Vorschlag von Lewin:

```
Grenzen von Rowhammer:
  Braucht fehlerhafte Bits
  Keine direkten Angriffe über Netzwerke, da zu langsam (Muss Prozess starten können)
  Kann nur innerhalb der Refresh-Rate agieren

Bis jetzt noch kein dokumentierter Hack (But you never know)

Mögliche Rowhammer Angriffe
  - JavaSkript
  - Attacken über Intel-Software
  - Throw-Hammer
  - Handy-Angriff in 2 min
  - Jackhammer-Cloud-Angriffe
  -

Schutz gegen Rowhammer
  -
  -
```

Mögliche Arten von Attacken und Schlupflöcher in modernen Systemen Attacke über Microsoft Edge browser

Attacke über JavaScript im browser

Fist Solution

- ECC Memory (Error correcting code)

Versteckte attacken über Intel Software Fuard Extensions:

Klauen von SSH Key so keine Entschlüsselung nötig

Throw hammer

remote Angriff über Netzwerkpakete

- https://download.vusec.net/papers/throwhammer_atc18.pdf
- aber nur über ultra schnelle netzwerke aber server haben solche anschlüsse

Schwer duchzuführen

- Fachwissen
- zeit
- CPU power

GPUs (ohhh ohhh)

- einbrechen innerhalb von 2 minuten in ein handy

JackHammer

[1912.11523] JackHammer: Efficient Rowhammer on Heterogeneous FPGA-CPU Platforms

- FPGA haben direkten zugriff auf den Speicher (kein OS oder Firmeware)
- finden erhöhte nutzung in der cloud
- SLL Service geknackt

Tatsächliche Attacken wie davor Schützen

- Keine aufgezeichneten attacken
- Jedoch meinstens nicht erkennbar da unterhalb von firmware OS und apps
- Gefahr für die zukunft
- Intel hat ein Patent für Target Row Refresh falls eine attacke erkannt wird
- Testen des rams in der Produktion
- Memory refresh rate erhöhen