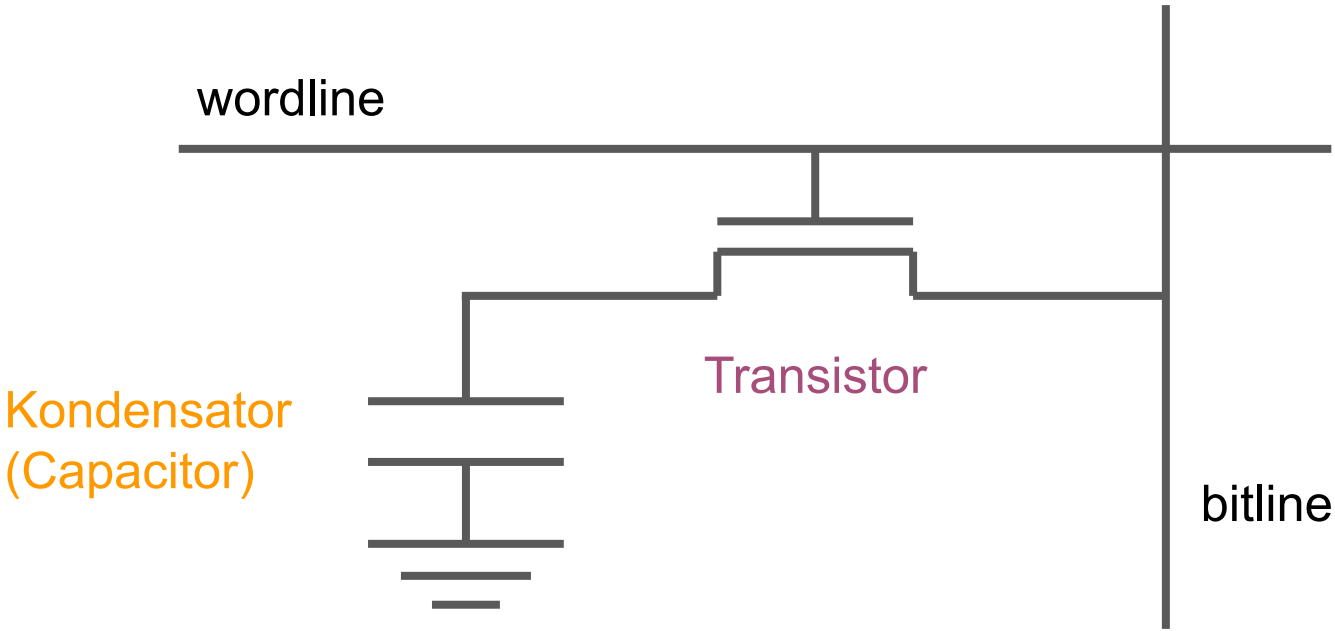
Rowhammer

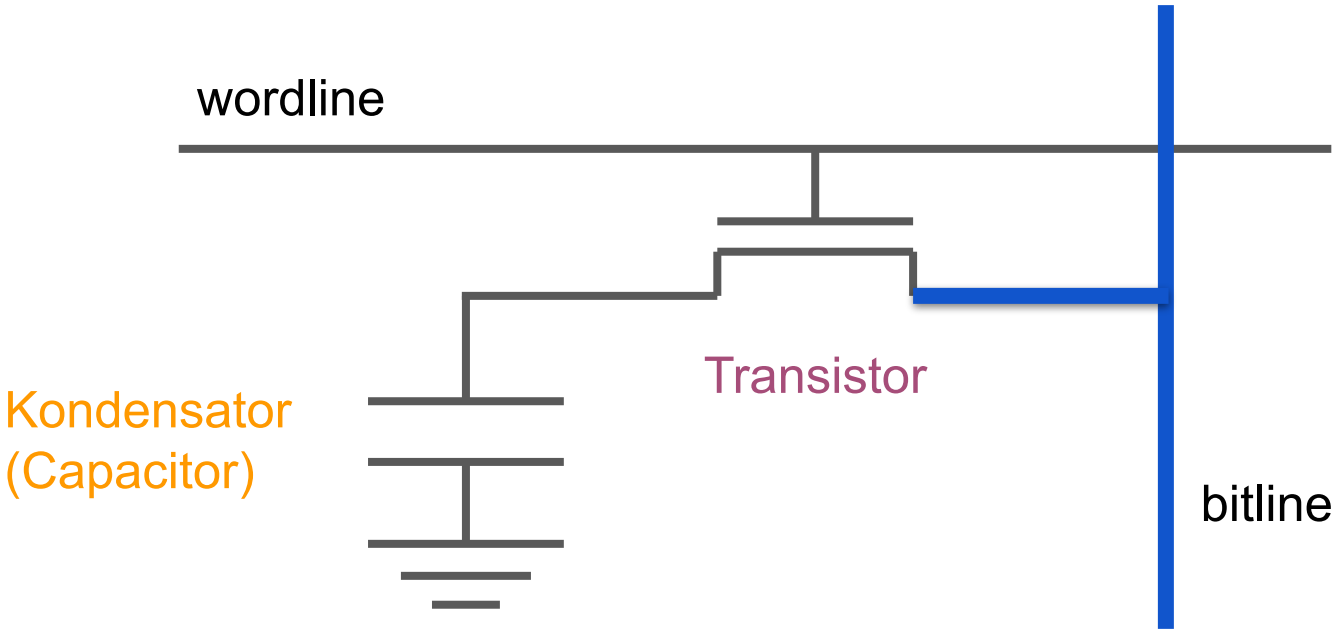
Problem ohne Lösung

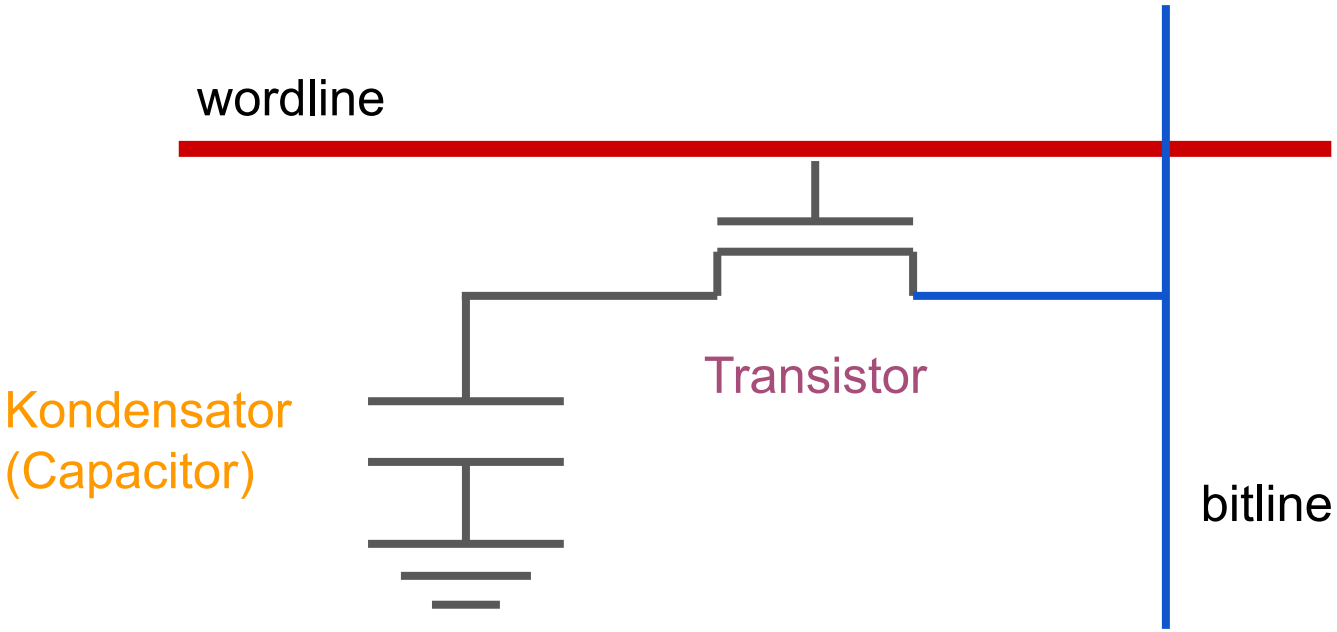
Überblick

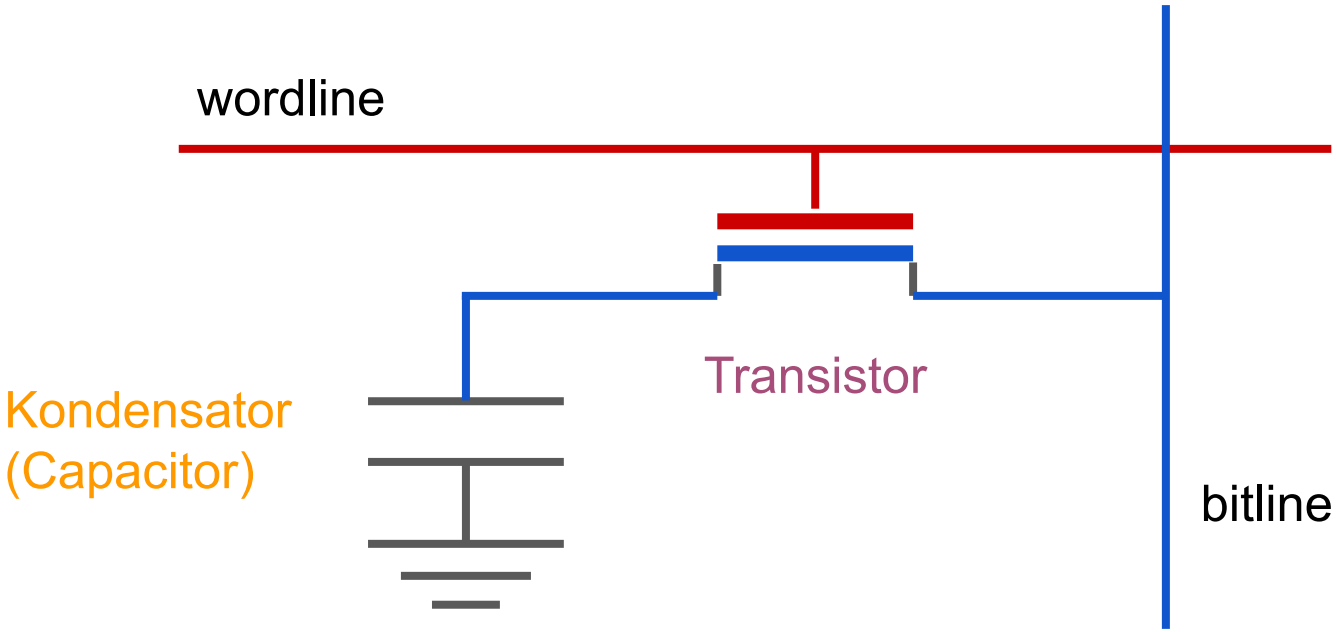
1. Theorie
2. Angriff auf Linux Kernel
3. Rowhammer in der Realität
4. Schutz gegen Rowhammer

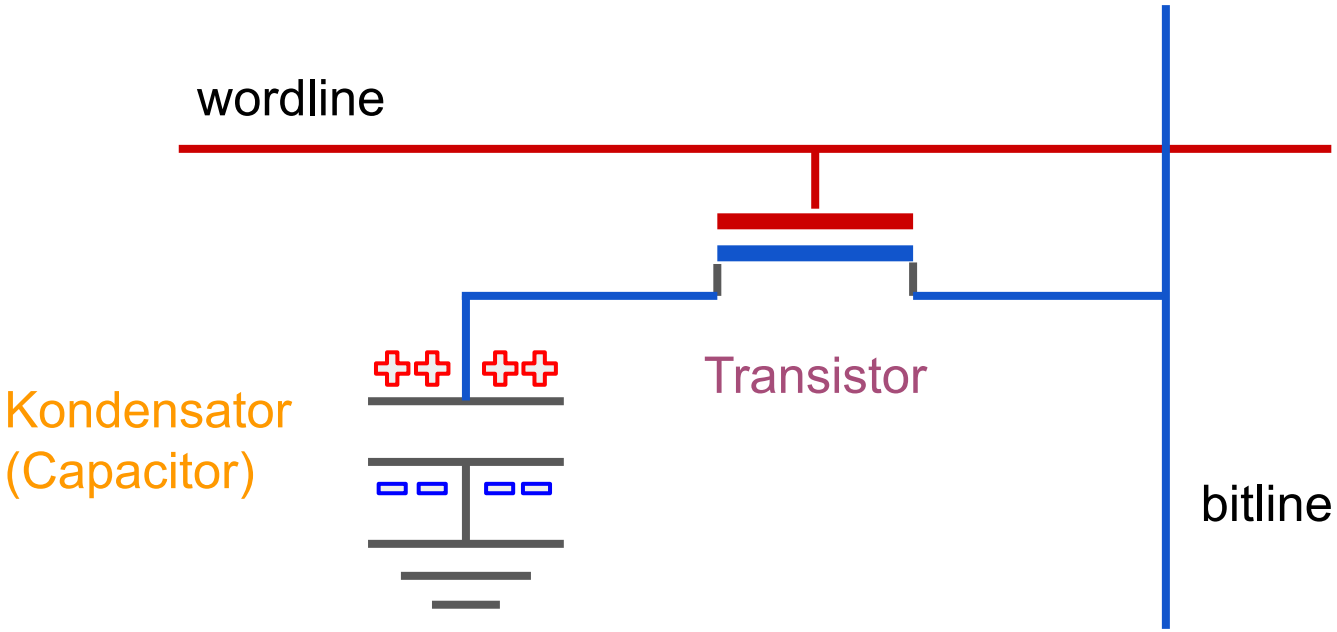
DRAM-BIT

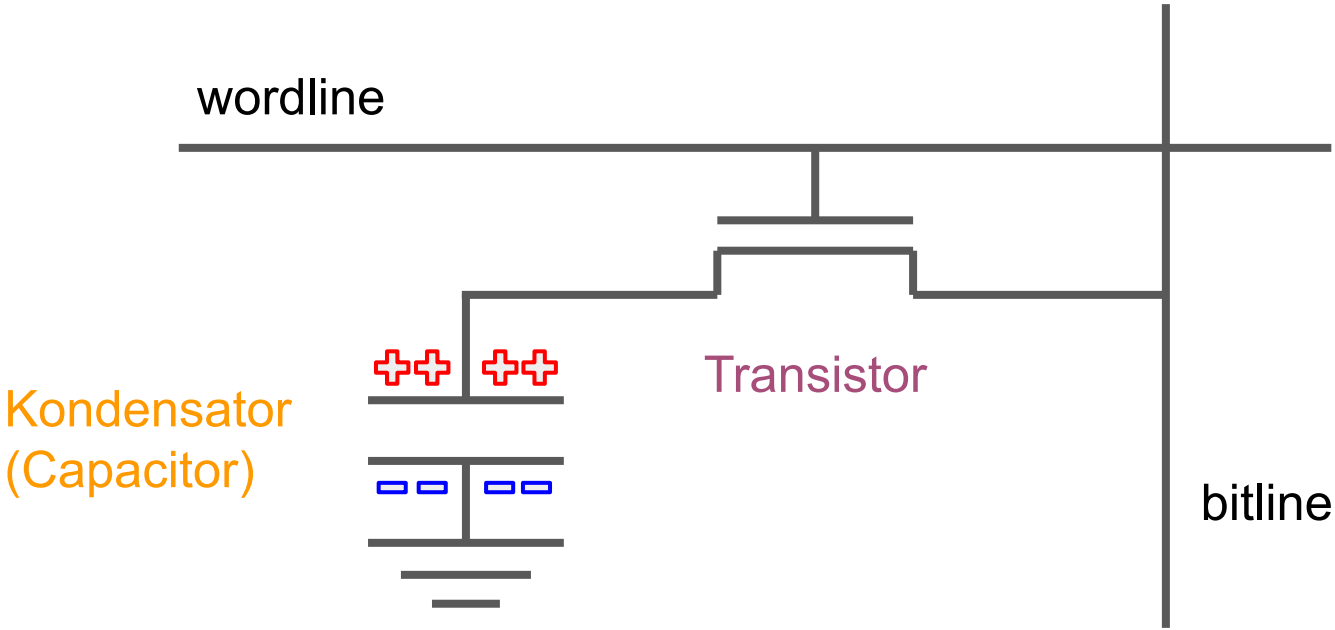



wordline
Transistor
Kondensator
(Capacitor)
bitline

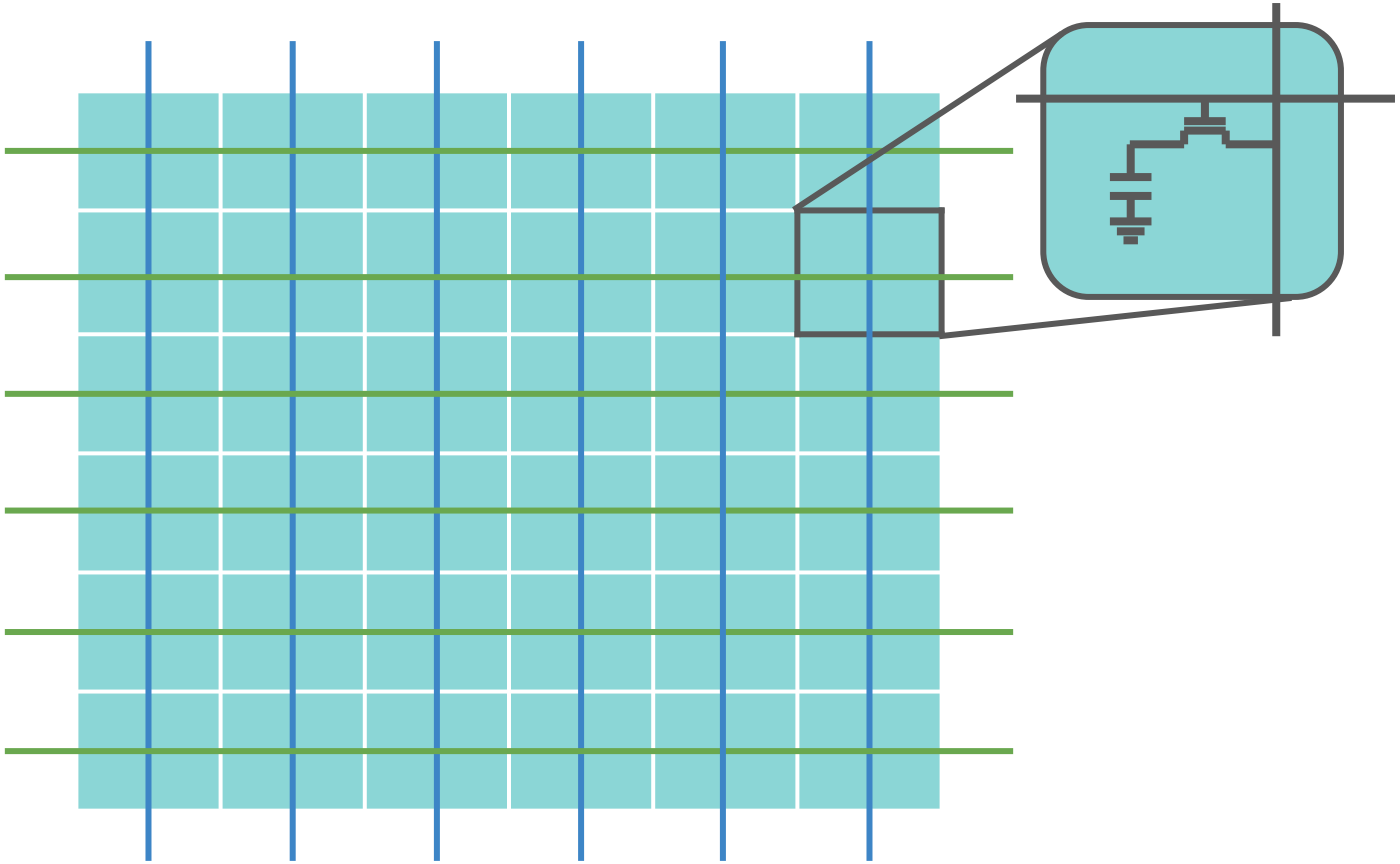

wordline
Transistor
Kondensator
(Capacitor)
bitline

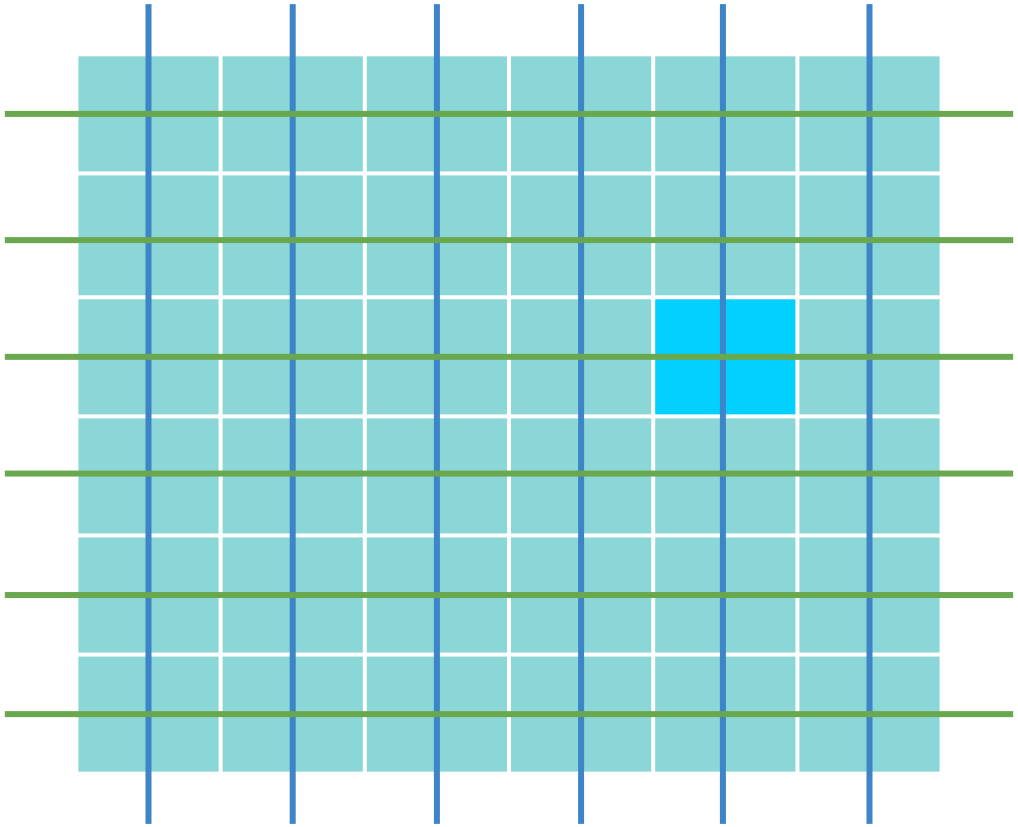

wordline
Transistor
Kondensator
(Capacitor)
bitline

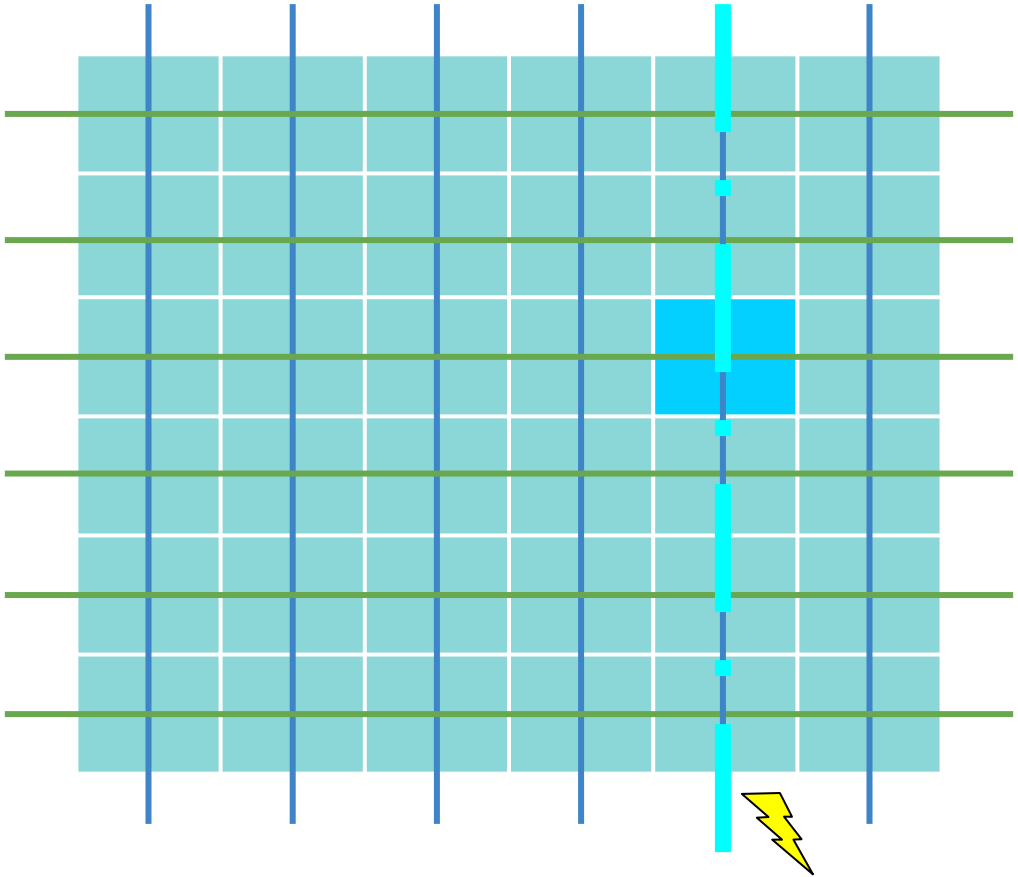

wordline
Transistor
Kondensator
(Capacitor)
bitline

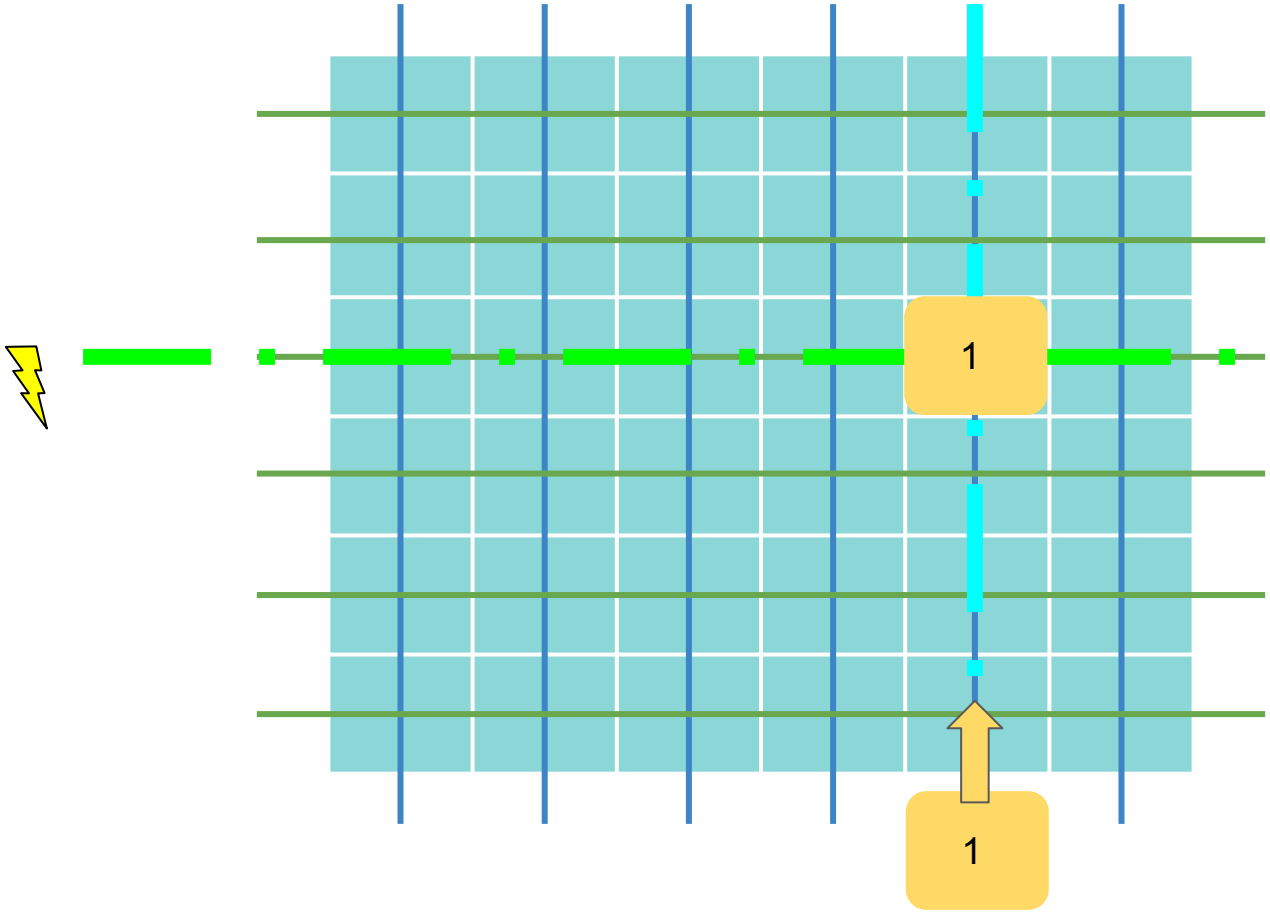

wordline
Transistor
Kondensator
(Capacitor)
bitline

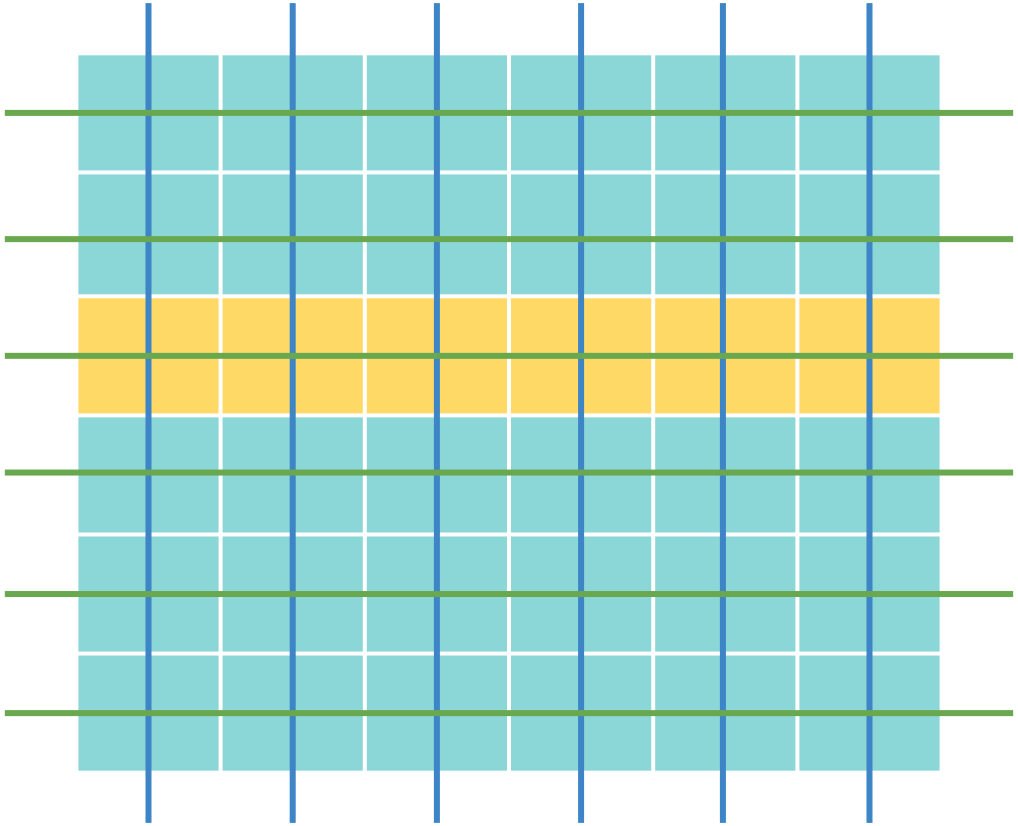
DRAM-
MATRIX

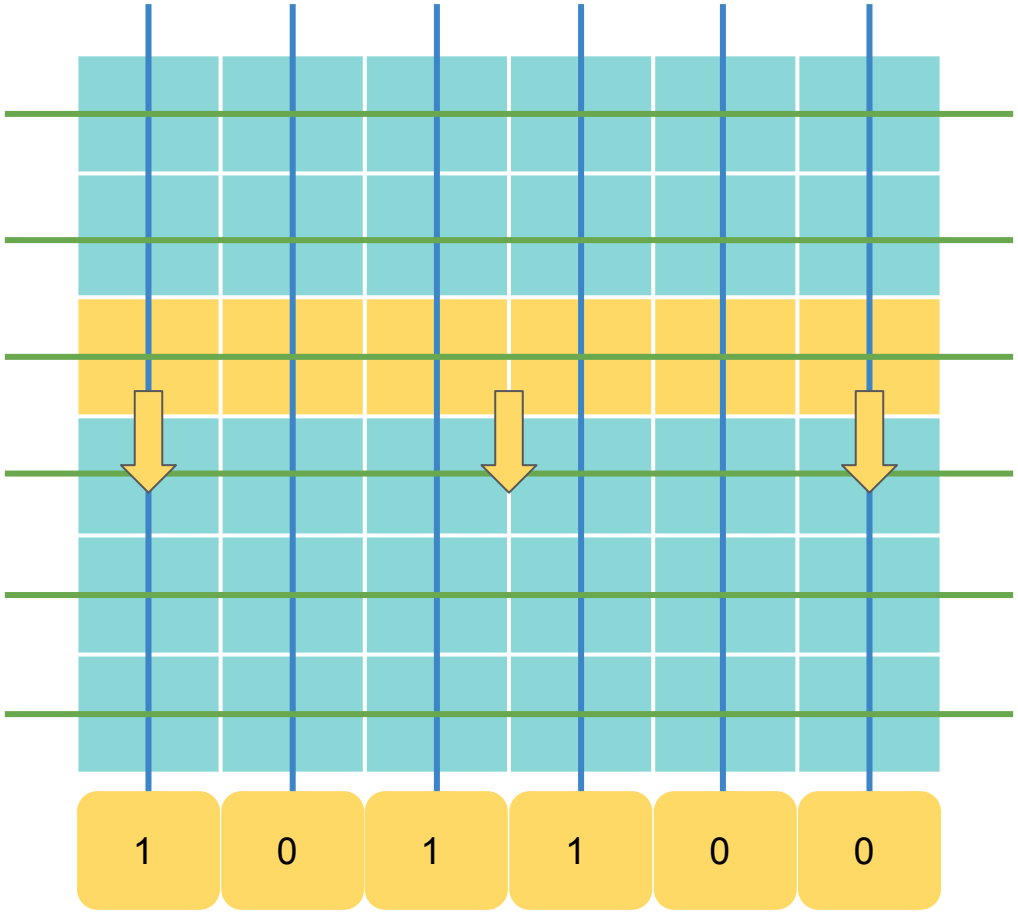







1
1




1
0
1
1
0
0

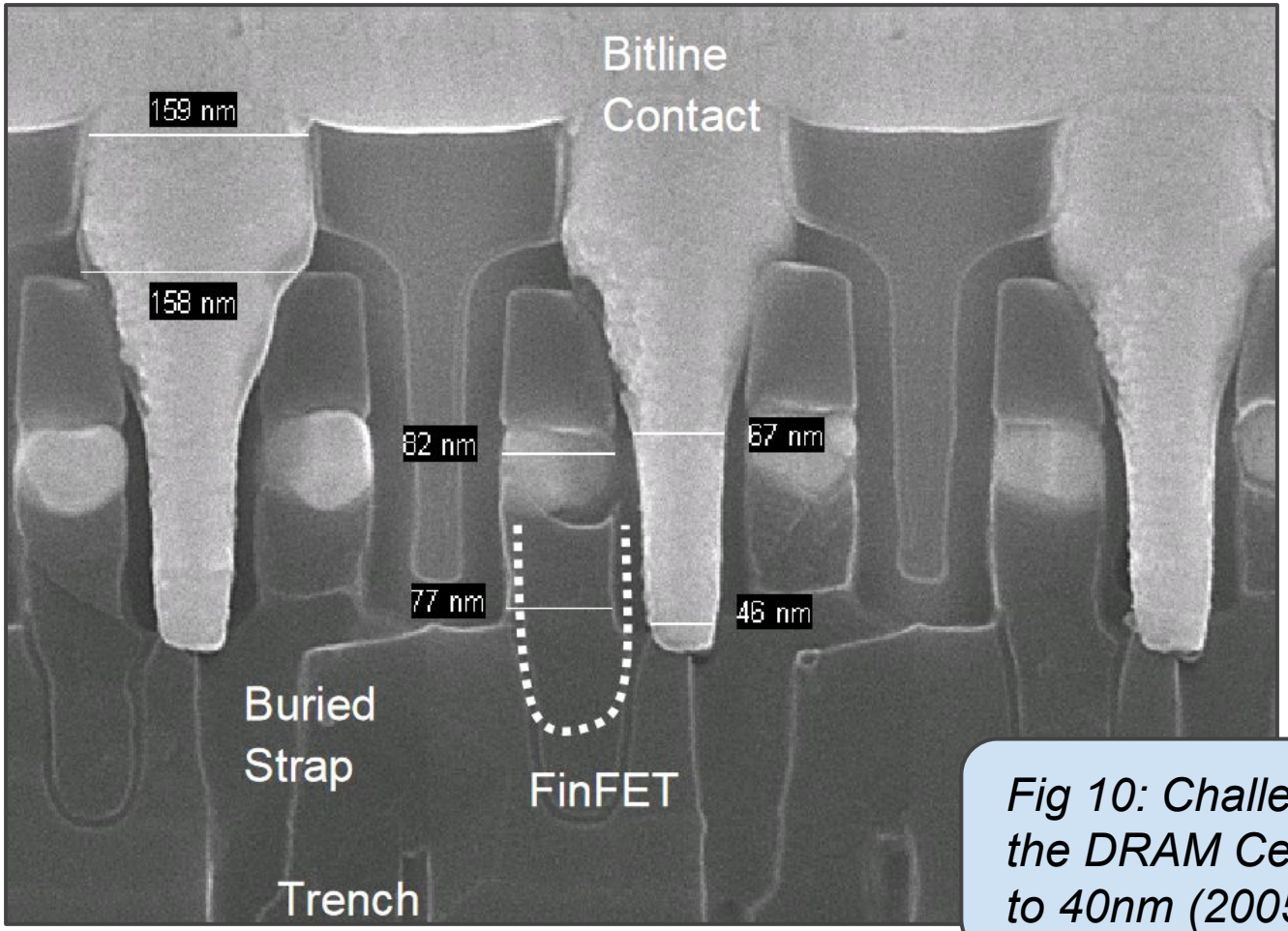
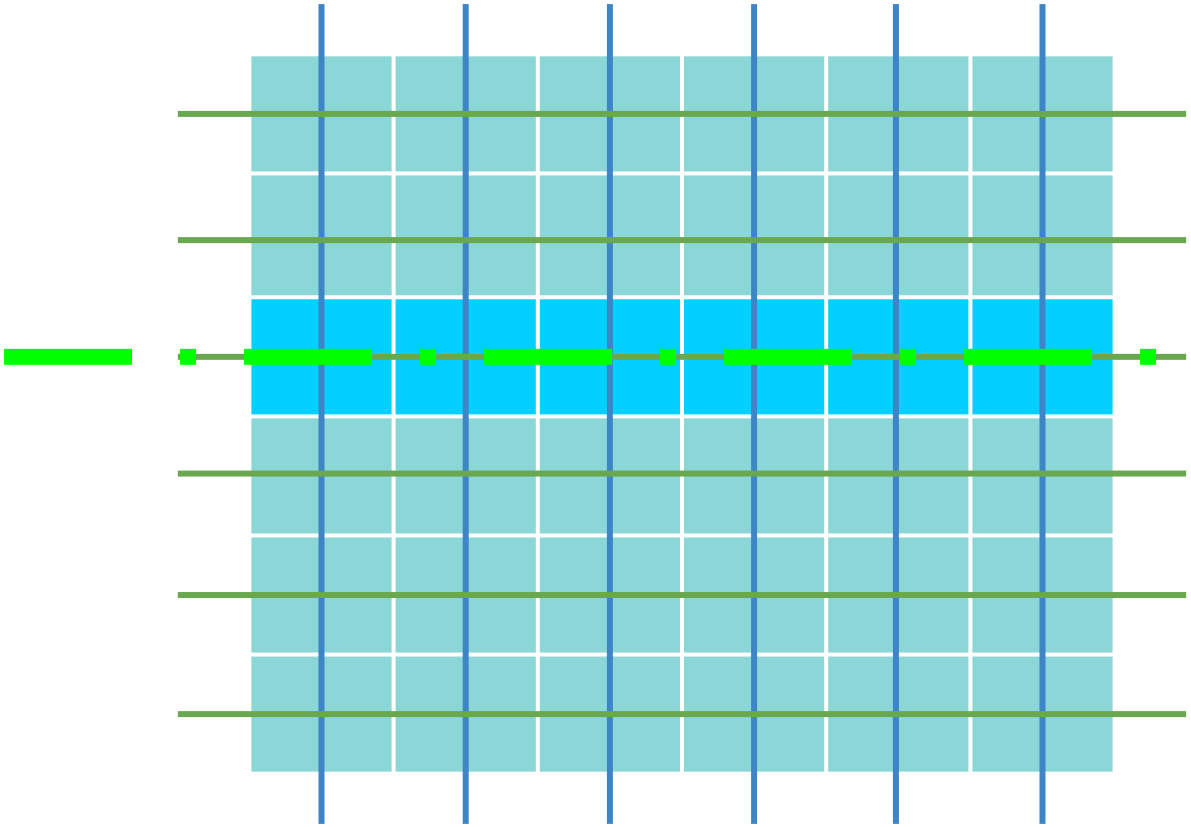
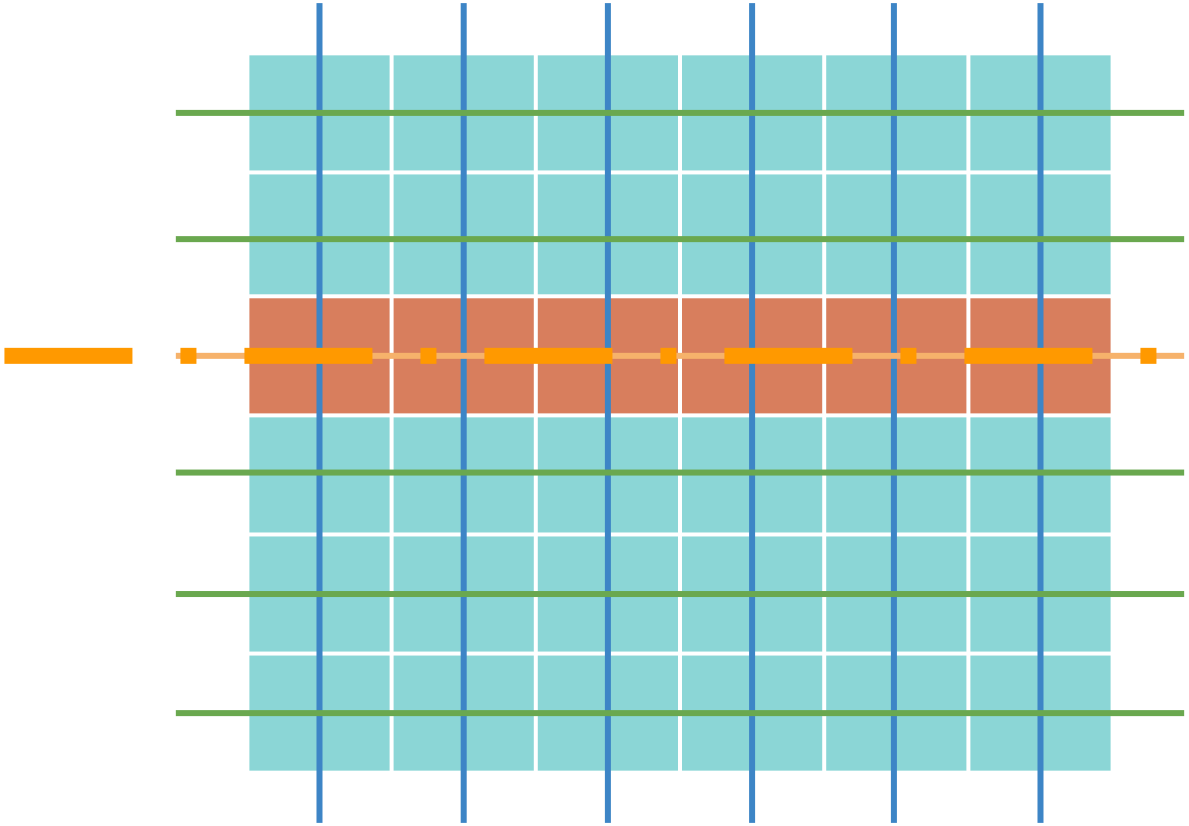
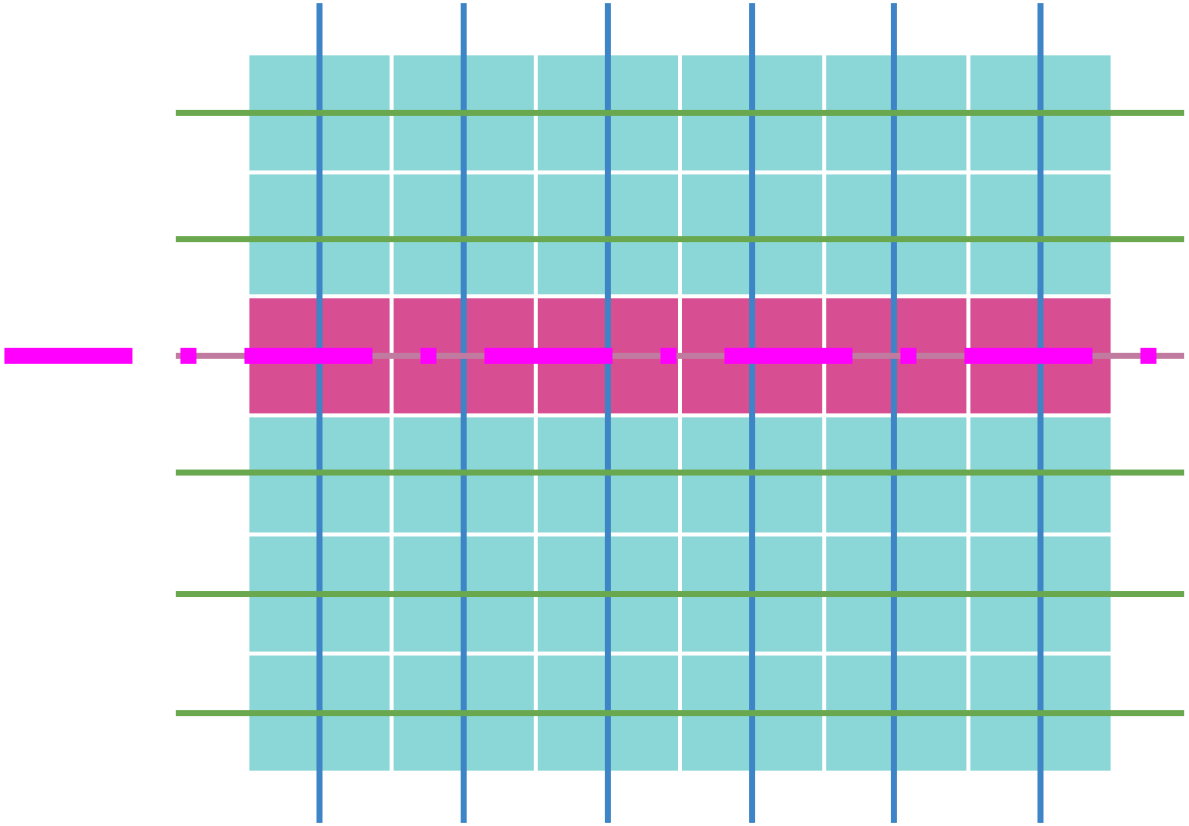
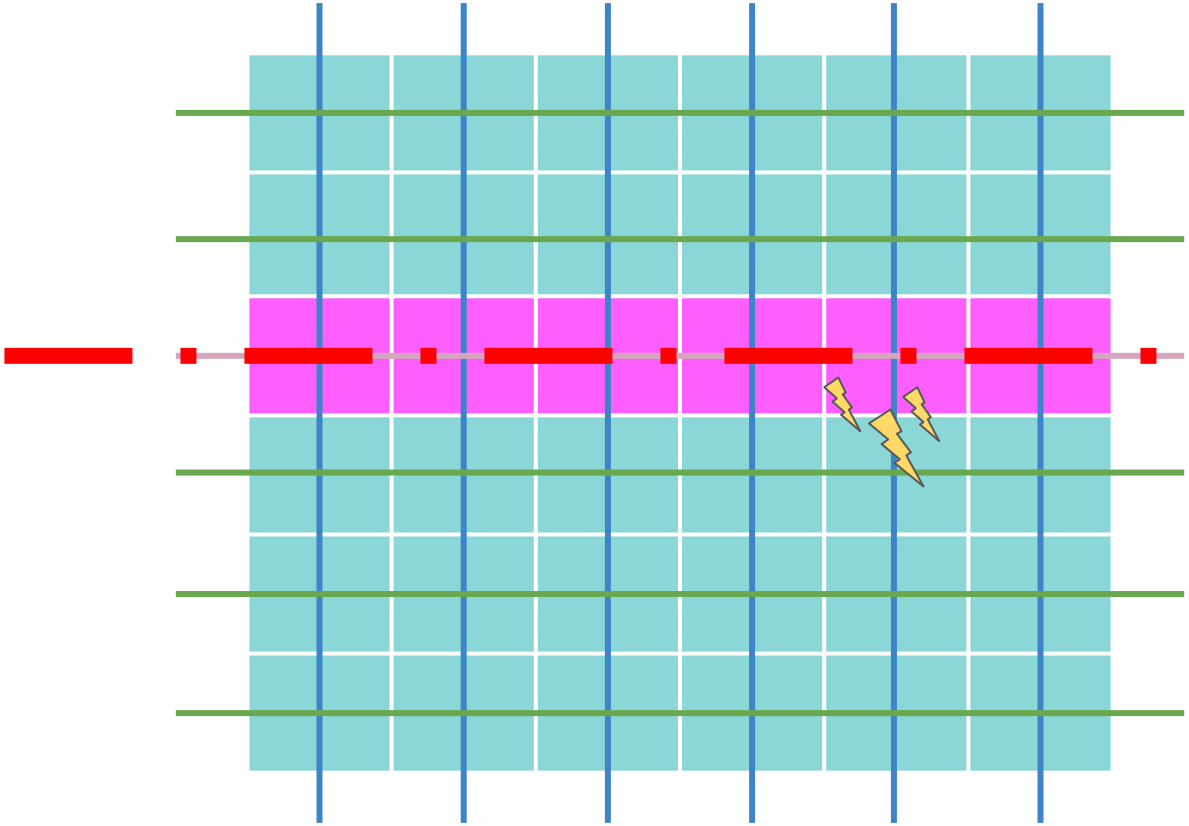


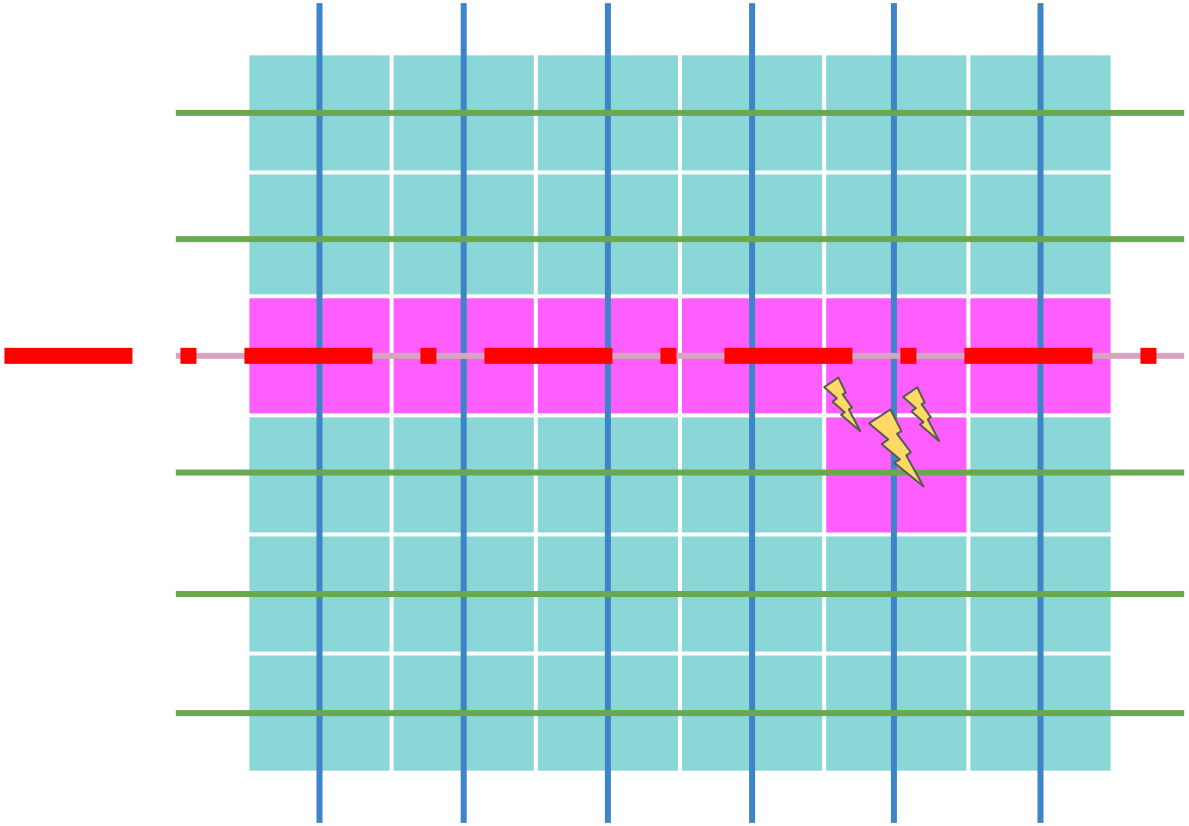
Fig 10: Challenges for the DRAM Cell Scaling to 40nm (2005)



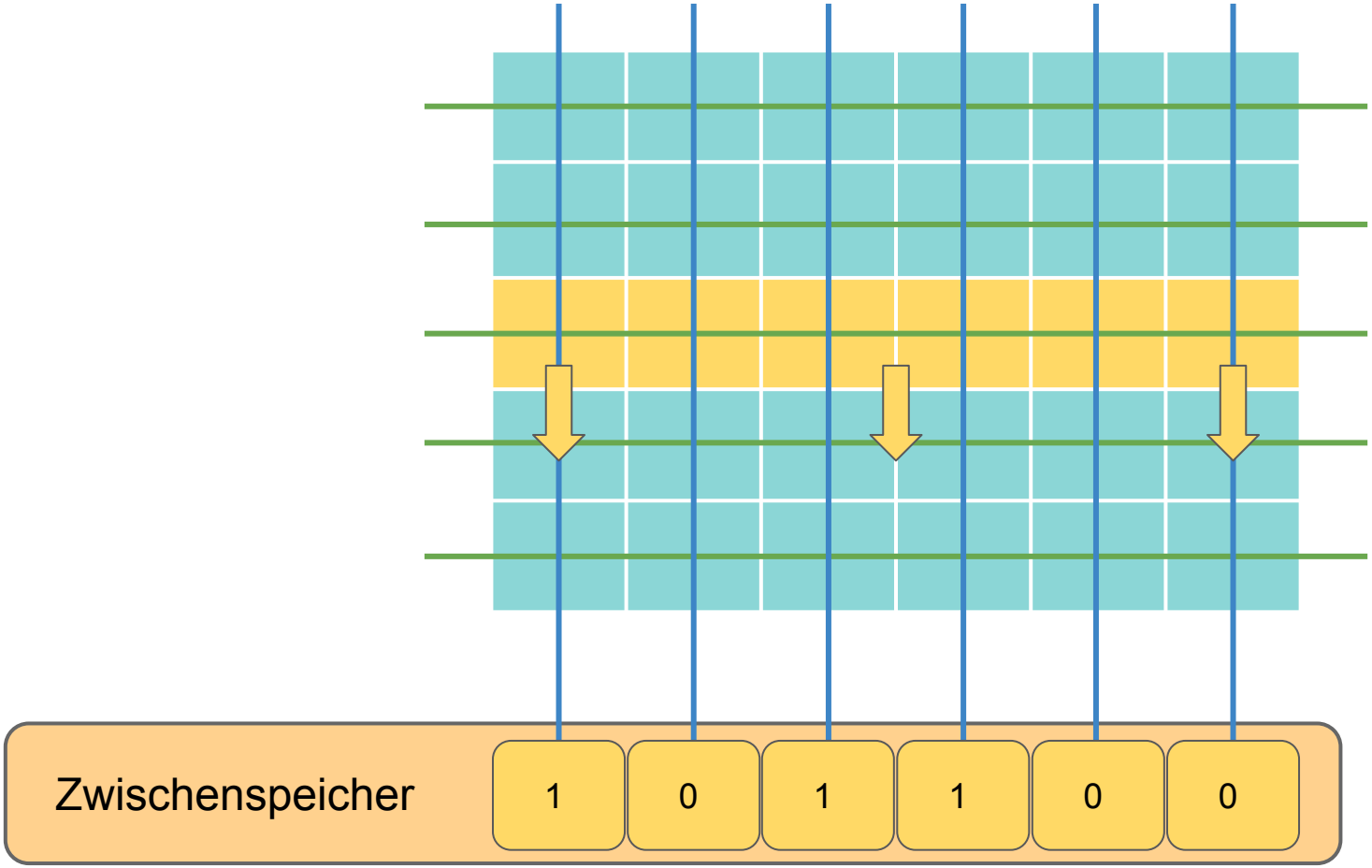






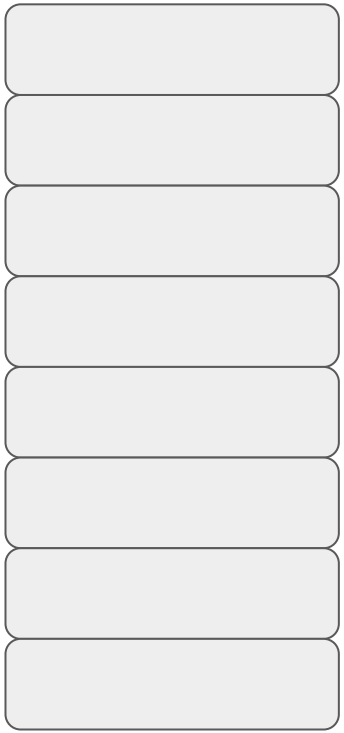


```
1 code1a:
2     move(X), %eax
3     move(Y), %ebx
4     clflush (X)
5     clflush (Y)
6     mfence
7     jmp code1a
```

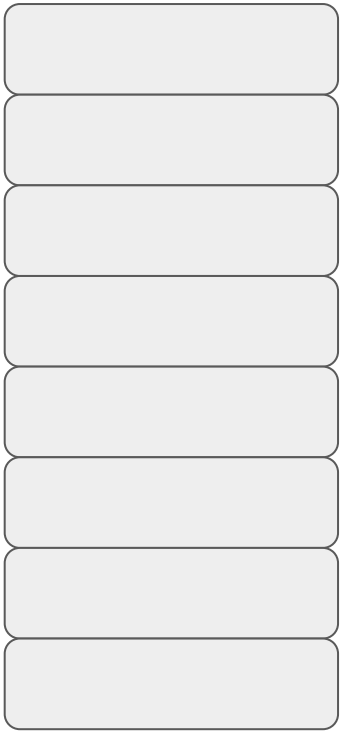

Zwischenspeicher
1
0
1
1
0
0

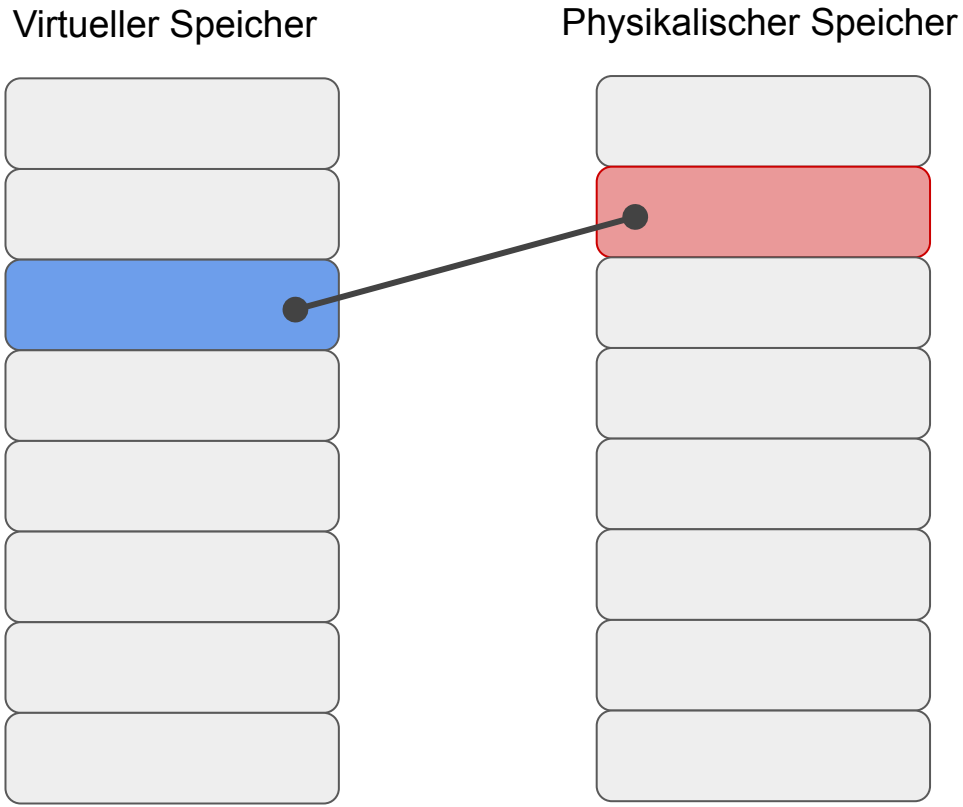
Praxis: Angriff auf den Linux Kernel

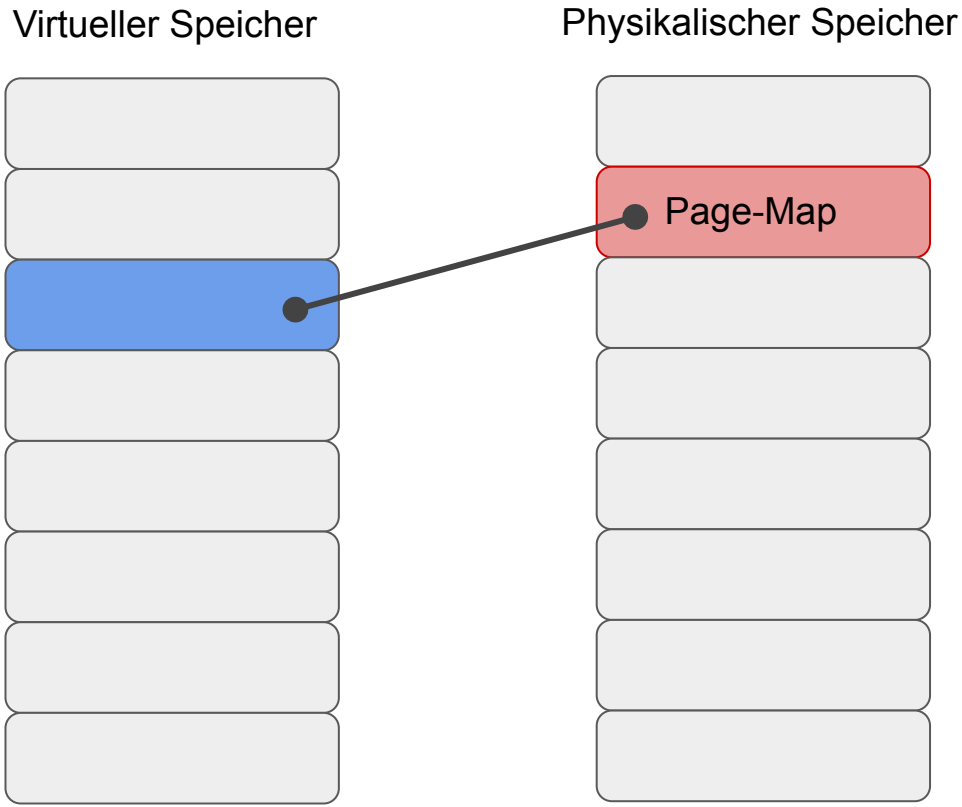
Virtueller Speicher

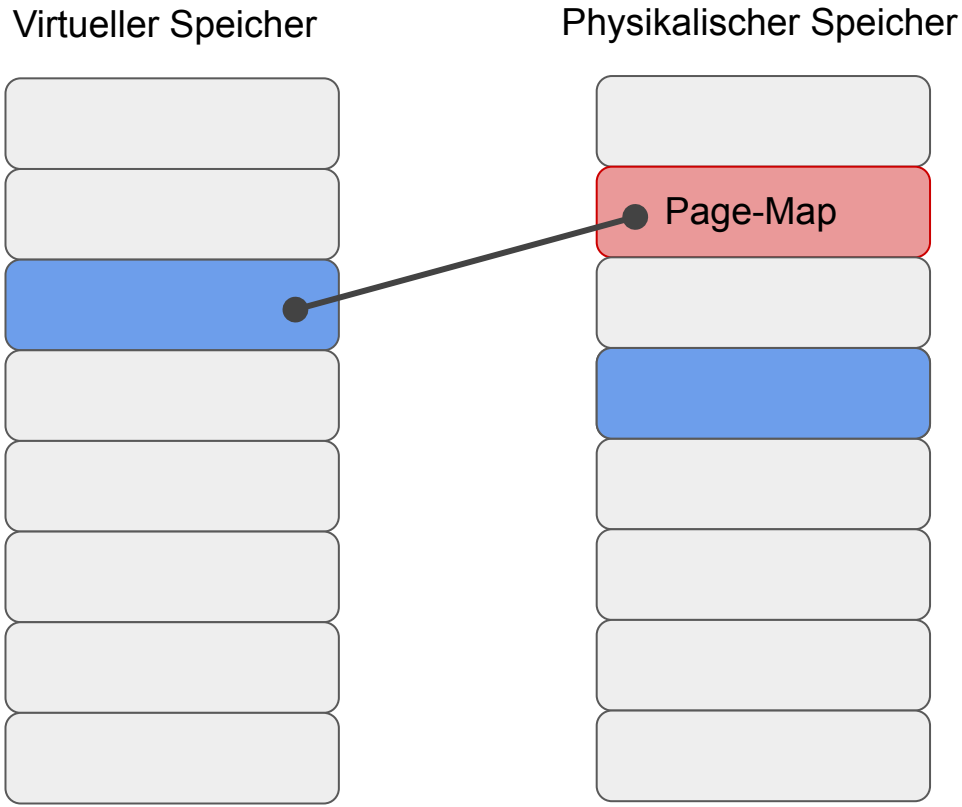


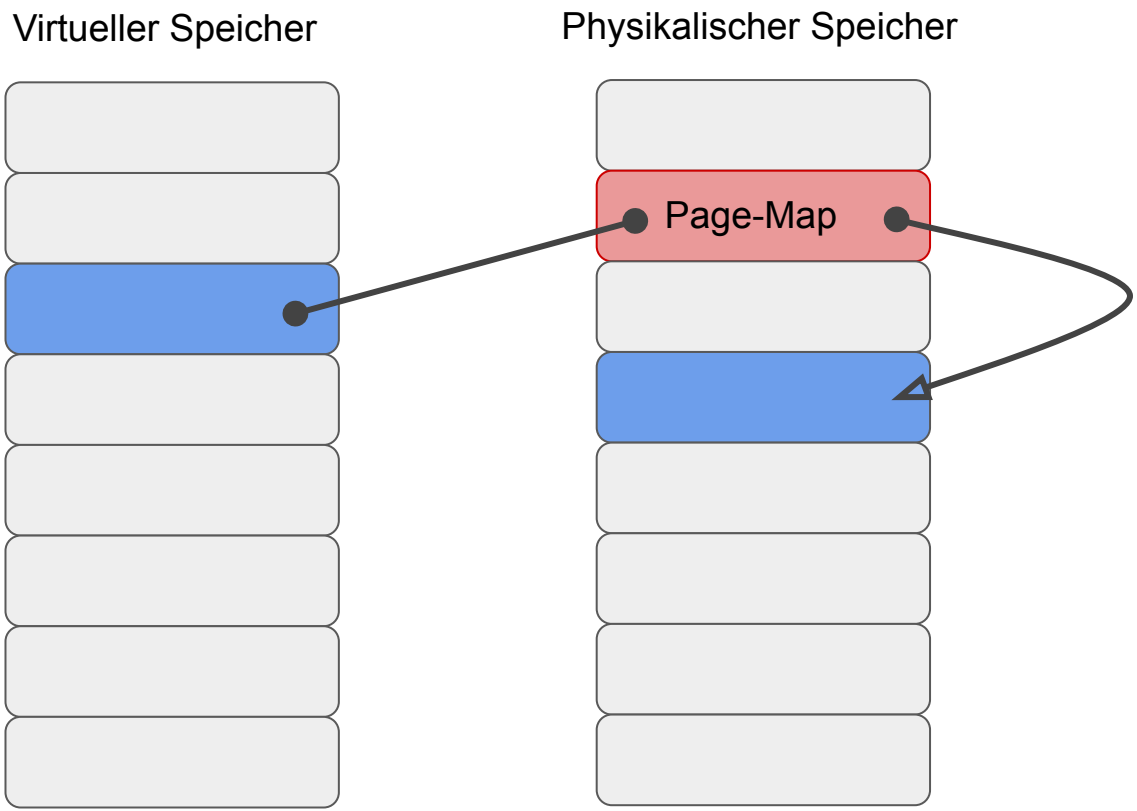
Physikalischer Speicher

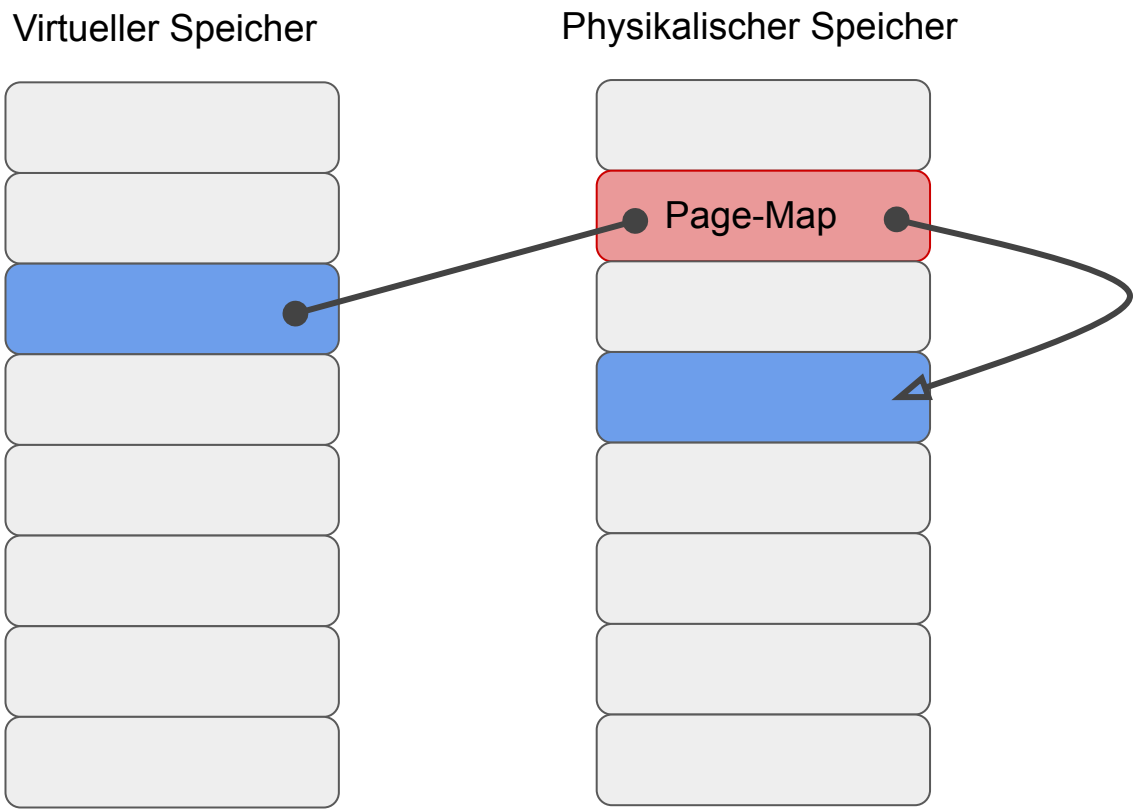


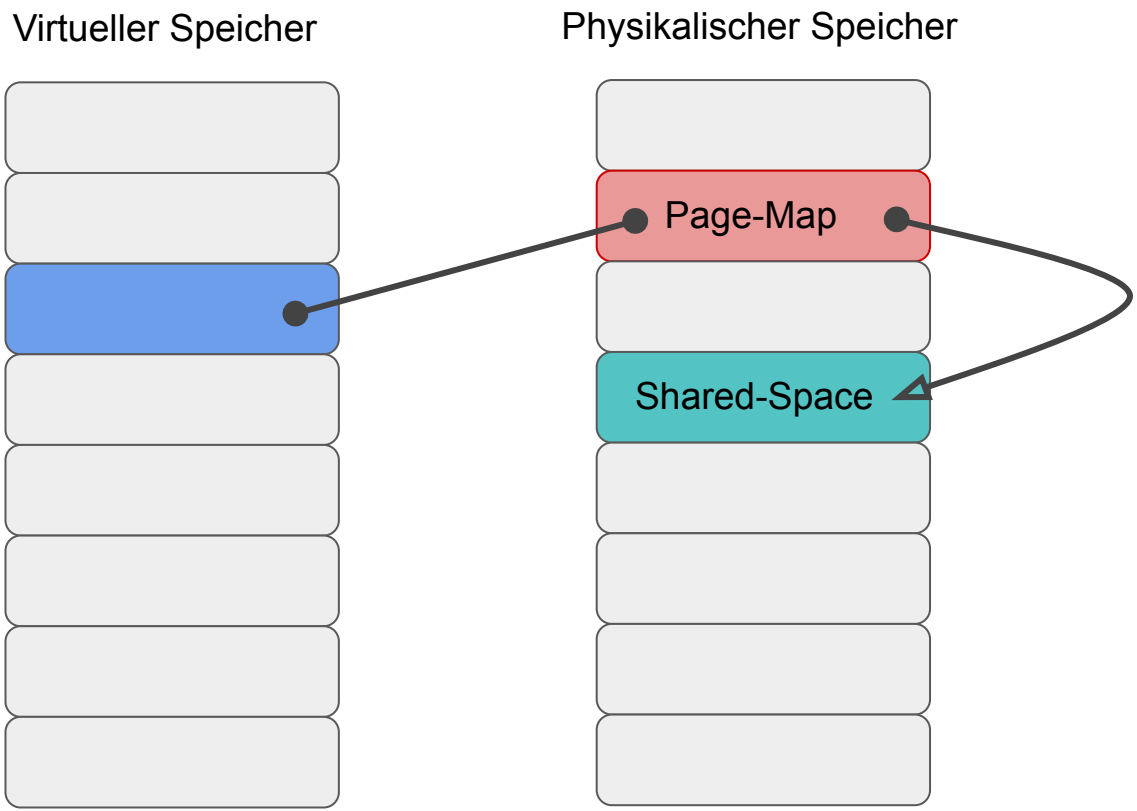

Virtueller Speicher
Physikalischer Speicher

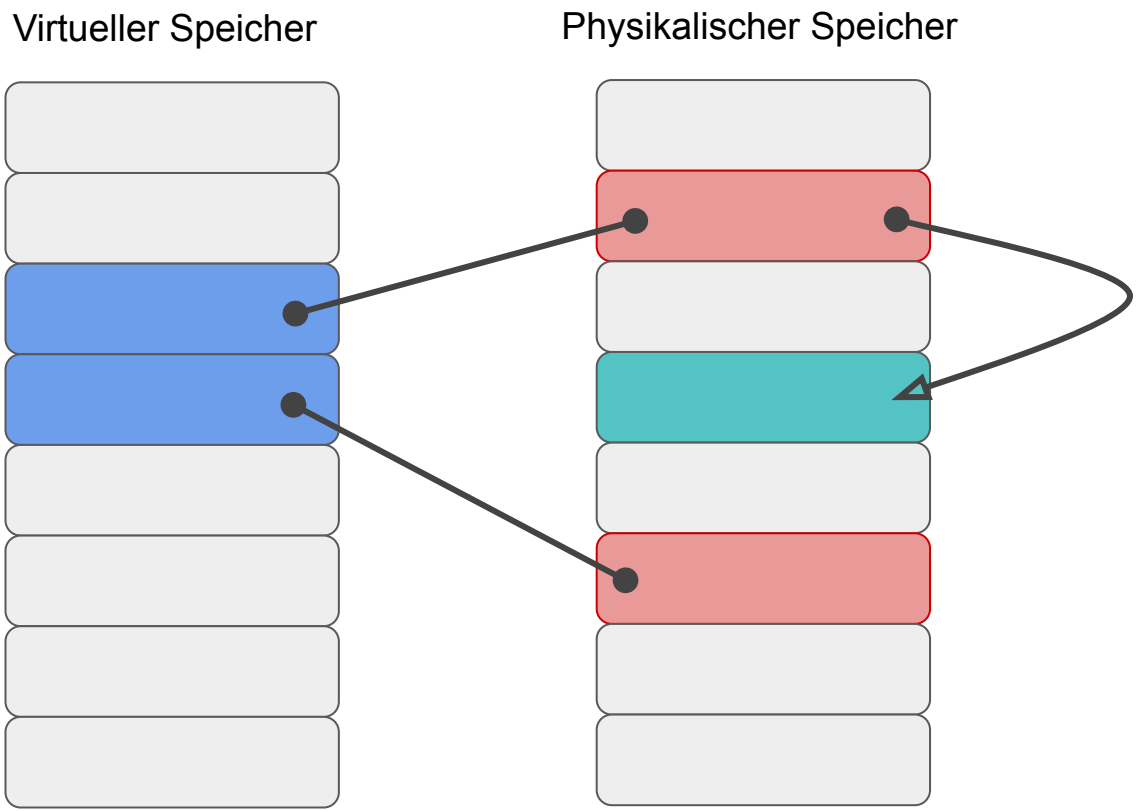

Virtueller Speicher
Physikalischer Speicher
Page-Map

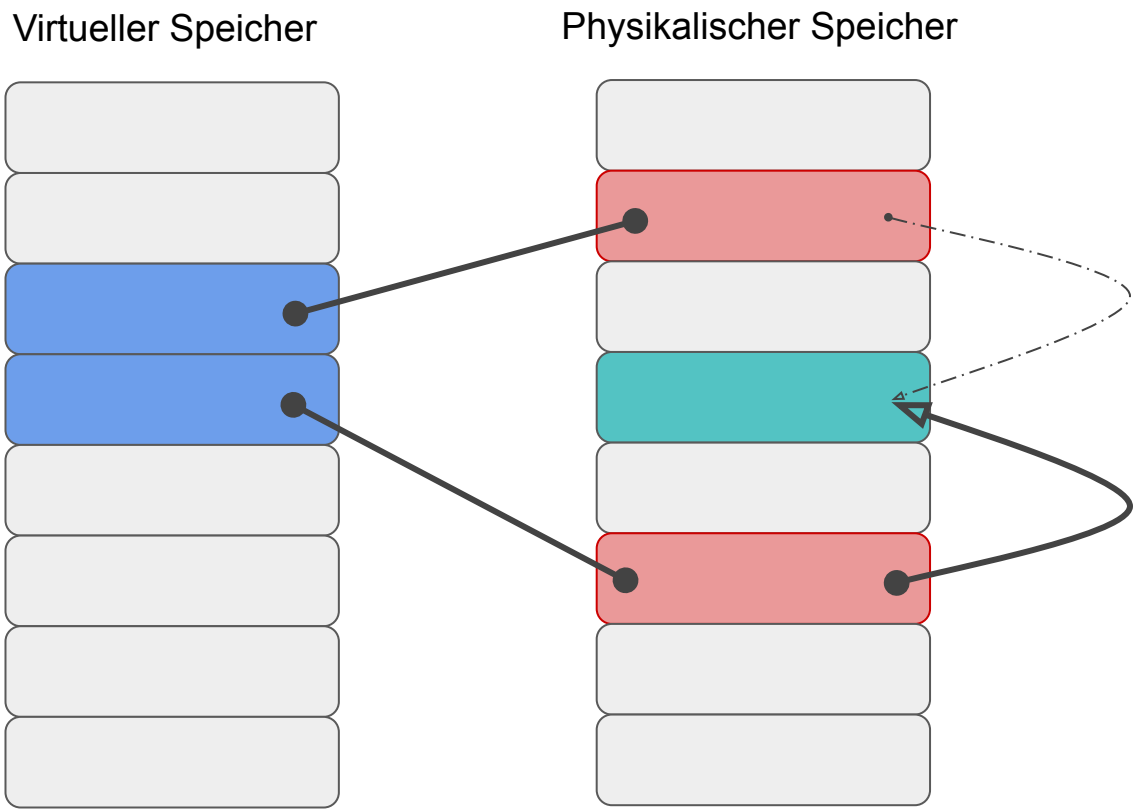

Virtueller Speicher
Physikalischer Speicher
Page-Map

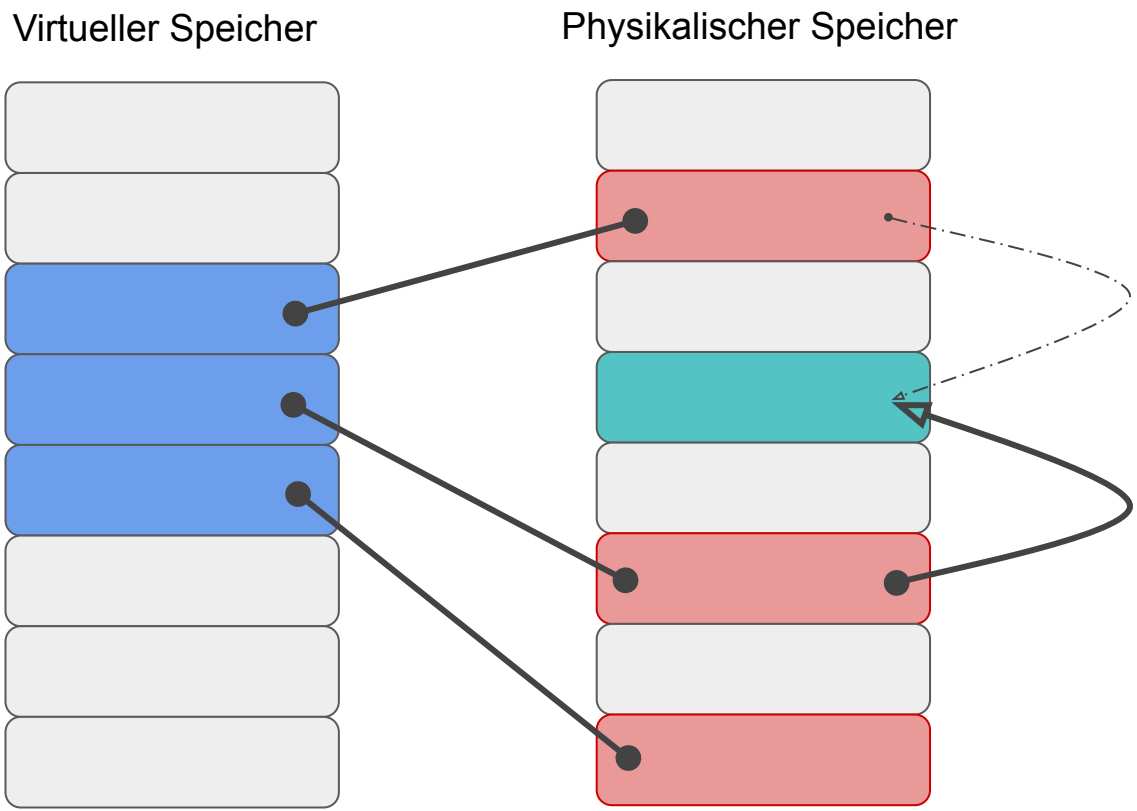

Virtueller Speicher
Physikalischer Speicher
Page-Map

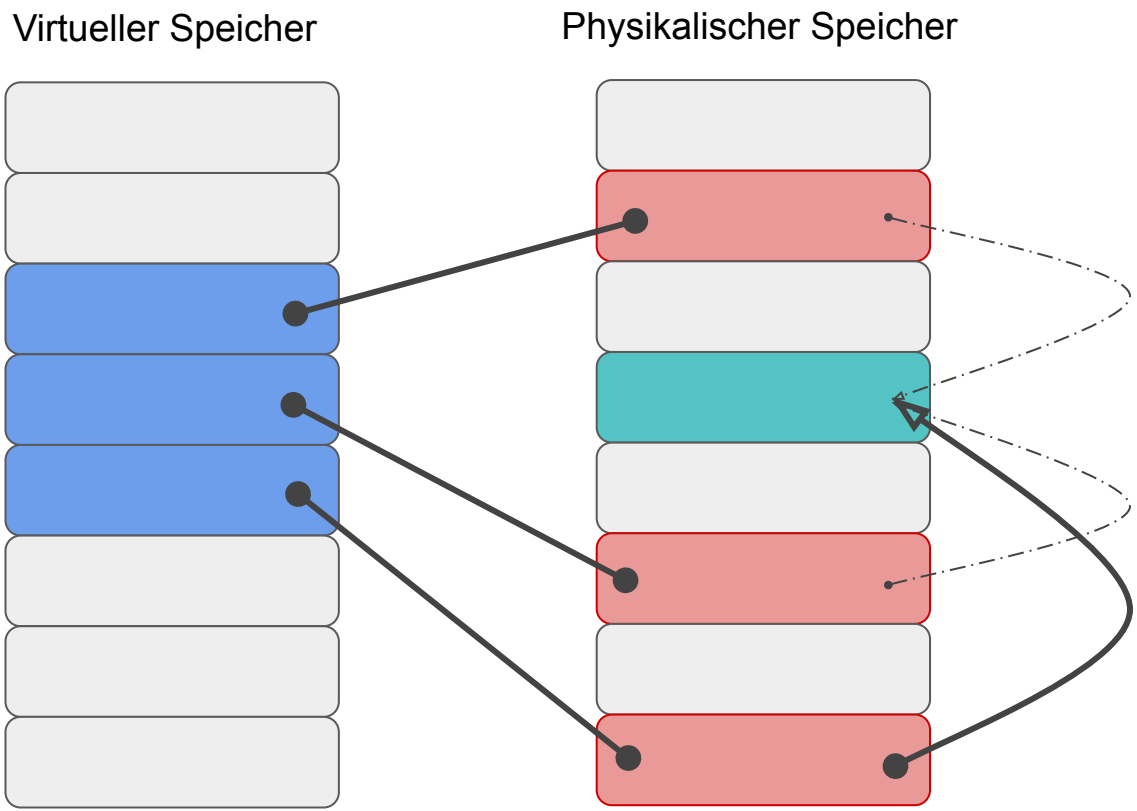

Virtueller Speicher
Physikalischer Speicher
Page-Map

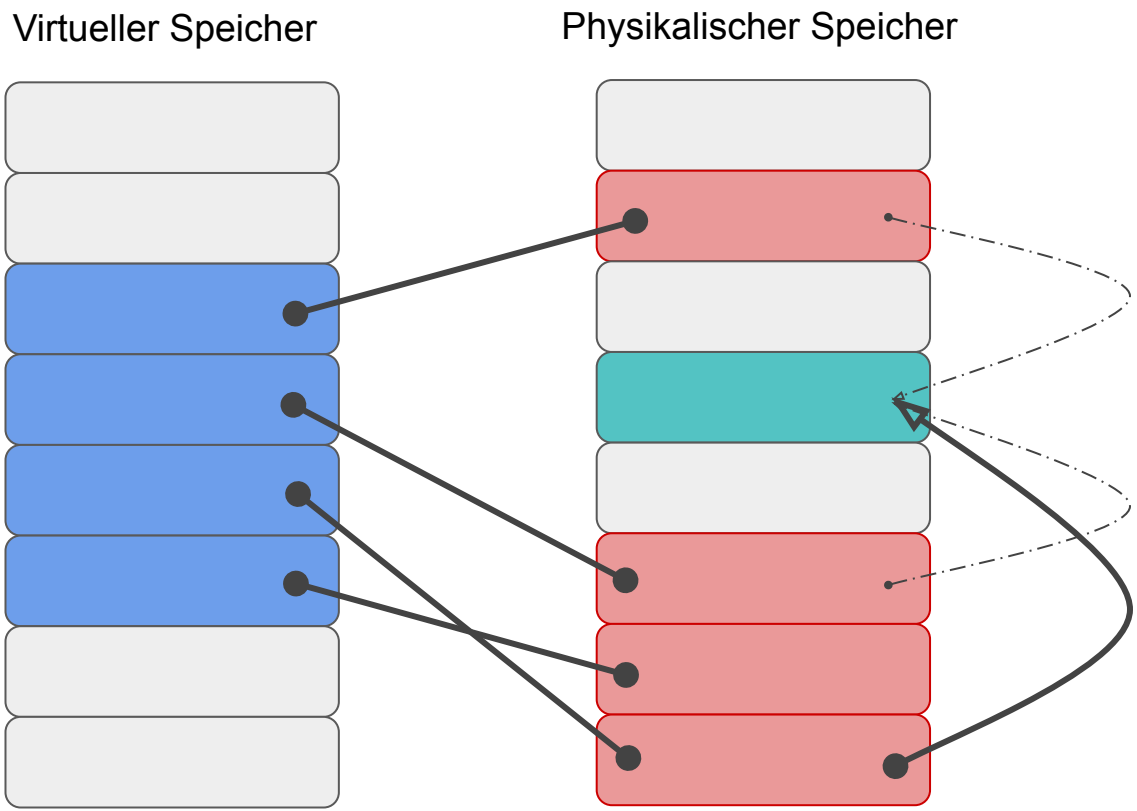

Virtueller Speicher
Physikalischer Speicher
Page-Map
Shared-Space

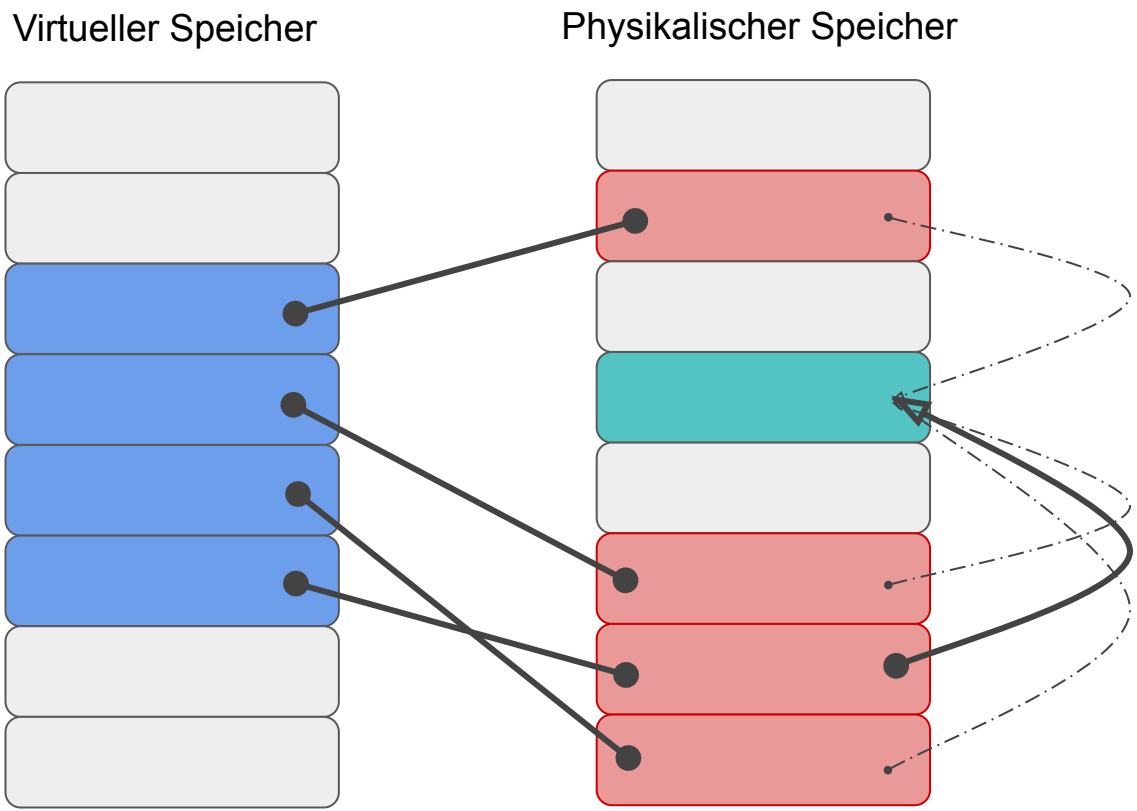

Virtueller Speicher
Physikalischer Speicher

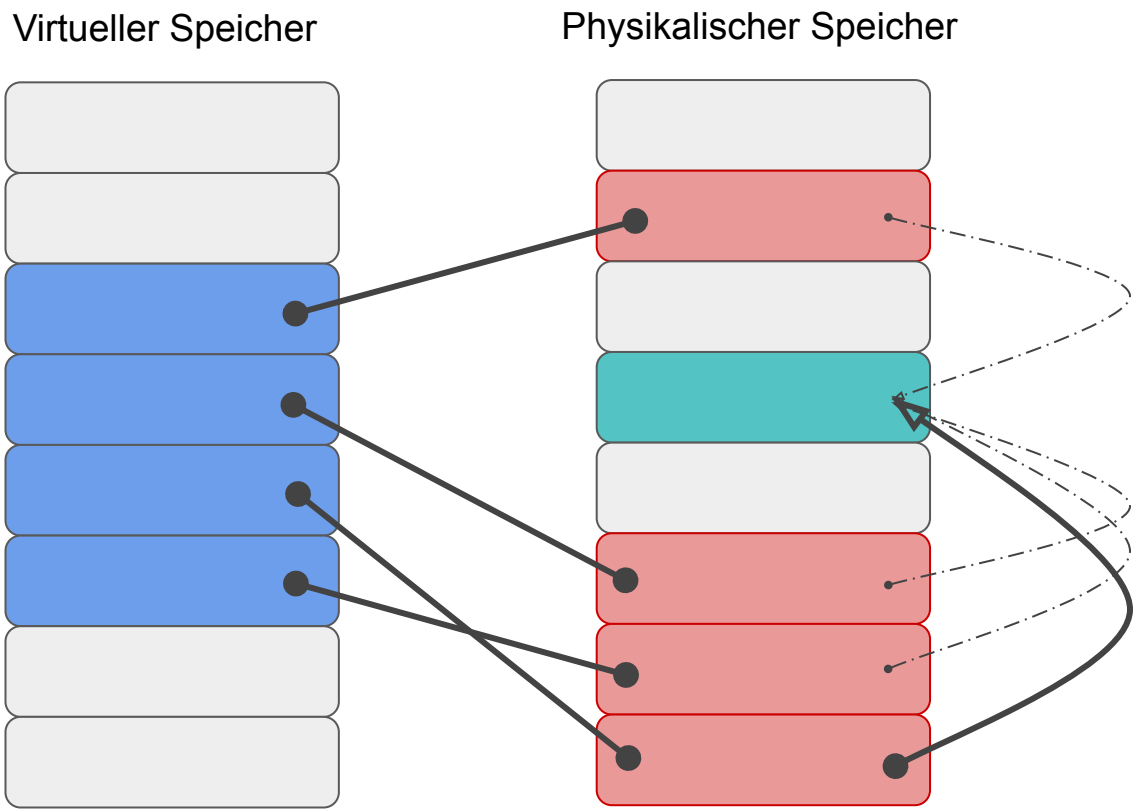

Virtueller Speicher
Physikalischer Speicher

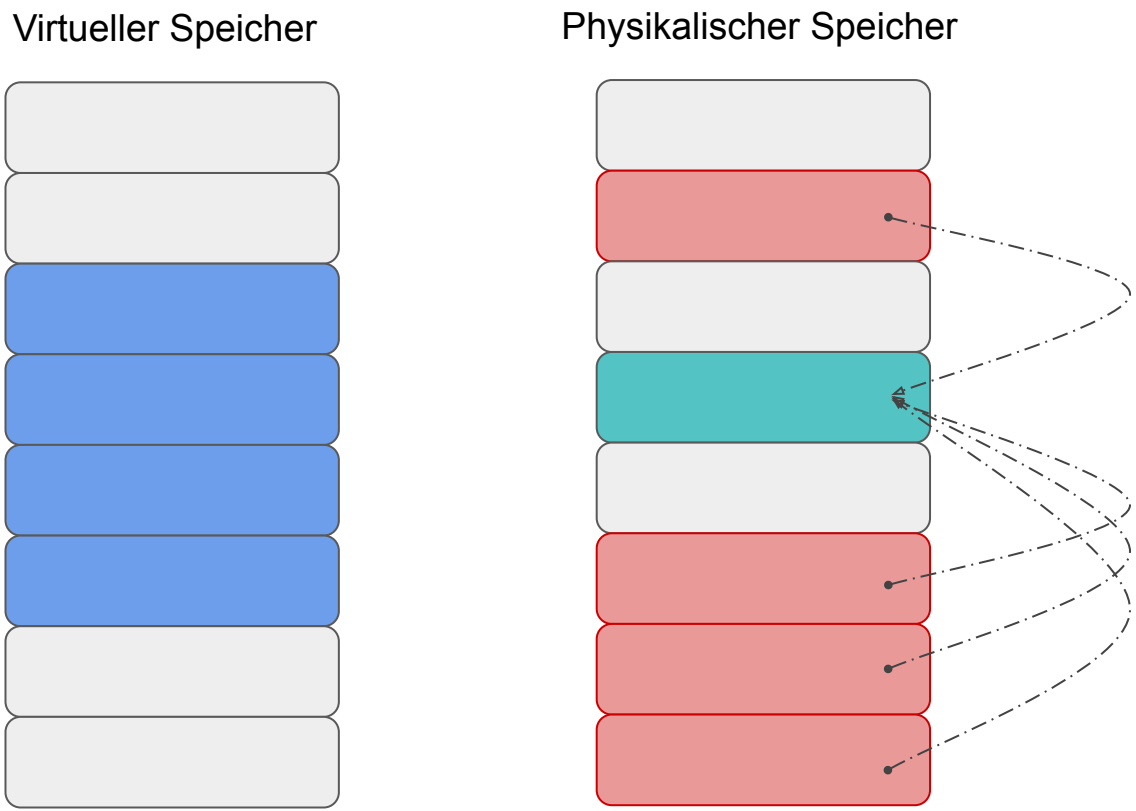

Virtueller Speicher
Physikalischer Speicher

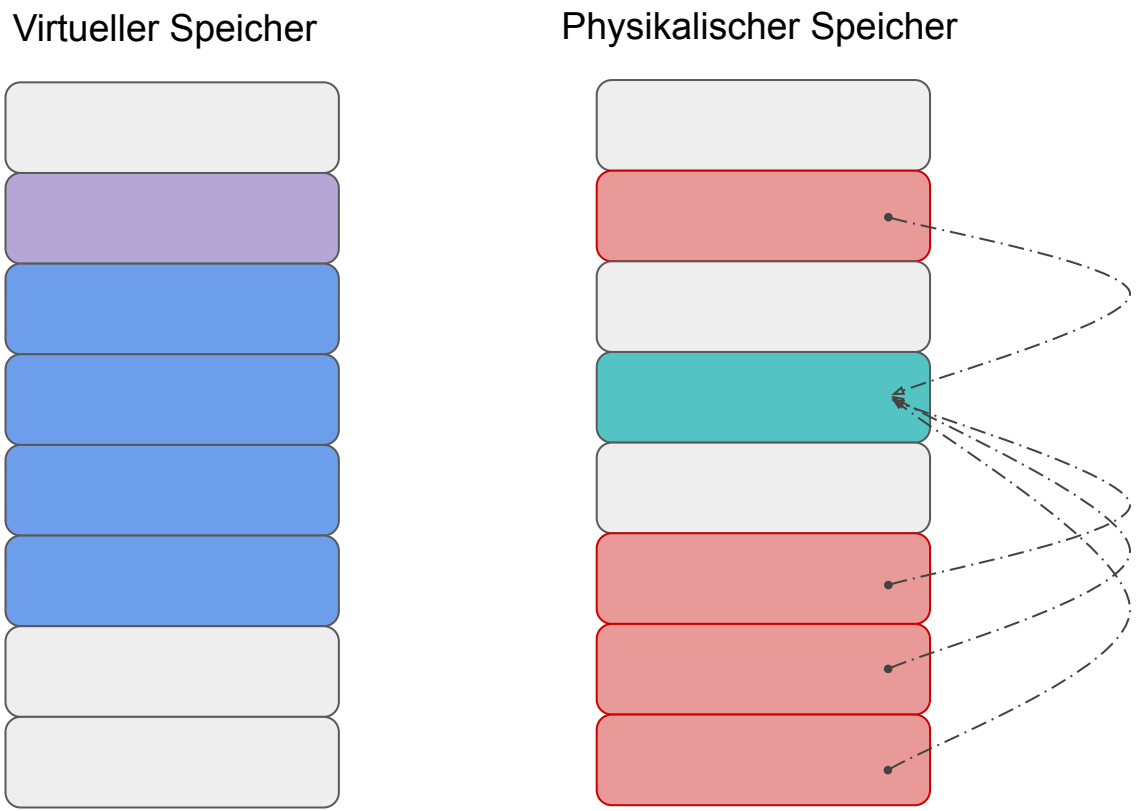

Virtueller Speicher
Physikalischer Speicher

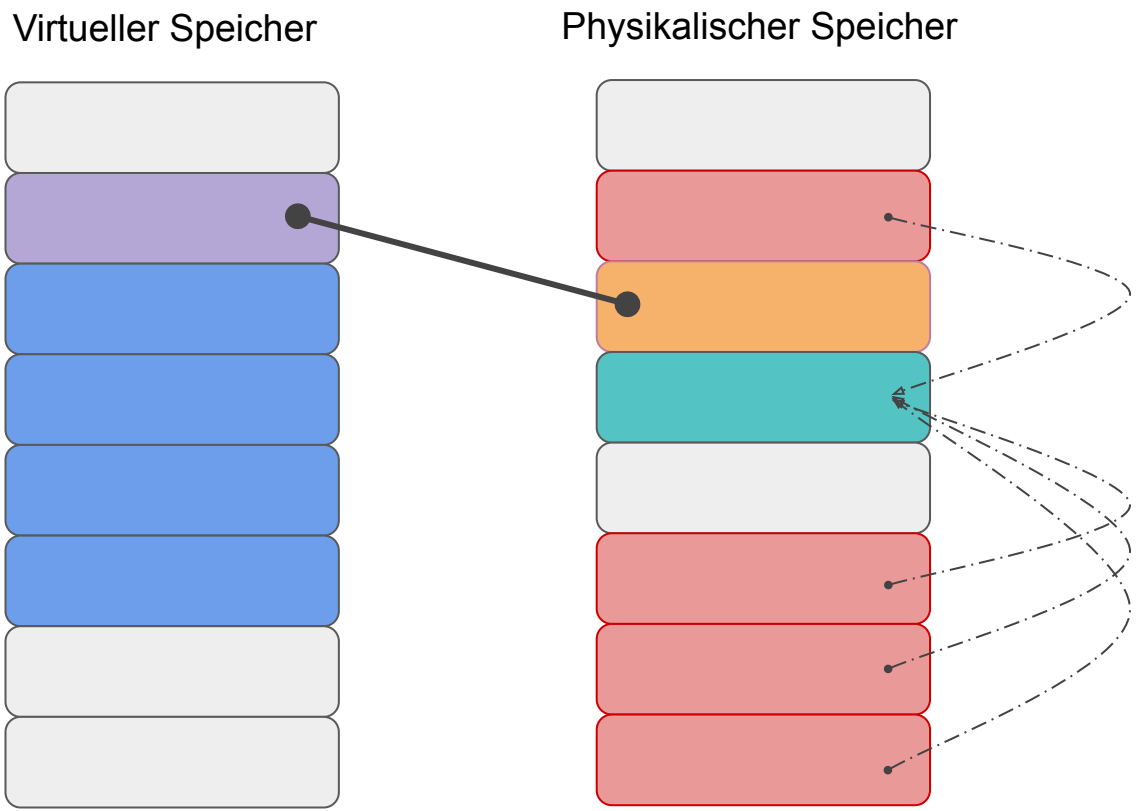

Virtueller Speicher
Physikalischer Speicher

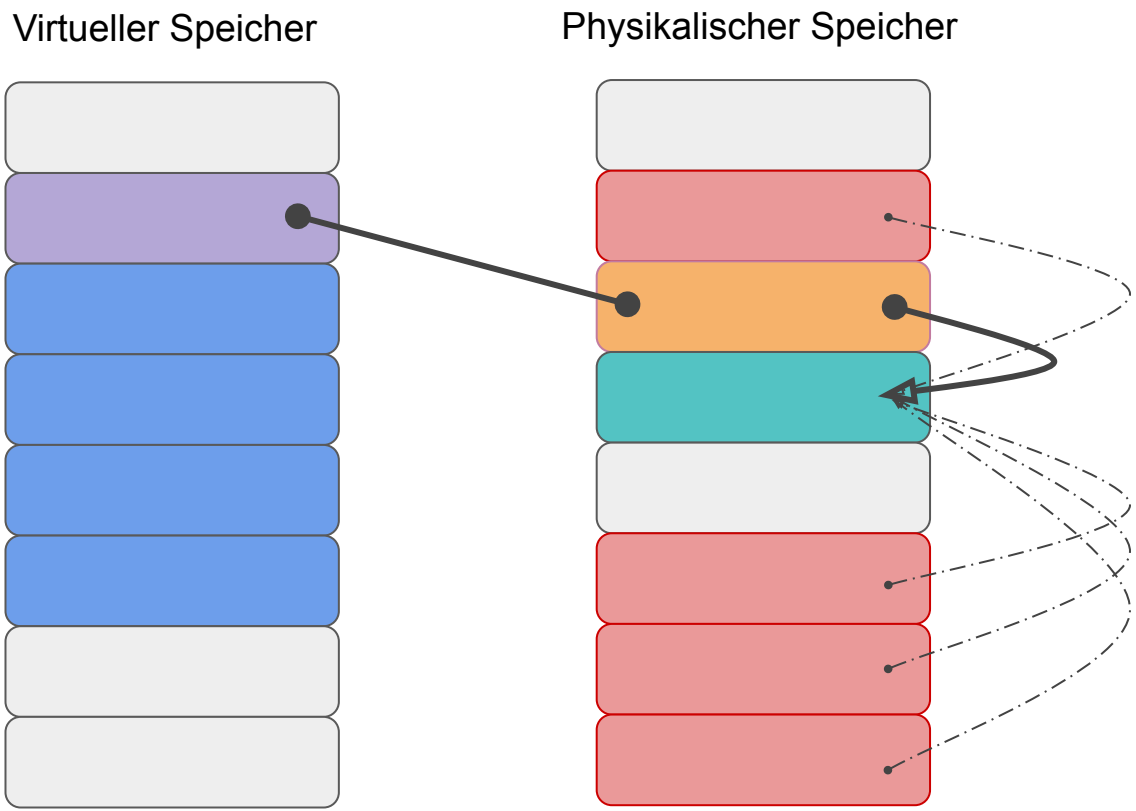

Virtueller Speicher
Physikalischer Speicher

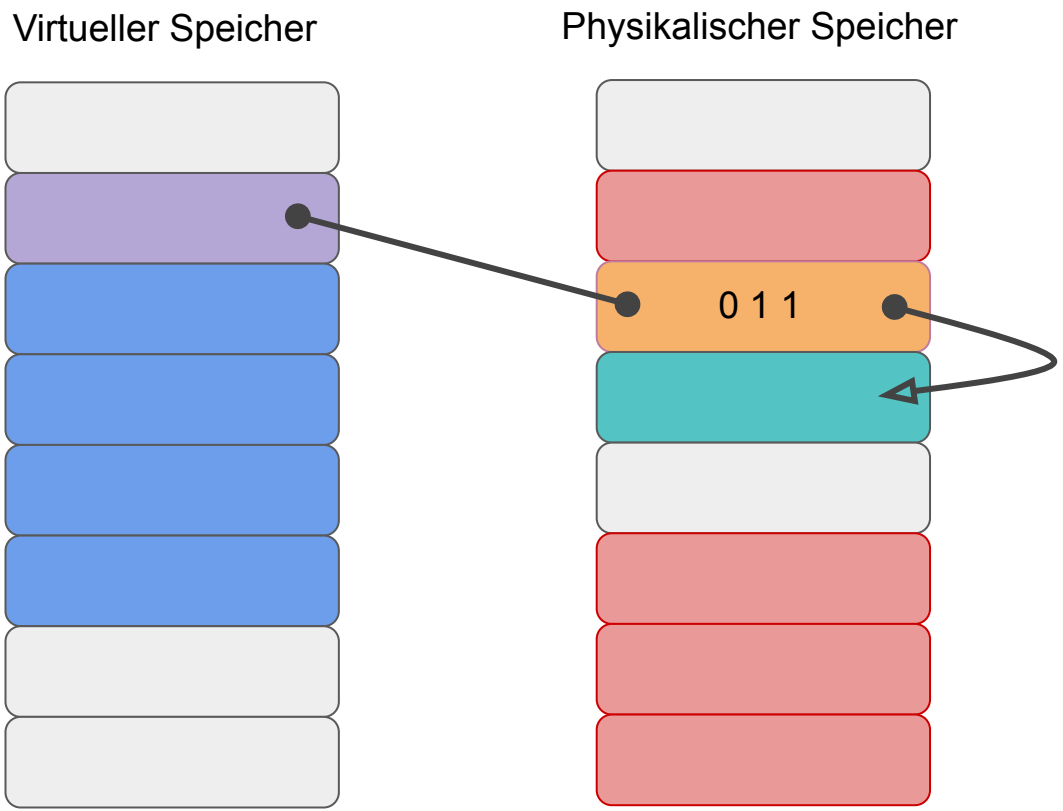

Virtueller Speicher
Physikalischer Speicher

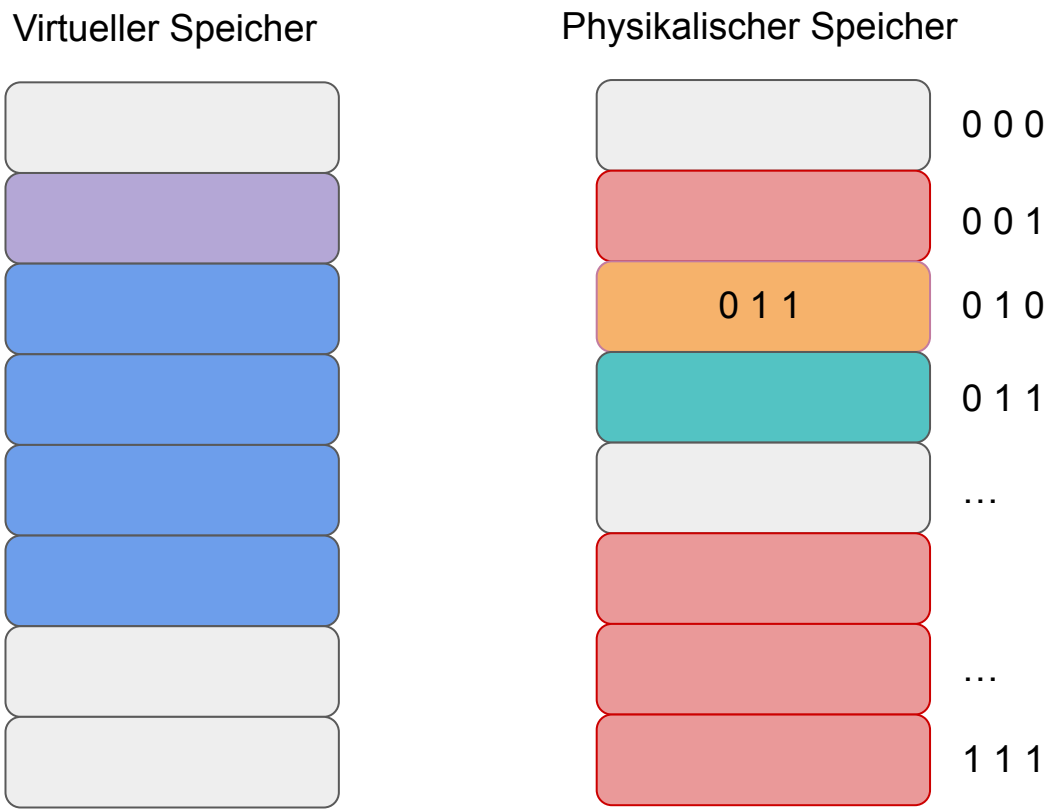

Virtueller Speicher
Physikalischer Speicher

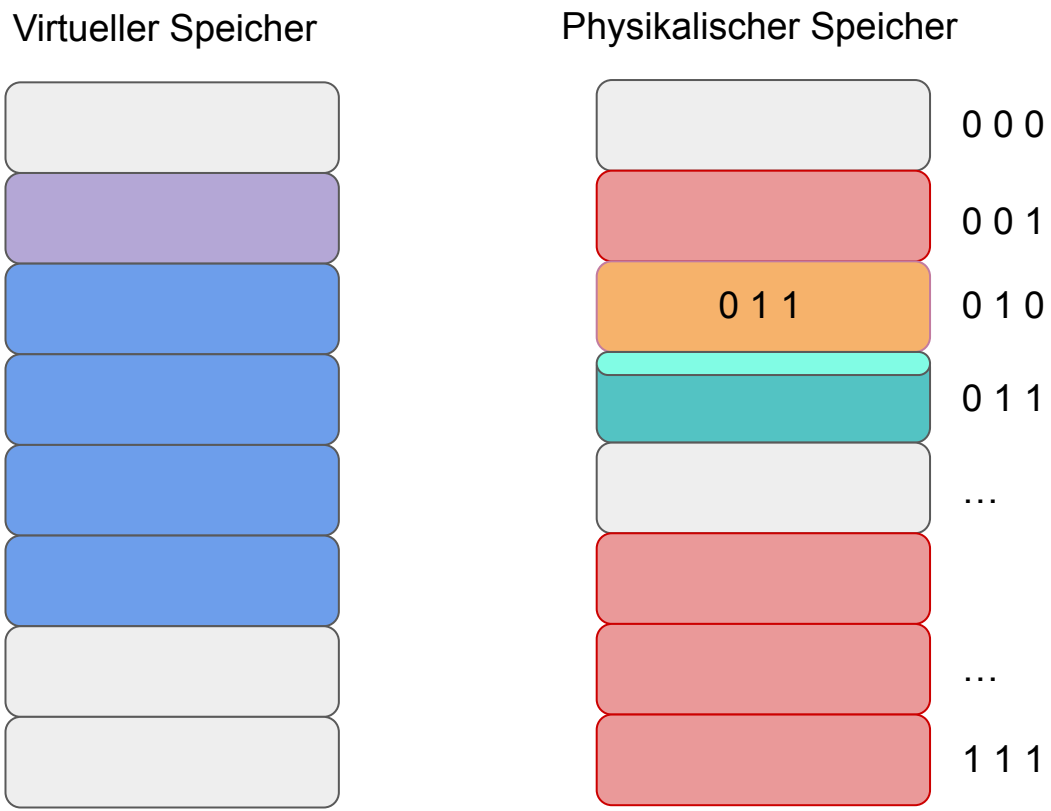

Virtueller Speicher
Physikalischer Speicher

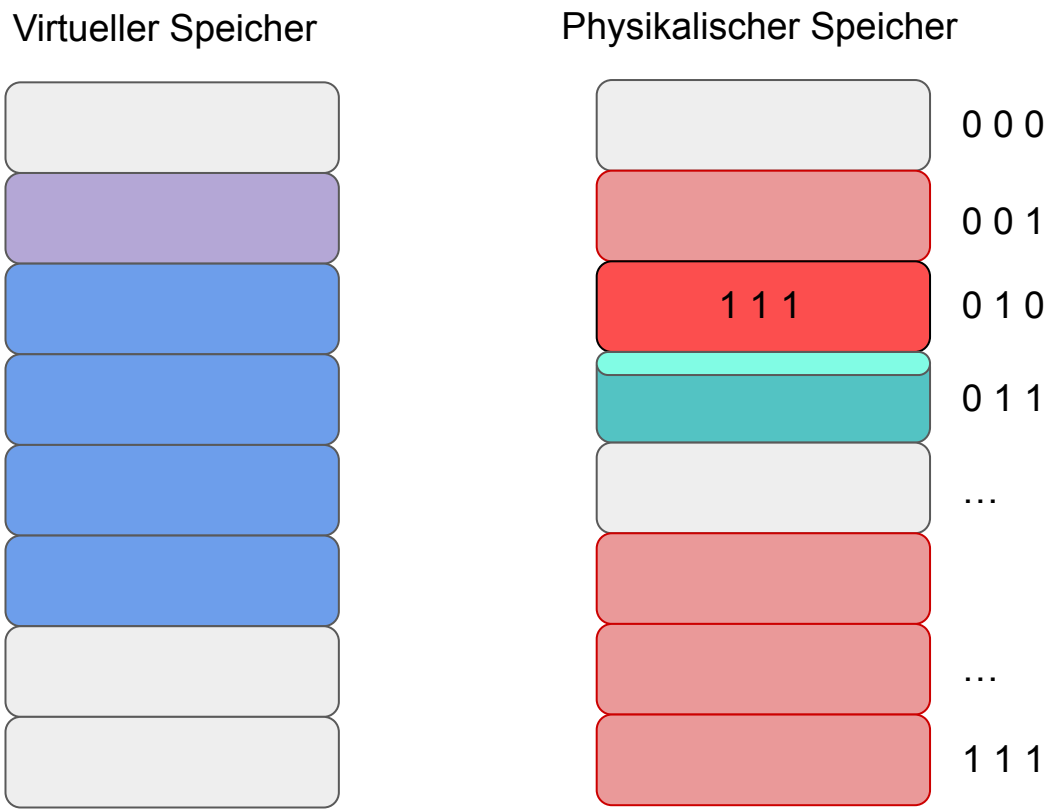

Virtueller Speicher
Physikalischer Speicher

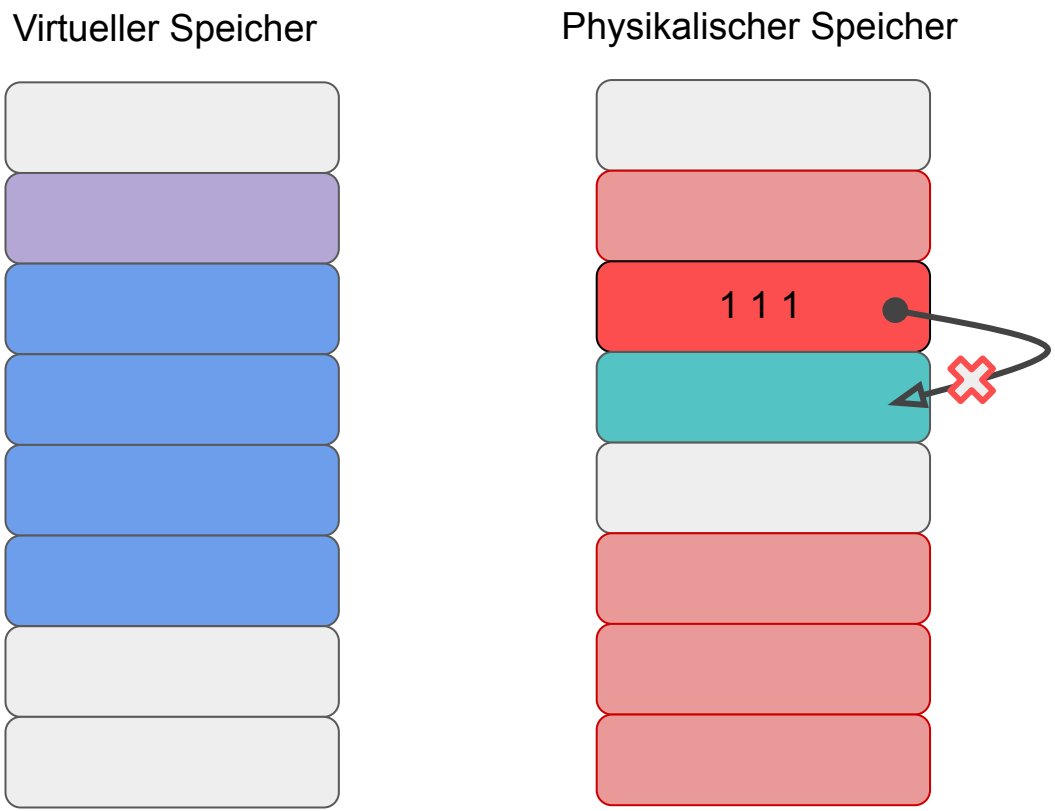

Virtueller Speicher
Physikalischer Speicher

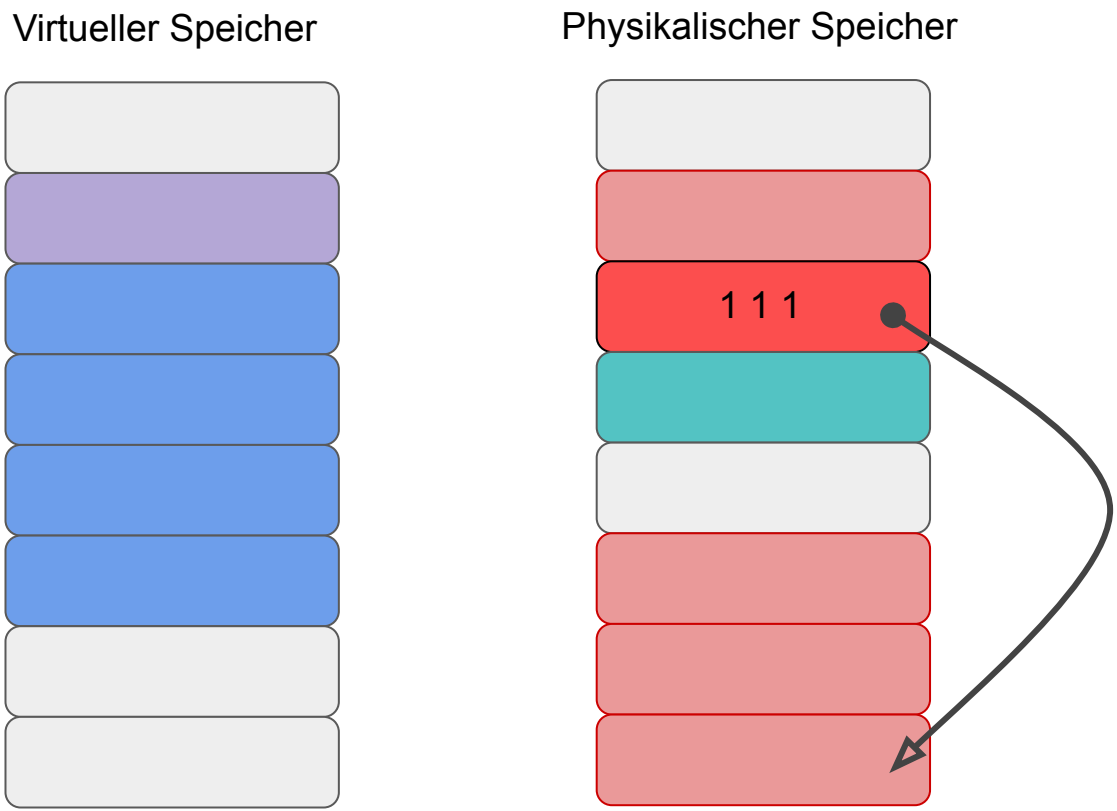

Virtueller Speicher
Physikalischer Speicher
0 1 1

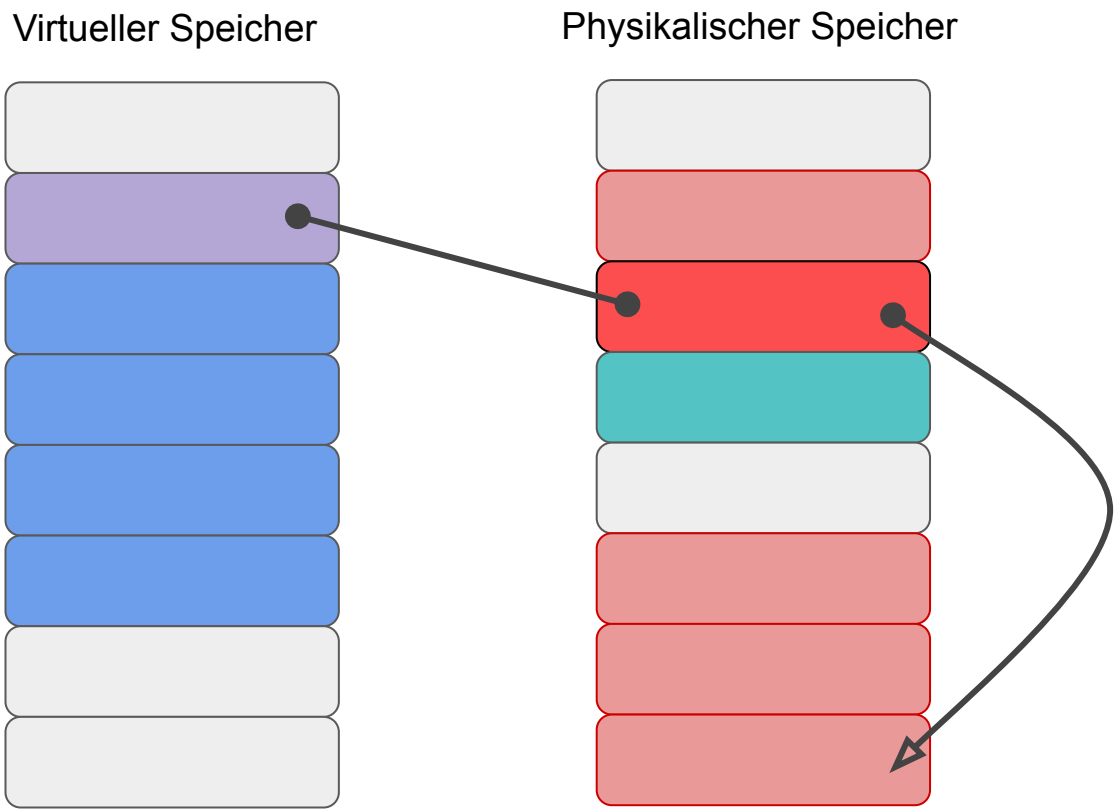

Virtueller Speicher
Physikalischer Speicher
0 0 0
0 0 1
0 1 1
0 1 0
0 1 1
…
…
1 1 1

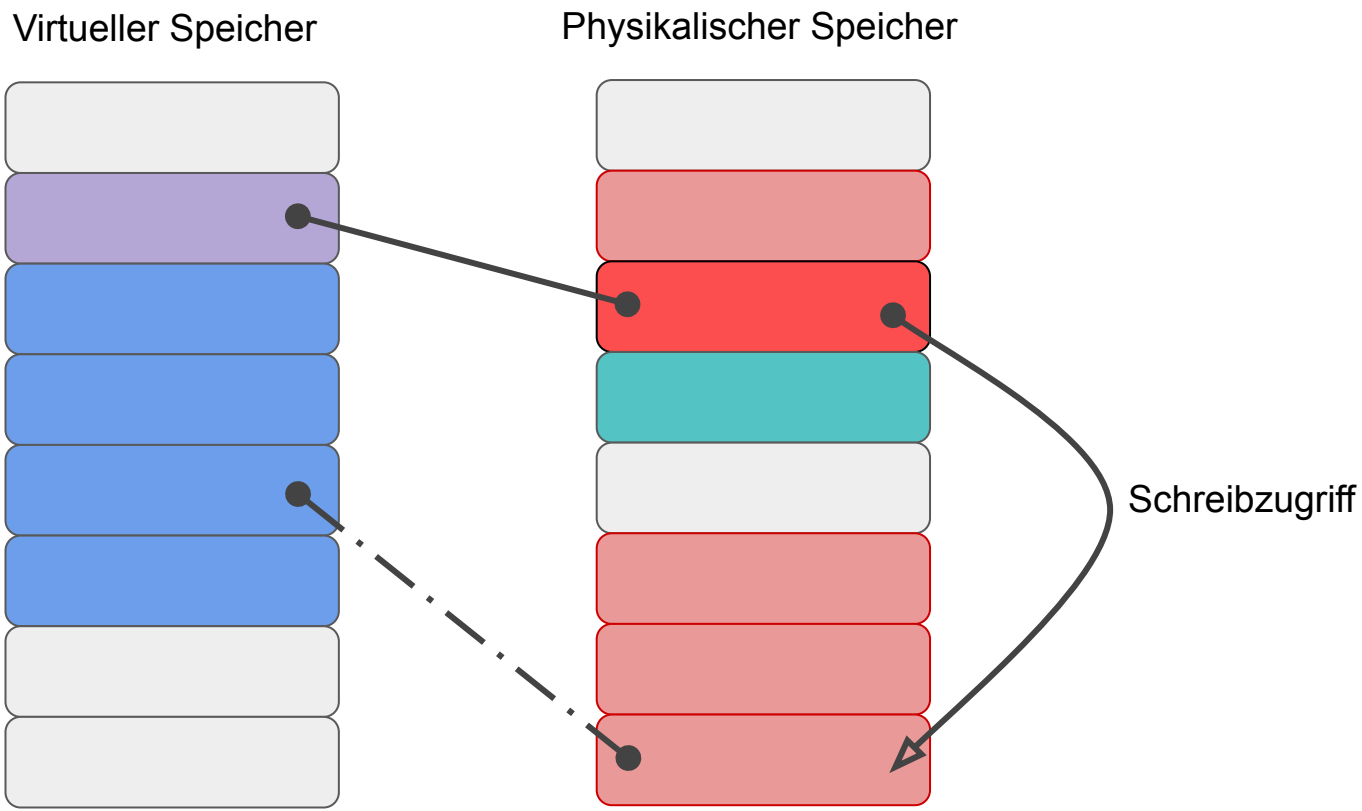

Virtueller Speicher
Physikalischer Speicher
0 1 1
0 0 0
0 0 1
0 1 0
0 1 1
…
…
1 1 1

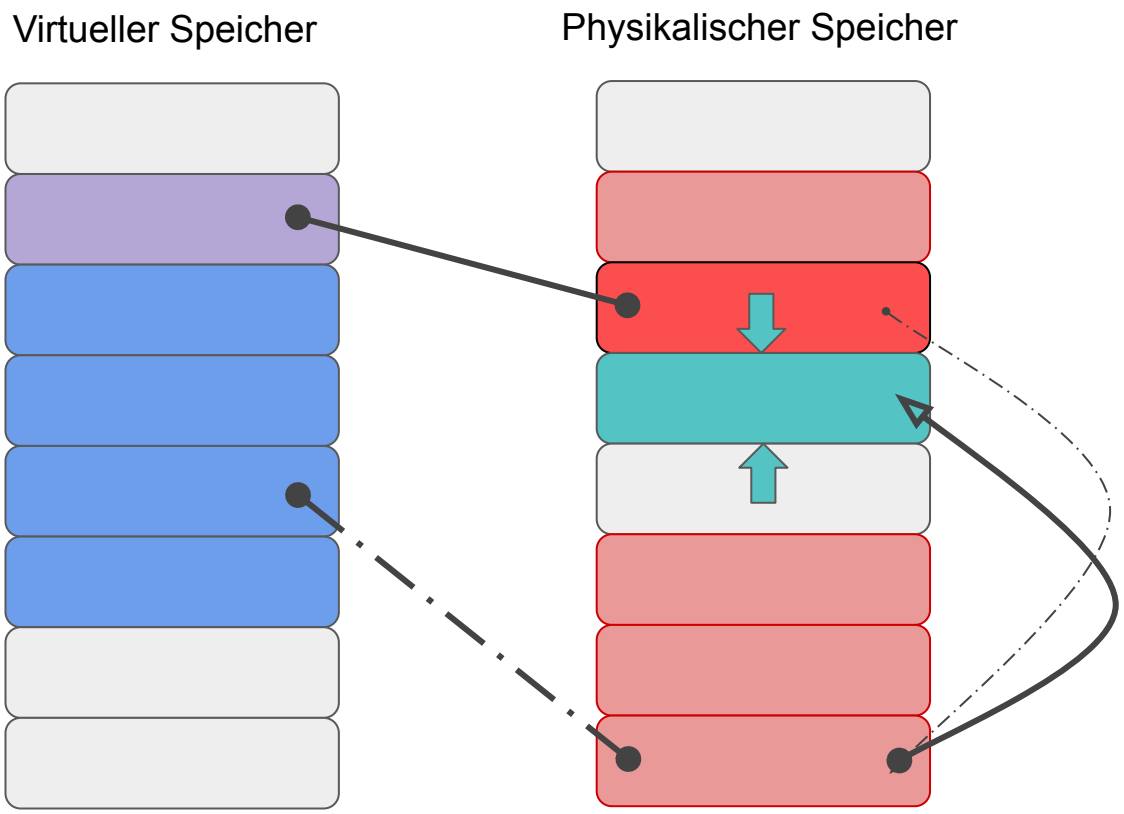

Virtueller Speicher
Physikalischer Speicher
0 0 0
0 0 1
1 1 1
0 1 0
0 1 1
...
...
1 1 1

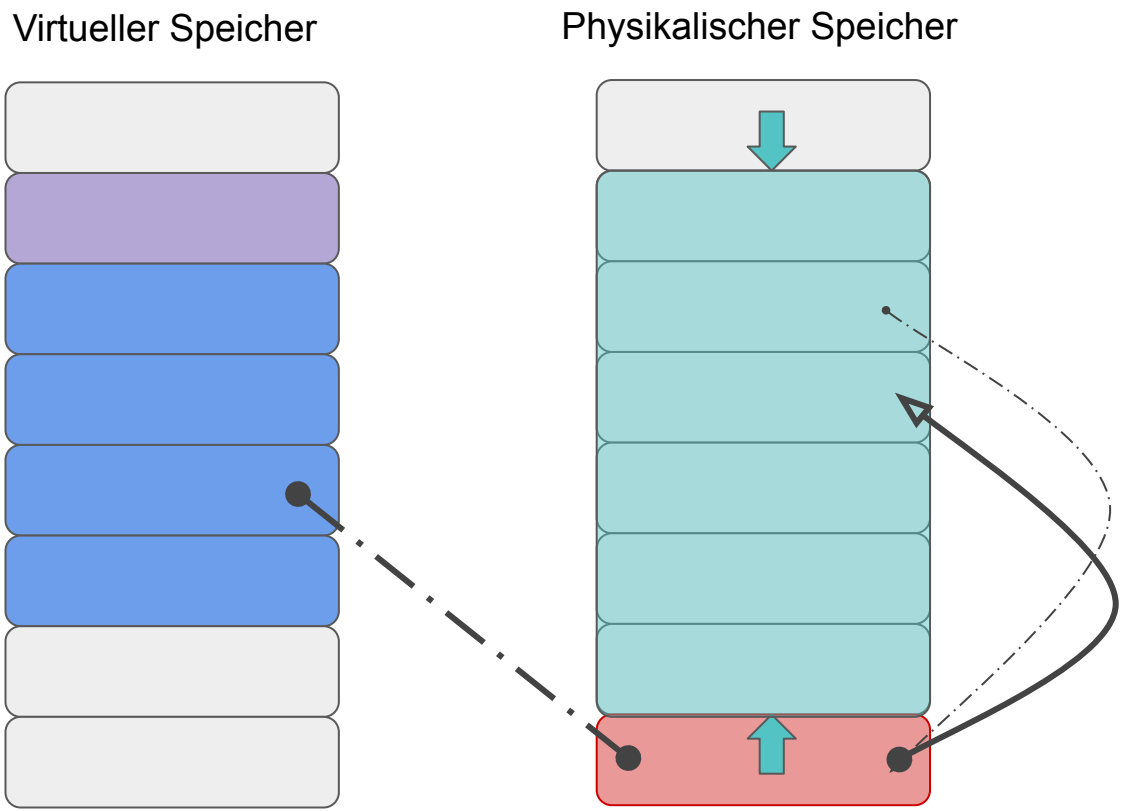

Virtueller Speicher
Physikalischer Speicher
1 1 1

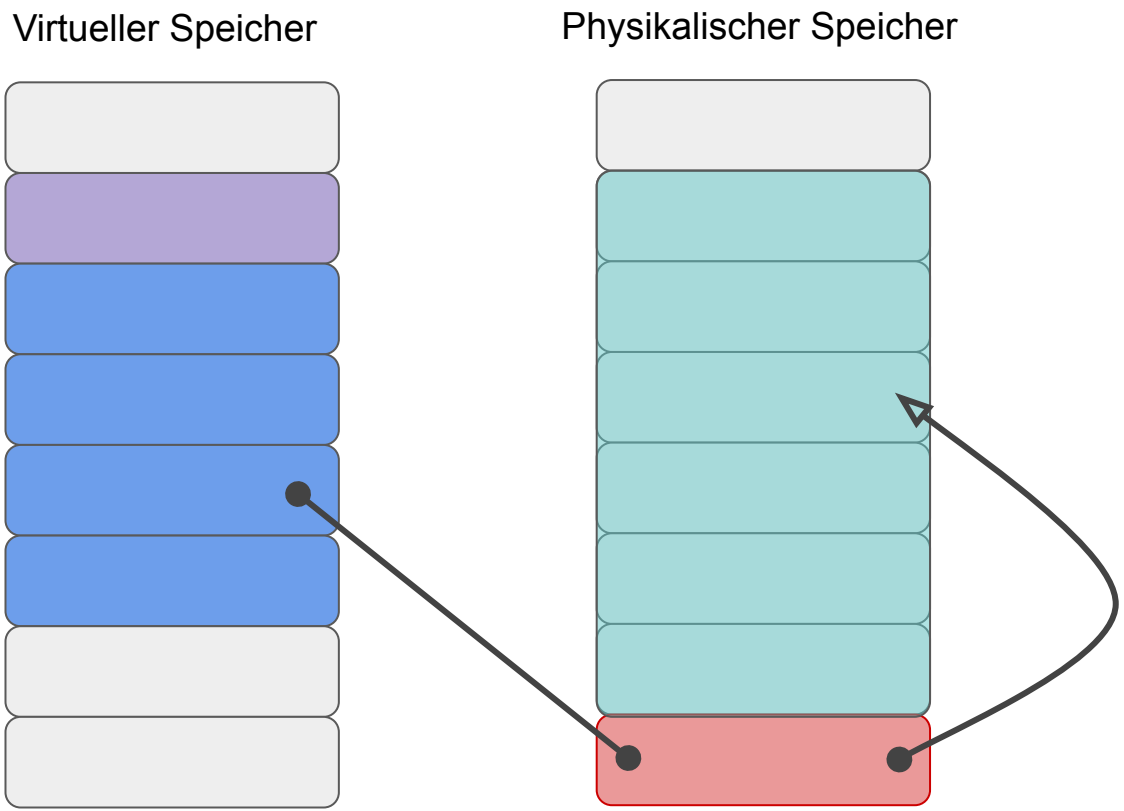

Virtueller Speicher
Physikalischer Speicher
1 1 1


Virtueller Speicher
Physikalischer Speicher


Virtueller Speicher
Physikalischer Speicher
Schreibzugriff


Virtueller Speicher
Physikalischer Speicher


Virtueller Speicher
Physikalischer Speicher


Virtueller Speicher
Physikalischer Speicher

Rowhammer in der Realität

Throwhammer

- Remote-Angriff über Netzwerk daher Throwhammer (inspiriert von Thor)
- Ziel: Cloud-Services (aws)
- Vorrausetzungen:
  1. 10 Gbit/s Netzwerkanbindung
  2. Einen normalen Userzugang
  3. zusammenhängenden Speicher allokieren
  4. abwechselnd mit einsen und nullen füllen
- Schon hat man zugriff auf fremde speicher und kann Schabernack treiben

JS

Jackhammer.js

Attacke über Browser mit JavaScript

Problem:

- JavaScript keine Pointer & keine Funktion Speicher direkt zu allokieren

Lösung:

- Große Arrays werden als 2MB Pages allokiert (Browser-abhängig)
- Nun kann wiederholt über das Array iteriert werden um ein Bit zu flippen

Vorsicht welche Webseiten ihr besucht

Firefox Add-ons Blog | Extension Workshop | Developer Hub | Log in

Firefox Browser ADD-ONS

Extensions | Themes | More...

java-script

177 results found for "java-script"

Filter results

Sort by

Relevance

Add-on Type

All

Search results

NoScript Security Suite Recommended

341,701 users

The best security you can get in a web browser! Allow potentially malicious web content to run only from sites you trust. Protect yourself against XSS other web security exploits.

Giorgio Maone

Schutz gegen Rowhammer

Bessere Chips bauen

1. Eine andere Art von Ram erfinden
2. Bei der Herstellung prüfen
   - extrem aufwendig = kostspielig
3. Software zur Überprüfung ausliefern

Kaputte Zellen auf Ersatzzellen auslagern

ECC (Error Correction Code)

gerade Anzahl an Einsen

0	1	1	0
1	0	1	0
1	1	1	1
0	0	0	0

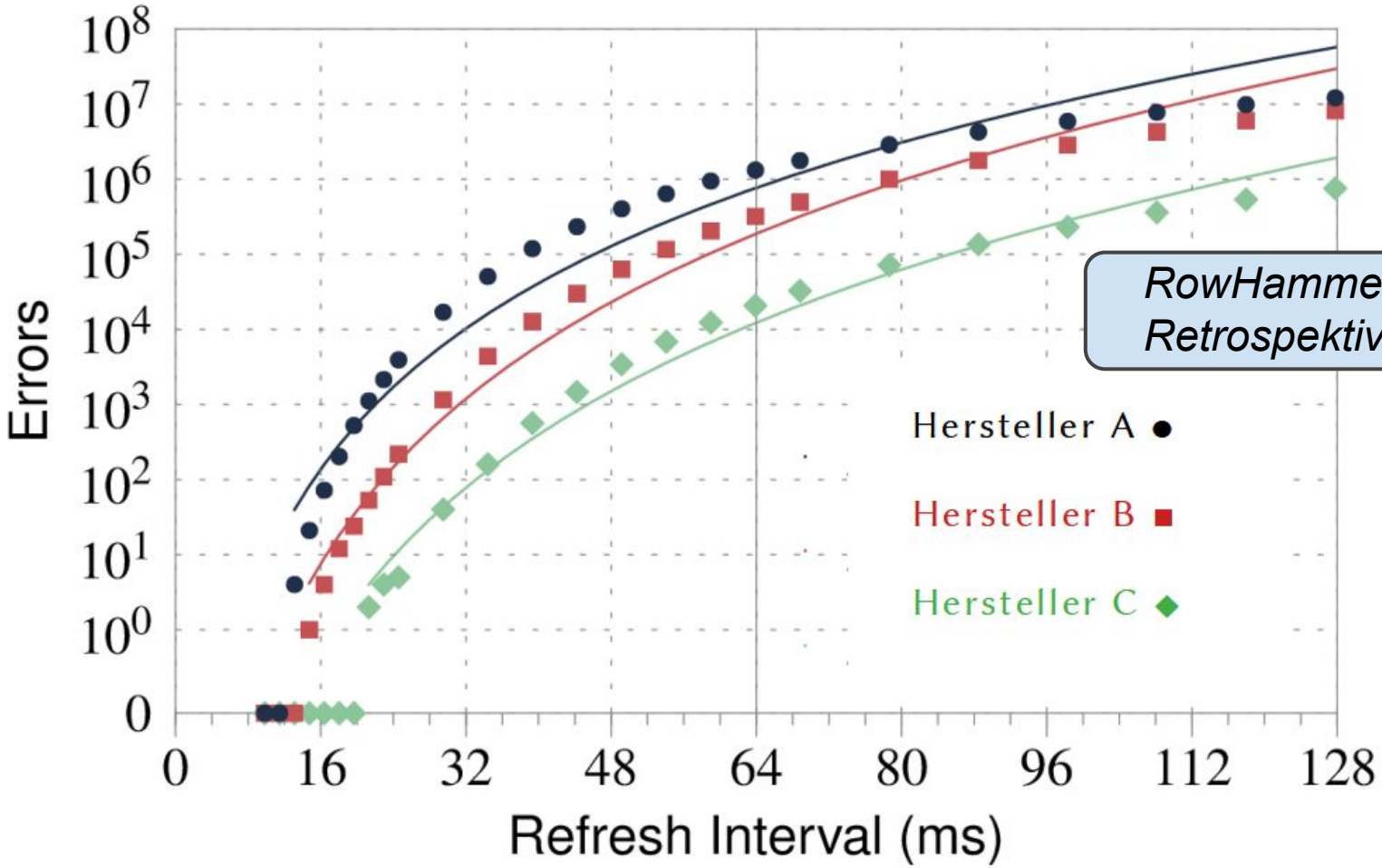
ECC (Error Correction Code)

Kontroll-bit
falsch

0	1	1	0
1	0	1	0
1	1	1	1
0	0	1	0

bit-flip

Erhöhung der Refresh Rate



RowHammer: a Retrospektive

Fazit

- Keine Attacken bekannt
- DDR4 > DDR3
- Gefahr steigt für die Zukunft

google / rowhammer-test Public

Watch 81

Code | Pull requests | Actions | Projects | Security | Insights

master | Go to file | Add file | Code

Mark Seaborn cached_rowhammer.cc: Remove unused c... ... on 11 Aug 2015 73

cache_analysis	Cache analysis: Display miss table for an atte...	7 years ago
cached_rowhammer	cached_rowhammer.cc: Remove unused code	7 years ago
docs	Notes: Add further note about "Active-Precha...	7 years ago
dram_physaddr_map...	Add script that analyses physical addresses o...	7 years ago
extended_test	rowhammer_test: Clean up logging for the "c...	7 years ago
physmem_alloc_anal...	Analyze contiguous physical memory chunks ...	7 years ago

Danke für eure Aufmerksamkeit

Quellen

https://luis-stumpf.github.io/bsys-vortrag/

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

https://arxiv.org/pdf/1904.09724.pdf

https://googleprojectzero.blogspot.com/2015/03/exploiting-dram-rowhammer-bug-to-gain.html