Daten löschen, aber richtig
Über die Besonderheiten von SSDs

Alexander Neumann - RedTeam Pentesting GmbH
alexander.neumann@redteam-pentesting.de
https://www.redteam-pentesting.de

LeetCon, Hannover, 2. November 2016

RedTeam Pentesting, Daten & Fakten

- ★ Gegründet 2004 in Aachen
- ★ Spezialisierung ausschließlich auf Penetrationstests
- ★ Weltweite Durchführung von Penetrationstests
- ★ Forschung im Bereich der IT-Sicherheit

Daten Löschen

Daten Löschen

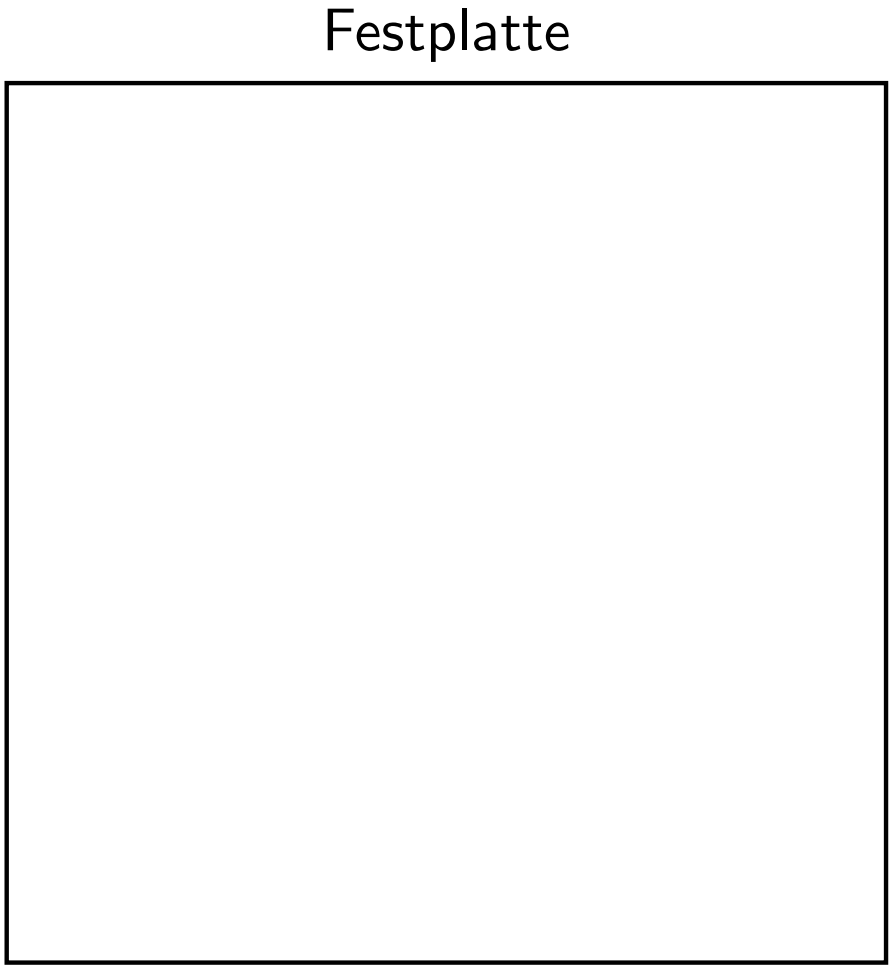
Definition Löschen

Für uns bedeutet „Löschen“:

- ★ Vernichten/„unwiederbringlich“
- ★ Auch ich selbst kann die Daten nicht wiederherstellen

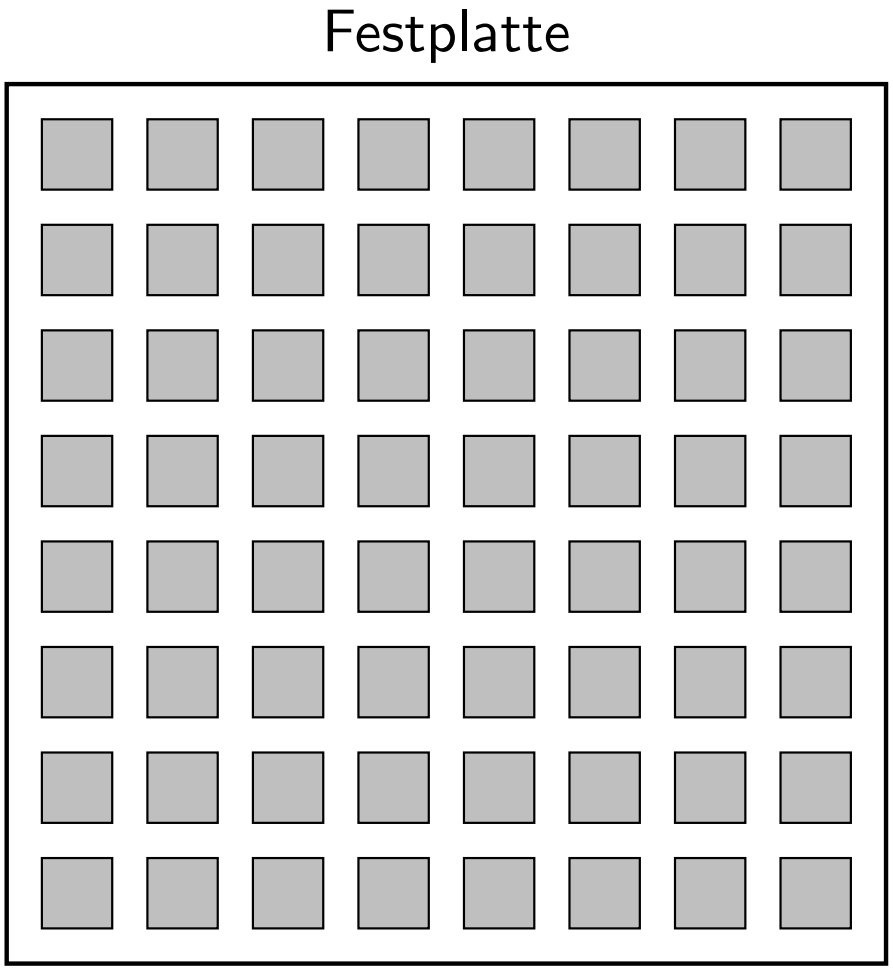
Einführung

- Festplatte
- Blöcke
- Partitionen
- Datei A
- Datei B
- Datei C
- Datei D



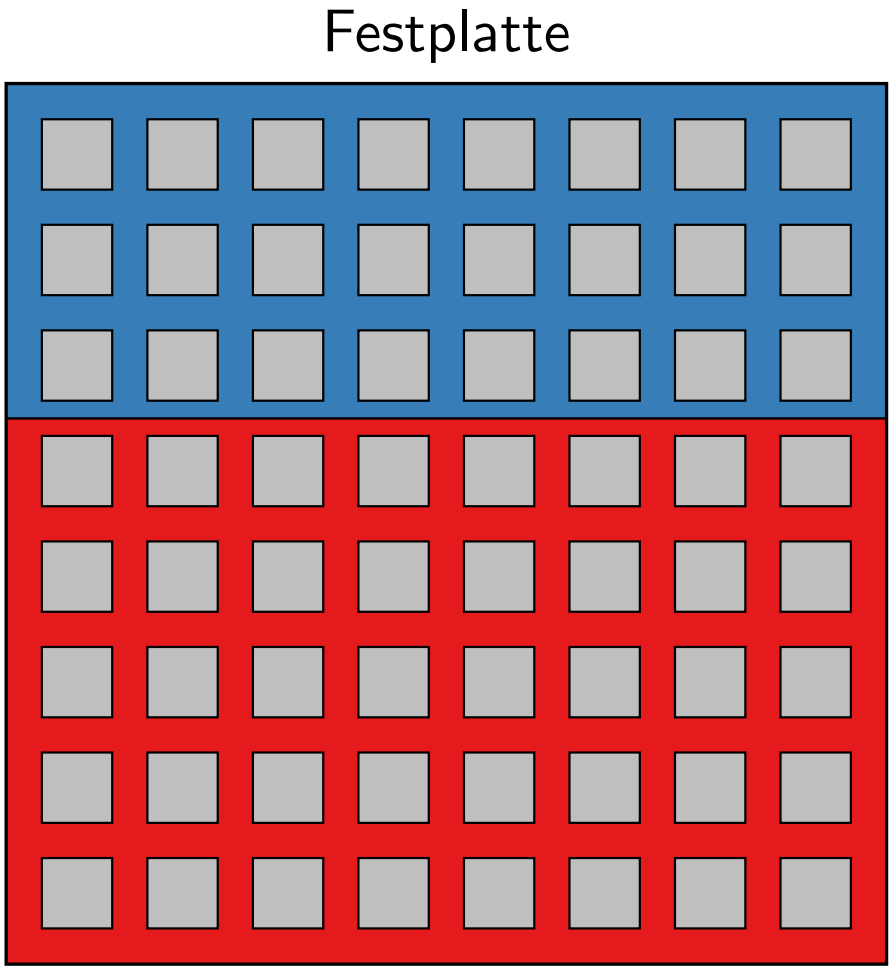
Einführung

- ★ Festplatte
- ★ Blöcke
- ★ Partitionen
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D



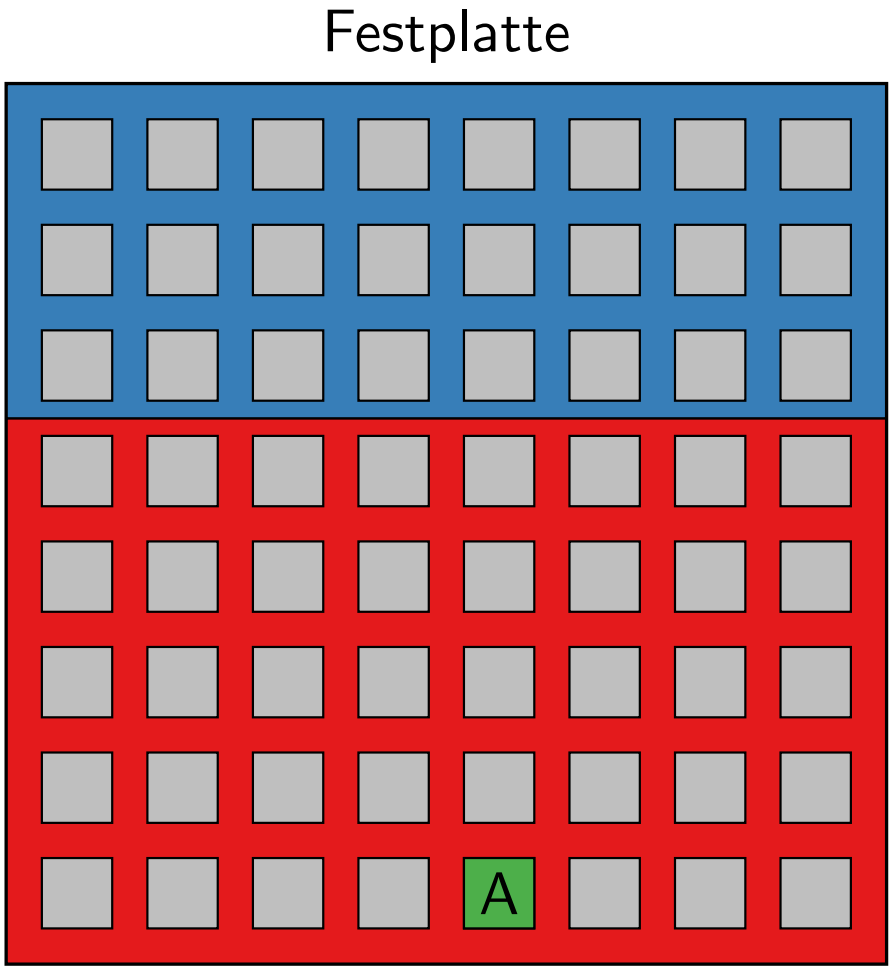
Einführung

- ★ Festplatte
- ★ Blöcke
- ★ Partitionen
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D



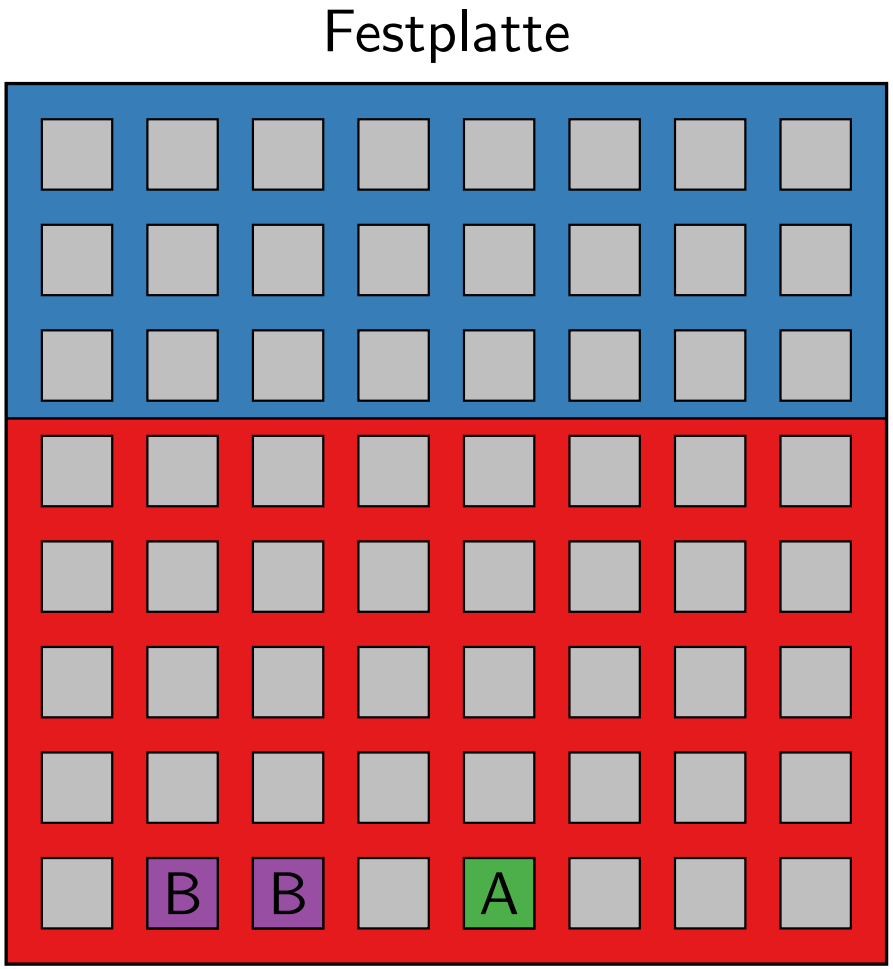
Einführung

- ★ Festplatte
- ★ Blöcke
- ★ Partitionen
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D



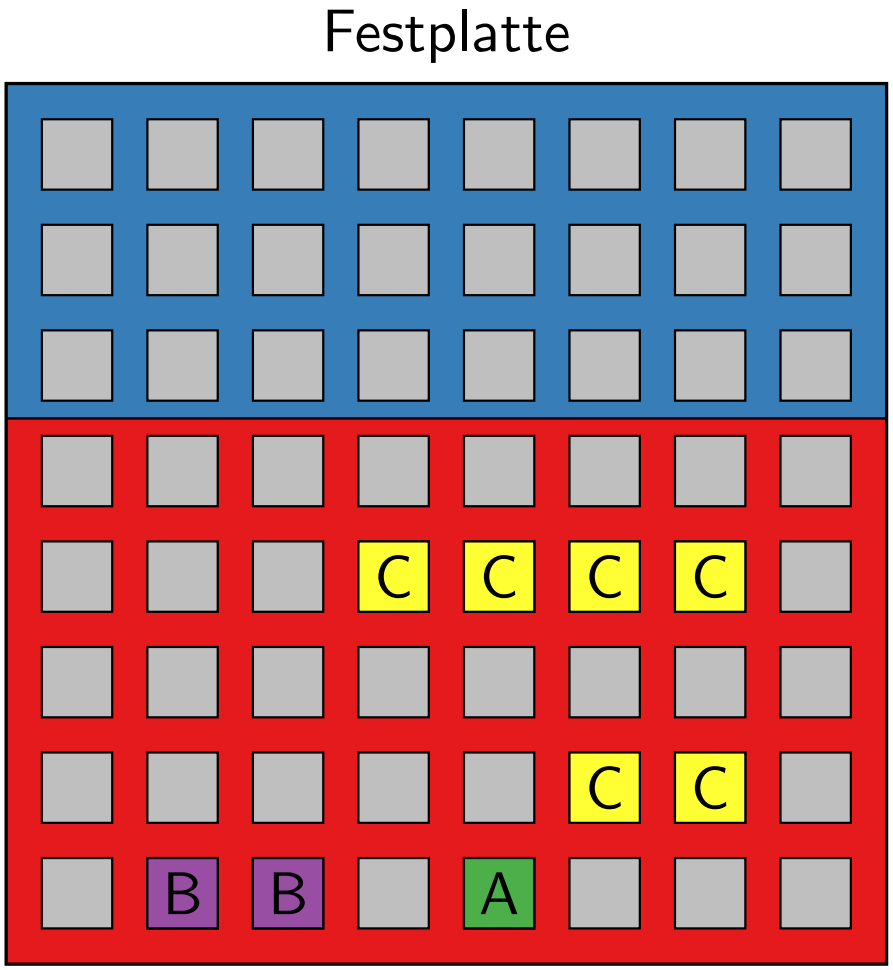
Einführung

- ★ Festplatte
- ★ Blöcke
- ★ Partitionen
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D



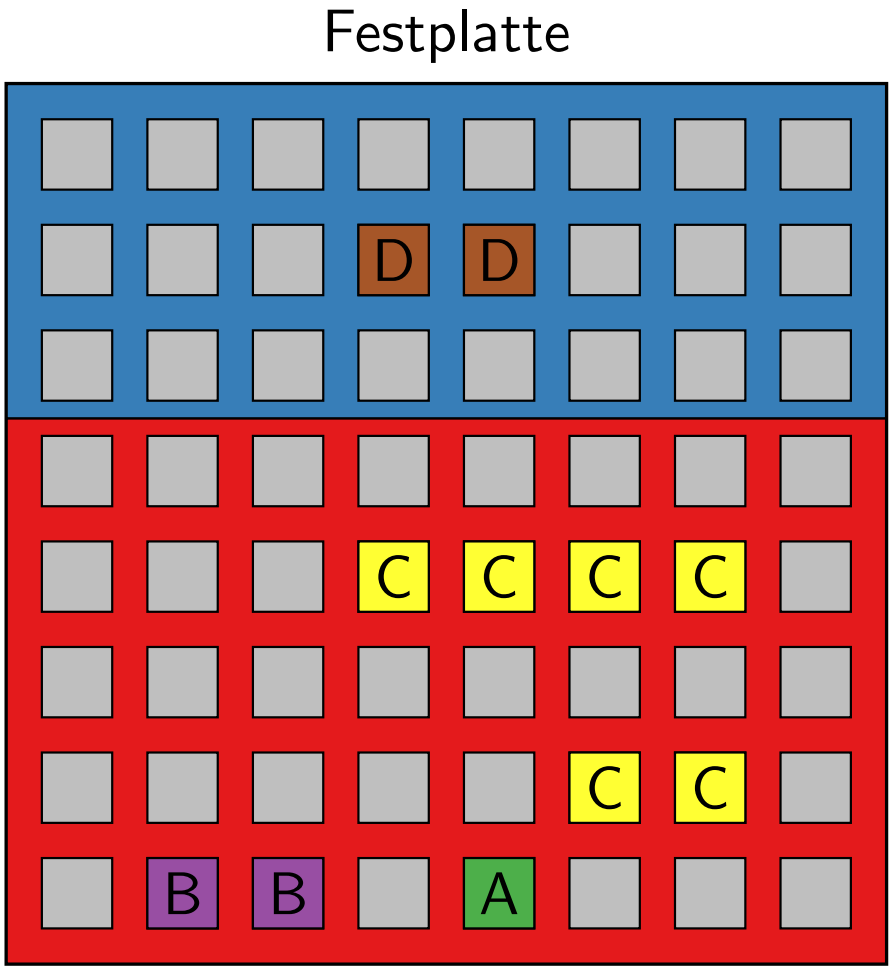
Einführung

- ★ Festplatte
- ★ Blöcke
- ★ Partitionen
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D



Einführung

- ★ Festplatte
- ★ Blöcke
- ★ Partitionen
- ★ Datei A
- ★ Datei B
- ★ Datei C
- ★ Datei D



Löschen von ganzen Festplatten

Standardverfahren für Festplatten:

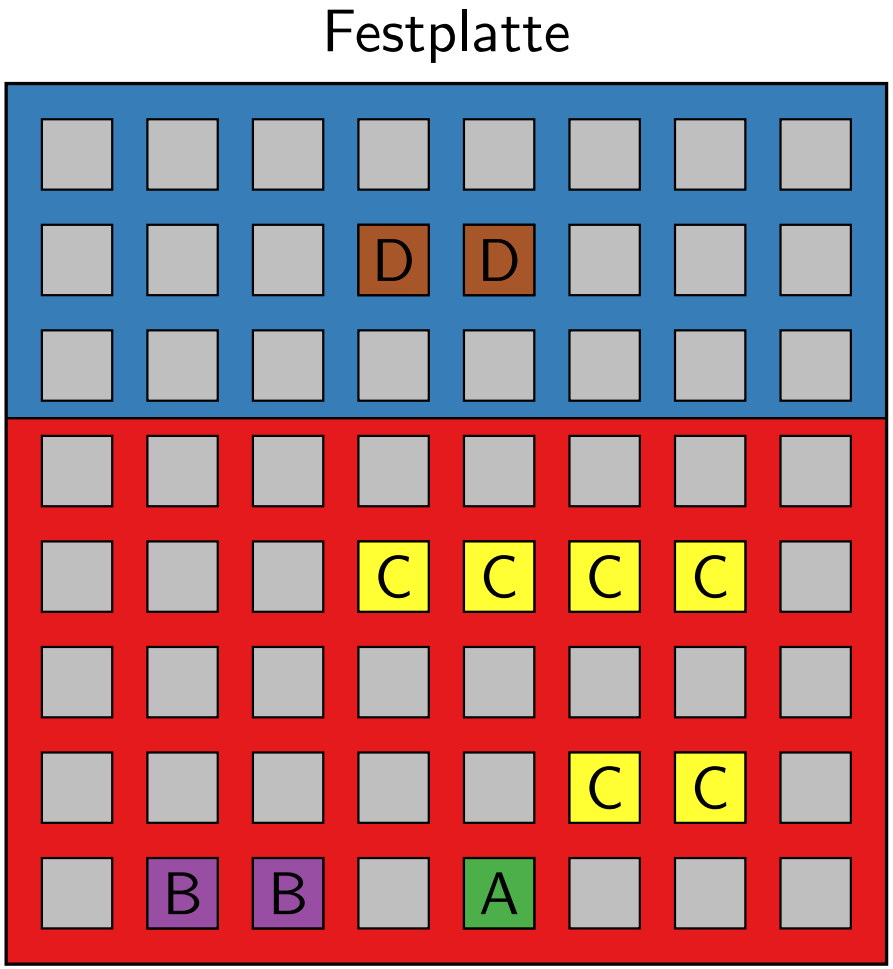
- ★ Überschreiben des gesamten Speichers
- ★ Löschfunktion des Datenträgers (ATA_SECURE_ERASE)
- ★ Physisches Zerstören

Daten löschen in Partitionen

- ★ Ein Partition enthält ein eigenes Dateisystem
- ★ Gut abgegrenzt auf der Festplatte, einfach zu erkennen welche Blöcke eine Partition enthält
- ★ Partition kann „am Stück“ überschrieben werden
- ★ Das entfernt alle Datenreste (temporäre Dateien, Metadaten)
- ★ Gut geeignet, um zu löschende Daten abzulegen

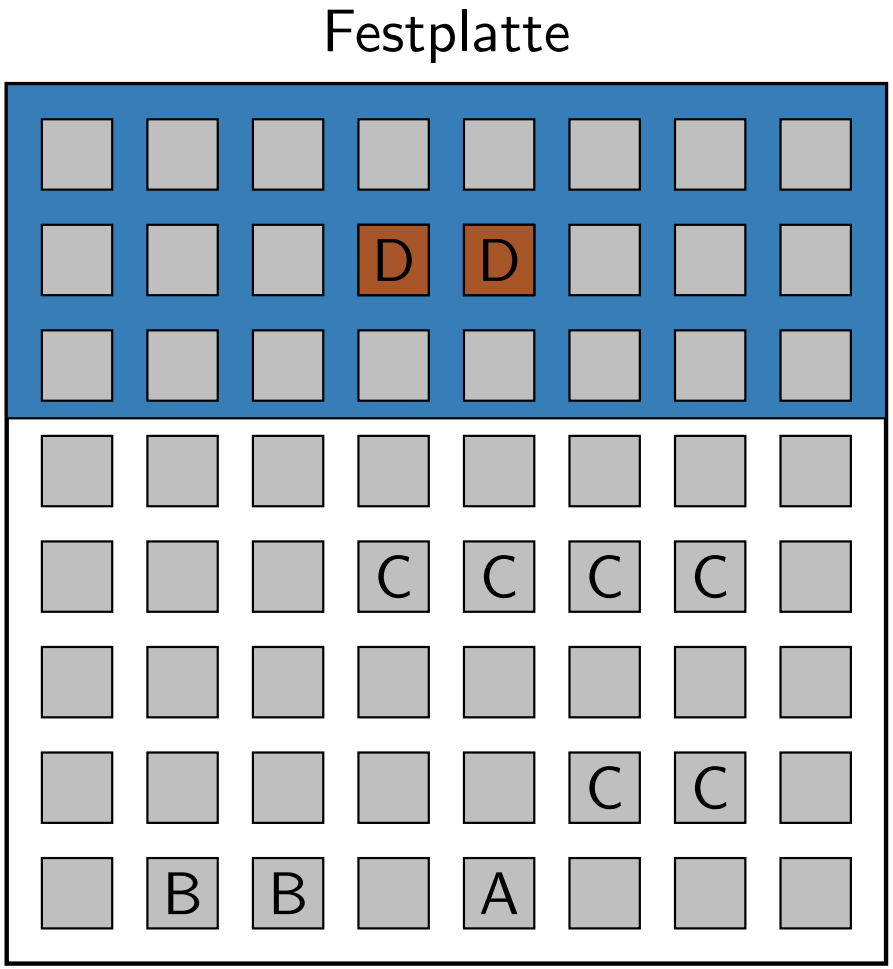
Daten löschen in Partitionen

Überschreibe Partition



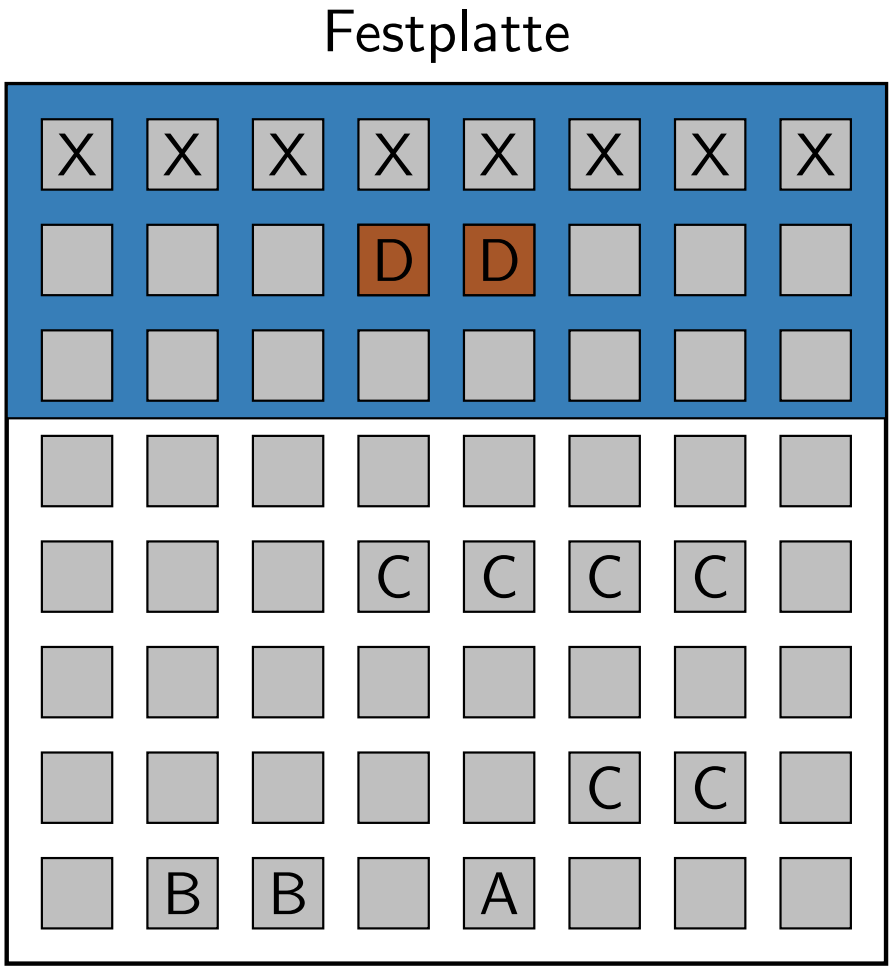
Daten löschen in Partitionen

Überschreibe Partition



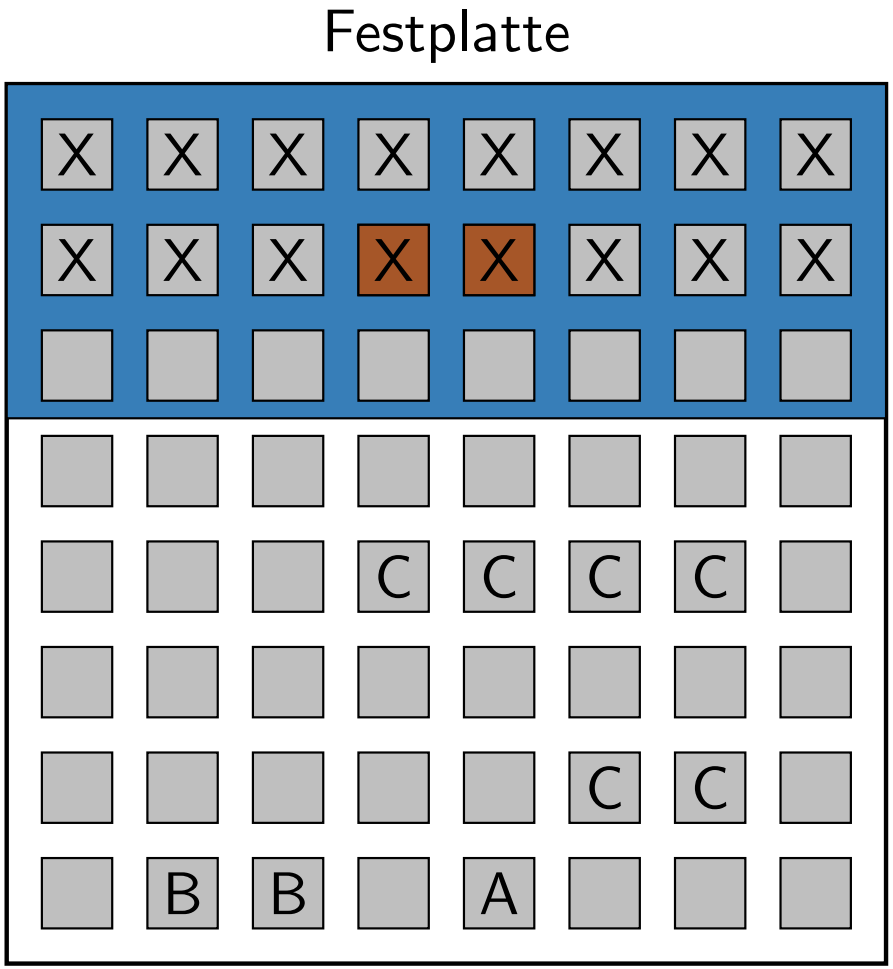
Daten löschen in Partitionen

Überschreibe Partition



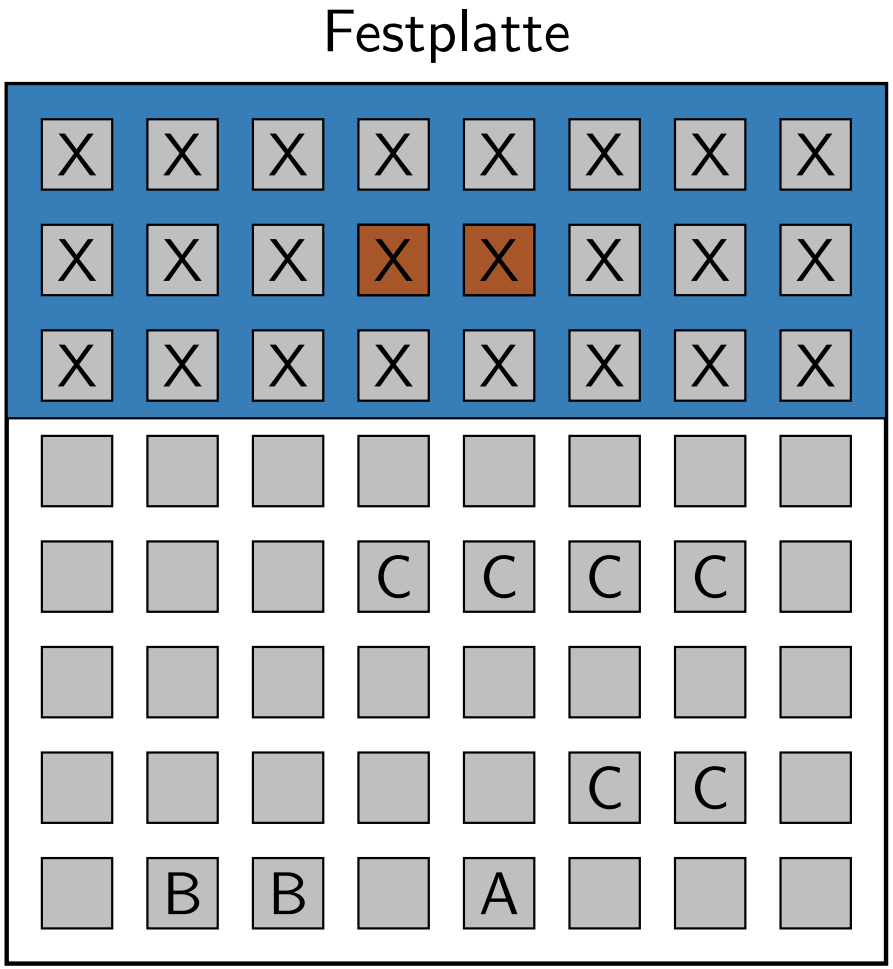
Daten löschen in Partitionen

Überschreibe Partition



Daten löschen in Partitionen

Überschreibe Partition



Dateien löschen

Verfahren für Dateien: Überschreiben mit anderen Daten

Problem: Wo liegen die Daten einer Datei genau?

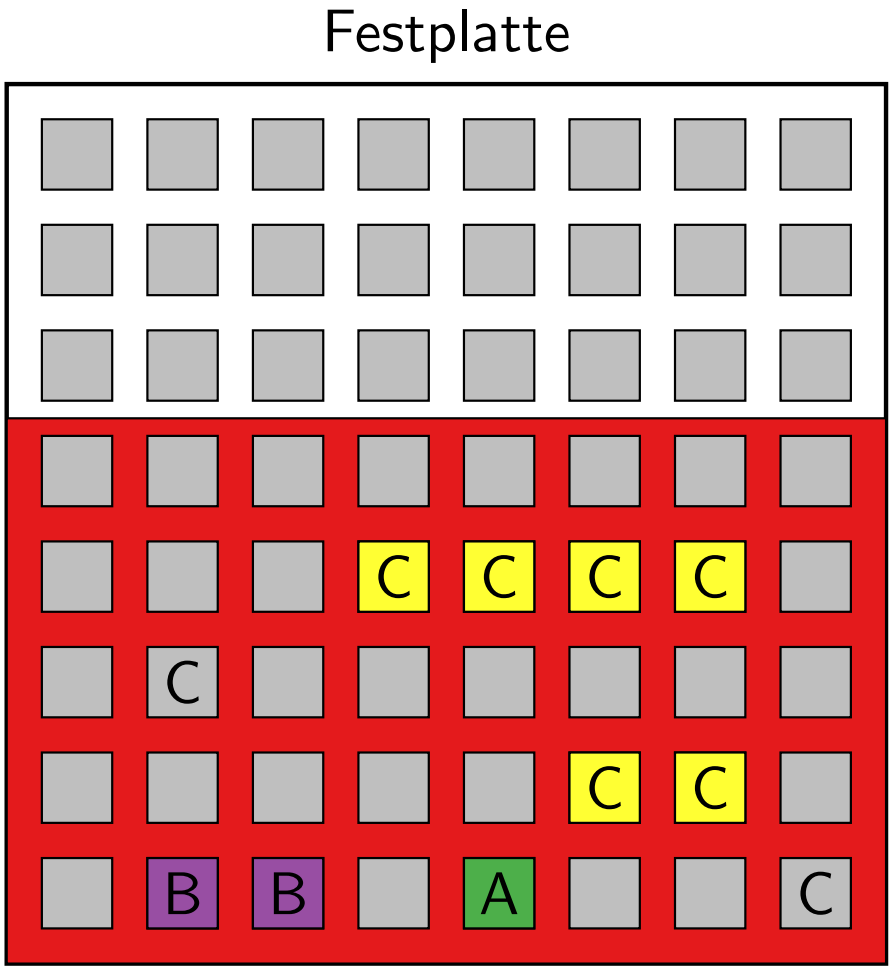
Probleme beim Löschen von Dateien

- ★ Dateisysteme bieten kein Interface, um einzelne Blöcke zu finden
- ★ Schwierig, genaue die richtigen Blöcke zu überschreiben
- ★ Temporäre Kopien werden nicht überschrieben, Dateien sind eventuell gar nicht mehr vorhanden
- ★ Metadaten wie Dateiname bleibt eventuell erhalten
- ★ Forensik macht sich dies zu nutze
- ★ Optimierungen (z.B. Journaling) erschweren das Überschreiben
- ★ Freier Speicher der Partition muss überschrieben werden

Dateien löschen

Lösche Datei C:

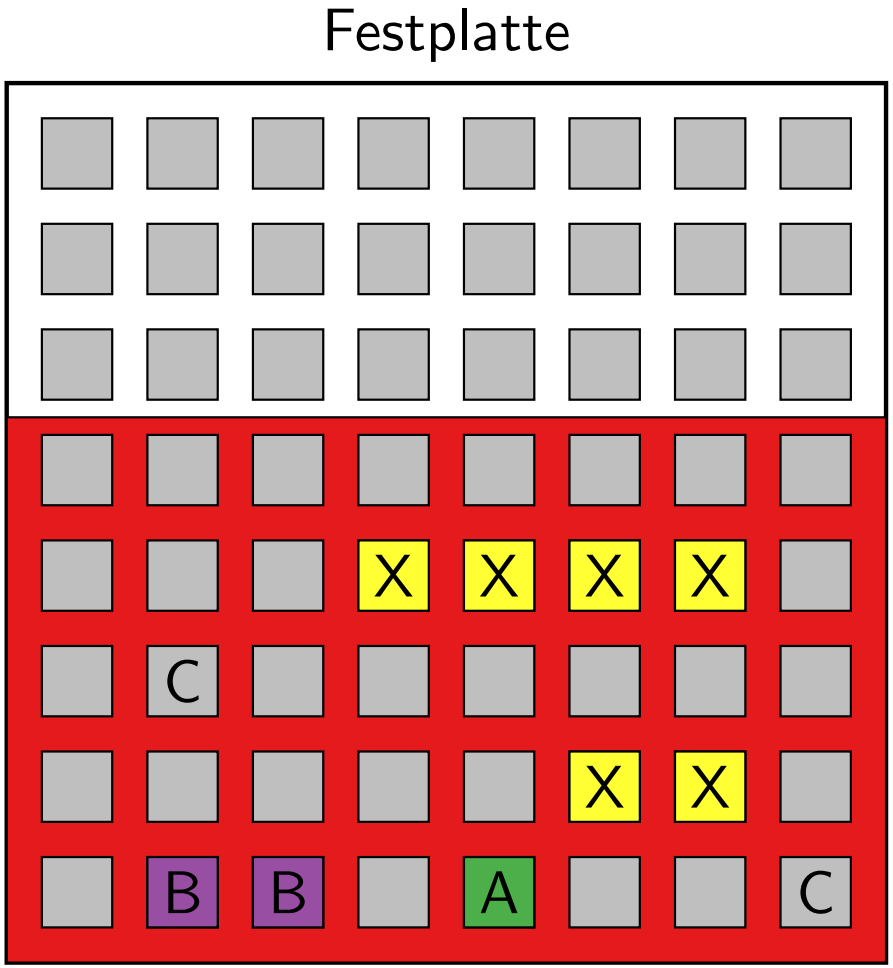
- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben



Dateien löschen

Lösche Datei C:

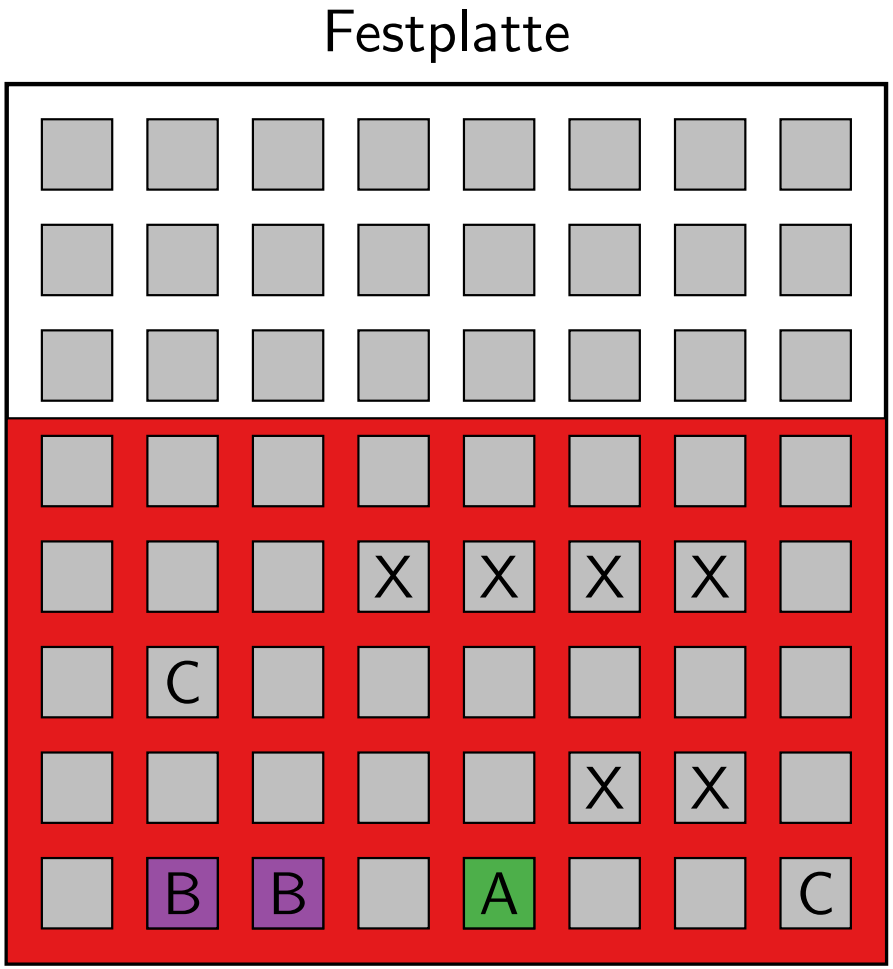
- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben



Dateien löschen

Lösche Datei C:

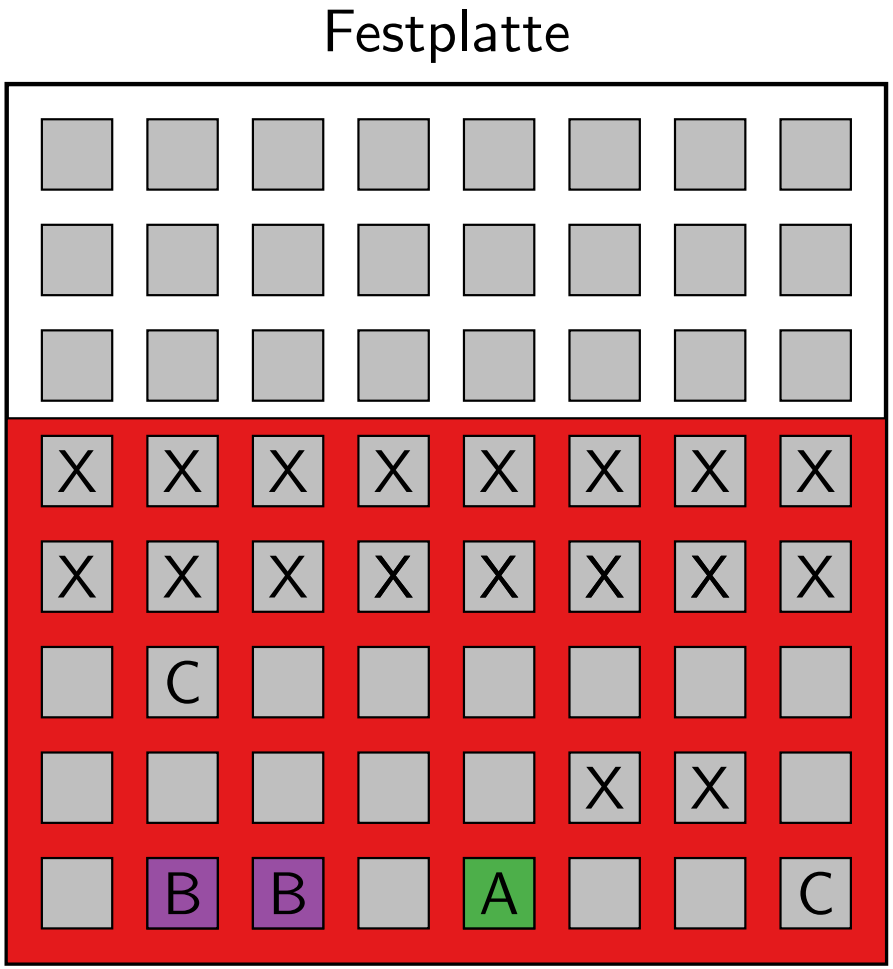
- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben



Dateien löschen

Lösche Datei C:

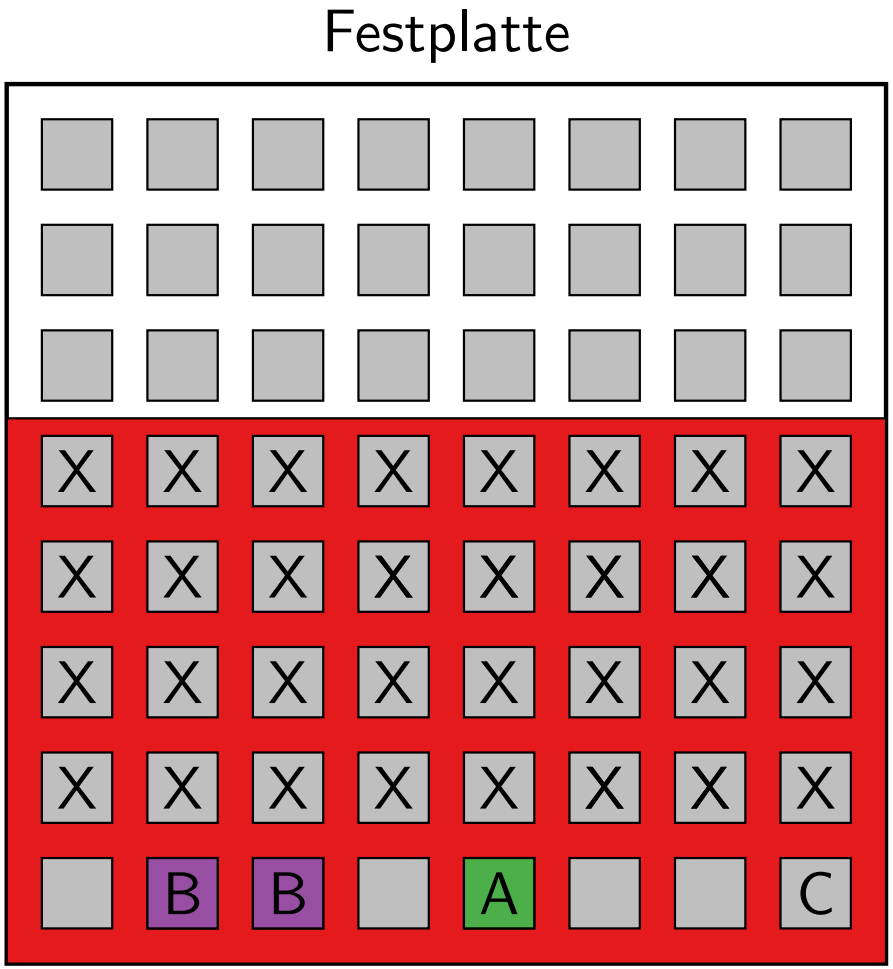
- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben



Dateien löschen

Lösche Datei C:

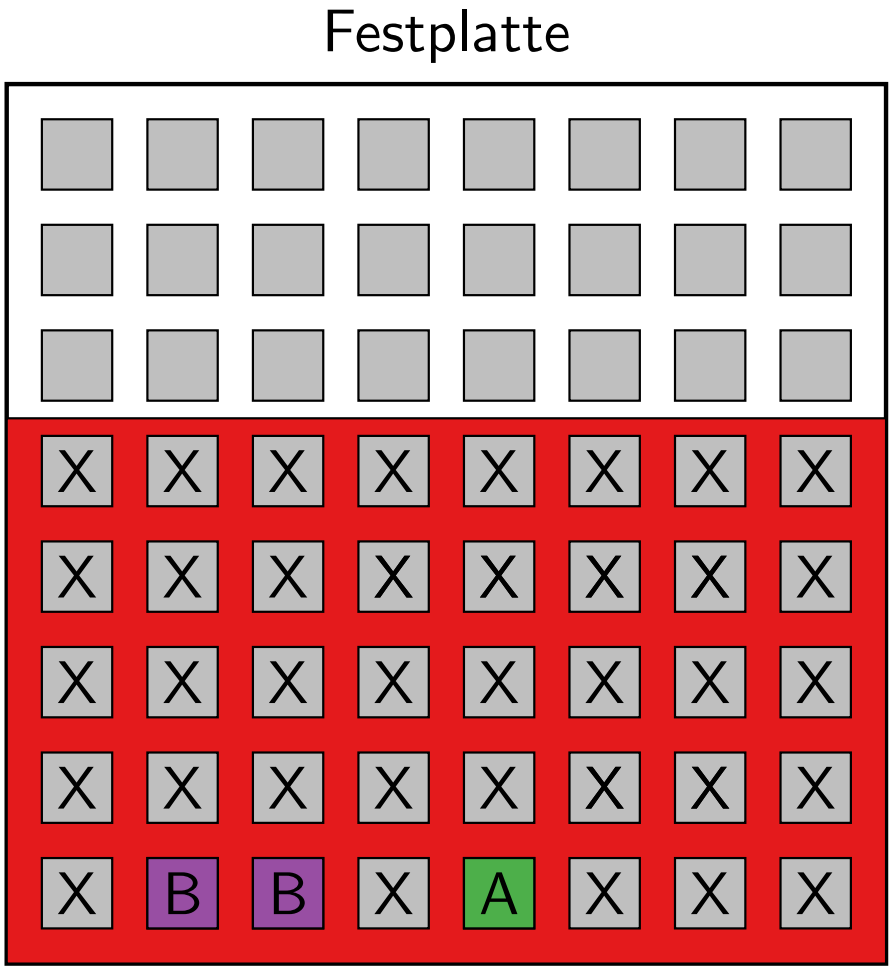
- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben



Dateien löschen

Lösche Datei C:

- ★ Blöcke überschreiben
- ★ Datei löschen
- ★ Freie Blöcke überschreiben



Zwischenfazit

- ★ Löschen von ganzen Datenträgern sicher und einfach
- ★ Löschen von Partitionen gut möglich, wenig Aufwand
- ★ Löschen von einzelnen Dateien schwierig
  (dabei bleiben meist Metadaten übrig)
- ★ Sicheres Löschen ist aufwendig aber möglich (einfacher bei guter Vorbereitung)

Einführung SSDs

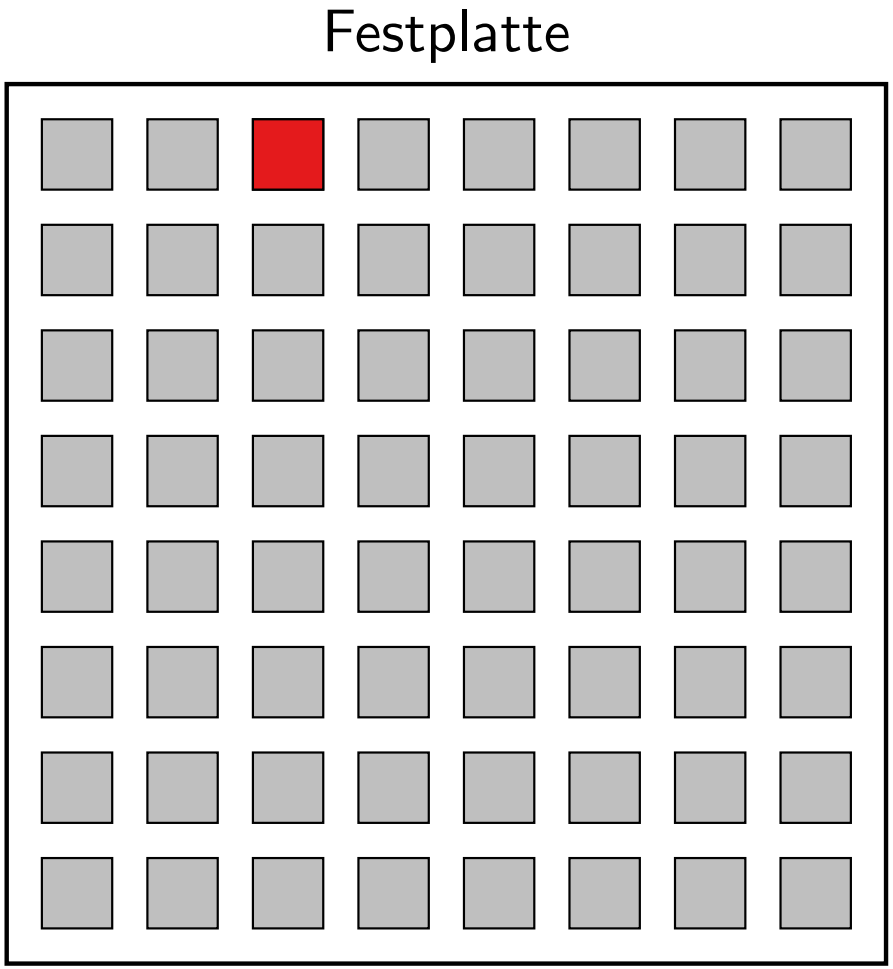
- ★ Flash-Speicher
- ★ Keine mechanischen Komponenten mehr beteiligt
- ★ Erschütterungsresistent
- ★ Wahlfreier Zugriff ohne Latenz
- ★ Sehr hohe Datentransferrate

Besonderheiten von SSDs

- ★ Over Provisioning: 5-20% mehr Speicher intern
- ★ Jeder Block kann nur ein mal geschrieben werden
- ★ Blöcke können nur seitenweise geleert werden
- ★ Wear Leveling: Gleichmäßige Nutzung des Flash-Speichers
- ★ Dazu: Flash Translation Layer (FTL)
- ★ Daten können nicht direkt gelesen werden

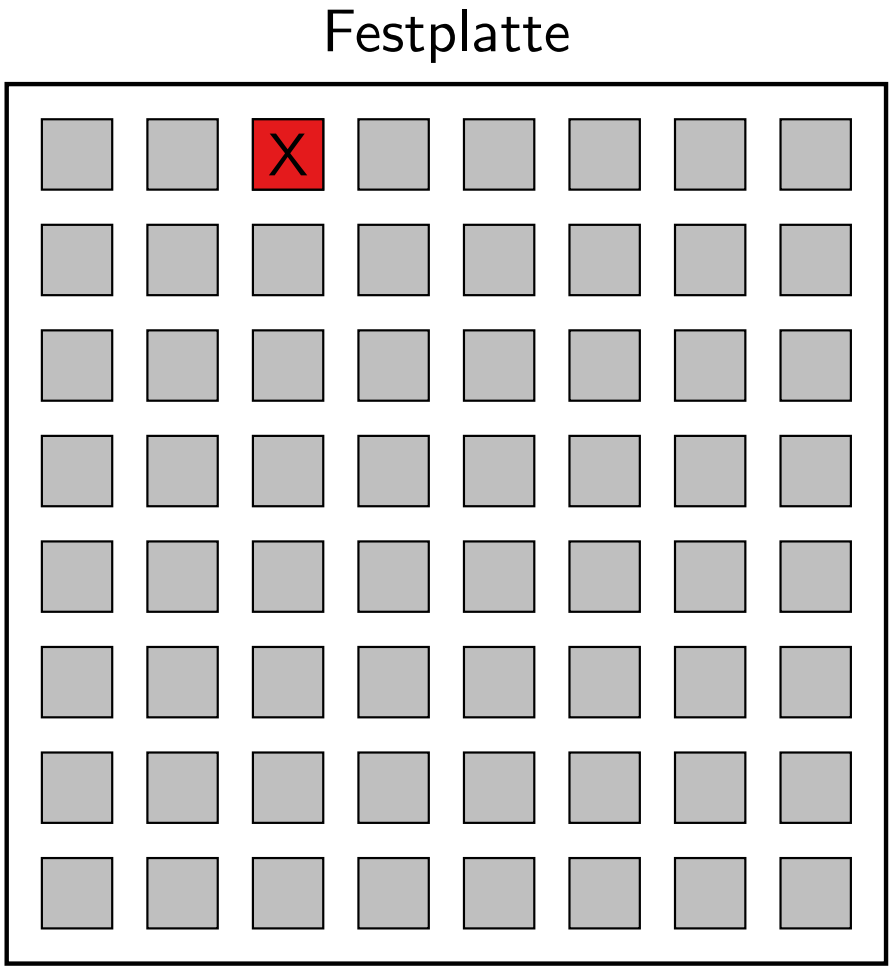
Schreiben von Blöcken einer Festplatte

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



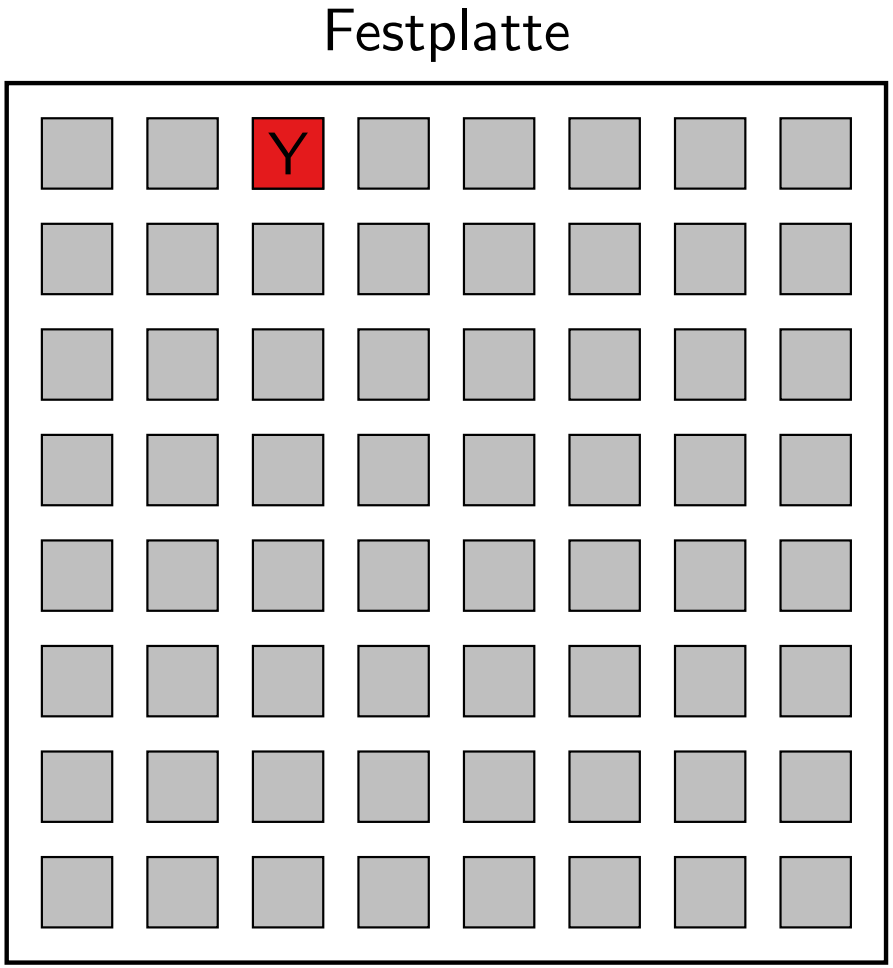
Schreiben von Blöcken einer Festplatte

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



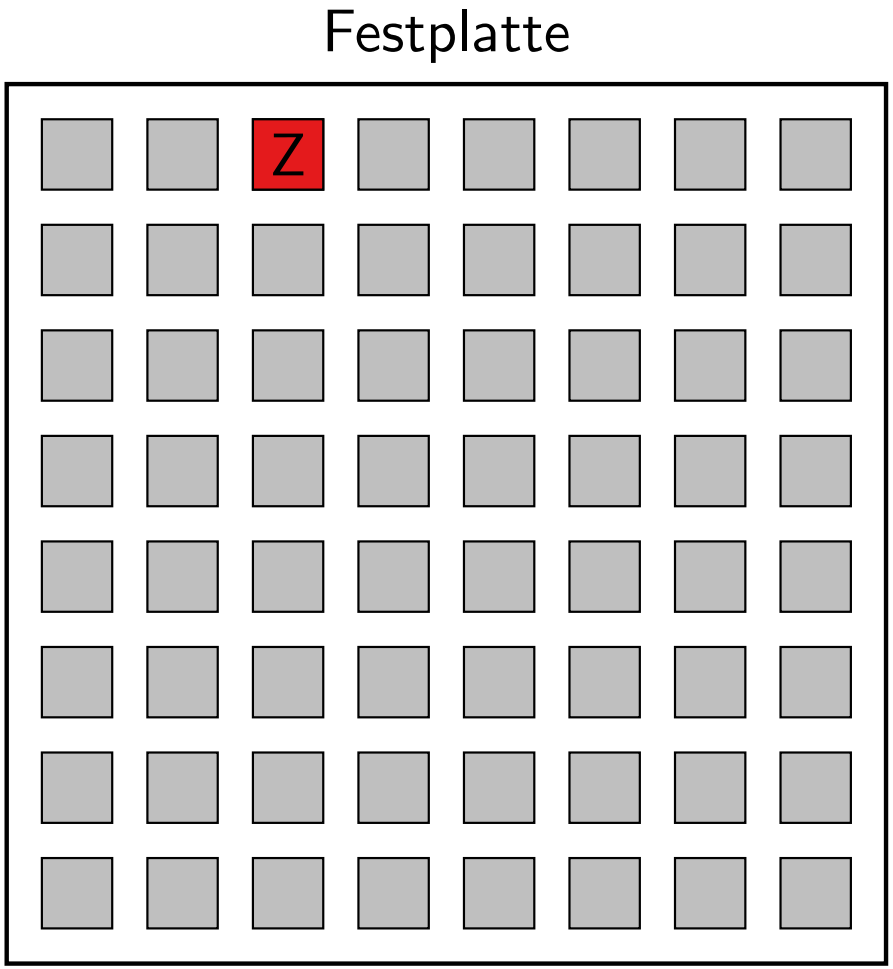
Schreiben von Blöcken einer Festplatte

- Schreibe „X“ in Block 3
- **Schreibe „Y“ in Block 3**
- Schreibe „Z“ in Block 3



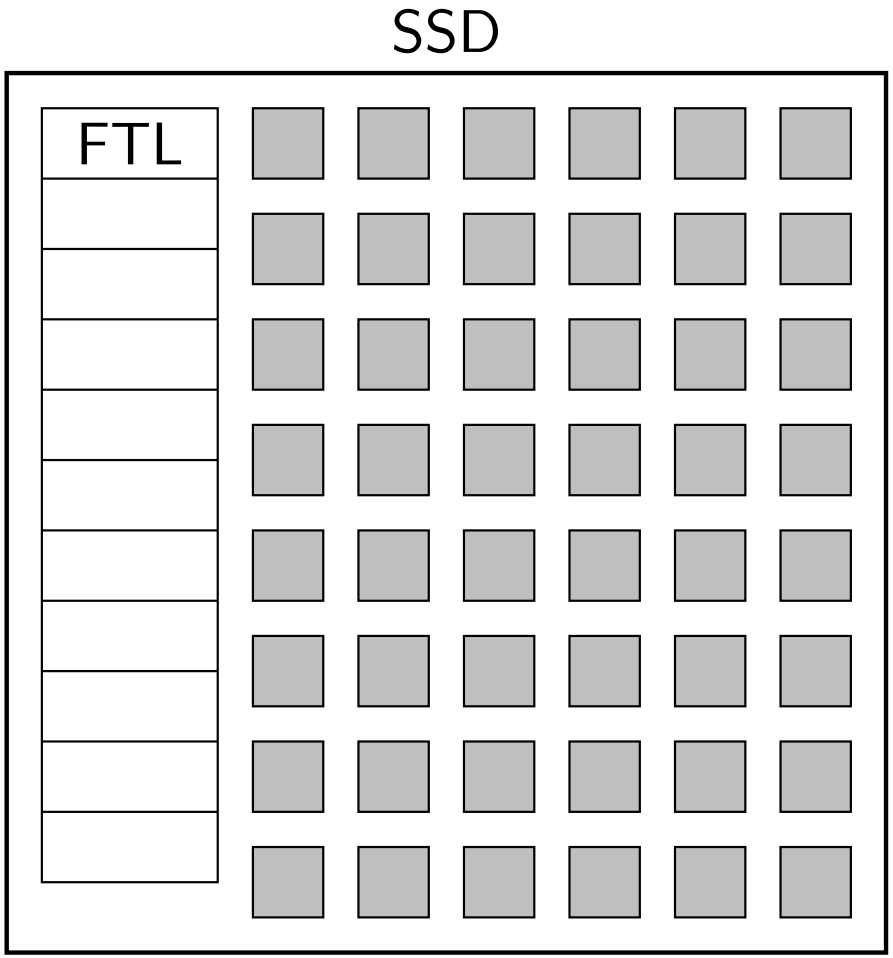
Schreiben von Blöcken einer Festplatte

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



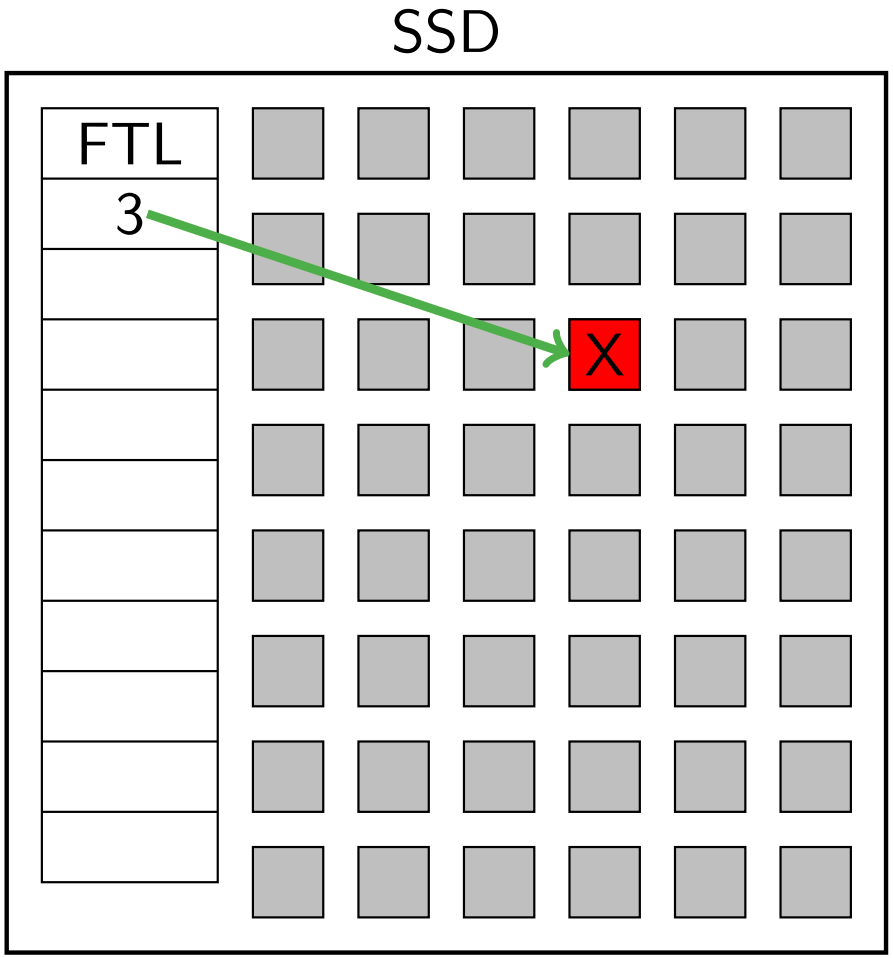
Flash Translation Layer (FTL)

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



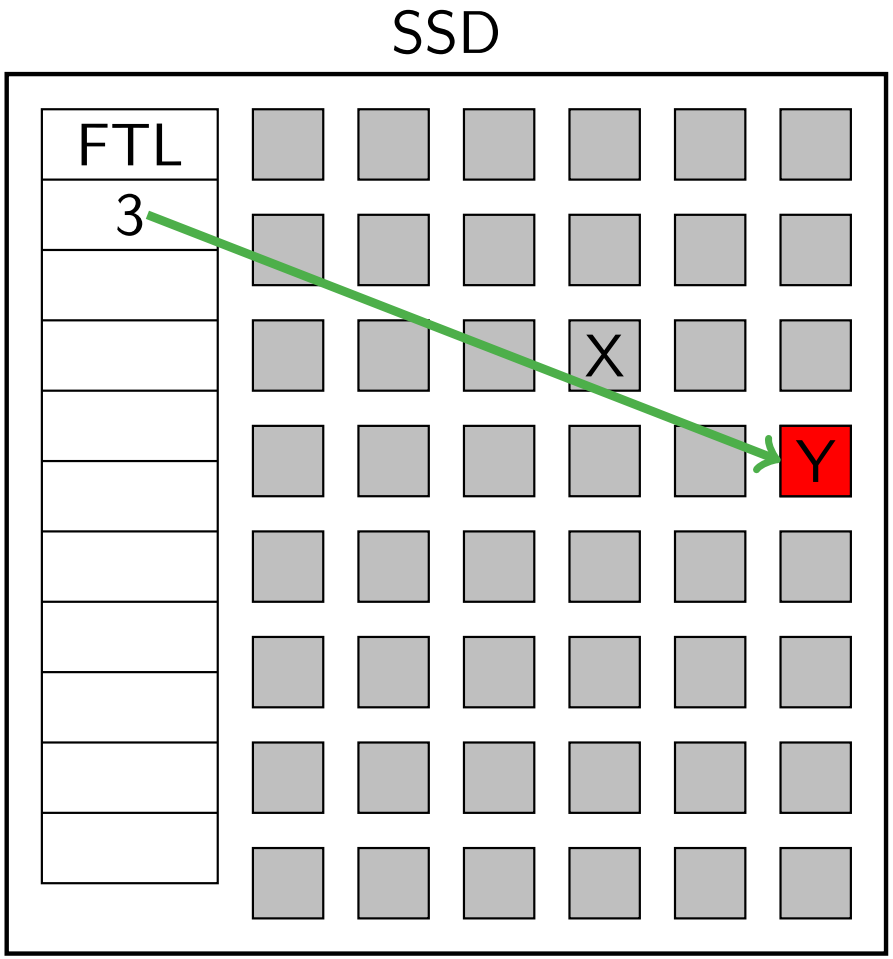
Flash Translation Layer (FTL)

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



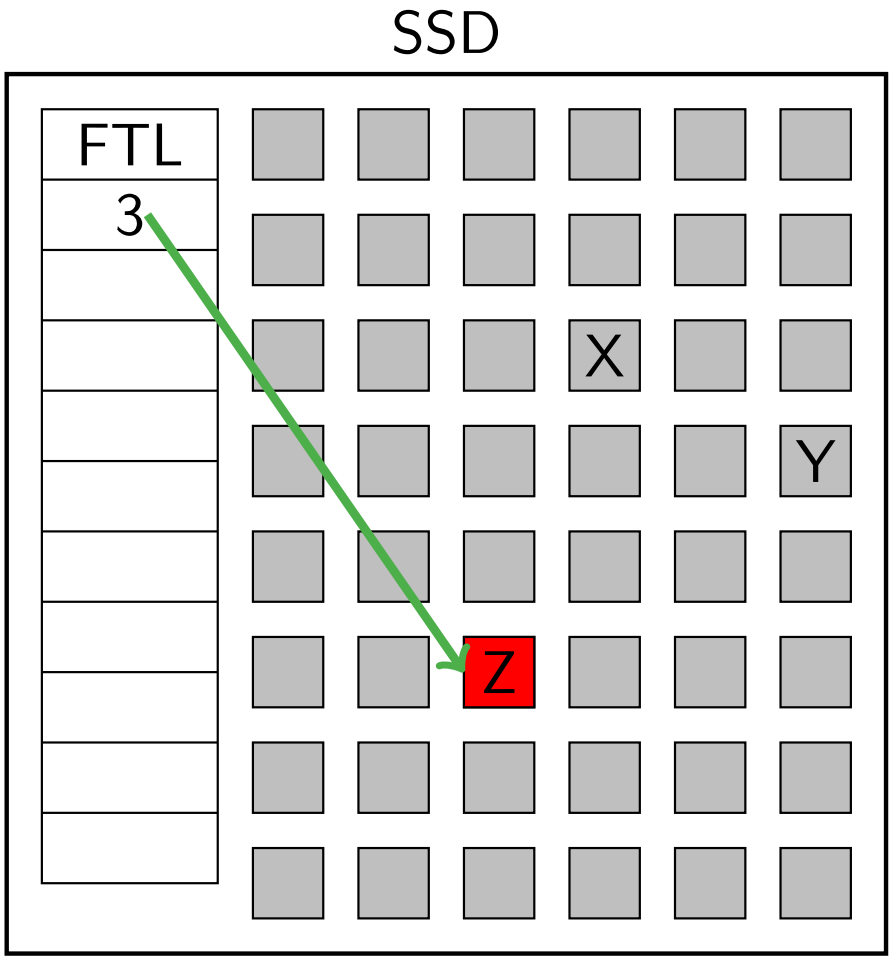
Flash Translation Layer (FTL)

- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



Flash Translation Layer (FTL)

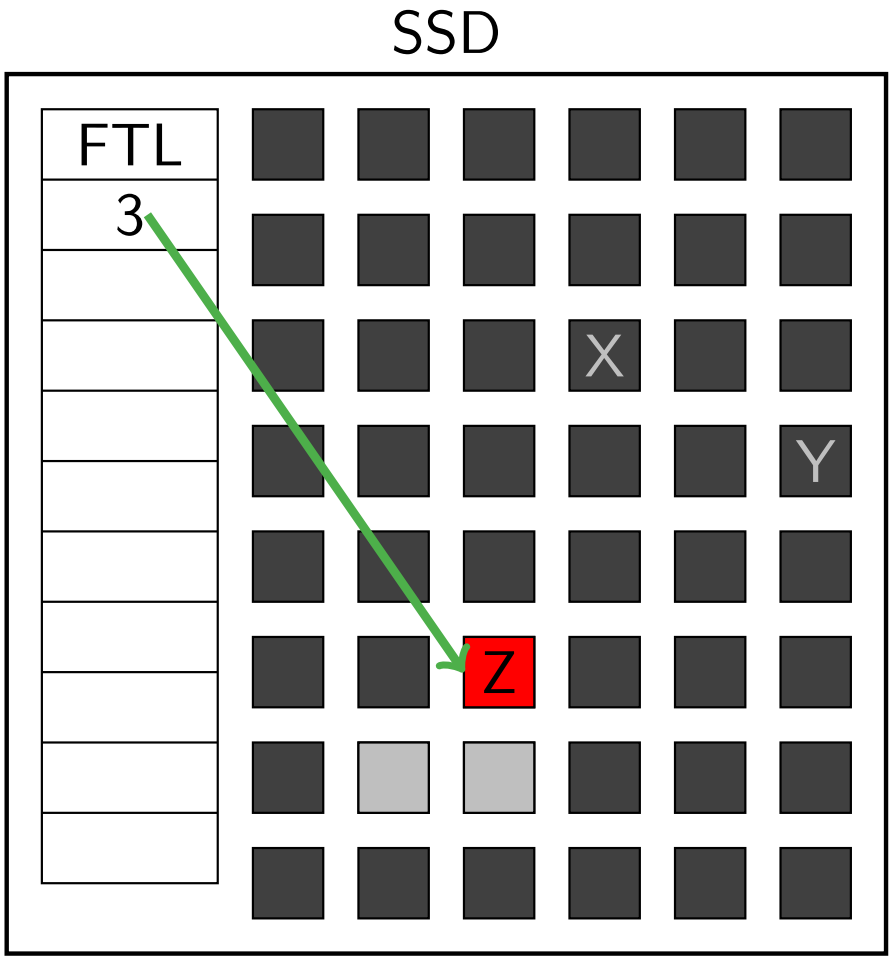
- ★ Schreibe „X“ in Block 3
- ★ Schreibe „Y“ in Block 3
- ★ Schreibe „Z“ in Block 3



Seitenweises Löschen von Blöcken

Schreibe 4 Blöcke:

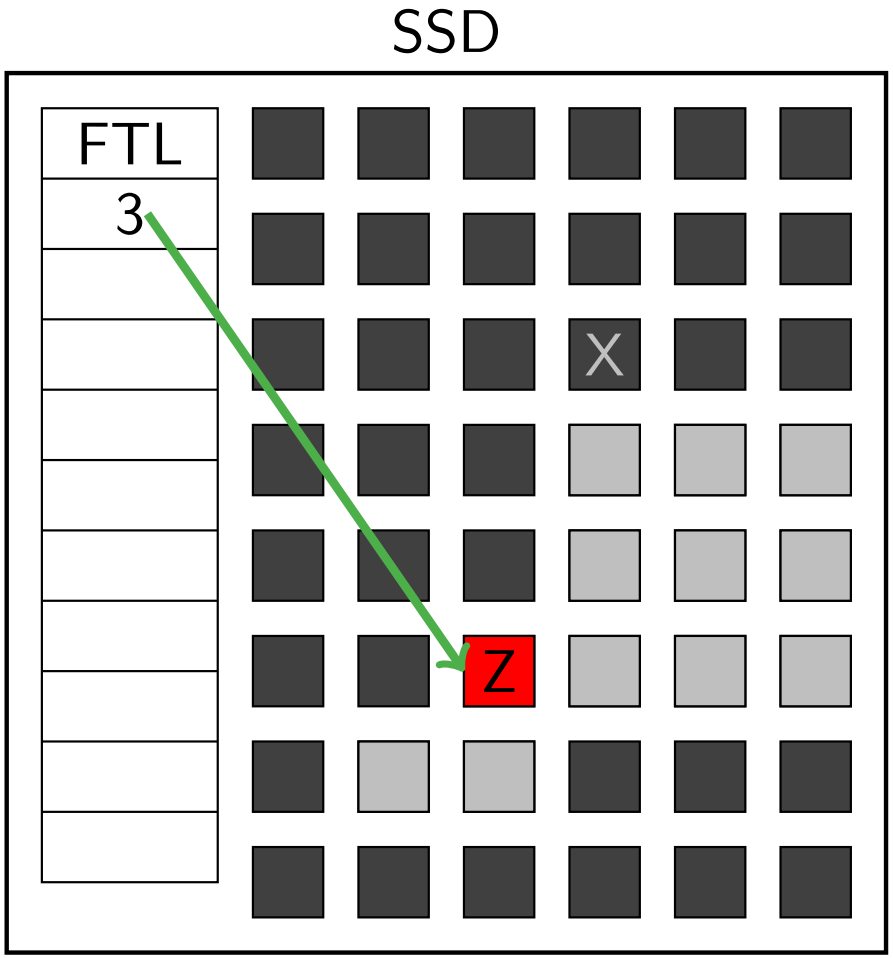
- ★ Zu wenig freie Blöcke
- ★ Lösche ganze Seite
- ★ Schreibe Blöcke



Seitenweises Löschen von Blöcken

Schreibe 4 Blöcke:

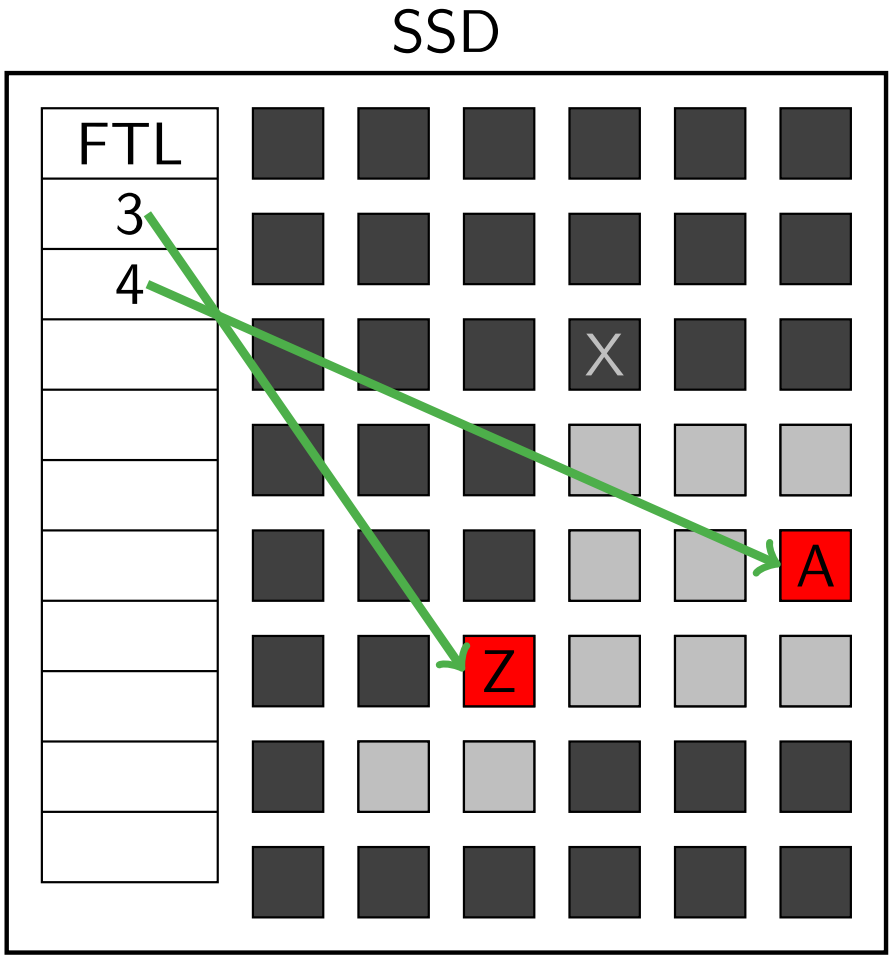
- ★ Zu wenig freie Blöcke
- ★ Lösche ganze Seite
- ★ Schreibe Blöcke



Seitenweises Löschen von Blöcken

Schreibe 4 Blöcke:

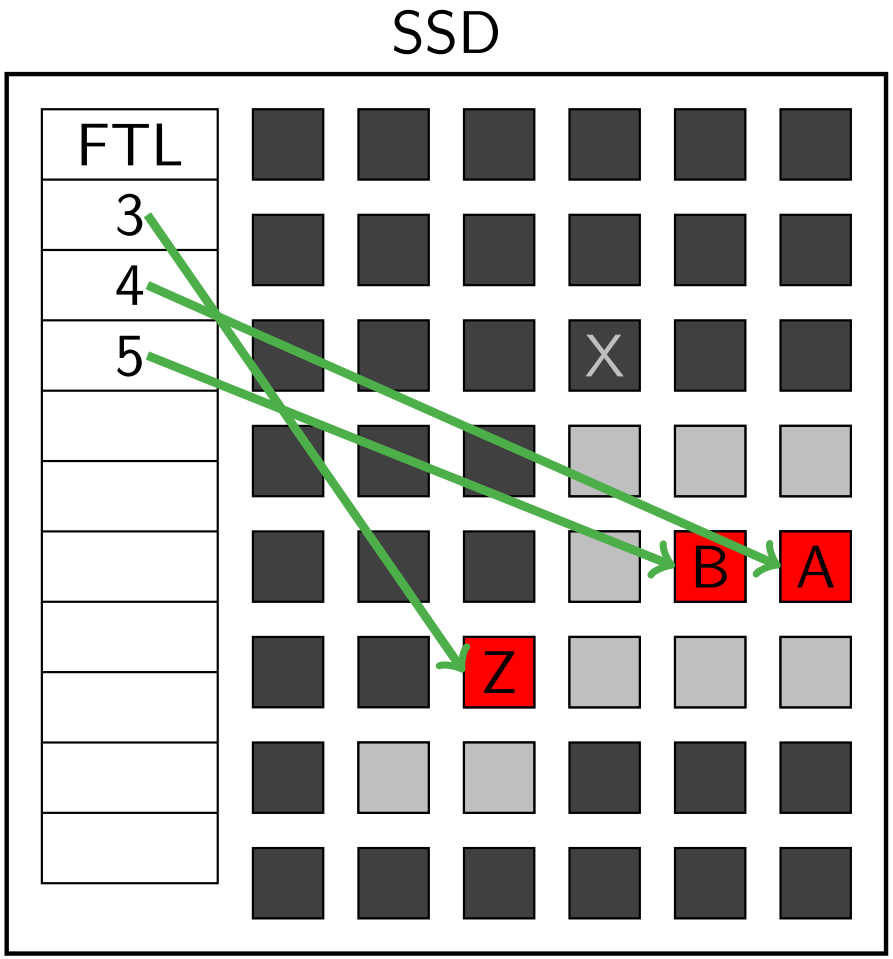
- ★ Zu wenig freie Blöcke
- ★ Lösche ganze Seite
- ★ Schreibe Blöcke



Seitenweises Löschen von Blöcken

Schreibe 4 Blöcke:

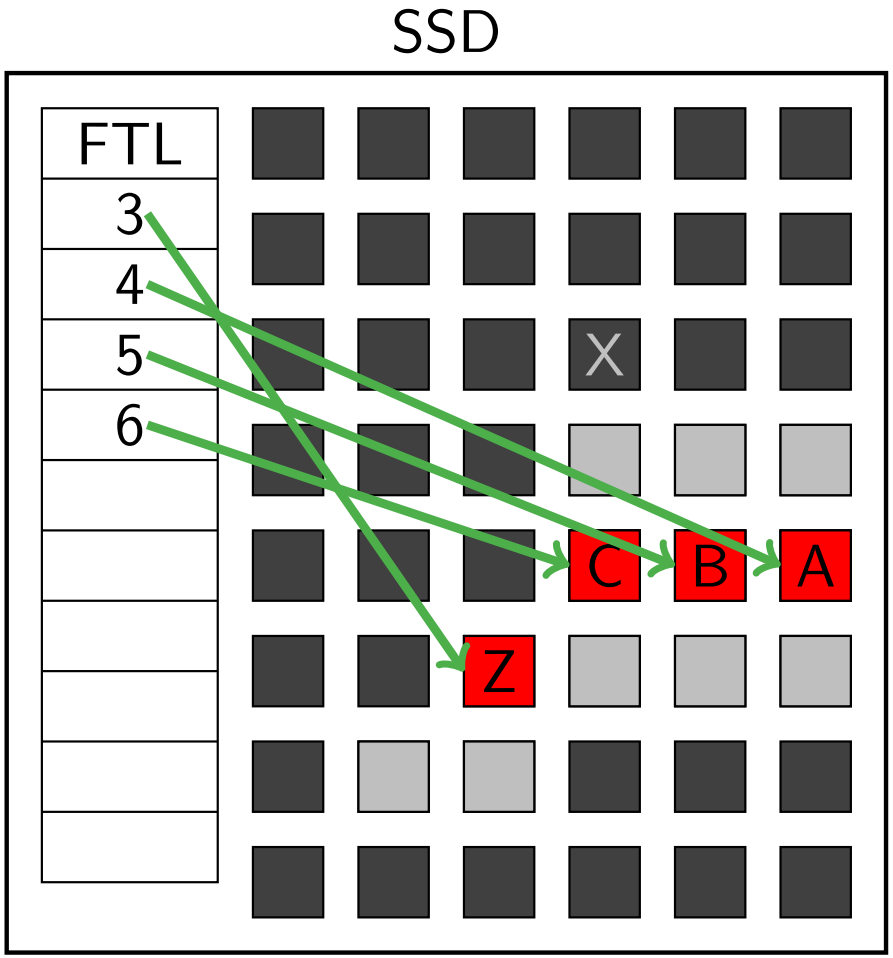
- ★ Zu wenig freie Blöcke
- ★ Lösche ganze Seite
- ★ Schreibe Blöcke



Seitenweises Löschen von Blöcken

Schreibe 4 Blöcke:

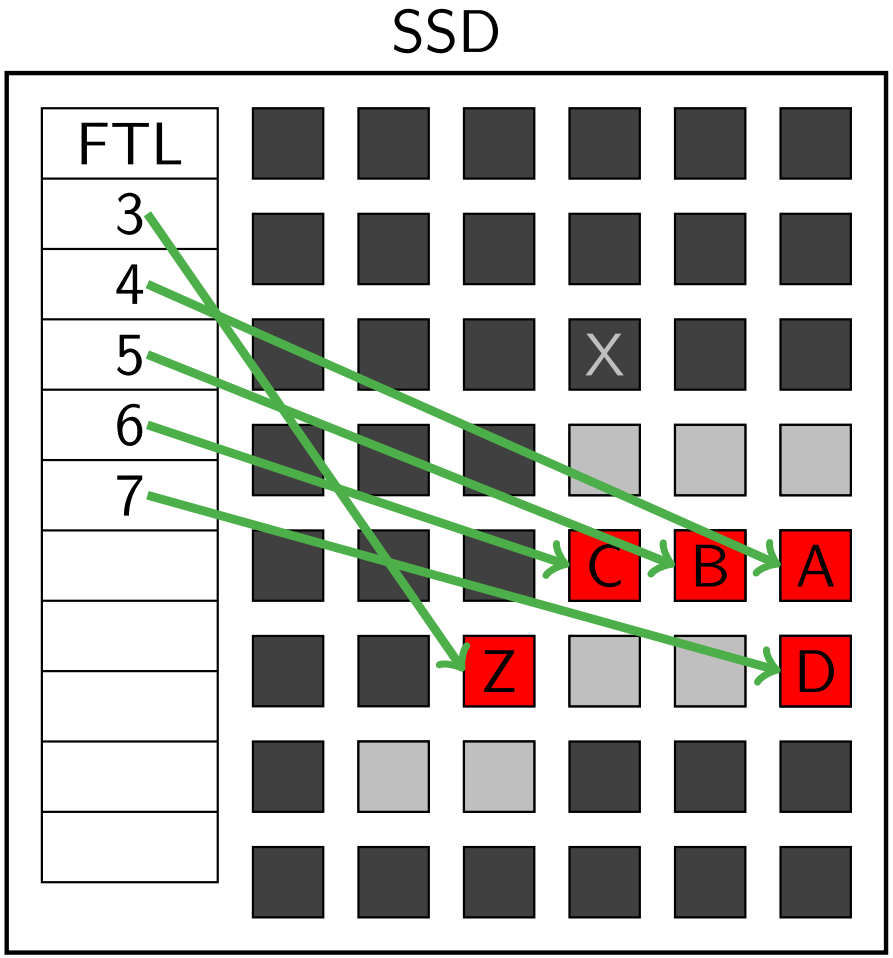
- ★ Zu wenig freie Blöcke
- ★ Lösche ganze Seite
- ★ Schreibe Blöcke



Seitenweises Löschen von Blöcken

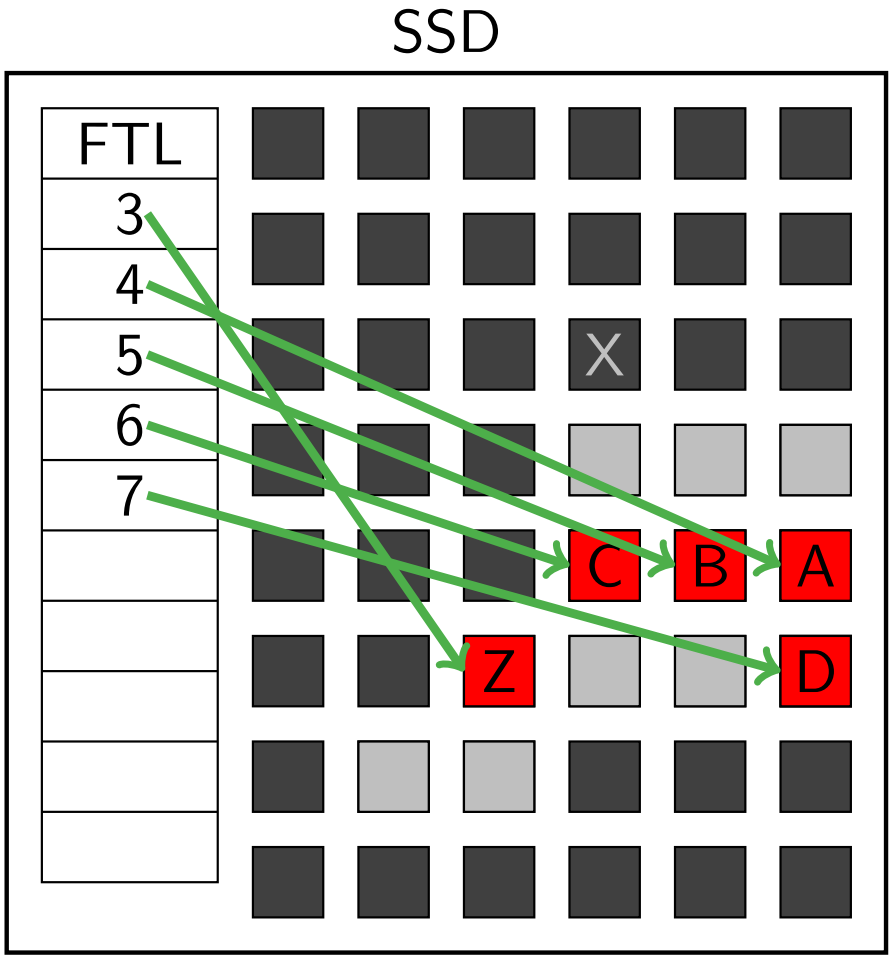
Schreibe 4 Blöcke:

- ★ Zu wenig freie Blöcke
- ★ Lösche ganze Seite
- ★ Schreibe Blöcke



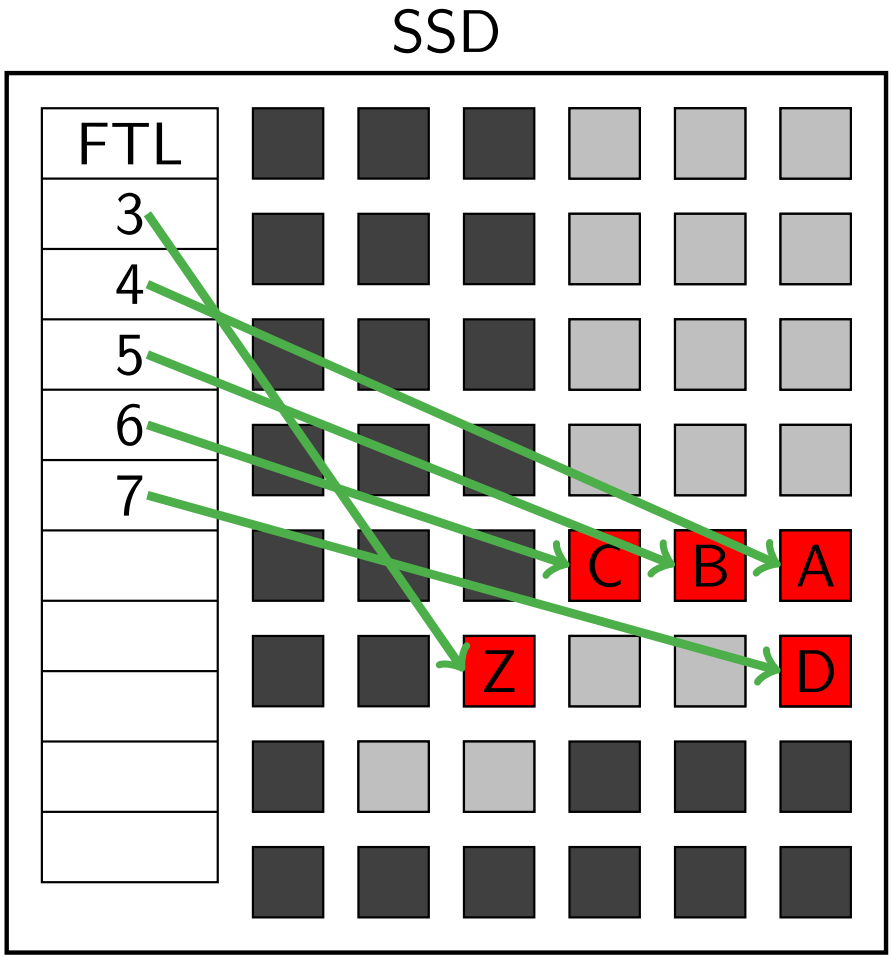
Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



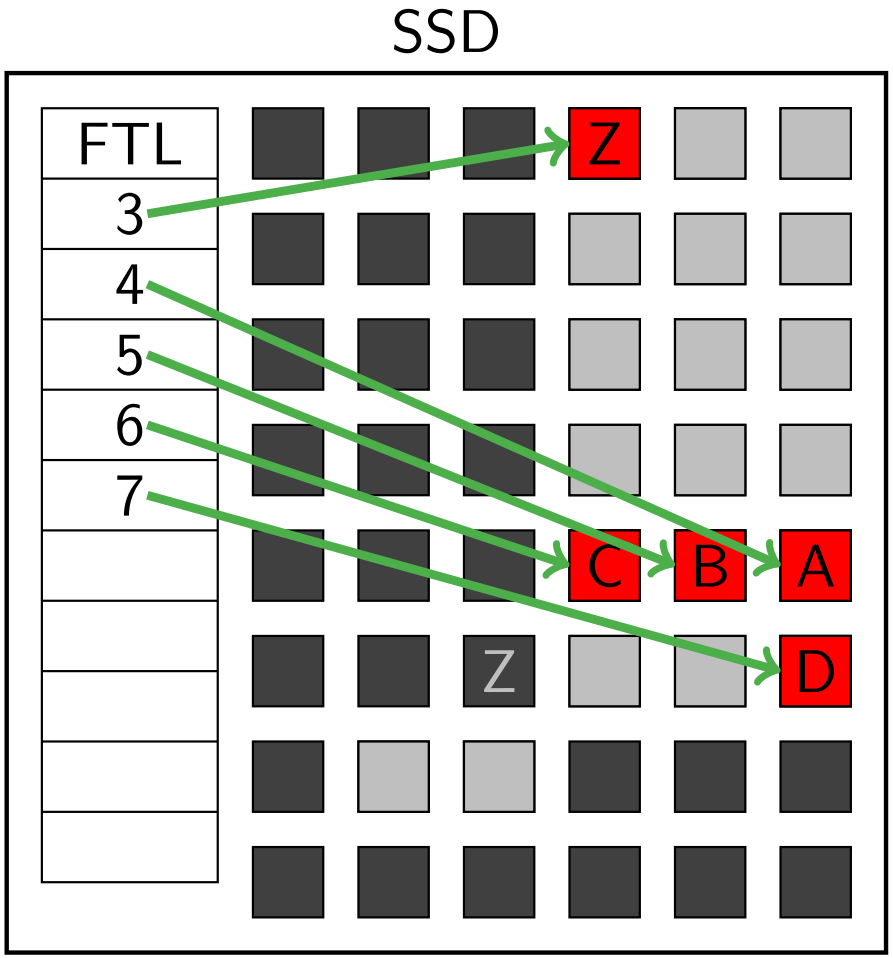
Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



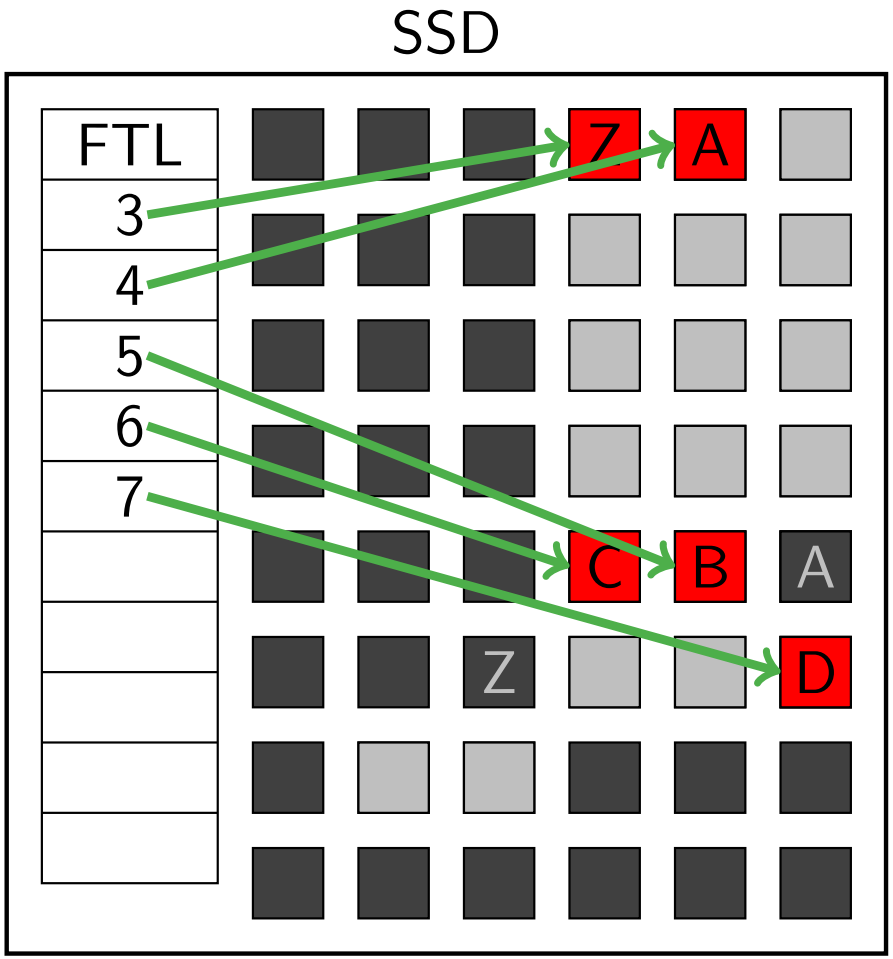
Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



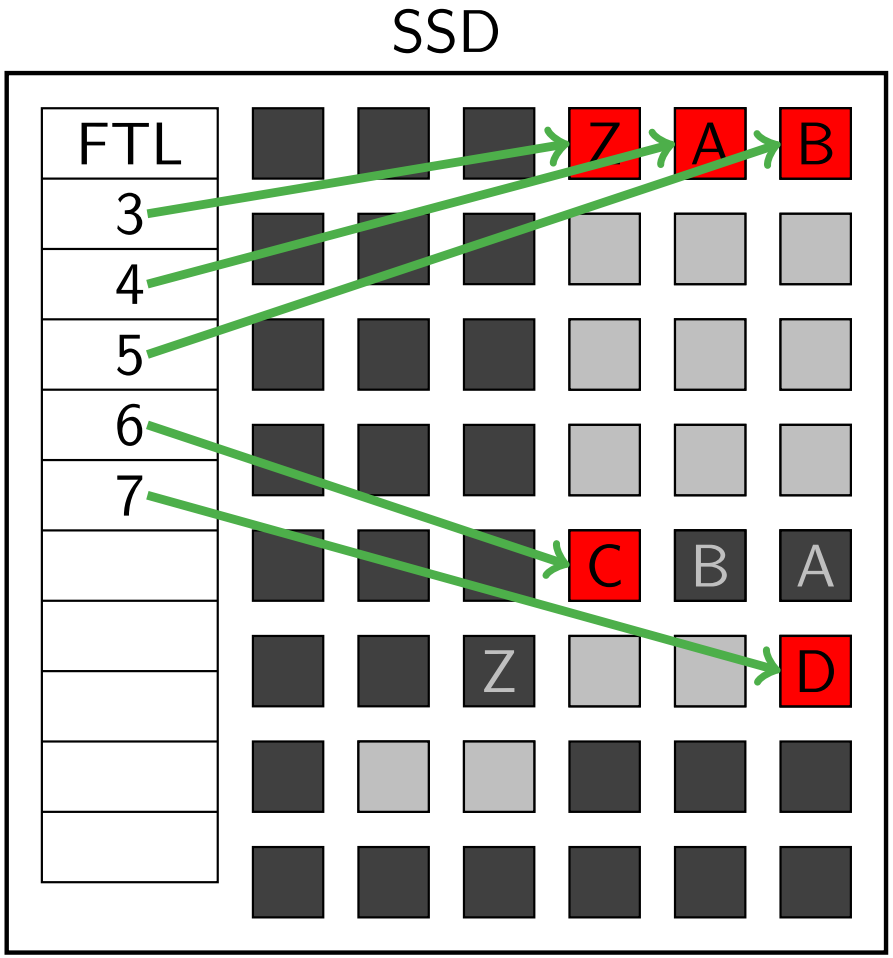
Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



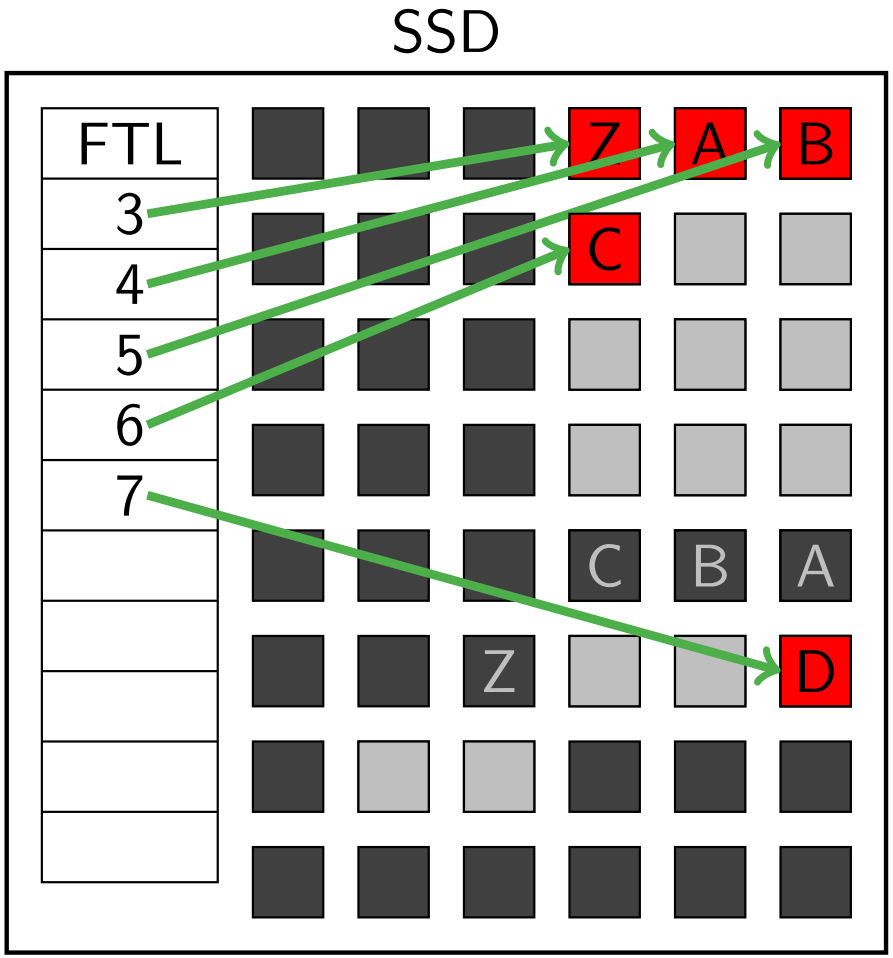
Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



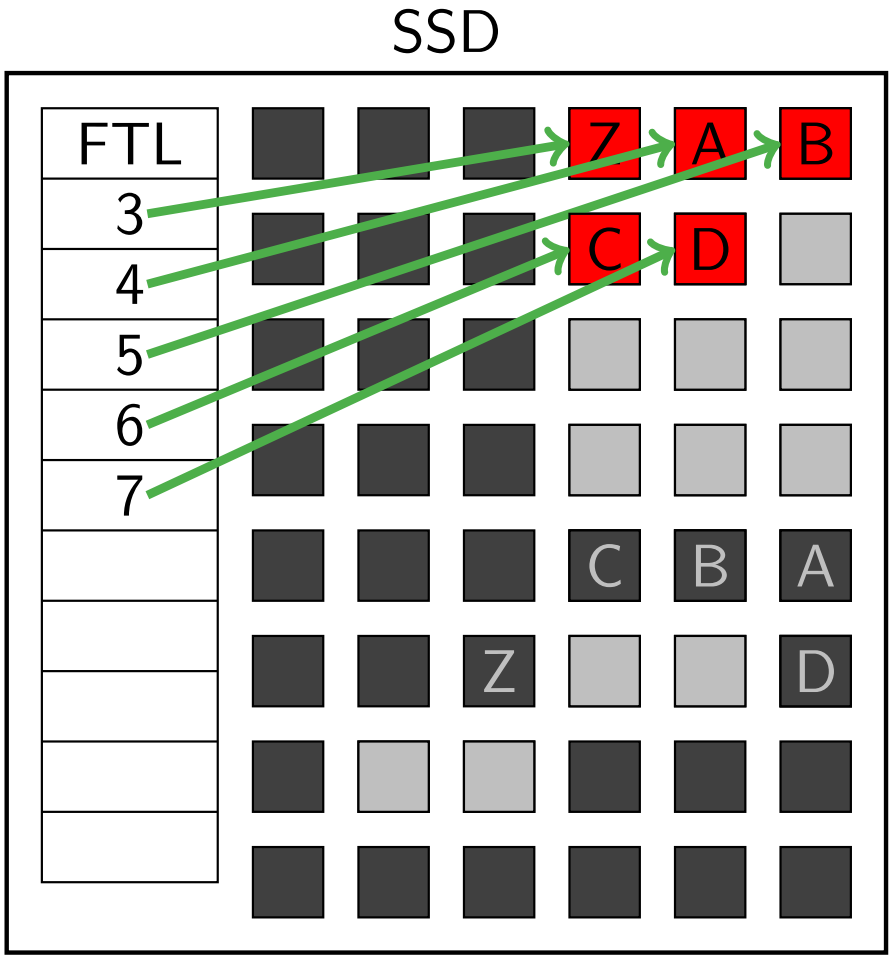
Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



Garbage Collection

- ★ SSDs führen GC durch
- ★ Von außen nicht ersichtlich
- ★ Daten werden kopiert



Löschen einer ganzen SSD

- ★ Überschreiben aller Blöcke reicht nicht aus
- ★ Zusätzlicher Speicher ist nicht zugänglich, 5-20% der Daten „bleiben übrig“
- ★ Möglichkeiten: ATA_SECURE_ERASE (BSI) oder zerstören

Löschen von Partitionen und Dateien

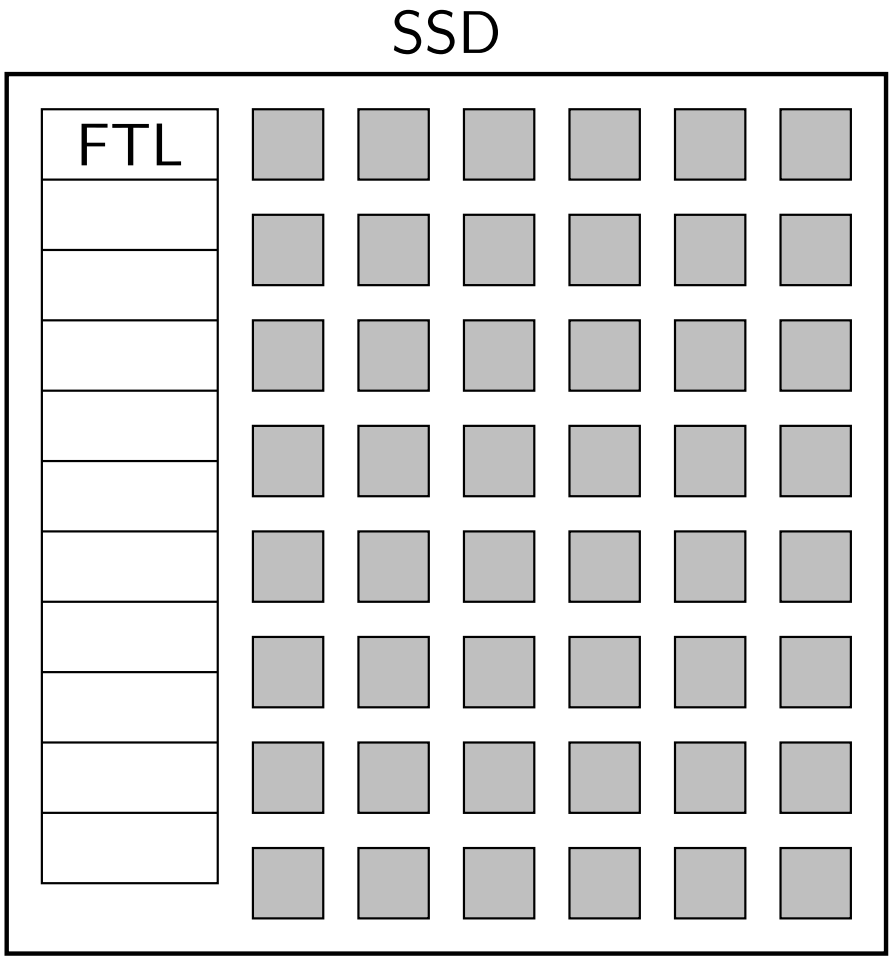
- ★ FTL verhindert Überschreiben von Blöcken
- ★ Daten (oder Kopien davon) können noch gespeichert sein
- ★ Daten bleiben potentiell sehr lange erhalten
- ★ Es besteht keinerlei Kontrolle über die Firmware der SSD
- ★ Damit sind die Daten nicht „unwiederbringlich“ entfernt
- ★ Aber: Zugriff auf solche Daten ist schwierig

TRIM/DISCARD

- ★ Betriebssystem teilt SSD mit: Block wird nicht mehr benötigt (TRIM)
- ★ Daten können direkt nach dem Markieren (TRIM) nicht mehr gelesen werden
- ★ Aktuelle SSDs implementieren „Read Zero After Trim“ (RZAT)
- ★ Aber: Immer noch gespeichert
- ★ Direktes Auslesen des Flash-Speichers weiterhin möglich (sehr aufwendig)
- ★ SSD ist „Black-Box“, keine Kontrolle

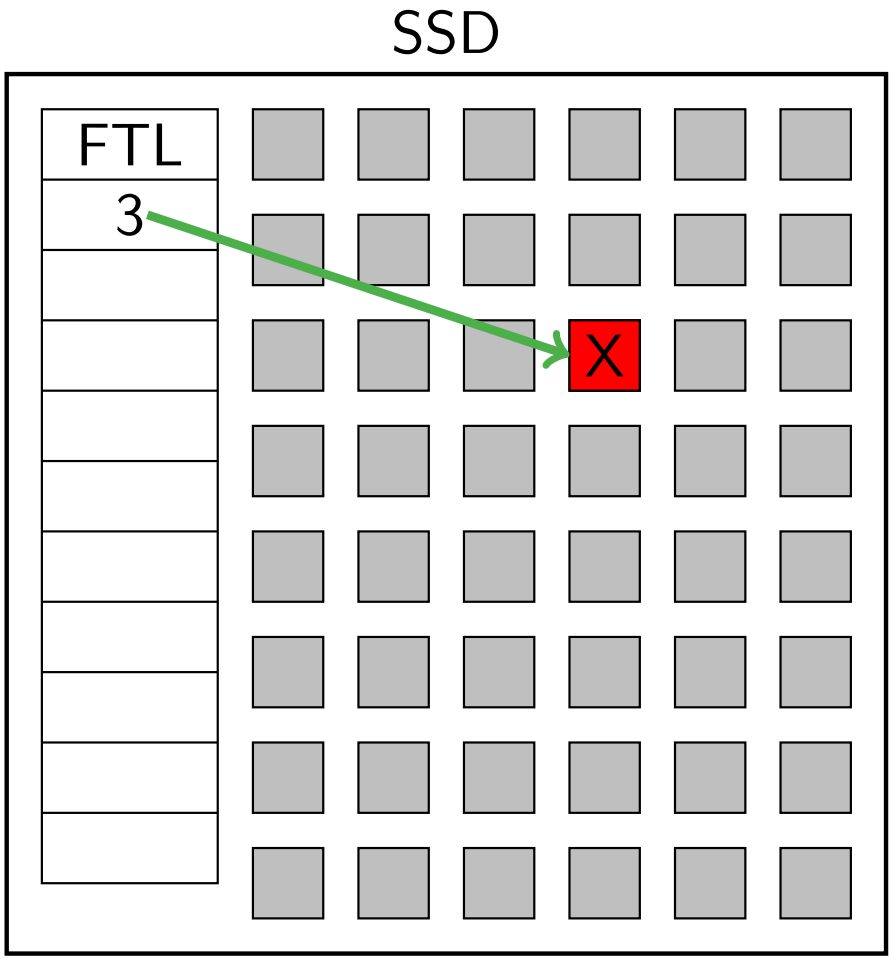
TRIM/DISCARD

- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)



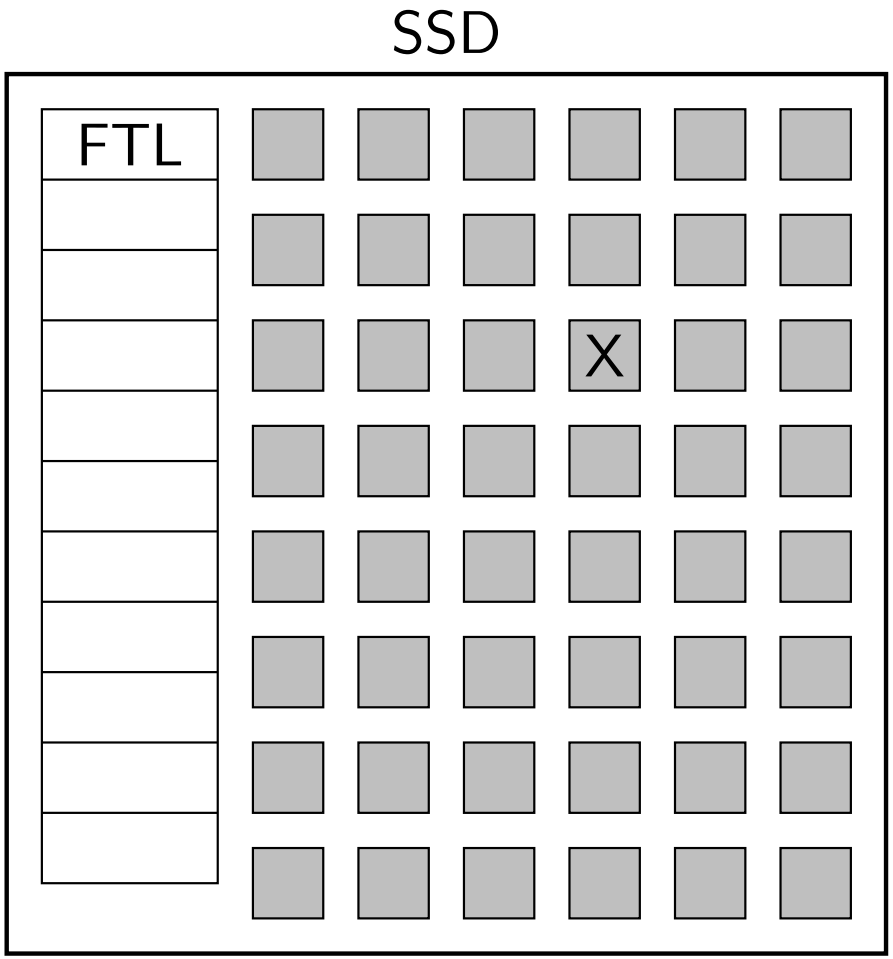
TRIM/DISCARD

- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)



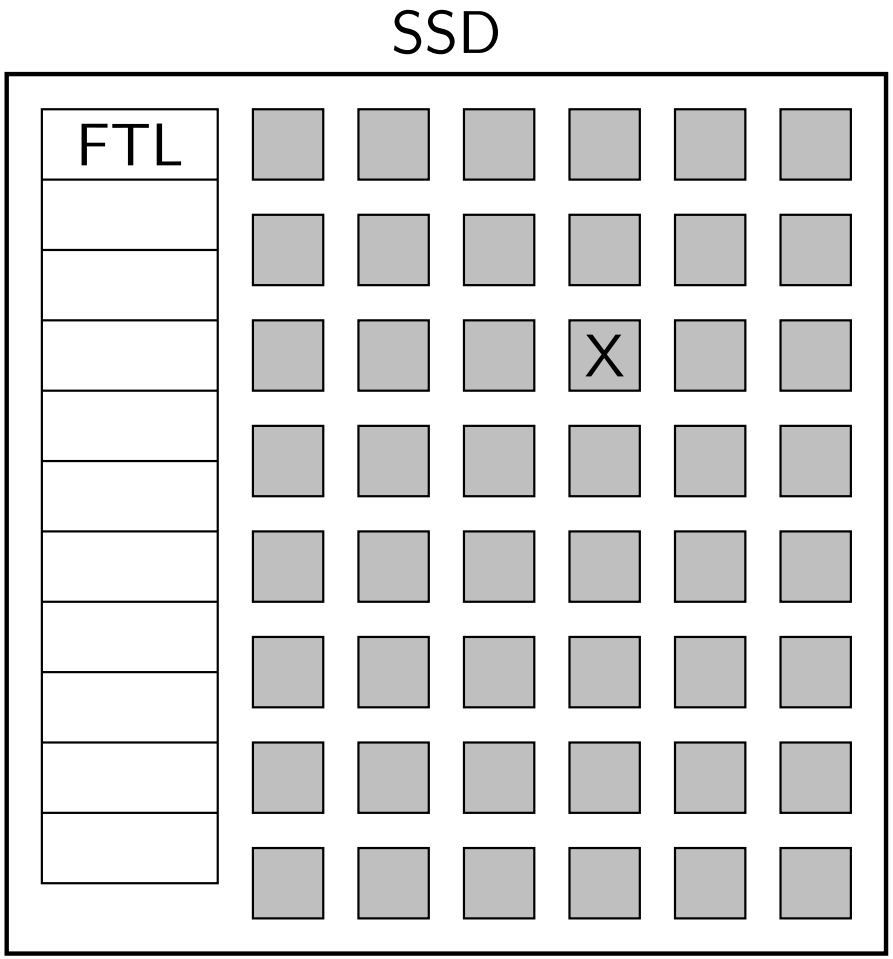
TRIM/DISCARD

- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)



TRIM/DISCARD

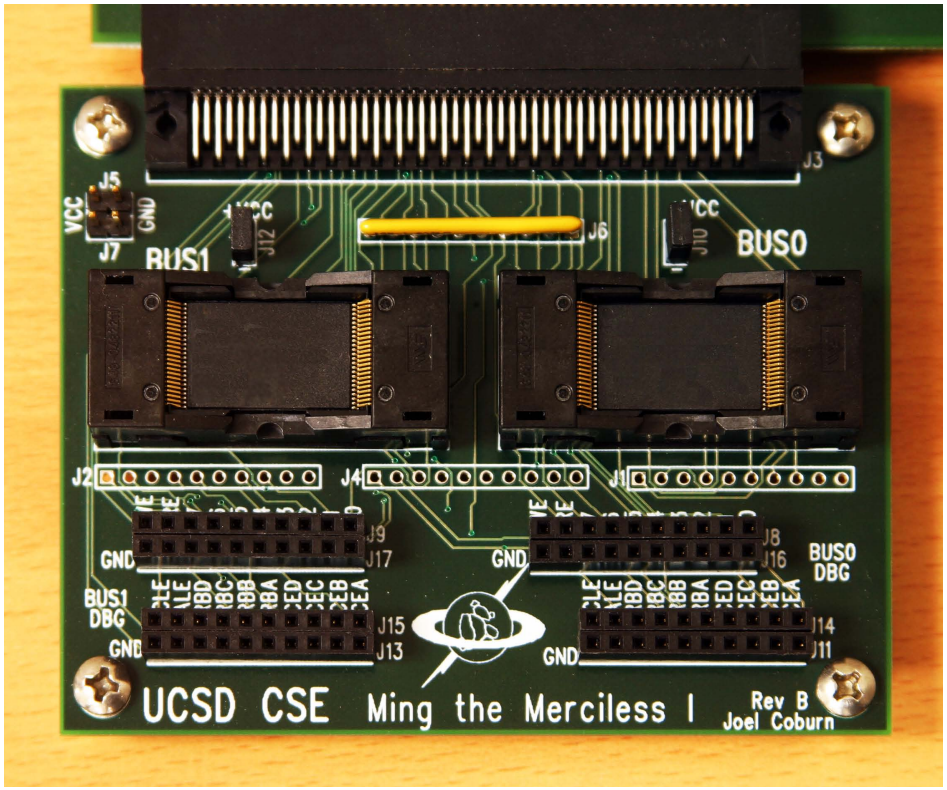
- ★ Schreibe „X“ in Block 3
- ★ Block 3 wird nicht mehr benötigt (TRIM)
- ★ SSD liefert nur Nullen zurück (RZAT)



Auslesen Flash direkt

- Wei et.al. (2011): „Reliably Erasing Data From Flash-Based Solid State Drives“
- Unter anderem: Direktes Auslesen des Flash
- Bis zu 16 Kopien einer einzelnen Datei gefunden
- Hardware entwickelt, Kosten damals etwa $1000

Flash-Leser


J3
J5
VCC
GND
J7
BUS1
J12
J6
J10
BUS0
J2
J4
J1
J9
J17
GND
BUS1
DBG
GND
J15
J13
J8
J16
GND
BUS0
DBG
J14
J11
GND
UCSD CSE
Ming the Merciless I
Rev B
Joel Coburn

Vergleich

Löschen	Festplatte	SSD
ganzes Medium		
Partition		
Datei		

Vergleich

Löschen	Festplatte	SSD
ganzes Medium	✓	
Partition	✓	
Datei	(✓)	

Vergleich

Löschen	Festplatte	SSD
ganzes Medium	✓	✓
Partition	✓	✗
Datei	(✓)	✗

Idee: Daten verschlüsseln

- ★ Wenn die Daten nicht richtig gelöscht werden können, verschlüsseln wir sie
- ★ Daten löschen → Schlüssel (Passwort) löschen
- ★ Problem: Das Passwort ist eventuell lange bekannt
- ★ Damit ist dies nicht „unwiederbringlich“

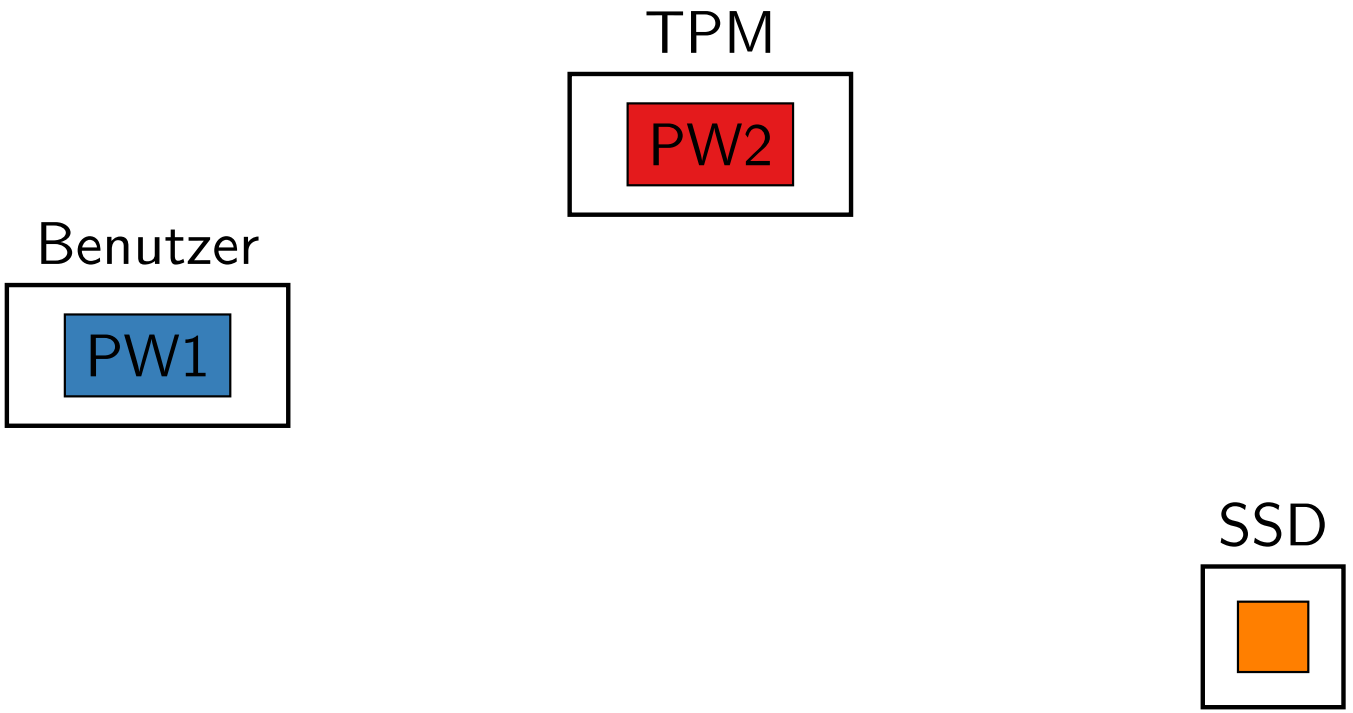
Trusted Computing Platform (TPM)

- ★ Fast alle Laptops (und viele anderen PCs) haben einen TPM-Chip eingebaut
- ★ Hat (ein wenig) Speicher für Schlüssel
- ★ Kann sicher gelöscht/überschrieben werden
- ★ Idee: Speichern eines (Teil)Passworts im TPM-Chip

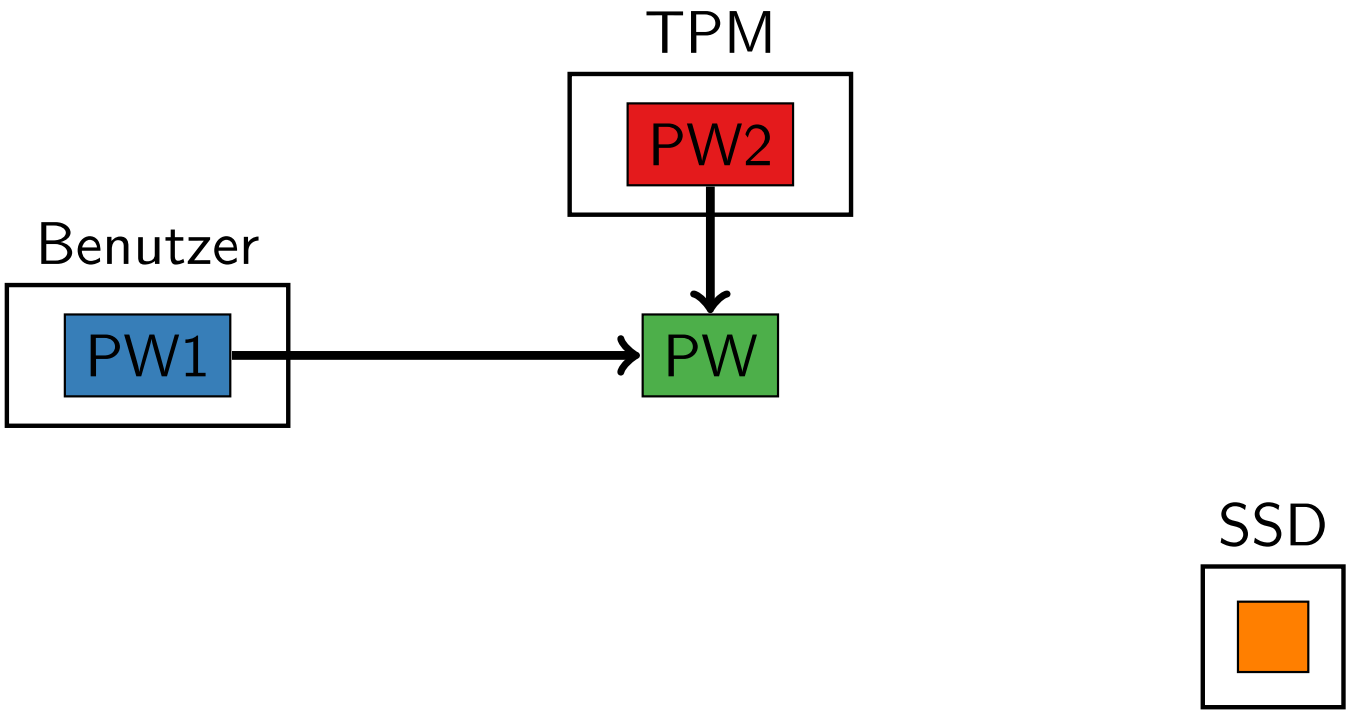
Lösung

- Verschlüsseln aller Daten einer Partition mit einem Passwort
- Passwort ist zusammengesetzt:
  - Passwort des Benutzers (PW1)
  - Zufällig gewähltes Passwort (PW2)
- PW2 wird im TPM-Chip gespeichert
- Bei der Eingabe des Benutzerpassworts automatisch angehängt
- Erweiterung zu cryptsetup (Linux)
- Benutzer bekommt PW2 nicht angezeigt

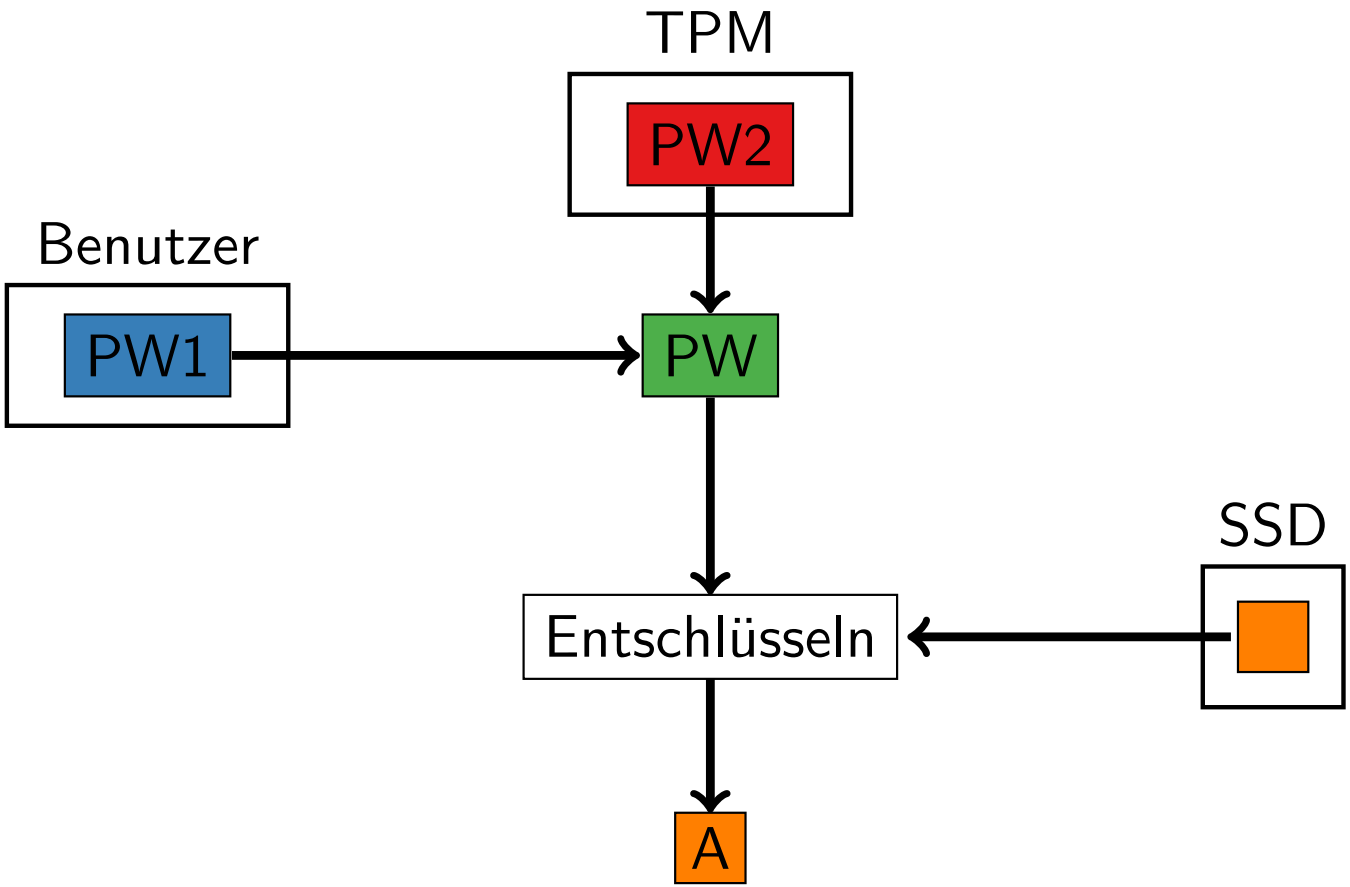
Passwort im TPM-Chip



Passwort im TPM-Chip



Passwort im TPM-Chip



Fazit

- ★ Großer Unterschied: Festplatten vs. SSDs
- ★ Unwiederbringliches Löschen von Dateien/Partitionen auf SSDs ist nicht möglich
- ★ Lösung vorgestellt: Verschlüsselung mit Teilpasswort im TPM-Chip
- ★ Demnächst: Integration in cryptsetup (Linux)

Ausblick

- ★ Halbleiterbasierte Speichermedien wie SSDs werden zunehmend eingesetzt
- ★ Teilweise auch als Hybridprodukte („SSHD“)
- ★ Festplatten werden ein ähnliches Problem bekommen
- ★ „Shingled Magnetic Recording“ (SMR)

Zeit für Fragen und Diskussionen

Vielen Dank für Ihre Aufmerksamkeit