COLD BOOT ATTACK on DDR2 and DDR3 RAM

Simon Lindenlauf, Marko Schuba, Hans Höfken

Aachen University of Applied Sciences, Germany

About

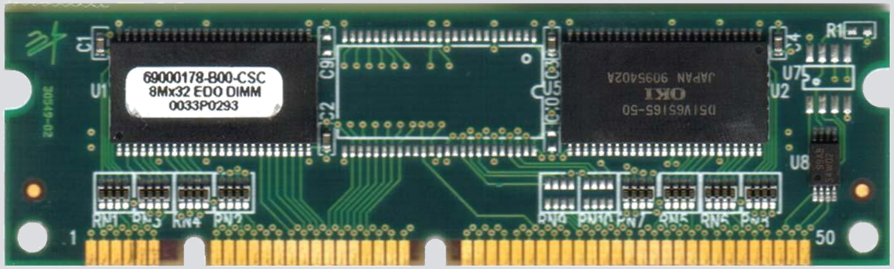
- Simon Lindenlauf
  - former BSc, now Master student at Aachen University of Applied Sciences (FH Aachen)
  - cold boot: topic of his bachelor thesis
- Marko Schuba
  - professor at FH Aachen (computer science)
  - topics of interest: security, forensics
- Hans Höfken
  - researcher at FH Aachen
  - topics of interest: practical stuff, ethical hacking etc.

Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions

DRAM

- DRAM = Dynamic Random-Access Memory
  - is a type of RAM
  - each bit stored in separate capacitor within integrated circuit (states: charged / discharged)

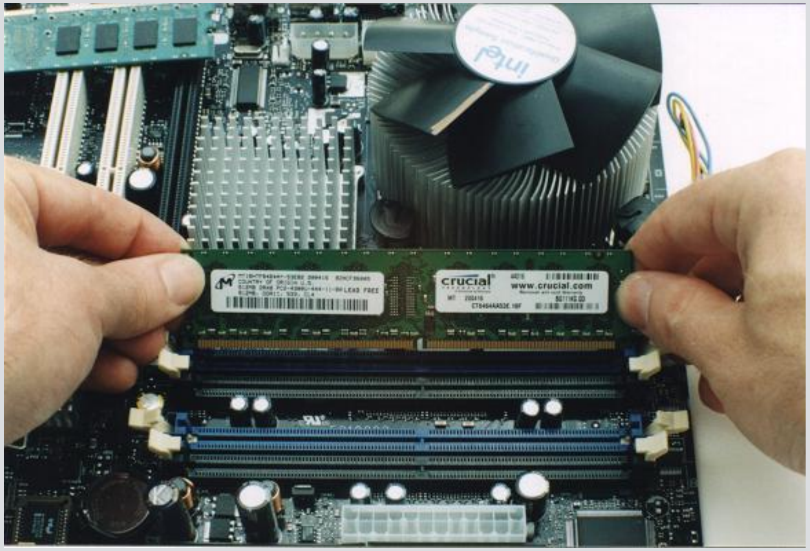


http://www.certificationkits.com/cisco-2600-32mb-dram/

- Leakage and refresh
  - capacitors leak, i.e. they slowly discharge
  - periodic refresh necessary (memory is “dynamic”)
- DRAM is main memory in computers today
  - high density, compared to static RAM

DDR SDRAM*

- DDR SDRAM is a widely used DRAM type
  - Types: DDR1, DDR2, DDR3 and recently DDR4
  - Have different peak transfer rates
    - basically doubling it with each generation
  - Most computers today use DDR2 or DDR3 SDRAM



http://www.ifitjams.com/ibuild3.htm

* Double data rate synchronous dynamic random-access memory

Refresh Rates & Retention Times

- As mentioned before:
  memory cells leak and thus require refresh

- Refresh rate depends on temperature
  - up to 85°C (185°F): 64 ms (standard refresh time)
  - between 85°C (185°F) and 95°C (203°F): 32 ms
  - obviously: leakage of cells increases with temperature

  - 64 ms refresh threshold to be on the safe side...
    - e.g. tests with DDR3
    - 45°C (113°F)
    - retention time for all cells >= 1.5 s

→ cooling RAM increases retention time

What is cold boot?

- Two options for rebooting a machine
  - cold reboot (or cold boot, hard boot)
  - warm reboot (or soft reboot)

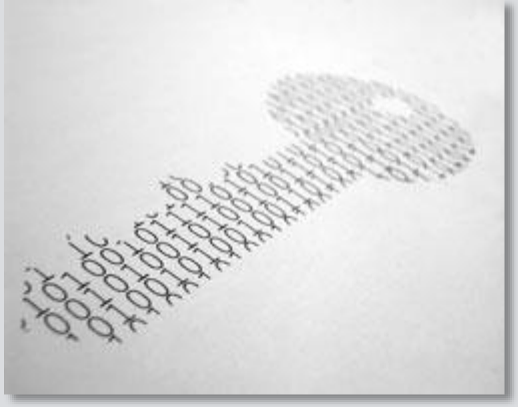
- Warm reboot (simplified)
  - restarting machine while it is powered on
    - e.g. Ctrl-Alt-Del on Windows, kexec on Linux
- Cold boot (simplified)
  - restarting machine from a power-less state
    - disconnecting cord/battery and starting machine again

What is a cold boot attack?

- Basic idea
  - DRAM memory content can be extracted after power has been cut
  - the lower the temperature of the DRAM the higher the probability that memory is unchanged
- Two ways to do it…memory dump can be done
  - on the original machine
    - DRAM stays where it is
    - original machine is cold booted
  - or on a different machine
    - DRAM is removed and plugged into a different computer
    - different computer is cold booted

Why all this?

- Main purpose: recovery of hard disk encryption key
  - Case: You are a digital forensics investigator
    - running machine which uses hard disk encryption
  - Machine not screen-locked: simple
  - Machine is screen-locked (& password unknown)
    - cannot simply copy disk
    - cannot shut down machine (& take out hard disk)
    - decryption key is in RAM:
      but as machine is locked, no way to
      dump image from the machine directly
  - Cold boot attack can help
    - attack provides an image of the RAM
    - might contain errors…
      but still keys can be recovered



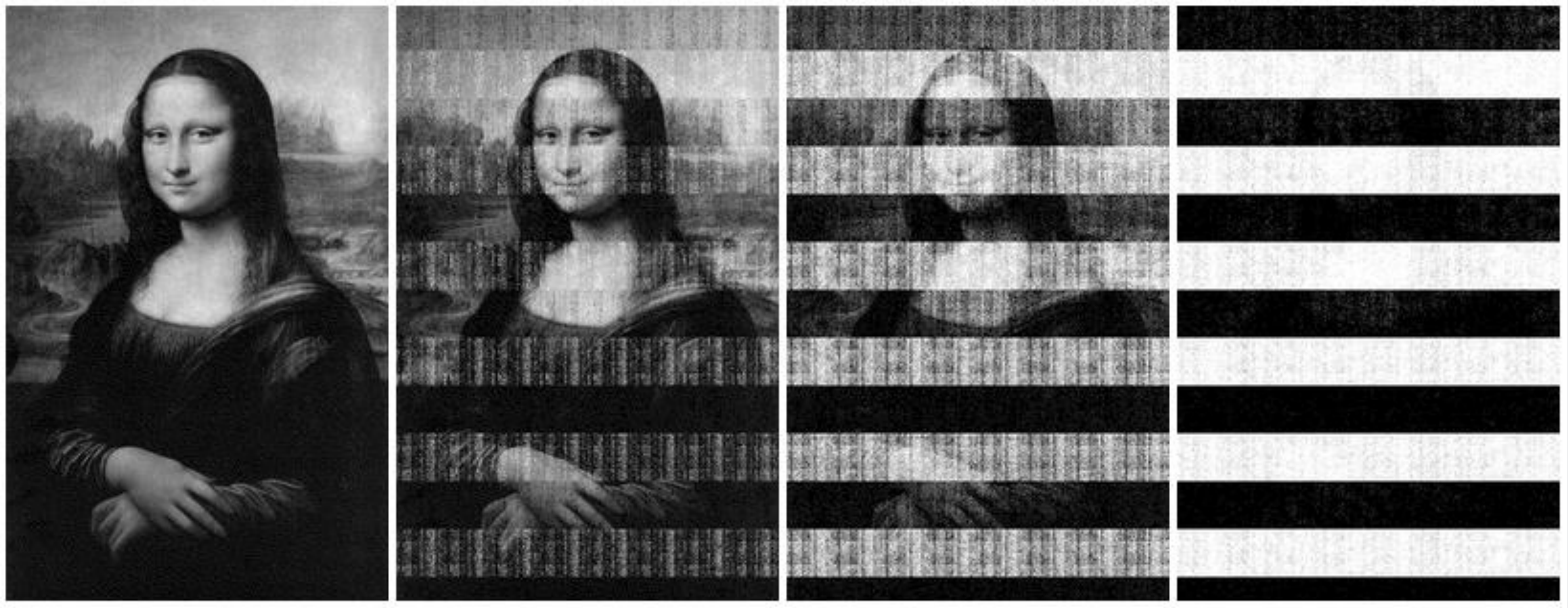
http://www.computerweekly.com/news/2240118660/
IT-departments-risk-losing-responsibity-for-IT-security

Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions

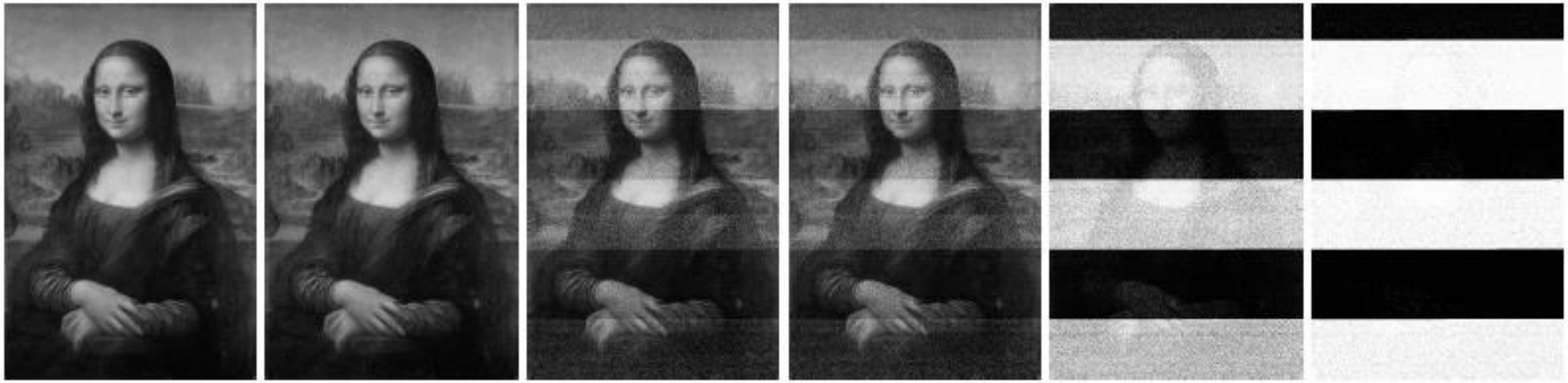
Lest We Remember...

- Halderman et al. published work on Cold Boot Attacks on Encryption Keys at USENIX Security '08
  - DDR and DDR2 SDRAM



On the Practicability of Cold Boot...

- 2013 Gruhn and Müller provide results for different DDR types 1, 2 and 3
  - Result: „we could not reproduce cold boot attacks against modern DDR3 chips“



(a) 0 sec / 100% (b) 2 sec / 99.2% (c) 3 sec / 93.4% (d) 4 sec / 93.1% (e) 5 sec / 61.4% (f) 6 sec / 51.9%

Figure 2: A picture of the Mona Lisa being recovered from system C's RAM at normal operational temperature of 20 to 25 °C after different amounts of time. Each picture's caption includes the percentage of *correct* bits that were recovered.

So, no cold boot attack on DDR3?

- Let‘s try it out...
  - What could be done differently?
  - Obvious... different picture...

Mona ⇨ Lena

http://en.wikipedia.org/wiki/Lenna

So, no cold boot attack on DDR3?

- Let‘s try it out...
  - What could be done differently?
  - Obvious... different picture...

    Mona ⇨ Lena
  - Ok, maybe something else...

    Mainboard
- But first a step back...

http://www.aliexpress.com/item-img/For-ASUS-60-N3GMB1800-B02-Laptop-motherboard-mainboard-K53SV-REV-3-0-45-days-warranty-works/1866829087.html#

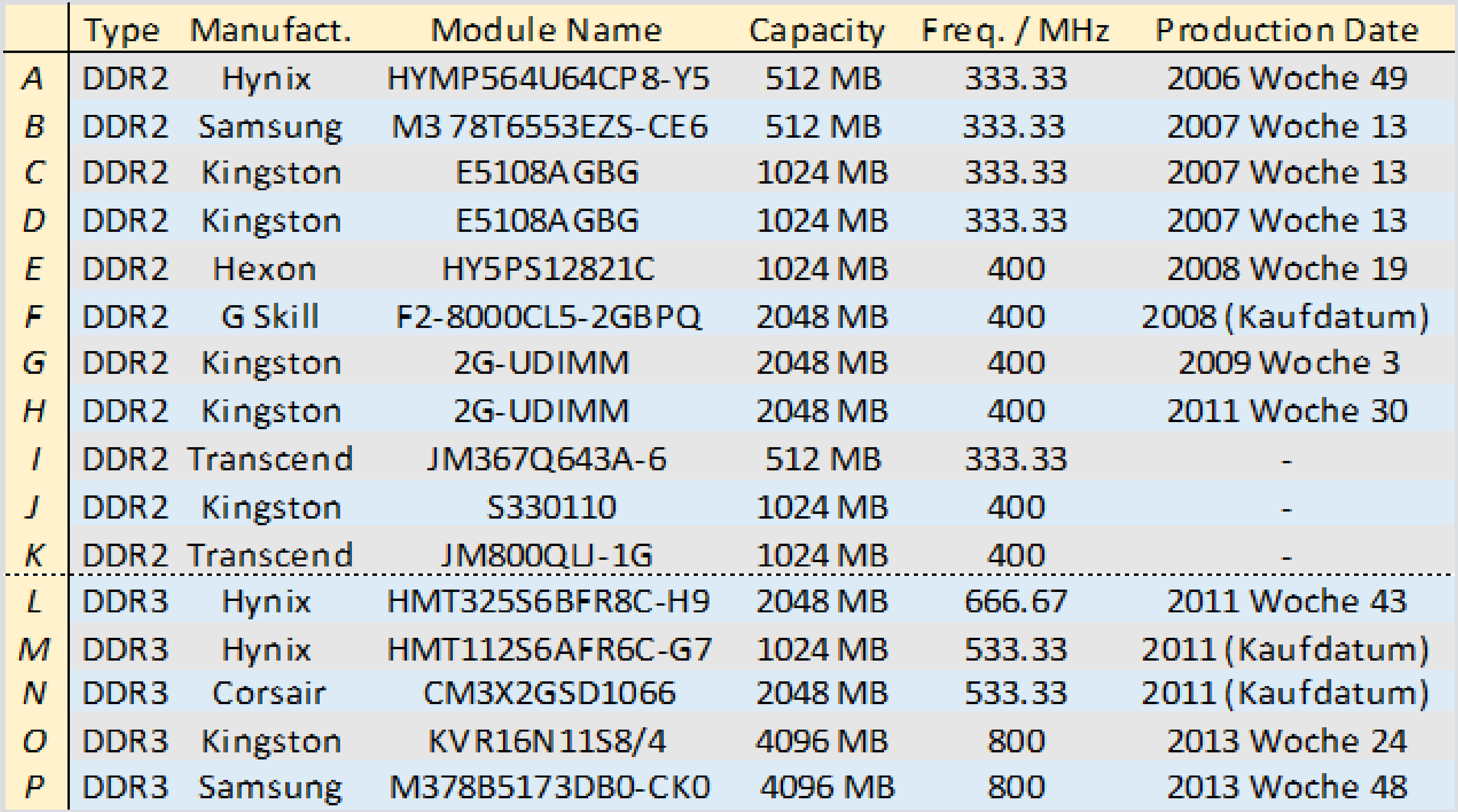
Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions

Considerations

- Cold boot attack results depend on
  - DRAM types ⇨ DDR2 and DDR3
  - DRAM manufacturer ⇨ 7 different manufacturers
  - individual DRAM ⇨ 16 different ones tested

Module Overview

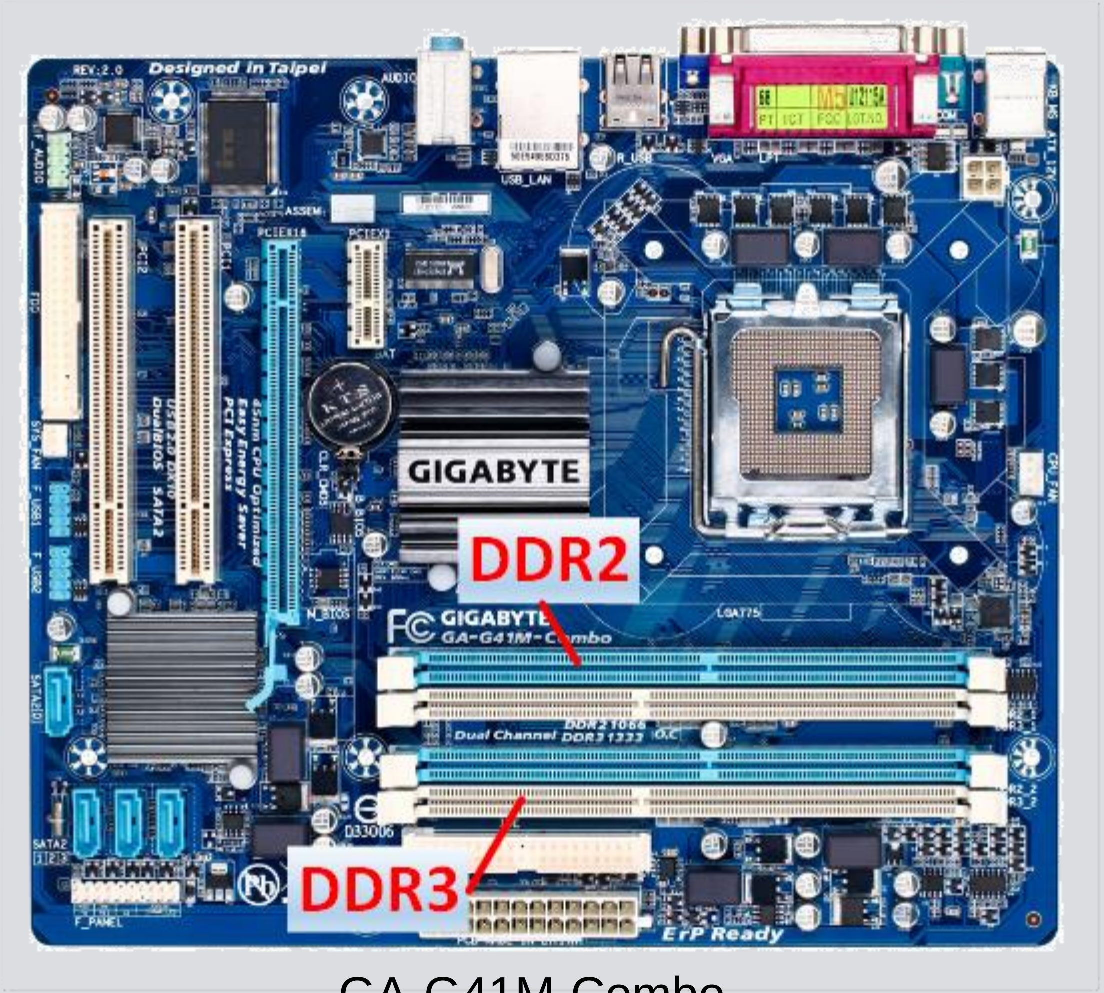


	Type	Manufact.	Module Name	Capacity	Freq. / MHz	Production Date
A	DDR2	Hynix	HYMP564U64CP8-Y5	512 MB	333.33	2006 Woche 49
B	DDR2	Samsung	M378T6553EZS-CE6	512 MB	333.33	2007 Woche 13
C	DDR2	Kingston	E5108AGBG	1024 MB	333.33	2007 Woche 13
D	DDR2	Kingston	E5108AGBG	1024 MB	333.33	2007 Woche 13
E	DDR2	Hexon	HY5PS12821C	1024 MB	400	2008 Woche 19
F	DDR2	G Skill	F2-8000CL5-2GBPQ	2048 MB	400	2008 (Kaufdatum)
G	DDR2	Kingston	2G-UDIMM	2048 MB	400	2009 Woche 3
H	DDR2	Kingston	2G-UDIMM	2048 MB	400	2011 Woche 30
I	DDR2	Transcend	JM367Q643A-6	512 MB	333.33	-
J	DDR2	Kingston	S330110	1024 MB	400	-
K	DDR2	Transcend	JM800QU-1G	1024 MB	400	-
L	DDR3	Hynix	HMT325S6BFR8C-H9	2048 MB	666.67	2011 Woche 43
M	DDR3	Hynix	HMT112S6AFR6C-G7	1024 MB	533.33	2011 (Kaufdatum)
N	DDR3	Corsair	CM3X2GSD1066	2048 MB	533.33	2011 (Kaufdatum)
O	DDR3	Kingston	KVR16N11S8/4	4096 MB	800	2013 Woche 24
P	DDR3	Samsung	M378B5173DB0-CK0	4096 MB	800	2013 Woche 48

Considerations

- Cold boot attack results depend on
  - DRAM types ⇨ DDR2 and DDR3
  - DRAM manufacturer ⇨ 7 different manufacturers
  - individual DRAM ⇨ 16 different ones tested
  - mainboard ⇨ 2 different ones

Mainboards used



GA-G41M-Combo

Notebook ASUS P53E mainboard

Considerations

- Cold boot attack results depend on
  - DRAM types ⇨ DDR2 and DDR3
  - DRAM manufacturer ⇨ 7 different manufacturers
  - individual DRAM ⇨ 16 different ones tested
  - mainboard ⇨ 2 different ones
  - Multi Channel Mode? ⇨ if yes, several impacts
  - DRAM temperature ⇨ tested different ones
  - DRAM seconds w/o power ⇨ tested different ones
  - footprint of cold boot OS ⇨ the smaller the better

Procedure

- Steps of cold boot attack
  - original machine: prepare it with test data (Lena + x)
  - cold boot machine: prepare boot USB stick & connect it
  - original machine (running): adjust DRAM temperature (e.g. cool it to increase retention time)
  - original machine: power it down
    - unplug power cable
      (notebook: battery to be removed before)
  - `if` original ≠ cold boot machine `then` move DRAM
  - cold boot machine: power-on (booting from USB)
  - program on USB stick reads and stores RAM data
  - analyse RAM data (offline)

Procedure

- Cold boot attack procedure
  - prepare … l boot machine
  - prepare … na)
  - cool DR… (to incre…
  - power d…
    - remov…
    - unplu…
  - if origina… M
  - power-o… USB)
  - program on USB stick reads and stores RAM data
  - analyse RAM data (offline)

Cold boot attack

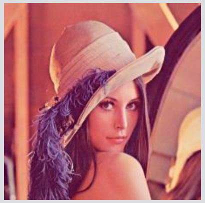
1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

Cold boot attack

1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

Prepare Test Data

- Task: same data in memory for each test
  - used small OS based on JamesM's kernel development tutorials (multiboot kernel) and GRUB bootloader
  - test data based on Lena image (X PixMap)
  - pixel area extracted and written to RAM (starting at fixed address)
  - additionally: 100 MB test file (starting at another fixed address)



Cold boot attack

1. prepare USB & data
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

Prepare Cold Boot USB

- Two small footprint OS (~ 2 MB) tested
  - msramdmp (Wesley McGrew; 32 bit OS)
    - used predominantly (single USB stick / multiple tests)
  - bios_memimage (Princeton University, 64 bit OS)
    - for DRAM > 4 GB
- When machine is cold booted from USB
  - both dump the RAM and save it to USB stick
  - msramdmp slightly modified to extract test data only
    - first 500 MB of DRAM
    - faster and sufficient for test data

Cold boot attack

1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

How to cool the DRAM?

- Option 1: move project to a cold location...
- Option 2: more cost efficient
  ⇨ cooling spray

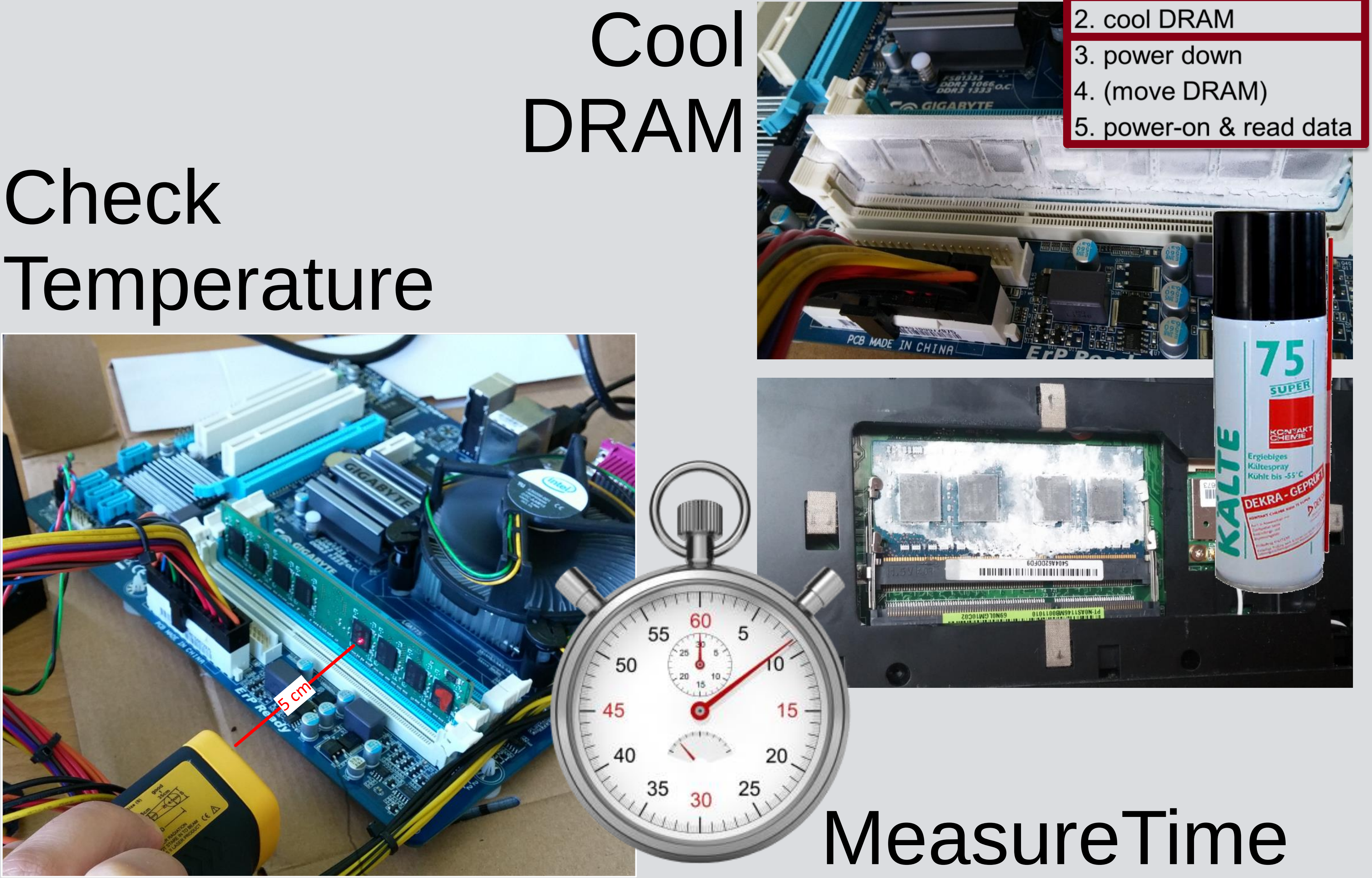
://www.hotel-tenz.com/sport-freizeit/ski-cavalese-alpe-cermis.html

Cold boot attack

1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

Cool DRAM

Check Temperature

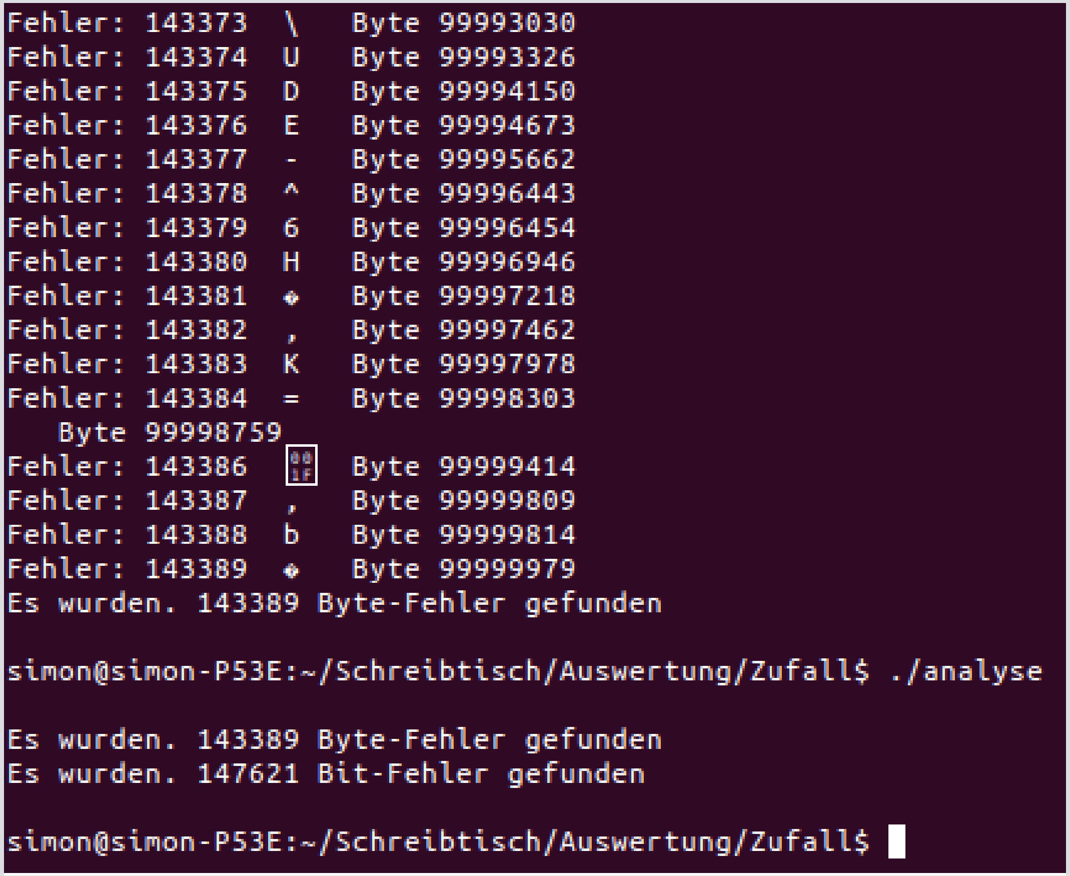


Measure Time

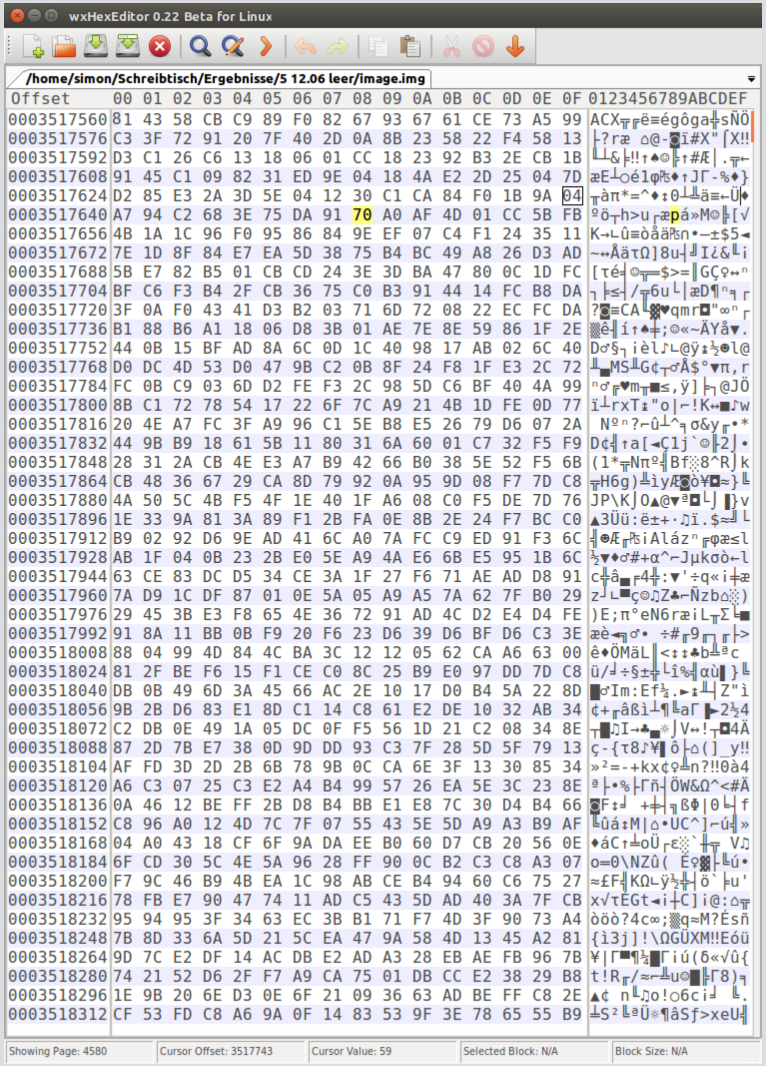
Cold boot attack
1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

Read & Analyse Data

- Determine byte & bit errors



```
Fehler: 143373  \   Byte 99993030
Fehler: 143374  U   Byte 99993326
Fehler: 143375  D   Byte 99994150
Fehler: 143376  E   Byte 99994673
Fehler: 143377  -   Byte 99995662
Fehler: 143378  ^   Byte 99996443
Fehler: 143379  6   Byte 99996454
Fehler: 143380  H   Byte 99996946
Fehler: 143381  ◆   Byte 99997218
Fehler: 143382  ,   Byte 99997462
Fehler: 143383  K   Byte 99997978
Fehler: 143384  =   Byte 99998303
   Byte 99998759
Fehler: 143386  ␟   Byte 99999414
Fehler: 143387  ,   Byte 99999809
Fehler: 143388  b   Byte 99999814
Fehler: 143389  ◆   Byte 99999979
Es wurden. 143389 Byte-Fehler gefunden

simon@simon-P53E:~/Schreibtisch/Auswertung/Zufall$ ./analyse

Es wurden. 143389 Byte-Fehler gefunden
Es wurden. 147621 Bit-Fehler gefunden

simon@simon-P53E:~/Schreibtisch/Auswertung/Zufall$ 
```



wxHexEditor 0.22 Beta for Linux

/home/simon/Schreibtisch/Ergebnisse/5 12.06 leer/image.img

```
Offset     00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F 0123456789ABCDEF
0003517560 81 43 58 CB C9 89 F0 82 67 93 67 61 CE 73 A5 99 ACX╦╔ë≡égôga╬sÑÖ
0003517576 C3 3F 72 91 20 7F 40 2D 0A 8B 23 58 22 F4 58 13 ├?ræ ⌂@-◙ï#X"⌠X‼
0003517592 D3 C1 26 C6 13 18 06 01 CC 18 23 92 B3 2E CB 1B ╙┴&╞‼↑♠☺╠↑#Æ│.╦←
0003517608 91 45 C1 09 82 31 ED 9E 04 18 4A E2 2D 25 04 7D æE┴○é1φ₧♦↑JΓ-%♦}
0003517624 D2 85 E3 2A 3D 5E 04 12 30 C1 CA 84 F0 1B 9A 04 ╥àπ*=^♦↕0┴╩ä≡←Ü♦
0003517640 A7 94 C2 68 3E 75 DA 91 70 A0 AF 4D 01 CC 5B FB ºö┬h>u┌æpá»M☺╠[√
0003517656 4B 1A 1C 96 F0 95 86 84 9E EF 07 C4 F1 24 35 11 K→∟û≡òåä₧∩•─±$5◄
0003517672 7E 1D 8F 84 E7 EA 5D 38 75 B4 BC 49 A8 26 D3 AD ~↔ÅäτΩ]8u┤╝I¿&╙¡
0003517688 5B E7 82 B5 01 CB CD 24 3E 3D BA 47 80 0C 1D FC [τé╡☺╦═$>=║GÇ♀↔ⁿ
0003517704 BF C6 F3 B4 2F CB 36 75 C0 B3 91 44 14 FC B8 DA ┐╞≤┤/╦6u└│æD¶ⁿ╕┌
0003517720 3F 0A F0 43 41 D3 B2 03 71 6D 72 08 22 EC FC DA ?◙≡CA╙▓♥qmr◘"∞ⁿ┌
0003517736 B1 88 B6 A1 18 06 D8 3B 01 AE 7E 8E 59 86 1F 2E ▒ê╢í↑♠╪;☺«~ÄYå▼.
0003517752 44 0B 15 BF AD 8A 6C 0D 1C 40 98 17 AB 02 6C 40 D♂§┐¡èl♪∟@ÿ↨½☻l@
0003517768 D0 DC 4D 53 D0 47 9B C2 0B 8F 24 F8 1F E3 2C 72 ╨▄MS╨G¢┬♂Å$°▼π,r
0003517784 FC 0B C9 03 6D D2 FE F3 2C 98 5D C6 BF 40 4A 99 ⁿ♂╔♥m╥■≤,ÿ]╞┐@JÖ
0003517800 8B C1 72 78 54 17 22 6F 7C A9 21 4B 1D FE 0D 77 ï┴rxT↨"o|⌐!K↔■♪w
0003517816 20 4E A7 FC 3F A9 96 C1 5E B8 E5 26 79 D6 07 2A  Nºⁿ?⌐û┴^╕σ&y╓•*
0003517832 44 9B B9 18 61 5B 11 80 31 6A 60 01 C7 32 F5 F9 D¢╣↑a[◄Ç1j`☺╟2⌡∙
0003517848 28 31 2A CB 4E E3 A7 B9 42 66 B0 38 5E 52 F5 6B (1*╦Nπº╣Bf░8^R⌡k
0003517864 CB 48 36 67 29 CA 8D 79 92 0A 95 9D 08 F7 7D C8 ╦H6g)╩ìyÆ◙ò¥◘≈}╚
0003517880 4A 50 5C 4B F5 4F 1E 40 1F A6 08 C0 F5 DE 7D 76 JP\K⌡O▲@▼ª◘└⌡▐}v
0003517896 1E 33 9A 81 3A 89 F1 2B FA 0E 8B 2E 24 F7 BC C0 ▲3Üü:ë±+·♫ï.$≈╝└
0003517912 B9 02 92 D6 9E AD 41 6C A0 7A FC C9 ED 91 F3 6C ╣☻Æ╓₧¡Alázⁿ╔φæ≤l
0003517928 AB 1F 04 0B 23 2B E0 5E A9 4A E6 6B E5 95 1B 6C ½▼♦♂#+α^⌐Jµkσò←l
0003517944 63 CE 83 DC D5 34 CE 3A 1F 27 F6 71 AE AD D8 91 c╬â▄╒4╬:▼'÷q«¡╪æ
0003517960 7A D9 1C DF 87 01 0E 5A 05 A9 A5 7A 62 7F B0 29 z┘∟▀ç☺♫Z♣⌐Ñzb⌂░)
0003517976 29 45 3B E3 F8 65 4E 36 72 91 AD 4C D2 E4 D4 FE )E;π°eN6ræ¡L╥Σ╘■
0003517992 91 8A 11 BB 0B F9 20 F6 23 D6 39 D6 BF D6 C3 3E æè◄╗♂∙ ÷#╓9╓┐╓├>
0003518008 88 04 99 4D 84 4C BA 3C 12 12 05 62 CA A6 63 00 ê♦ÖMäL║<↕↕♣b╩ªc 
0003518024 81 2F BE F6 15 F1 CE C0 8C 25 B9 E0 97 DD 7D C8 ü/╛÷§±╬└î%╣αù▌}╚
0003518040 DB 0B 49 6D 3A 45 66 AC 2E 10 17 D0 B4 5A 22 8D █♂Im:Ef¼.►↨╨┤Z"ì
0003518056 9B 2B D6 83 E1 8D C1 14 C8 61 E2 DE 10 32 AB 34 ¢+╓âßì┴¶╚aΓ▐►2½4
0003518072 C2 DB 0E 49 1A 05 DC 0F F5 56 1D 21 C2 08 34 8E ┬█♫I→♣▄☼⌡V↔!┬◘4Ä
0003518088 87 2D 7B E7 38 0D 9D DD 93 C3 7F 28 5D 5F 79 13 ç-{τ8♪¥▌ô├⌂(]_y‼
0003518104 AF FD 3D 2D 2B 6B 78 9B 0C CA 6E 3F 13 30 85 34 »²=-+kx¢♀╩n?‼0à4
0003518120 A6 C3 07 25 C3 E2 A4 B4 99 57 26 EA 5E 3C 23 8E ª├•%├Γñ┤ÖW&Ω^<#Ä
0003518136 0A 46 12 BE FF 2B D8 B4 BB E1 E8 7C 30 D4 B4 66 ◙F↕╛ +╪┤╗ßΦ|0╘┤f
0003518152 C8 96 A0 12 4D 7C 7F 07 55 43 5E 5D A9 A3 B9 AF ╚ûá↕M|⌂•UC^]⌐ú╣»
0003518168 04 A0 43 18 CF 6F 9A DA EE B0 60 D7 CB 20 56 0E ♦áC↑╧oÜ┌ε░`╫╦ V♫
0003518184 6F CD 30 5C 4E 5A 96 28 FF 90 0C B2 C3 C8 A3 07 o═0\NZû( É♀▓├╚ú•
0003518200 F7 9C 46 B9 4B EA 1C 98 AB CE B4 94 60 C6 75 27 ≈£F╣KΩ∟ÿ½╬┤ö`╞u'
0003518216 78 FB E7 90 47 74 11 AD C5 43 5D AD 40 3A 7F CB x√τÉGt◄¡┼C]¡@:⌂╦
0003518232 95 94 95 3F 34 63 EC 3B B1 71 F7 4D 3F 90 73 A4 òöò?4c∞;▒q≈M?Ésñ
0003518248 7B 8D 33 6A 5D 21 5C EA 47 9A 58 4D 13 45 A2 81 {ì3j]!\ΩGÜXM‼Eóü
0003518264 9D 7C E2 DF 14 AC DB E2 AD A3 28 EB AE FB 96 7B ¥|Γ▀¶¼█Γ¡ú(δ«√û{
0003518280 74 21 52 D6 2F F7 A9 CA 75 01 DB CC E2 38 29 B8 t!R╓/≈⌐╩u☺█╠Γ8)╕
0003518296 1E 9B 20 6E D3 0E 6F 21 09 36 63 AD BE FF C8 2E ▲¢ n╙♫o!○6c¡╛ ╚.
0003518312 CF 53 FD C8 A6 9A 0F 14 83 53 9F 3E 78 65 55 B9 ╧S²╚ªÜ☼¶âSƒ>xeU╣
```

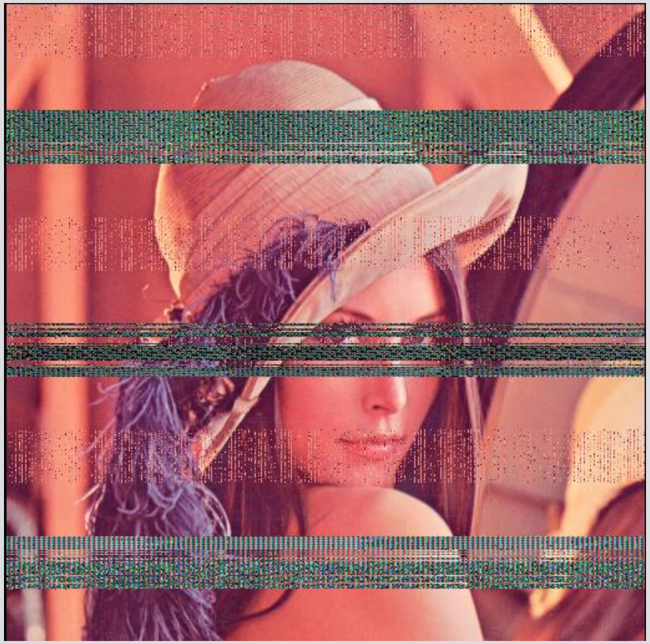
Showing Page: 4580 | Cursor Offset: 3517743 | Cursor Value: 59 | Selected Block: N/A | Block Size: N/A

Cold boot attack

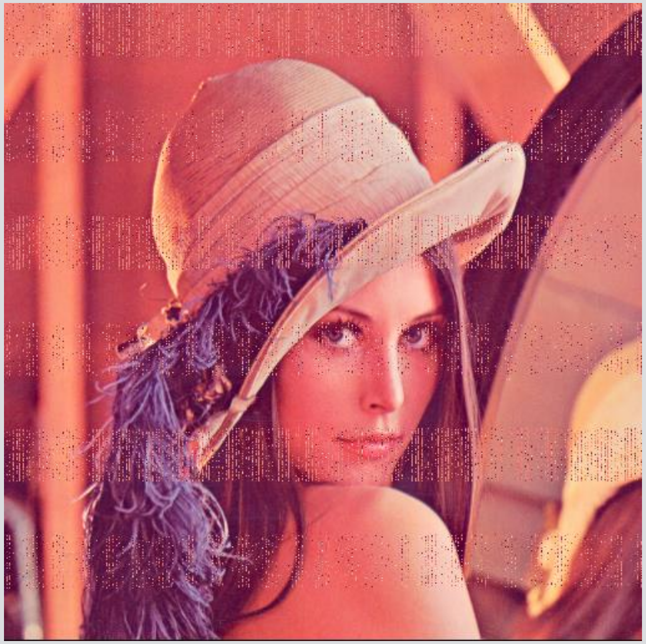
1. prepare data & USB
2. cool DRAM
3. power down
4. (move DRAM)
5. power-on & read data

Read & Analyse Data

- Determine byte & bit errors
- Reconstruct & view image

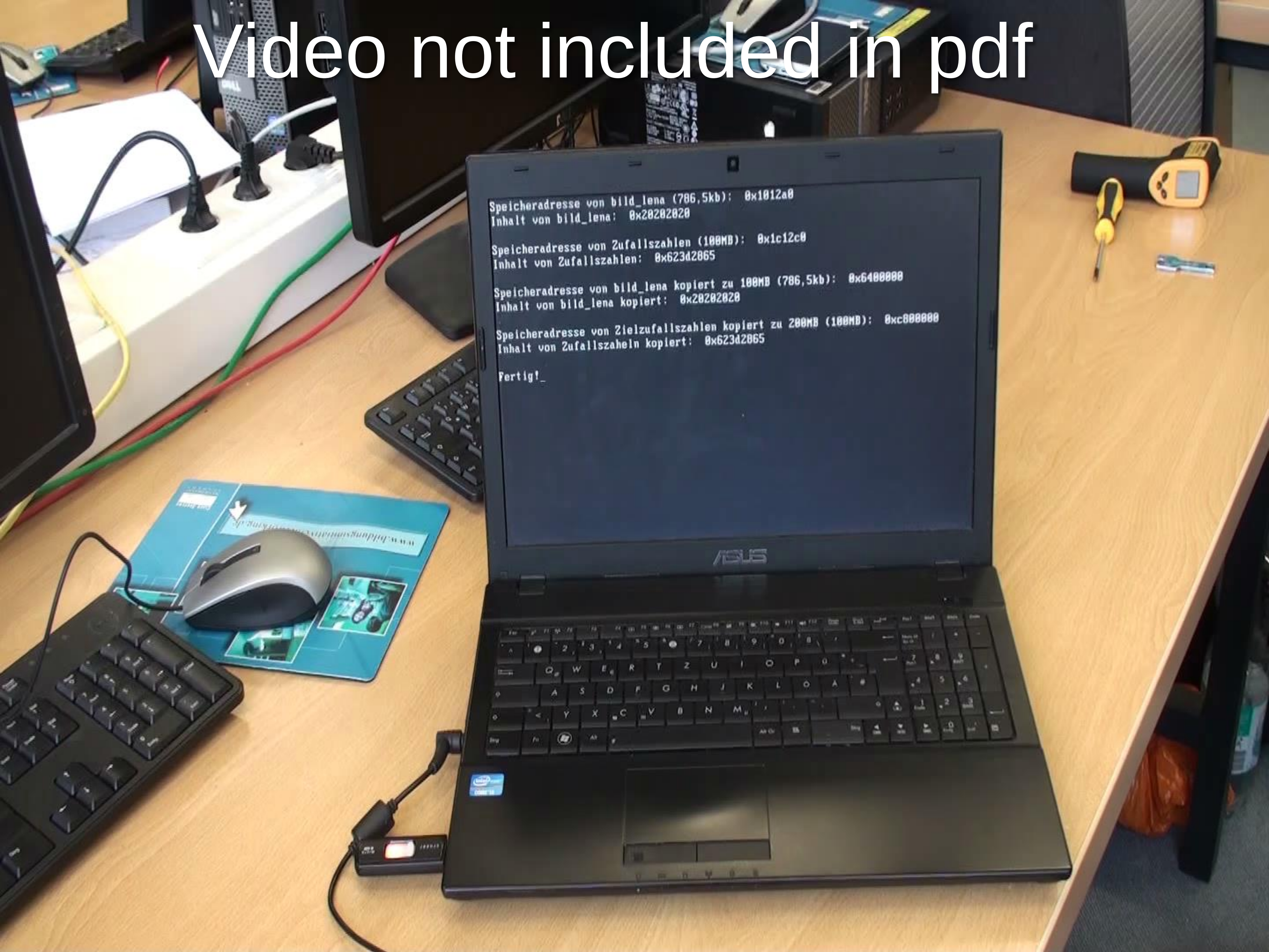


a) bit errors that change byte to quote character or null byte damage whole line



b) correction of quote characters and null bytes by one bit reduce this to pixel errors

Video not included in pdf

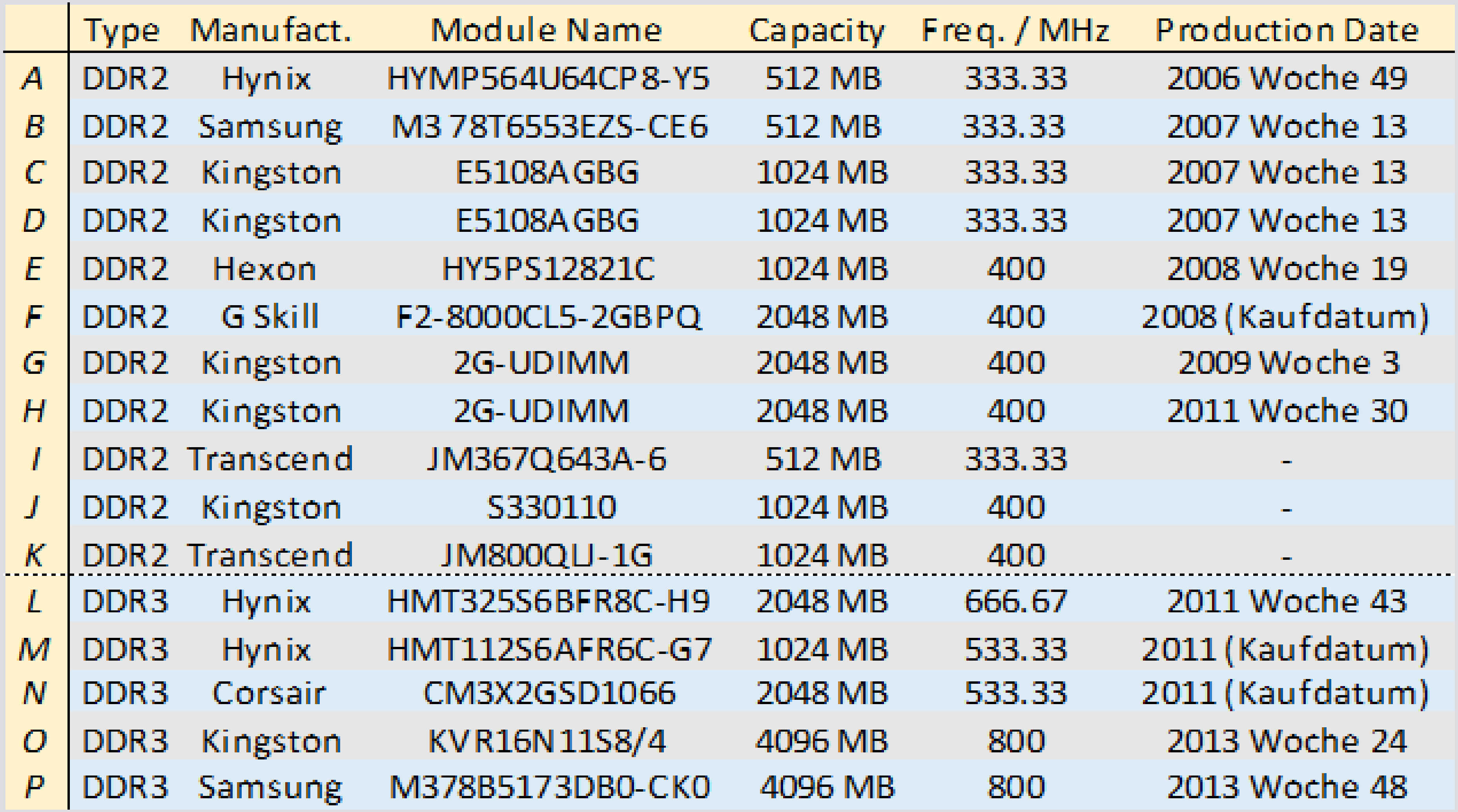


```
Speicheradresse von bild_lena (786,5kb):  0x1012a0
Inhalt von bild_lena:  0x20202020

Speicheradresse von Zufallszahlen (100MB):  0x1c12c0
Inhalt von Zufallszahlen:  0x623d2865

Speicheradresse von bild_lena kopiert zu 100MB (786,5kb):  0x6400000
Inhalt von bild_lena kopiert:  0x20202020

Speicheradresse von Zielzufallszahlen kopiert zu 200MB (100MB):  0xc800000
Inhalt von Zufallszaheln kopiert:  0x623d2865

Fertig!_
```

Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions

Module Overview



	Type	Manufact.	Module Name	Capacity	Freq. / MHz	Production Date
A	DDR2	Hynix	HYMP564U64CP8-Y5	512 MB	333.33	2006 Woche 49
B	DDR2	Samsung	M3 78T6553EZS-CE6	512 MB	333.33	2007 Woche 13
C	DDR2	Kingston	E5108AGBG	1024 MB	333.33	2007 Woche 13
D	DDR2	Kingston	E5108AGBG	1024 MB	333.33	2007 Woche 13
E	DDR2	Hexon	HY5PS12821C	1024 MB	400	2008 Woche 19
F	DDR2	G Skill	F2-8000CL5-2GBPQ	2048 MB	400	2008 (Kaufdatum)
G	DDR2	Kingston	2G-UDIMM	2048 MB	400	2009 Woche 3
H	DDR2	Kingston	2G-UDIMM	2048 MB	400	2011 Woche 30
I	DDR2	Transcend	JM367Q643A-6	512 MB	333.33	-
J	DDR2	Kingston	S330110	1024 MB	400	-
K	DDR2	Transcend	JM800QU-1G	1024 MB	400	-
L	DDR3	Hynix	HMT325S6BFR8C-H9	2048 MB	666.67	2011 Woche 43
M	DDR3	Hynix	HMT112S6AFR6C-G7	1024 MB	533.33	2011 (Kaufdatum)
N	DDR3	Corsair	CM3X2GSD1066	2048 MB	533.33	2011 (Kaufdatum)
O	DDR3	Kingston	KVR16N11S8/4	4096 MB	800	2013 Woche 24
P	DDR3	Samsung	M378B5173DB0-CK0	4096 MB	800	2013 Woche 48

Selected Results DDR2

10s without power at -35°C to -30°C

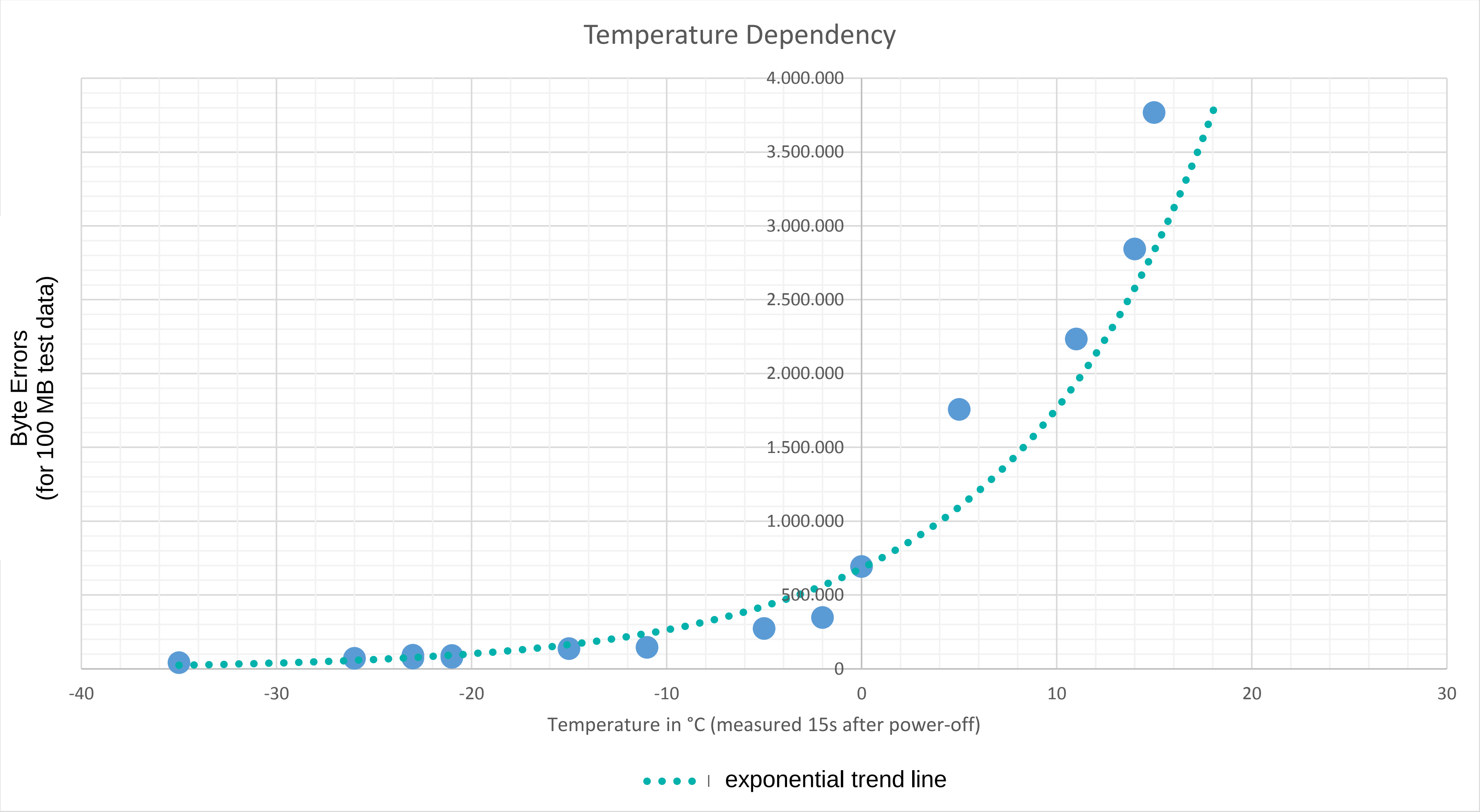
DDR2	RAM	Byte Errors	Bit Errors	Byte Error Rate	Bit Error Rate
1	B	236	236	0,000236%	0,000030%
2	F	2.204	2.212	0,002204%	0,000277%
3	G	3.675	3.943	0,003675%	0,000493%
4	C	82.539	85.766	0,0825%	0,0107%
5	H	239.263	558.522	0,239%	0,070%
6	D	729.380	795.702	0,729%	0,099%
7	J	2.248.293	2.477.976	2,248%	0,310%
8	I	4.763.617	7.862.582	4,764%	0,983%
9	A	12.870.663	28.379.907	12,87%	3,55%
10	E	20.997.916	71.909.648	21,00%	8,99%
11	K	35.475.736	88.992.338	35,48%	11,12%

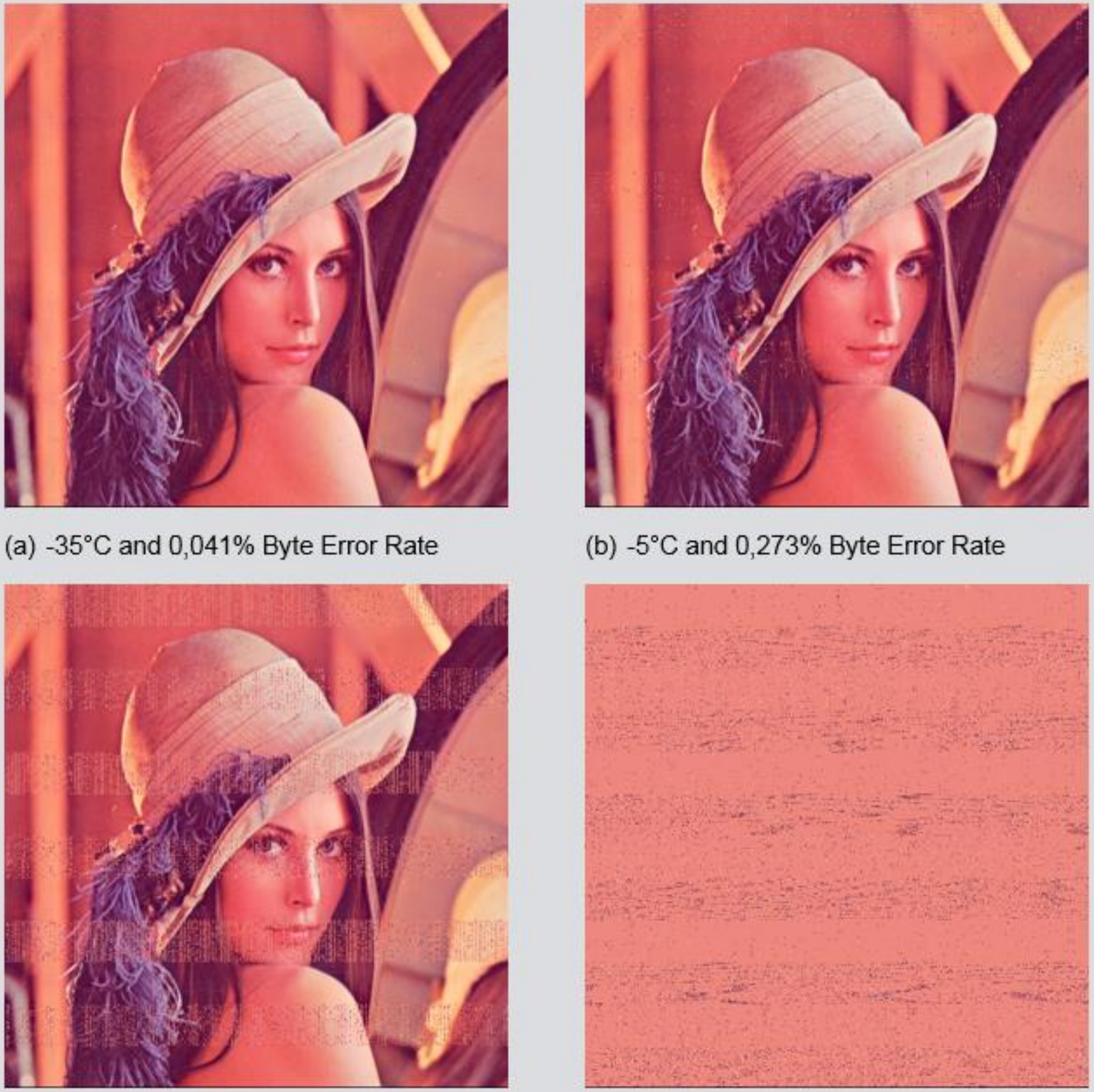
Selected Results DDR3

10s without power at -35°C to -30°C

DDR3	RAM	Byte Errors	Bit Errors	Byte Error Rate	Bit Error Rate
1	N	1.604	5.624	0,001604%	0,000703%
2	M	4.435	8.275	0,004435%	0,001034%
3	L	460.860	534.566	0,461%	0,067%

Error – Temperature Dependency





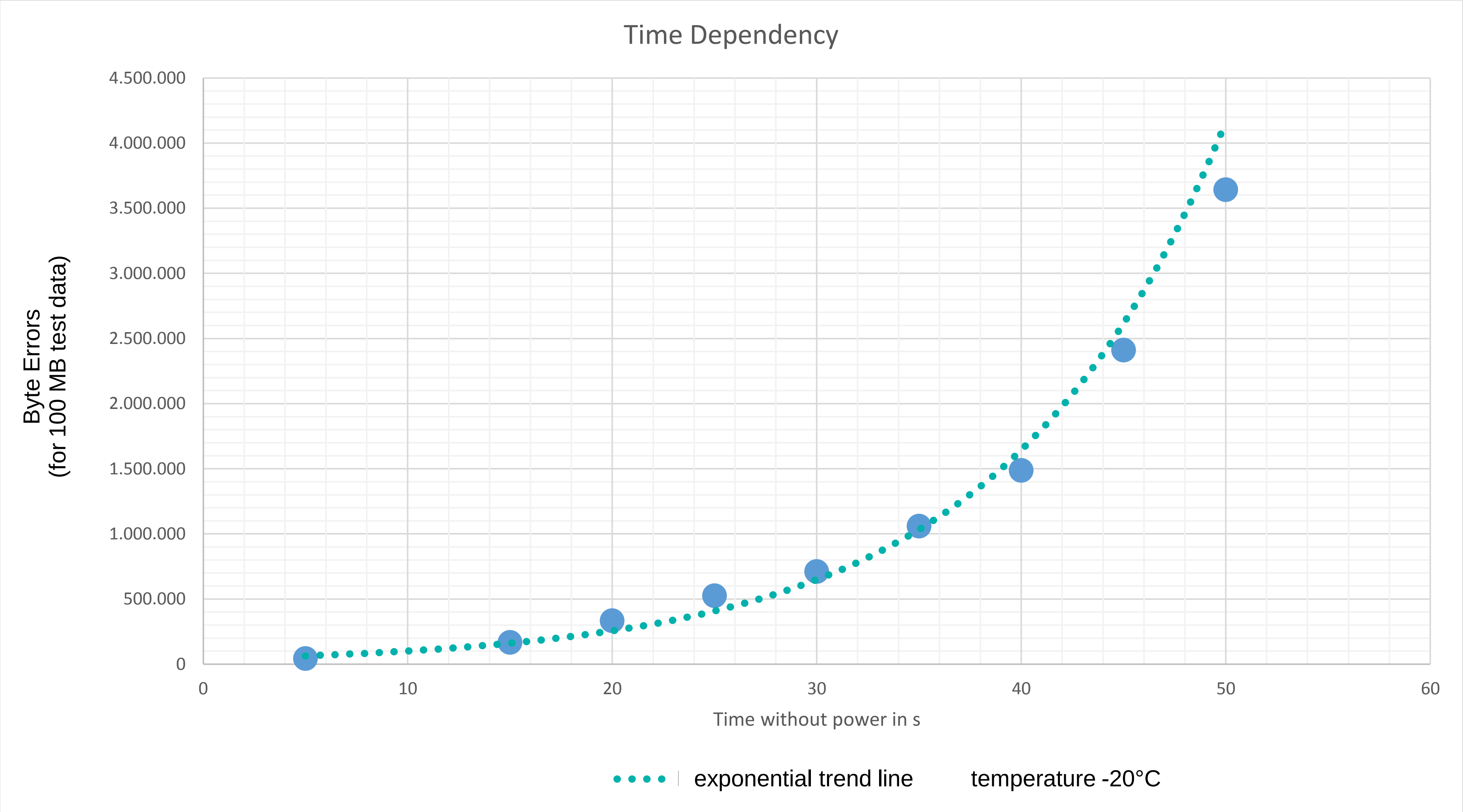
(a) -35°C and 0,041% Byte Error Rate

(b) -5°C and 0,273% Byte Error Rate

(c) +15°C and 1,756% Byte Error Rate

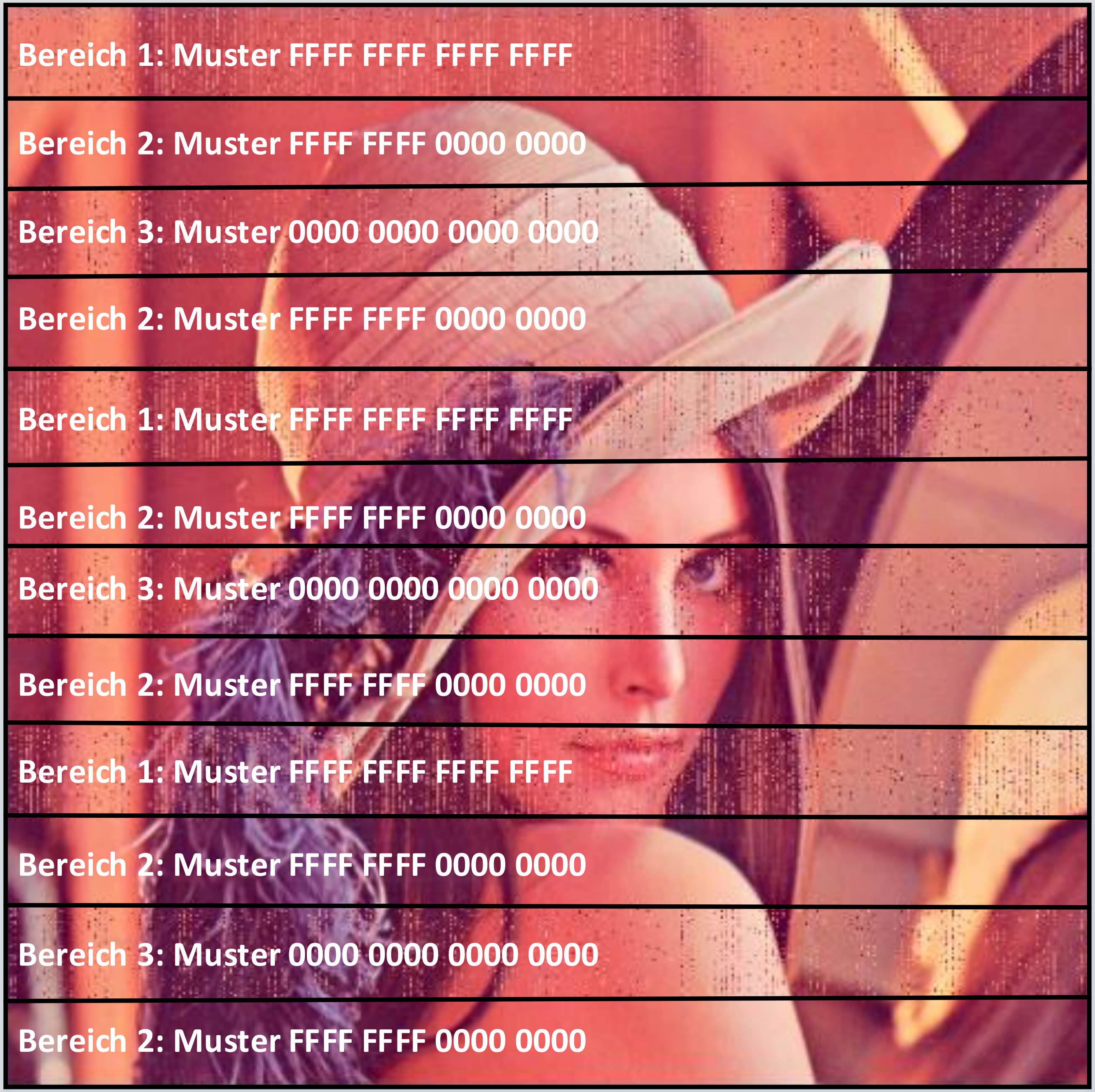
(d) +30°C and 34,284% Byte Error Rate

Error - Time Dependency



Error Patterns

- some DRAM show different error rates depending on ground state
- some areas error free
- reason not clear yet


Bereich 1: Muster FFFF FFFF FFFF FFFF
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 3: Muster 0000 0000 0000 0000
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 1: Muster FFFF FFFF FFFF FFFF
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 3: Muster 0000 0000 0000 0000
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 1: Muster FFFF FFFF FFFF FFFF
Bereich 2: Muster FFFF FFFF 0000 0000
Bereich 3: Muster 0000 0000 0000 0000
Bereich 2: Muster FFFF FFFF 0000 0000

Anti Cold Boot

- Enable POST in BIOS
  - overwrites complete RAM
- Password-protect boot device sequence
  - avoid booting of RAM dump software
- Password based pre-boot authentication
  - otherwise encryption key in RAM after restart
- Store encryption key outside RAM
  - e.g. possible in CPU registers
  - this even works if RAM is moved to different machine

Agenda

- What is a cold boot attack?
- Previous work by others
- Experiments
- Results
- Conclusions

Conclusions

- Cold boot attacks not as complicated as expected☺
  - could be feasible approach for digital forensics investigators

- Attacks on DDR3 are possible
  - admittedly, we have been lucky with the board…

Thank You

Marko Schuba

Aachen University of Applied Sciences
Germany

schuba@fh-aachen.de