor
CPU Status
GPU Status
Board Status
Logging
Performance Control
Clock/Voltage
Memory
BEMP
Fan Control
AMD Smart Profiles
Benchmark
Stability Test
Auto Clock
System Information
Basic
Detailed
Diagram
Enable Smart Profiles
Custom Rules
State
Profile Information
Profile
Core 0 Multiplier
Core 1 Multiplier
Core 2 Multiplier
Core 3 Multiplier
Core 4 Multiplier
Core 5 Multiplier
HT ref. Clock
PCIe® Speed
IGP Speed
SidePort Speed
CPU VID
NB VID
Mem VDDQ
Mem VTT
CPU VDDC
NB Core Voltage
NB PCIe® Voltage
CPU HT Voltage
Memory Clock
RAS to CAS Delay
Command Rate
Row Cycle Time
OK
Cancel
Apply
Discard
CPU-Tweaker 2.0
FreewareFiles.com
CPU
Model AMD Phenom(tm) II X4 965 Processor
CPUID F43
Rev. C3
Socket AM3 (941)
Tech. 45 nm
Cores/Threads 4 / 4
VCore 0.000 V
MotherBoard
Vendor ASUSTeK Computer INC.
Model M4A88TD-M/USB3
Chipset AMD 785GX
BIOS version 0902
Date 12/10/2010
Memory
Type DDR3
Manufacturer
Part Nb.
Size 2 x 4096
Speed 1000 (63Mhz) @ 7.5.5.17-
Chan. Unganged
System Frequency
BCLK 200.9 MHz
Cores x 4.00 803.6 MHz
UnCore x 10 2008.9 MHz
HT x 10 2008.9 MHz
RAM 3:10 669.6 MHz
EIST
C1E
Turbo
Timings
Channels A
VDimm 0.000 V
CAS# Latency (CL) 7
RAS# to CAS# Delay (tRCD) 9
RAS# Precharge (tRP) 9
Precharge Delay (tRAS) 24
Command Rate (CR) 1T
Apply
Save
reg.txt
SubTim.
spd
About
Exit

msr 0x150

Static & dynamic voltage

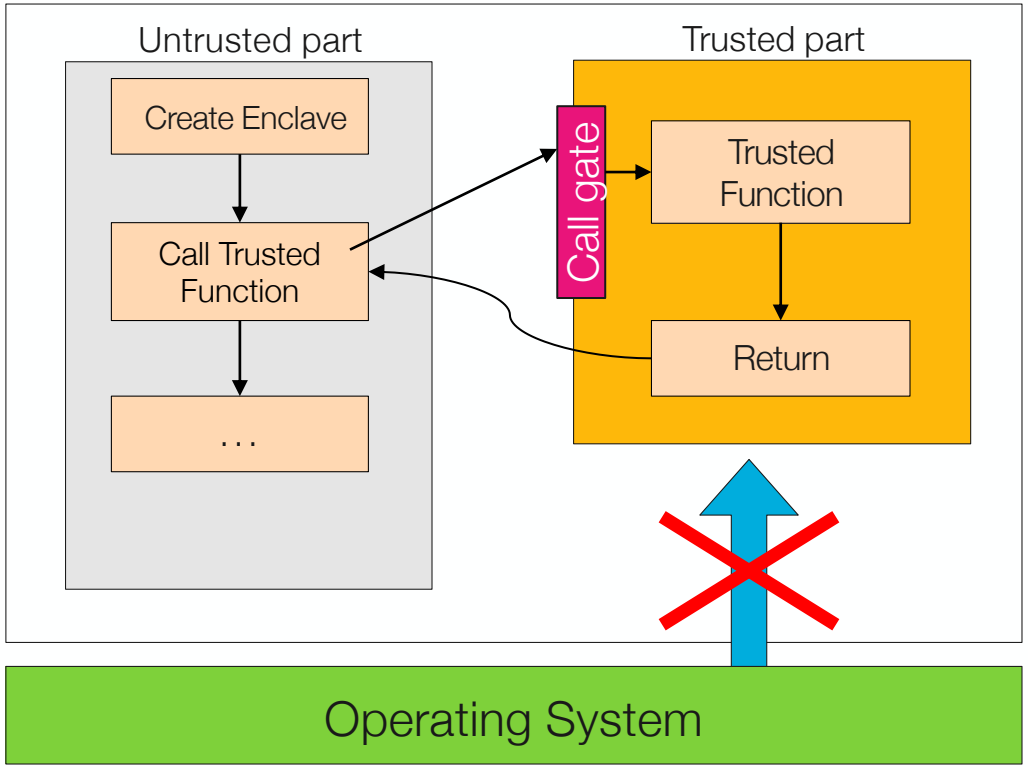


Will it fault?

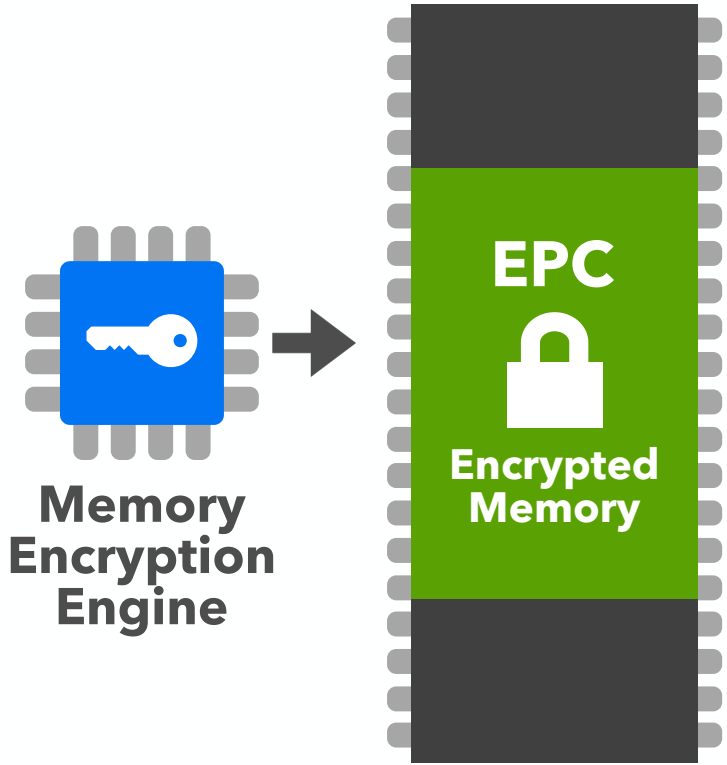

```
uint64_t multiplier       = 0x1122334455667788;
uint64_t correct          = 0xdeadbeef*multiplier;
uint64_t var              = 0xdeadbeef*multiplier;

// start undervolting

while ( var == correct )
{
     var = 0xdeadbeef * multiplier;
}
// stop undervolting
// Can we ever get here?
uint64_t flipped_bits = var ^ correct;
```

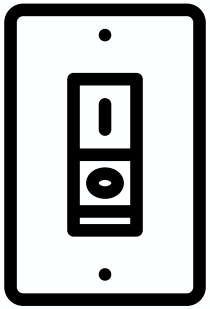
```
bagger>
```

Intel SGX


Untrusted part
Trusted part
Create Enclave
Call Trusted Function
...
Call gate
Trusted Function
Return
Operating System

Physical Memory

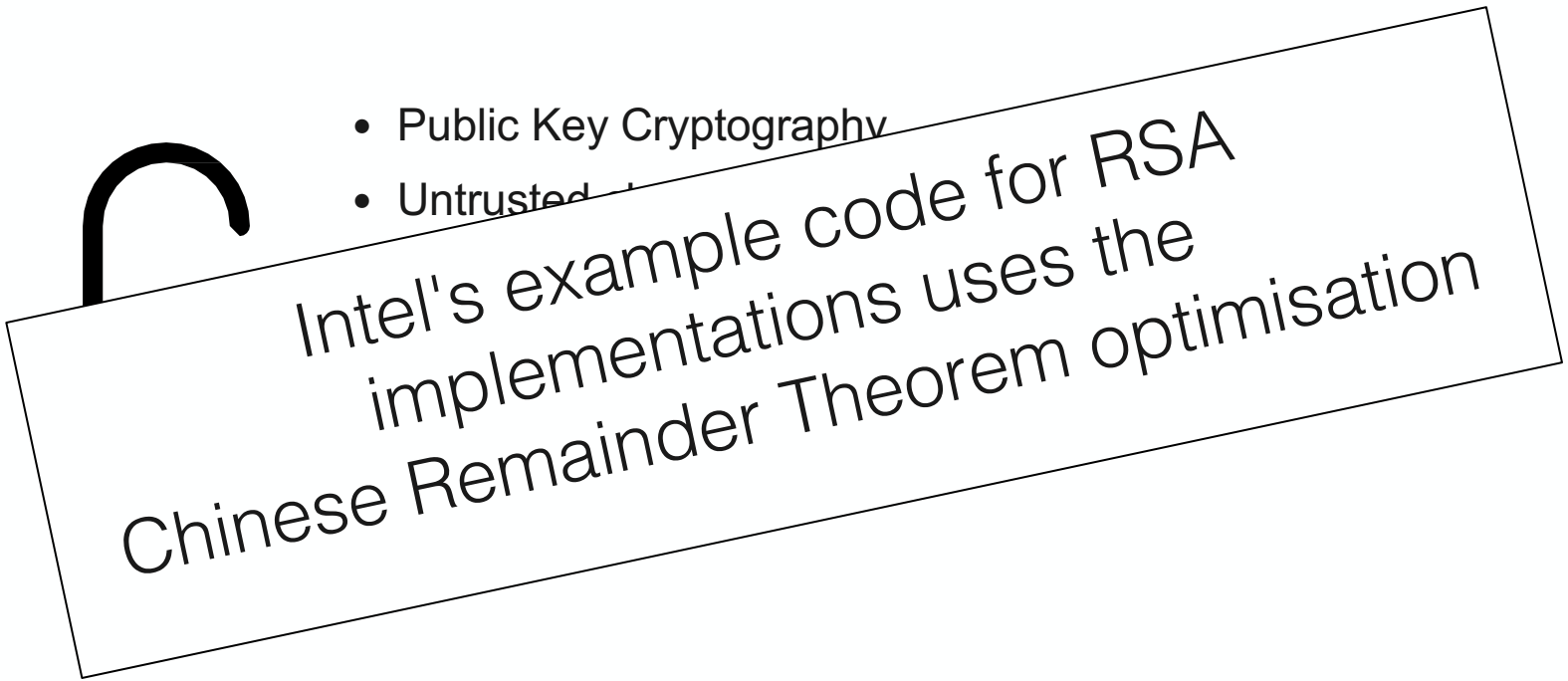




- Bit flips in the EPC?
- Integrity check fails!
- → **Lock up memory controller**
- → System halts immediately (no exploit, but DoS!)

Will Plundervolt work in SGX?

RSA Basics


• Public Key Cryptography
• Untrusted
Intel's example code for RSA implementations uses the Chinese Remainder Theorem optimisation

RSA Signature/Decryption with CRT

$n = p \times q$

$M = C^d \bmod n$

$d_p = d \bmod p - 1$

$d_q = d \bmod q - 1$

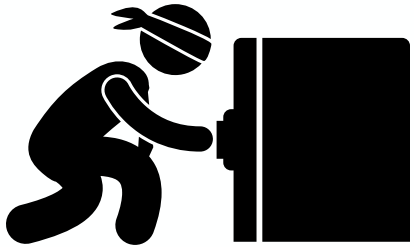
$m_p = C^{dp} \bmod p$

$m_q = C^{dq} \bmod q$

M'

$M = (p^{-1} \bmod q) \times (m_q - m_p) \times p + m_p$

Fault Attack on CRT-RSA



- Bellcore: $\gcd(M' - M, n)$
- Lenstra: $\gcd((M')^e - C, n)$
- yields p or q (and dividing n by it gives the other)

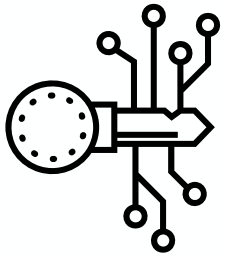
RSA Decryption


```
// Start undervolting
uint8_t rsa_dec_ecall(int iterations)
{
      //Waitforfirstfault
      trigger_fault(iterations);

      //Actualdecryption
      ippsRSA_Decrypt(ct,dec,pPrv,scratchBuffer);
}
// Stop undervolting
```

```
bagger> dog Enclave/encl
```

What else can we break?

AES basics



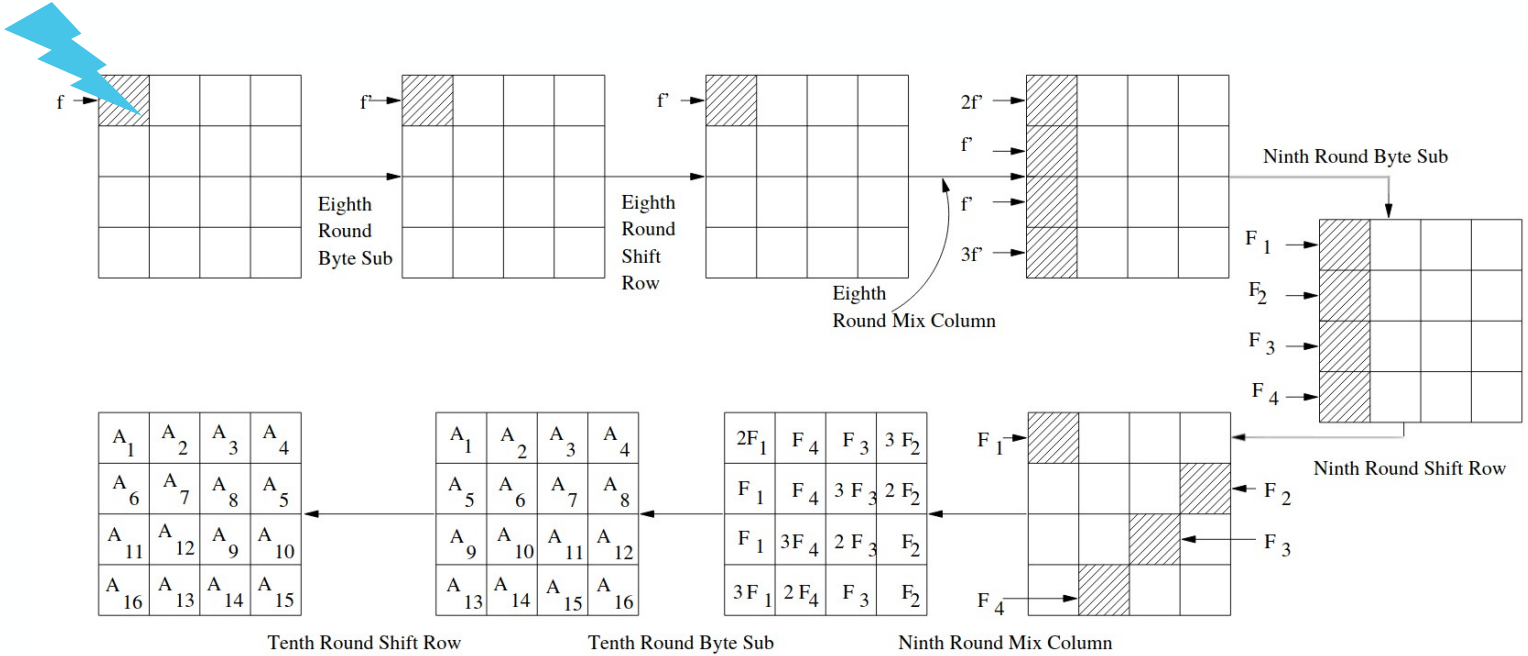
- Symmetric key crypto
- Encrypt messages for transfer over public channel and data for (untrusted) storage
- 4 ×4 byte state, 10 rounds:
  SubBytes, ShiftRows, MixColumns, AddRoundKey
- HW-accelerated with AES-NI

AES inside SGX

Instruction	Description
`AESENC`	Perform one round of an AES encryption flow
`AESENCLAST`	Perform the last round of an AES encryption flow
`AESDEC`	Perform one round of an AES decryption flow
`AESDECLAST`	Perform the last round of an AES decryption flow
`AESKEYGENASSIST`	Assist in AES round key generation
`AESIMC`	Assist in AES Inverse Mix Columns
`PCLMULQDQ`	Carryless multiply (CLMUL)

Differential Fault Analysis Attack

Differential Fault Attack on AES



Proof-of-concept


```
// Start undervolting
do
{
            plaintext= <randomlygenerated>;
            result1=aes128_encryption(plaintext);
            result2=aes128_encryption(plaintext);

} while(result1 == result2)
// Stop undervolting
```

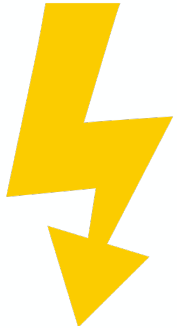
```
bagger> sudo ./aes-encrypt 100000 -262
```

It's not just crypto!

Memory Corruption


```
struct_foo_t *foo = &arr[offset];
foo->foo = enclave_secret;
```

```
foo = arr + offset 0x24
```



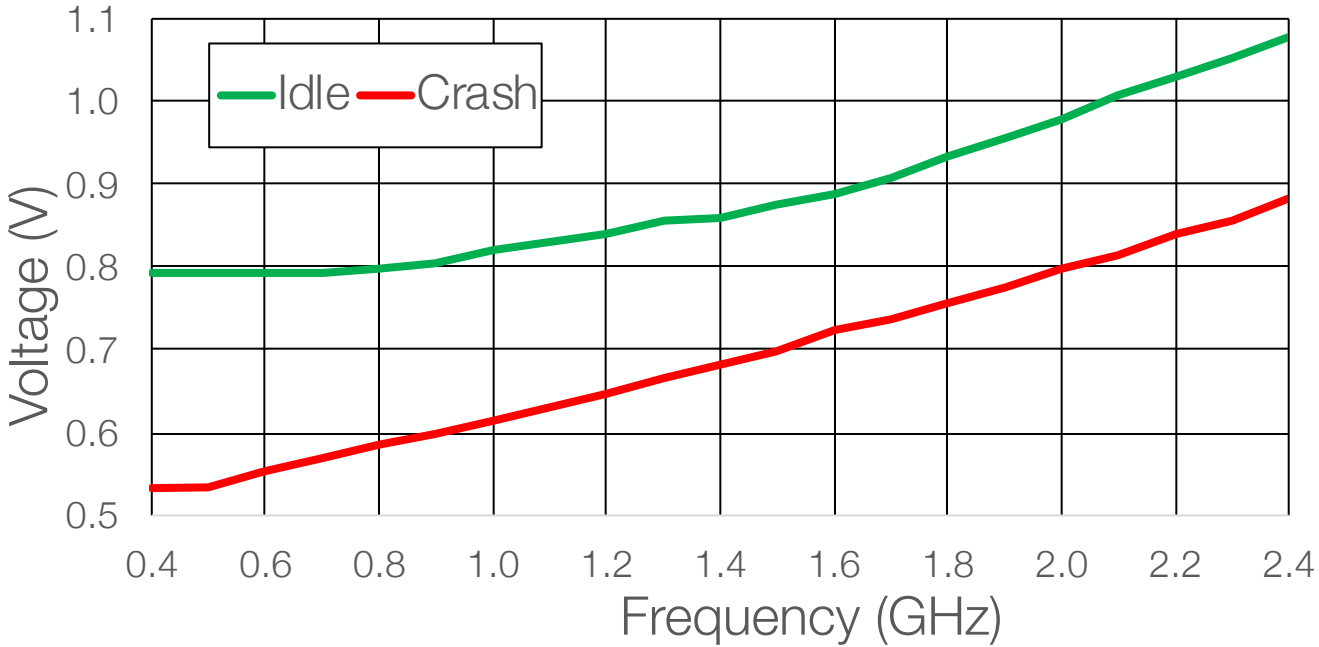
```
Creating enclave...
==== Victim Enclave ====
[pt.c] /dev/sgx-step opened!
Enclave Base:   0x7f001a000000
```

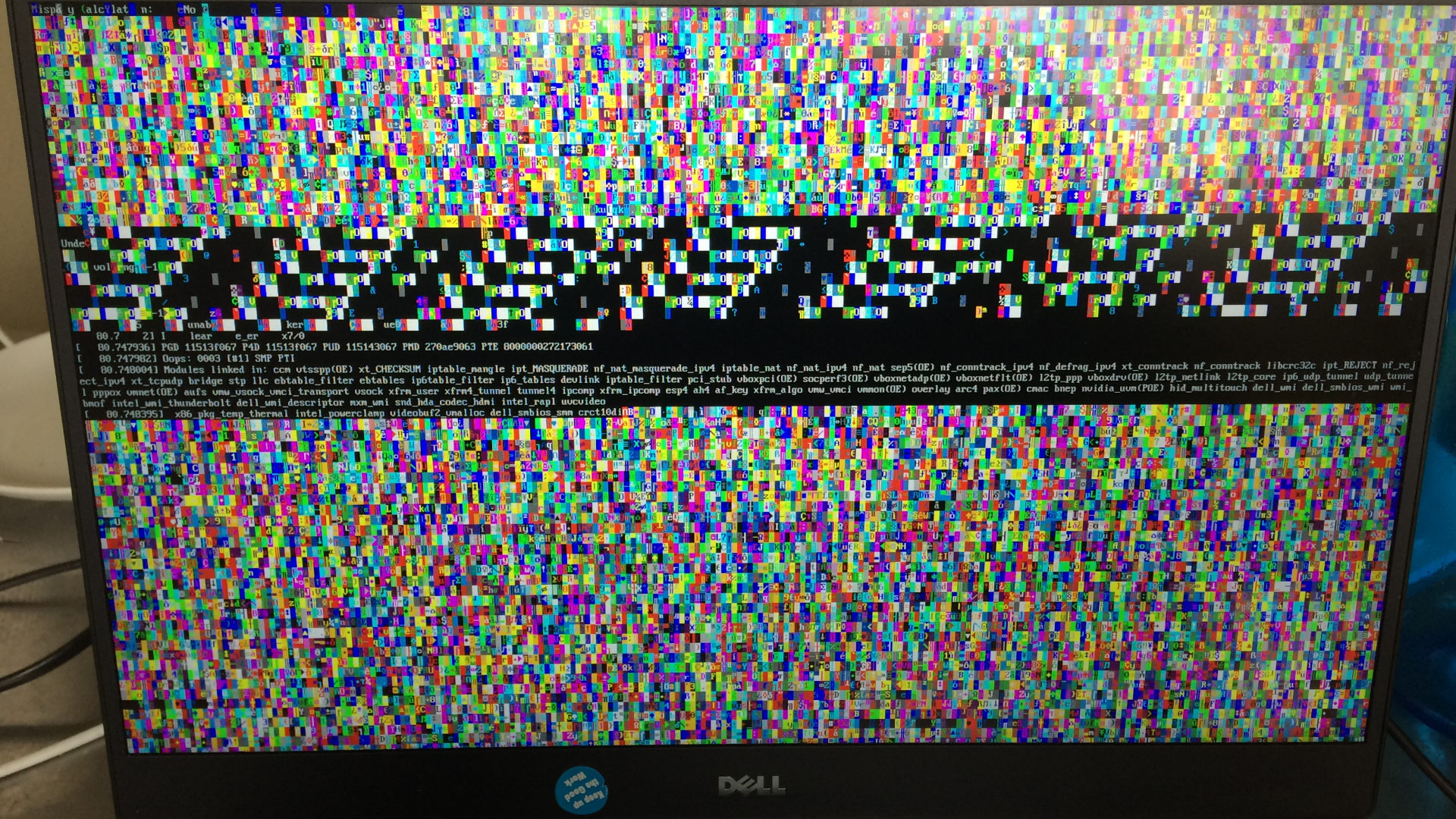
Voltage
0.584V

Undervolting
-235mV

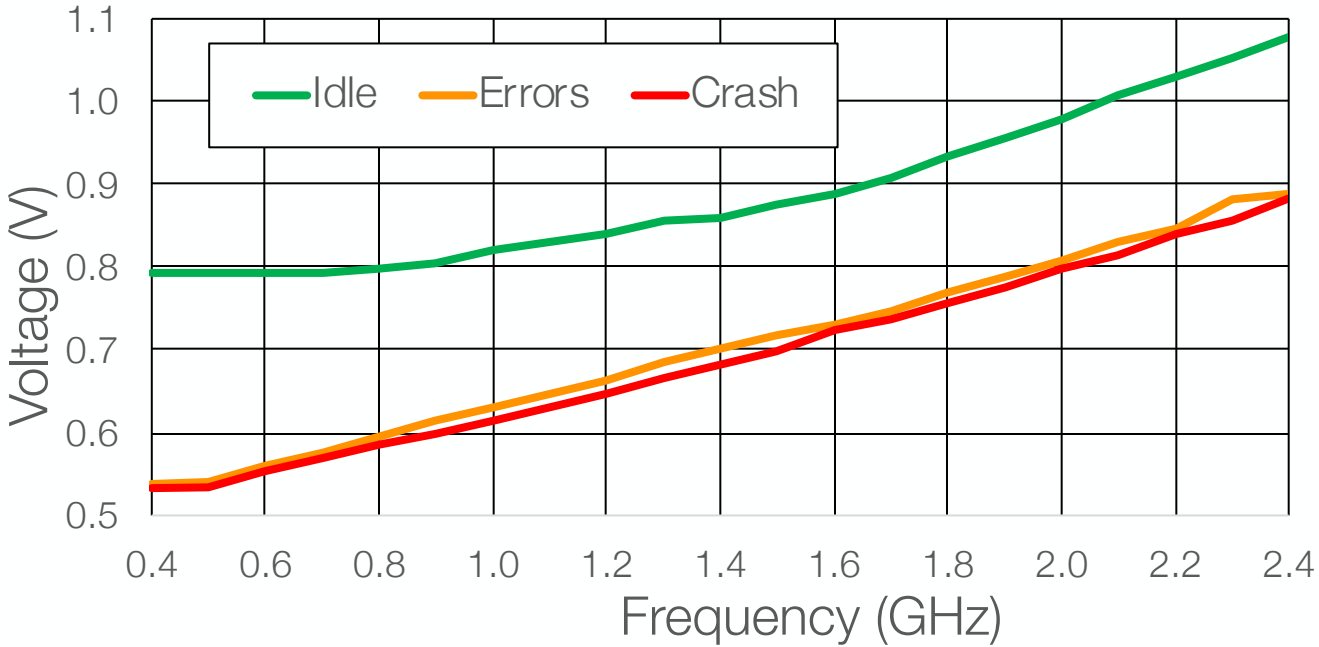
How difficult to fault is it?

Idle & crash voltage – Intel(R) Core i3-7100U CPU

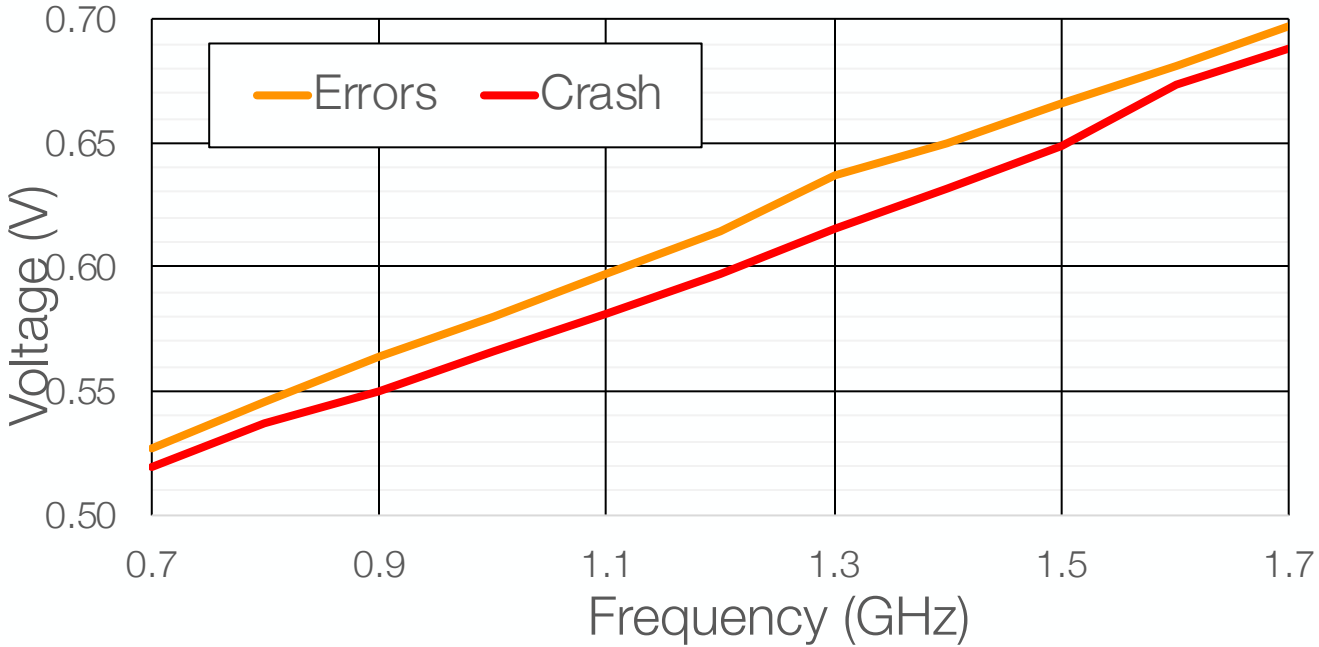



[80.7 2] I lear e_er x7/0
[80.747936] PGD 11513f067 P4D 11513f067 PUD 115143067 PMD 270ae9063 PTE 8000000272173061
[80.747982] Oops: 0003 [#1] SMP PTI
[80.748004] Modules linked in: ccm vtsspp(OE) xt_CHECKSUM iptable_mangle ipt_MASQUERADE nf_nat_masquerade_ipv4 iptable_nat nf_nat_ipv4 nf_nat sep5(OE) nf_conntrack_ipv4 nf_defrag_ipv4 xt_conntrack nf_conntrack libcrc32c ipt_REJECT nf_rej
ect_ipv4 xt_tcpudp bridge stp llc ebtable_filter ebtables ip6table_filter ip6_tables devlink iptable_filter pci_stub vboxpci(OE) socperf3(OE) vboxnetadp(OE) vboxnetflt(OE) l2tp_ppp vboxdrv(OE) l2tp_netlink l2tp_core ip6_udp_tunnel udp_tunne
l pppox vmnet(OE) aufs vmw_vsock_vmci_transport vsock xfrm_user xfrm4_tunnel tunnel4 ipcomp xfrm_ipcomp esp4 ah4 af_key xfrm_algo vmw_vmci vmmon(OE) overlay arc4 pax(OE) cmac bnep nvidia_uvm(POE) hid_multitouch dell_wmi dell_smbios_wmi wmi_
bmof intel_wmi_thunderbolt dell_wmi_descriptor mxm_wmi snd_hda_codec_hdmi intel_rapl uvcvideo
[80.748395] x86_pkg_temp_thermal intel_powerclamp videobuf2_vmalloc dell_smbios_smm crct10dif

Idle, error & crash voltages – Intel Core i3-7100U



Error & crash voltages – Intel Core i3-7100U

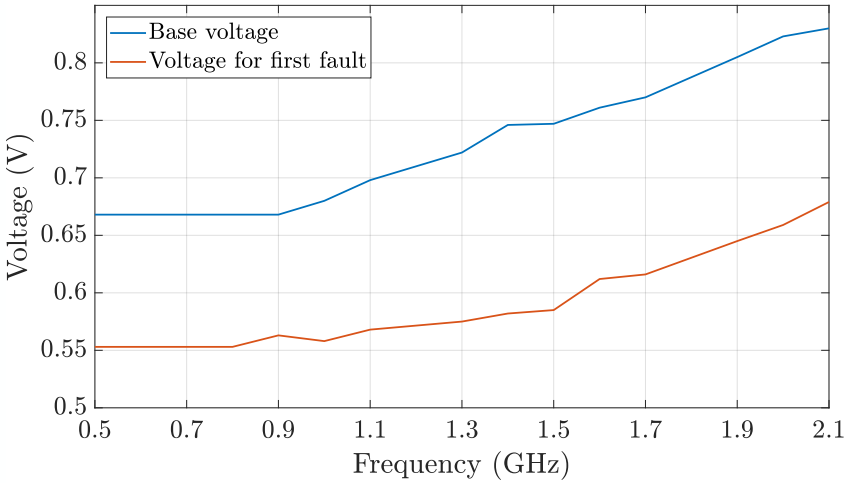


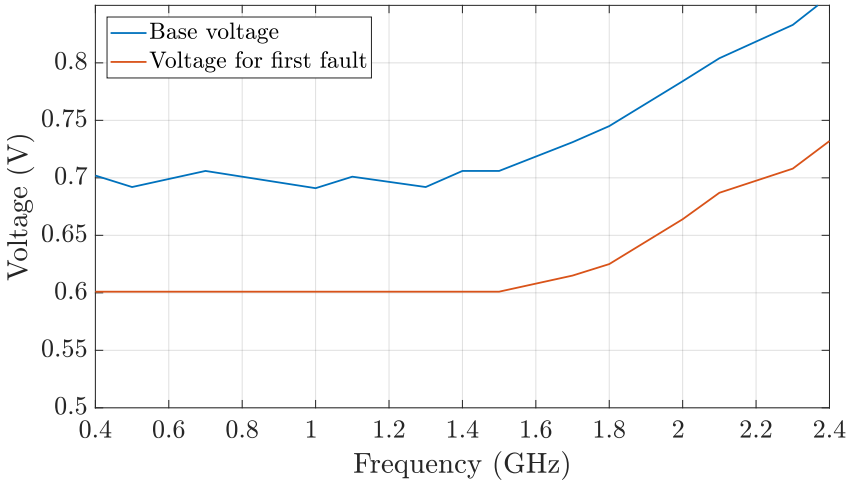
Faulting

Code Name	Model No	Frequency Tested
Skylake	i7-6700K	2.0GHz
Kaby Lake	i7-7700HQ	2.0GHz
	i3-7100U-A	1.0GHz
	i3-7100U-B	2.0GHz
	i3-7100U-C	2.0GHz
Kaby Lake-R	i7-8650U-A	1.9GHz
	i7-8650U-B	1.9GHz
	i7-8550U	2.6GHz
Coffee Lake-R	i9-9900U	3.6GHz

Two Intel Core i3-7100U CPUs

Two Intel Core i3-7100U CPUs





Faulting

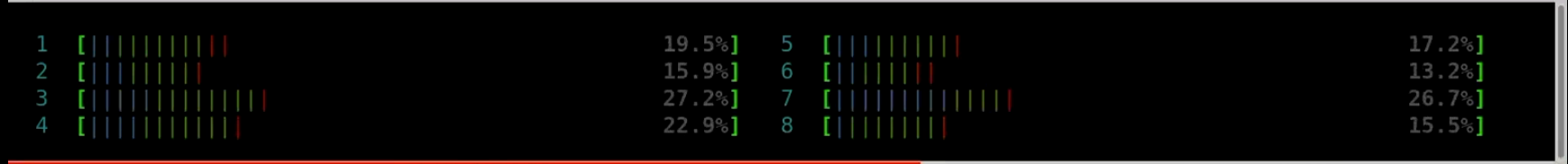
All faults were injected at normal ambient temperature

More undervolting

- Idle cores
- More crashes!

Less undervolting

- Cores maxed
- Fewer crashes



/bin/bash 74x32

```
versatile$
```

/bin/bash 57x34

```
versatile$
```

Faulting some random stuff

```
versatile$ ./operation   -m 200 -s -177 -X 5  -i 200  -o P -c   "cat backup/text_file.txt" -r 0 -t 8

Summary
-----------------------------------------------
time (ms) interval:      200
Iterations:              200
Start Voltage:           -177
End Voltage:             0
Stop after x drops:      5
Voltage steps:           1
Threads:                 8
Operand1:                0x000000ffffffffff
Operand2:                0x000000ffffffffff
Operand1 is:             maximum
Operand2 is:             maximum
Operand1 min is:         0x0000000000000000
Operand2 min is:         0x0000000000000000
Calculation only:        No
Display calculation:     No
Verbose:                 Yes
Option:                  Command Line
Command Line options
 > Command line:         cat backup/text_file.txt
 > Result code:          0
```

Concurrent work

Concurrent Work

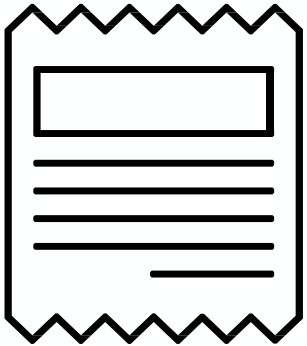
Kenjar, Zijo et al "V0LTpwn: Attacking x86 Processor Integrity from Software"
In: USENIX Security Symposium 2020

Qiu, P at al. "Breaking SGX by software-controlled voltage-induced hardware faults."
In AsianHOST 2019

Summary

- A new type of attack against Intel
- Breaks the integrity of SGX
- Within SGX
    - Retrieve keys using AES-NI
    - Retrieve RSA key
    - Induce memory corruption in bug free code
    - Make enclave write secrets to untrusted memory

Acknowledgements



This research is partially funded by the Research Fund KU Leuven, and by the Agency for Innovation and Entrepreneurship (Flanders). Jo Van Bulck is supported by a grant of the Research Foundation – Flanders (FWO). This research is partially funded by the Engineering and Physical Sciences Research Council (EPSRC) under grants EP/R012598/1, EP/R008000/1, and by the European Union's Horizon 2020 research and innovation programme under grant agreements No. 779391 (FutureTPM) and No. 681402 (SOPHIA).

Thank you