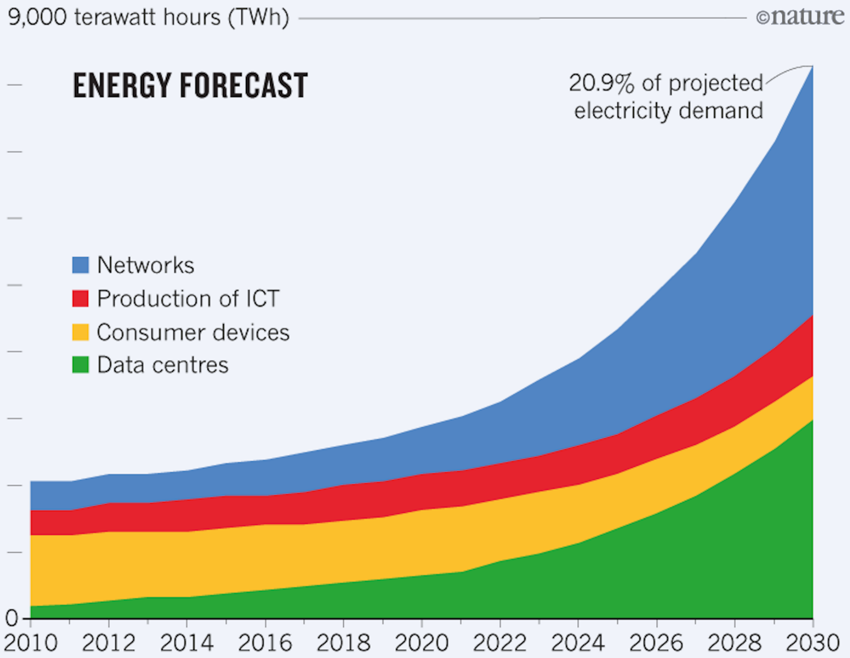
Mit Sicherheit effizient?

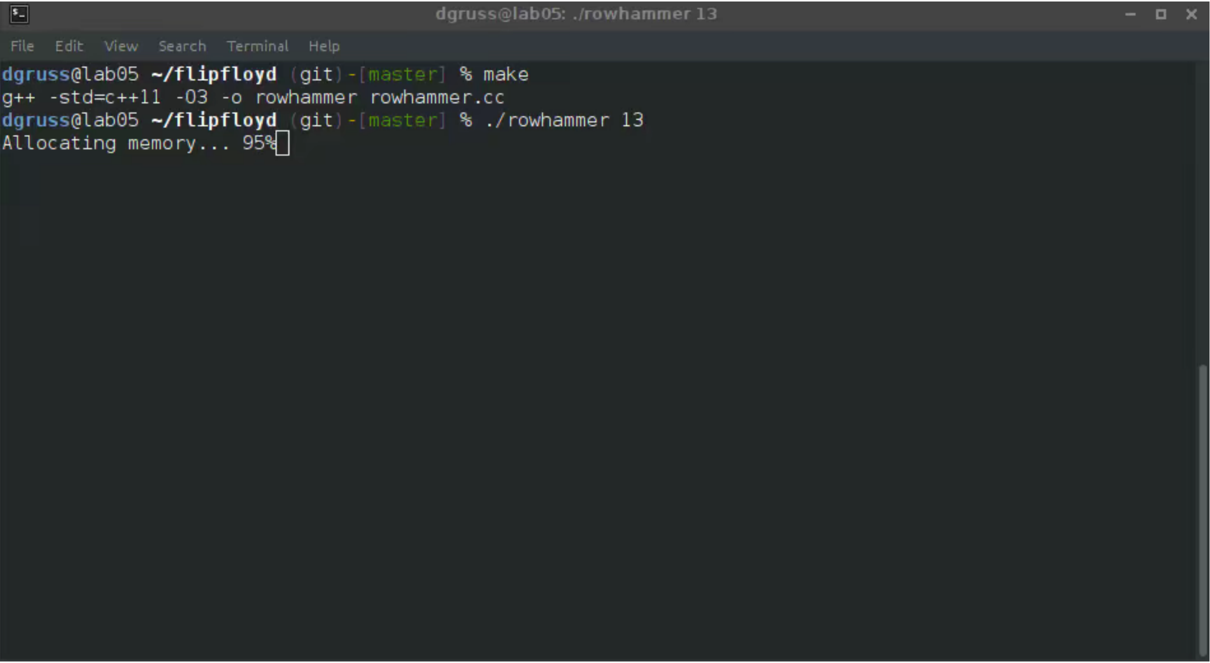
Daniel Gruss

TU Graz


9,000 terawatt hours (TWh)
©nature
ENERGY FORECAST
20.9% of projected electricity demand
🟦 Networks
🟥 Production of ICT
🟨 Consumer devices
🟩 Data centres
0
2010
2012
2014
2016
2018
2020
2022
2024
2026
2028
2030

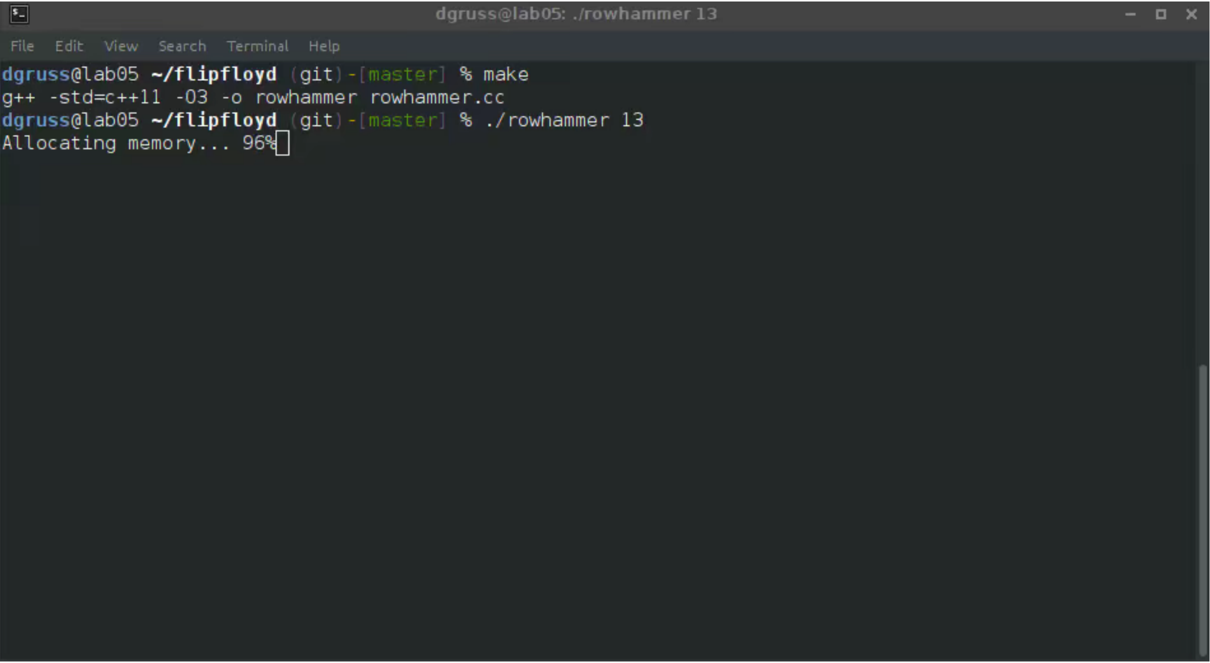
0.09%

0.40%

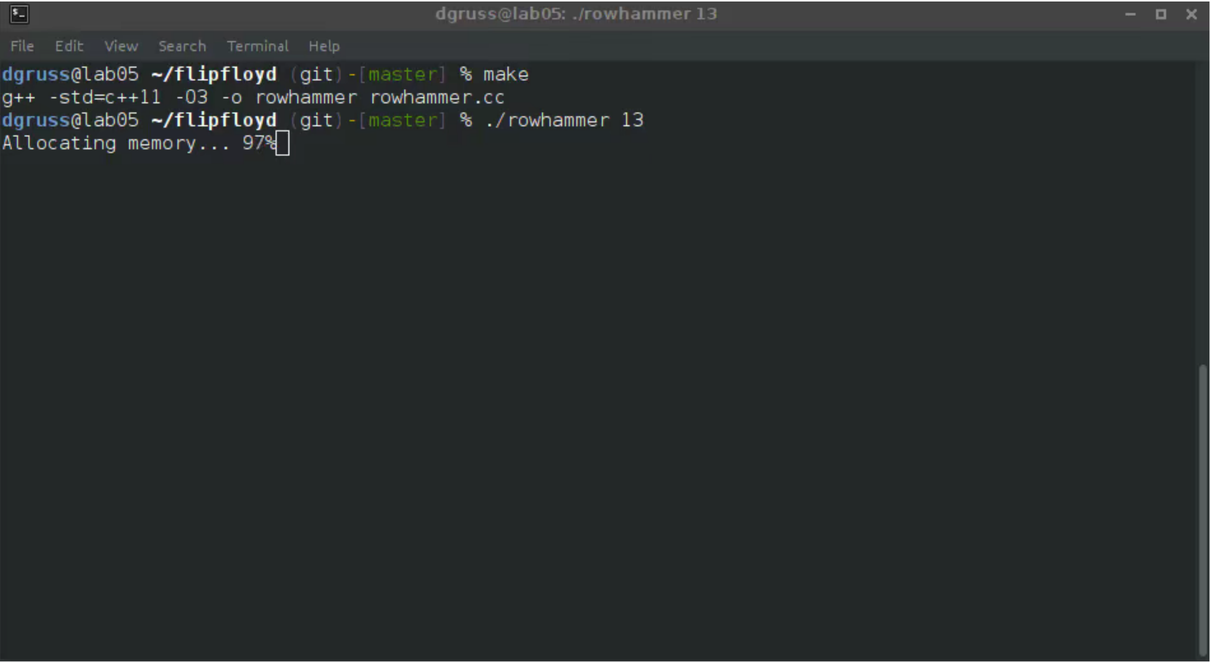


dgruss@lab05: ./rowhammer 13
File Edit View Search Terminal Help

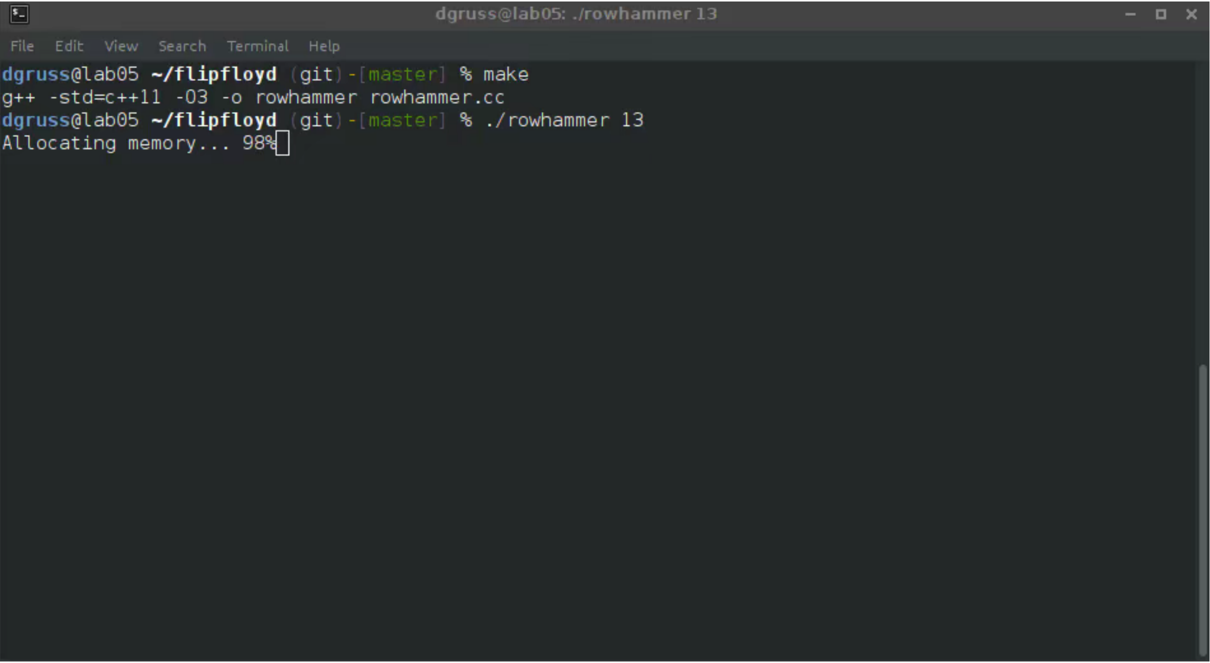
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Allocating memory... 95%
```



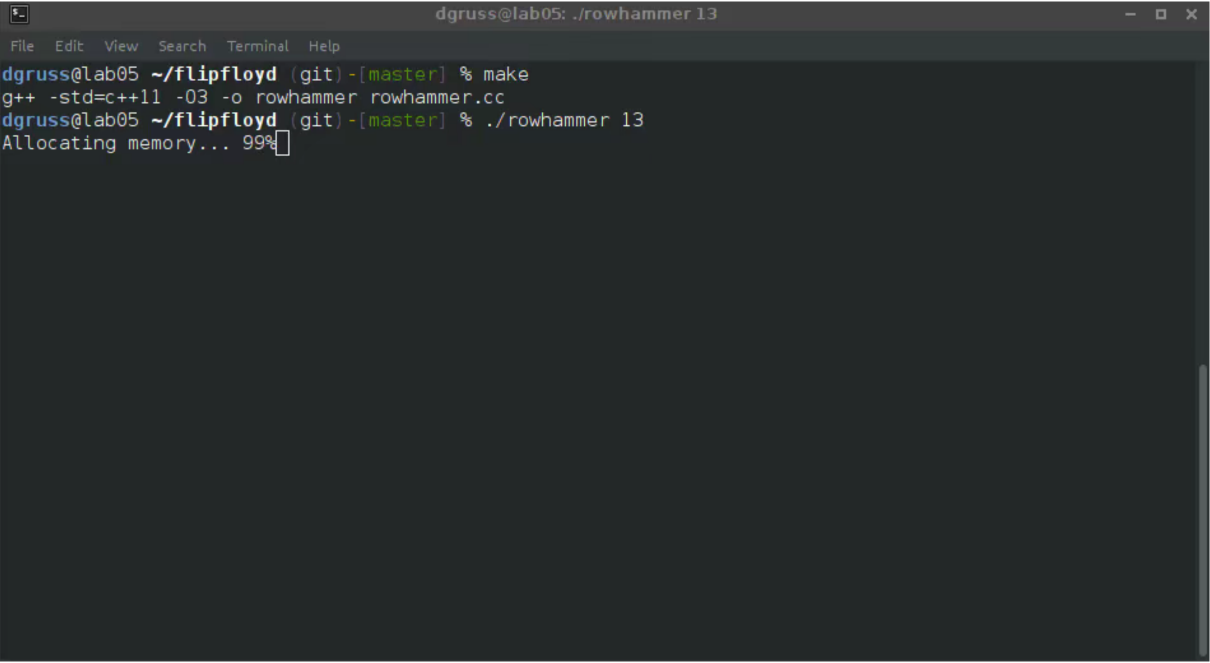
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Allocating memory... 96%
```



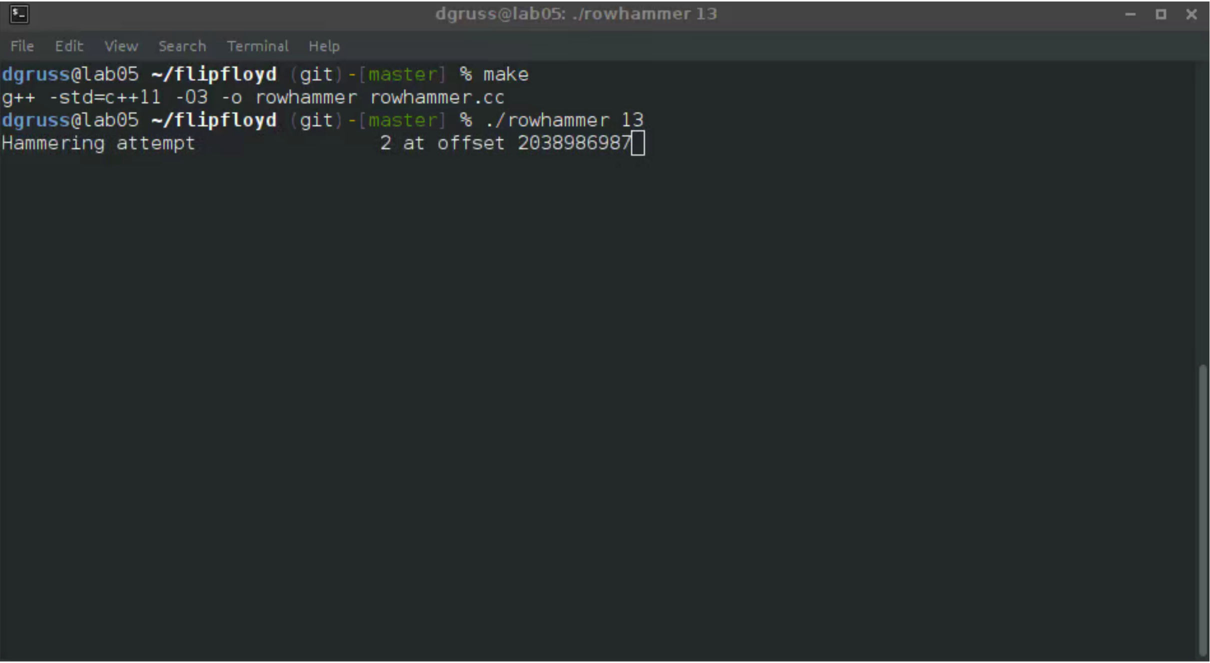
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Allocating memory... 97%
```



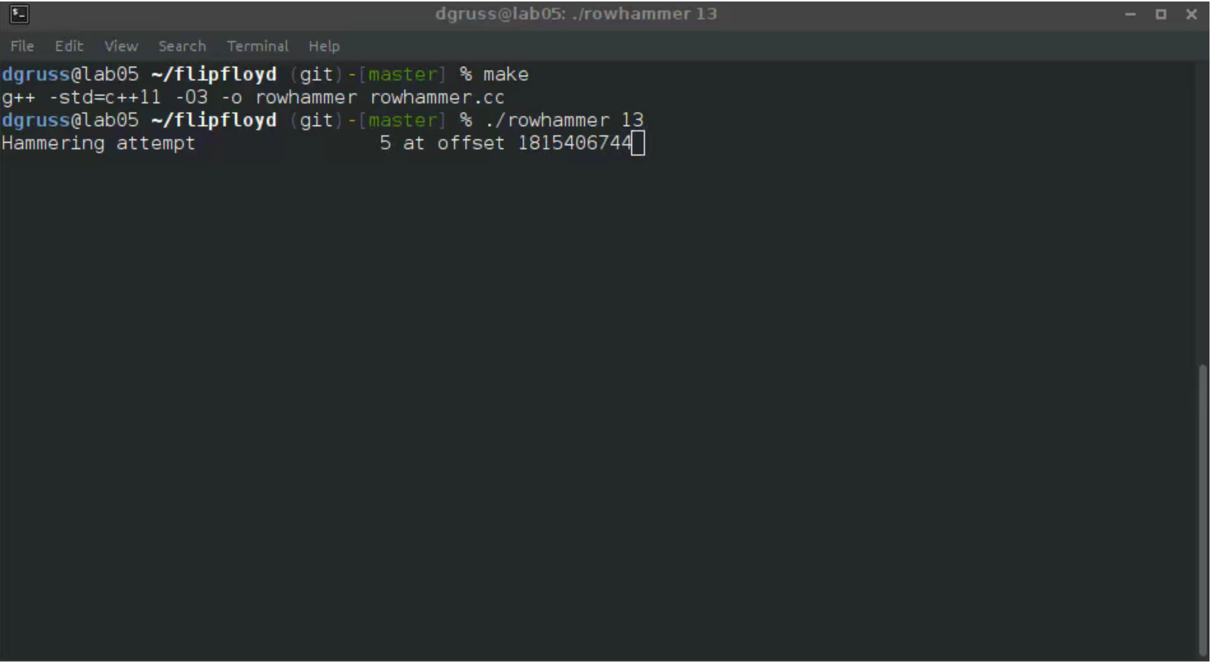
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Allocating memory... 98%
```



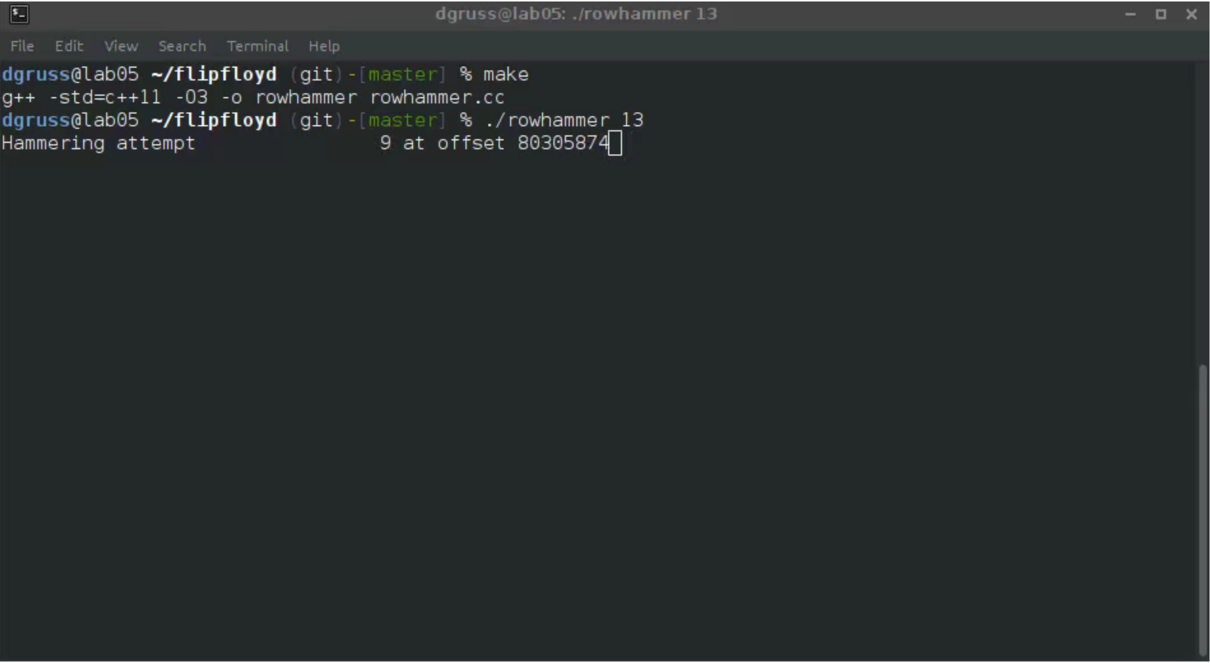
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Allocating memory... 99%
```



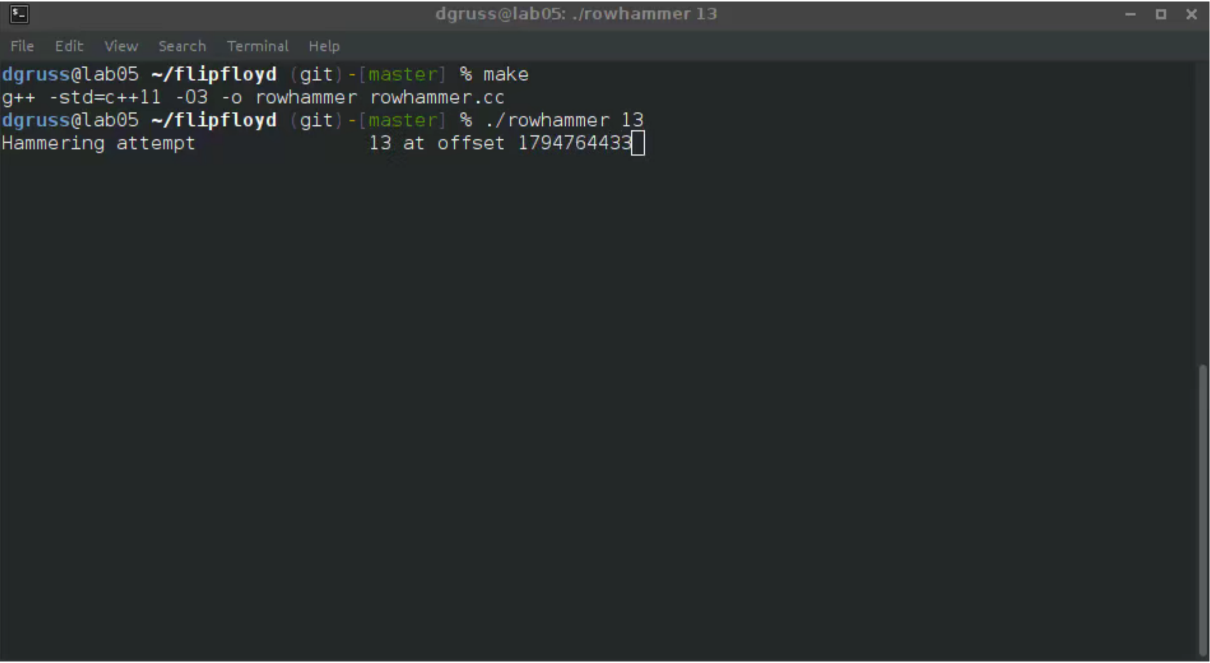
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt                2 at offset 2038986987
```



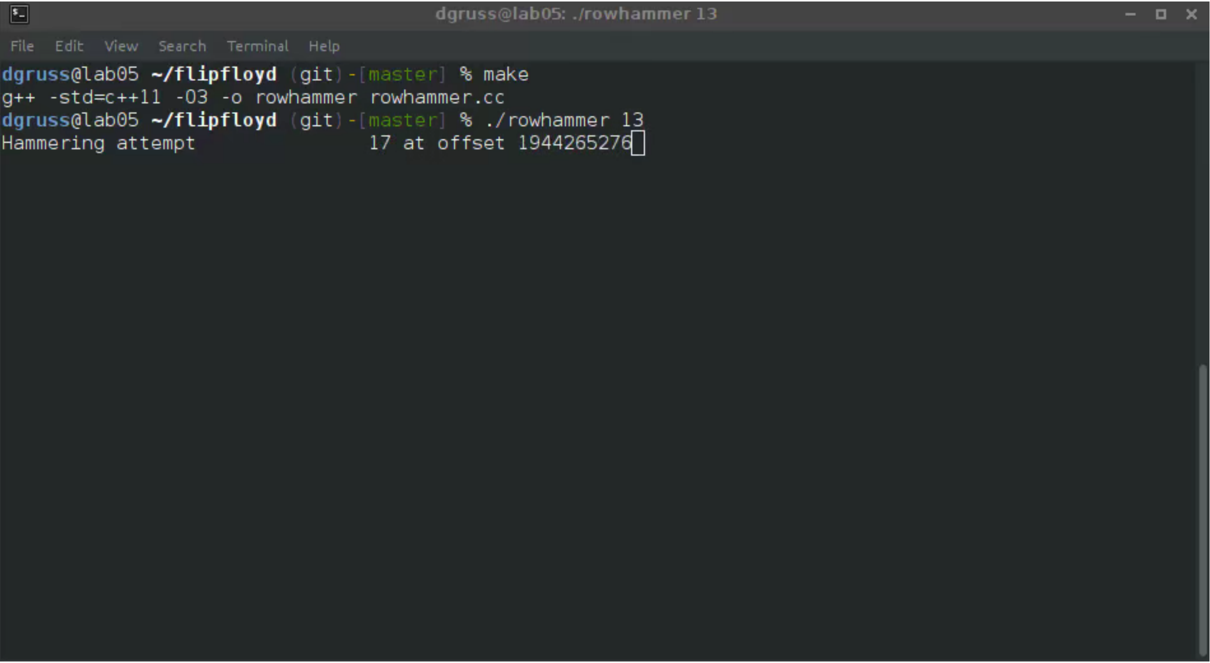
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt                5 at offset 1815406744
```



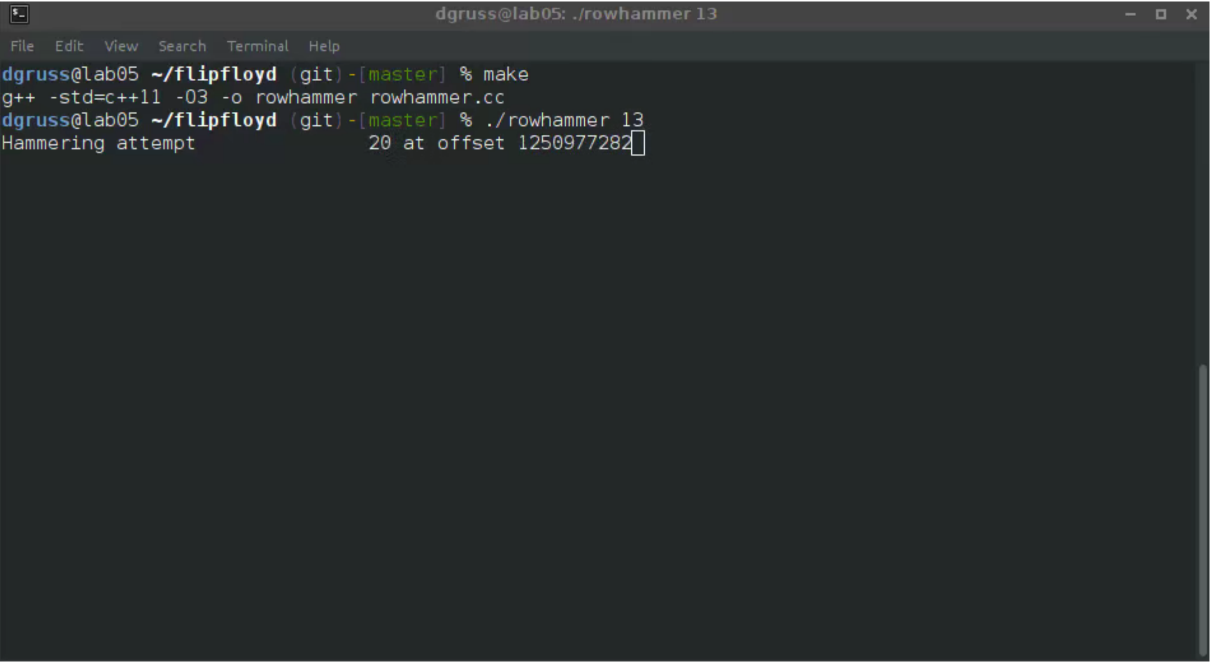
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt                9 at offset 80305874
```



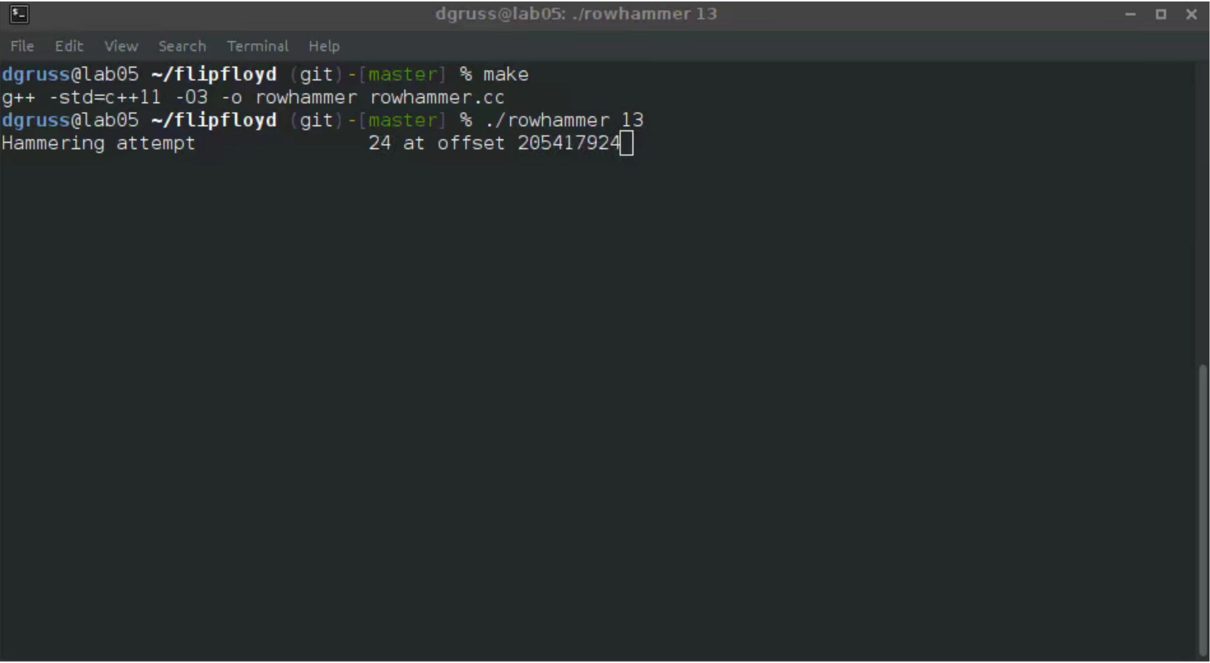
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt               13 at offset 1794764433
```



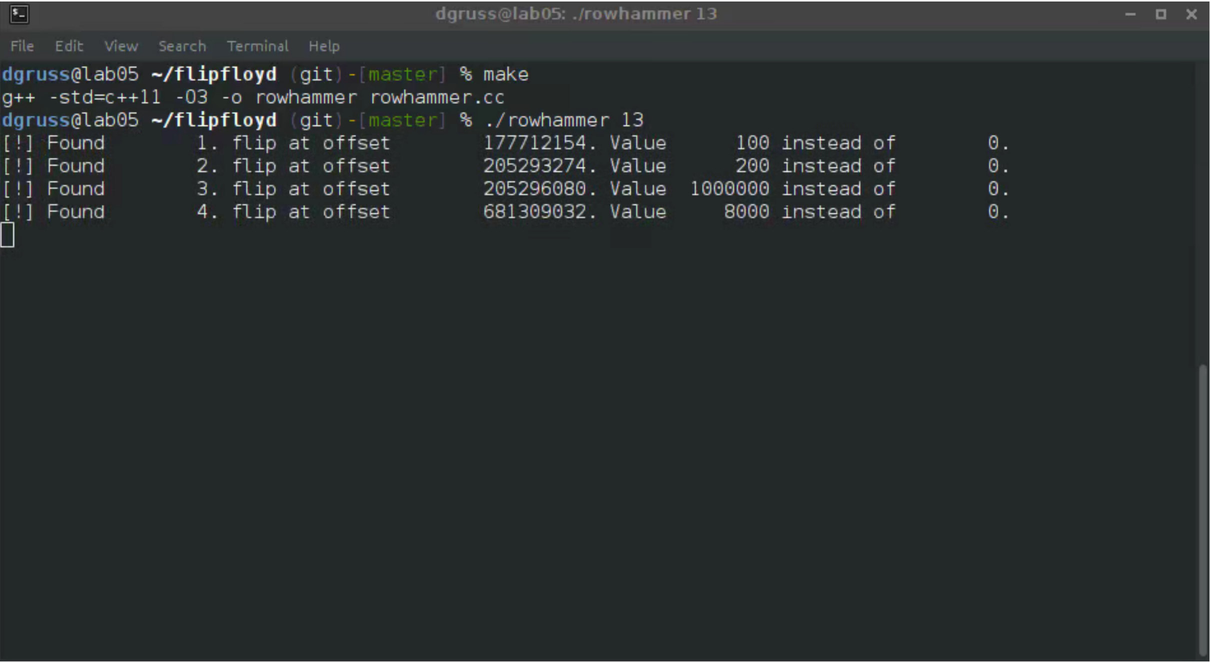
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt               17 at offset 1944265276
```



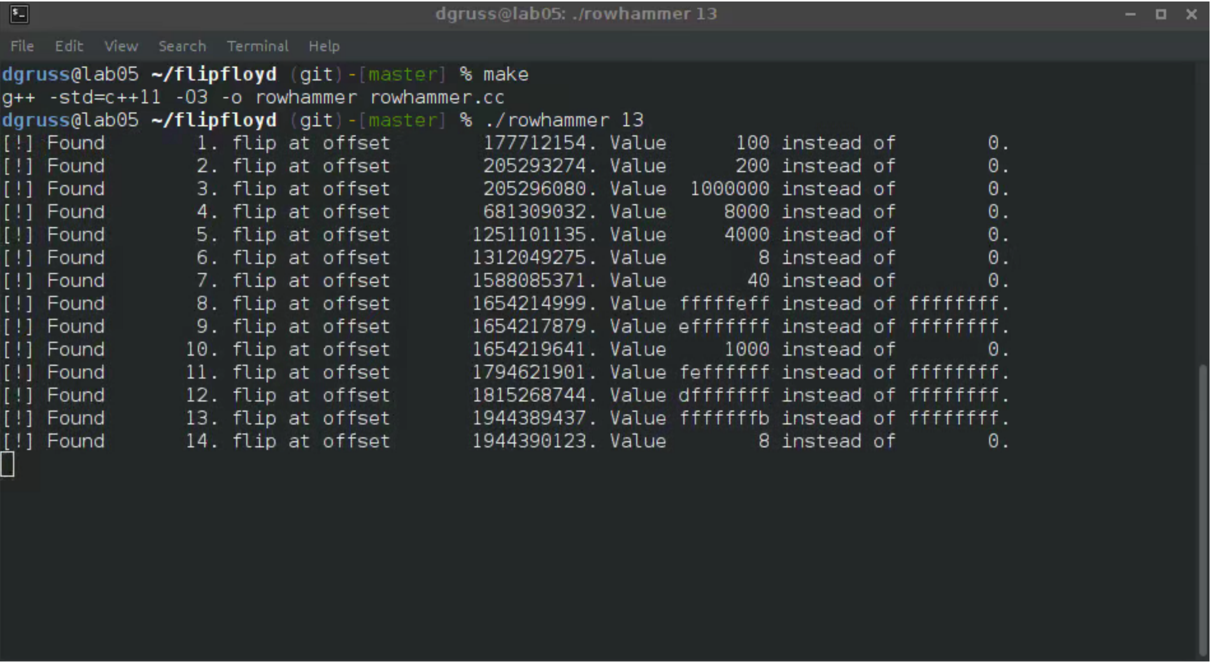
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt               20 at offset 1250977282
```


dgruss@lab05: ./rowhammer 13
File Edit View Search Terminal Help

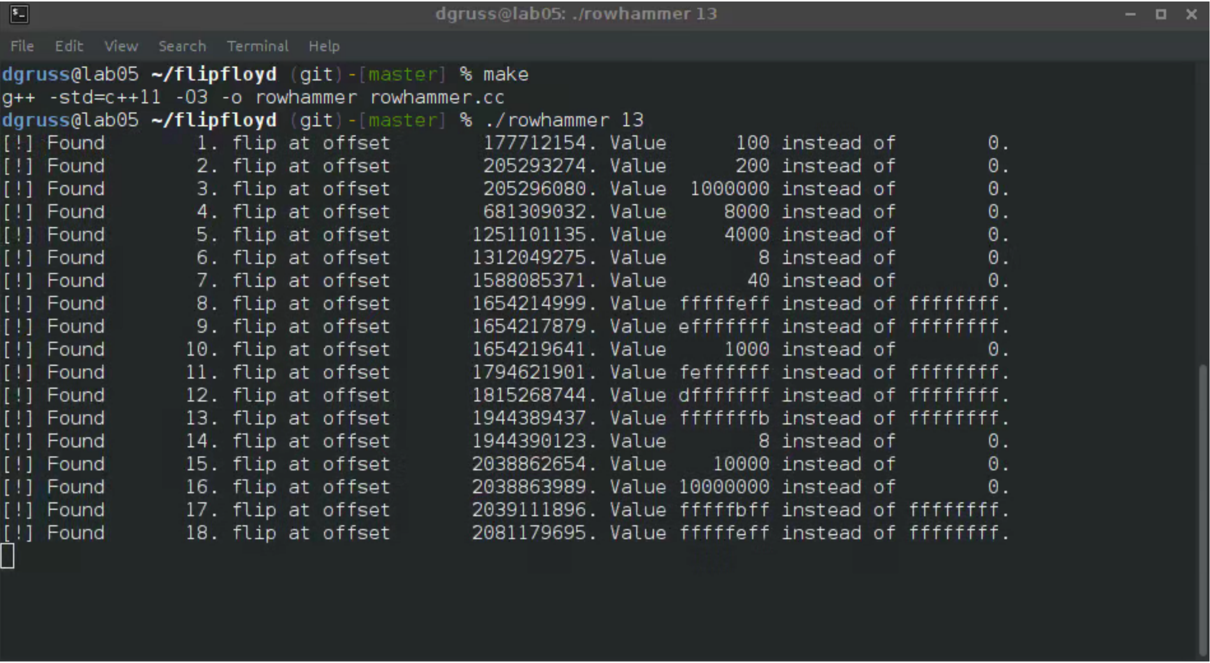
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
Hammering attempt               24 at offset 205417924
```



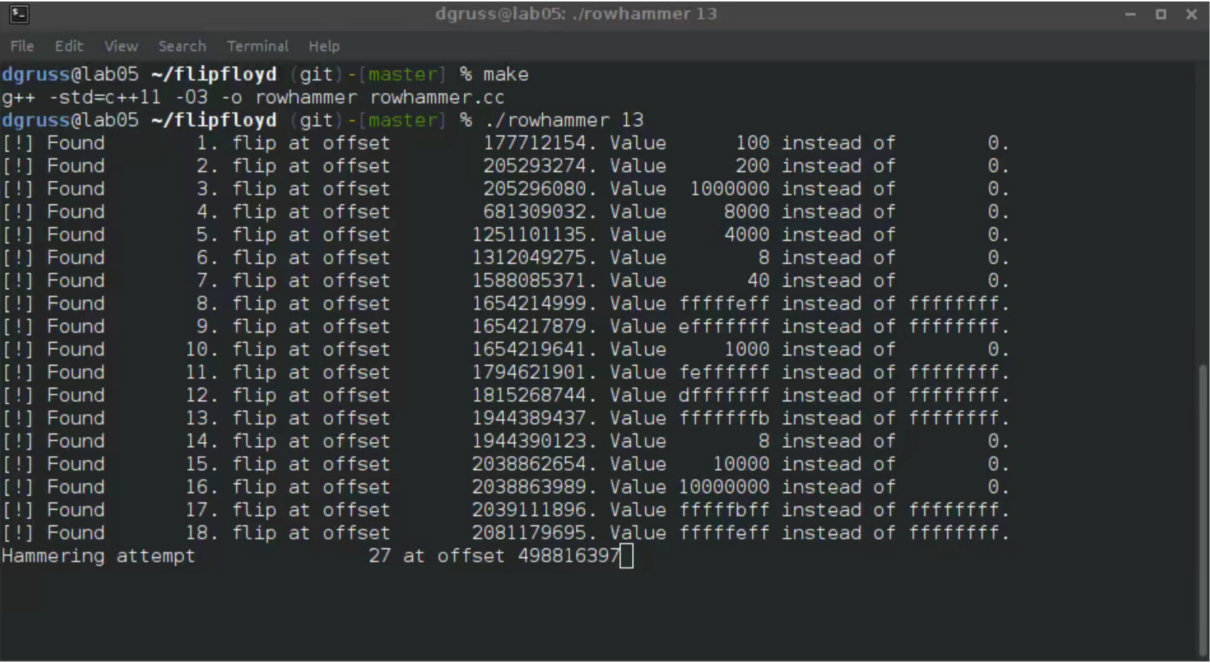
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset        177712154. Value      100 instead of        0.
[!] Found        2. flip at offset        205293274. Value      200 instead of        0.
[!] Found        3. flip at offset        205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset        681309032. Value     8000 instead of        0.
```



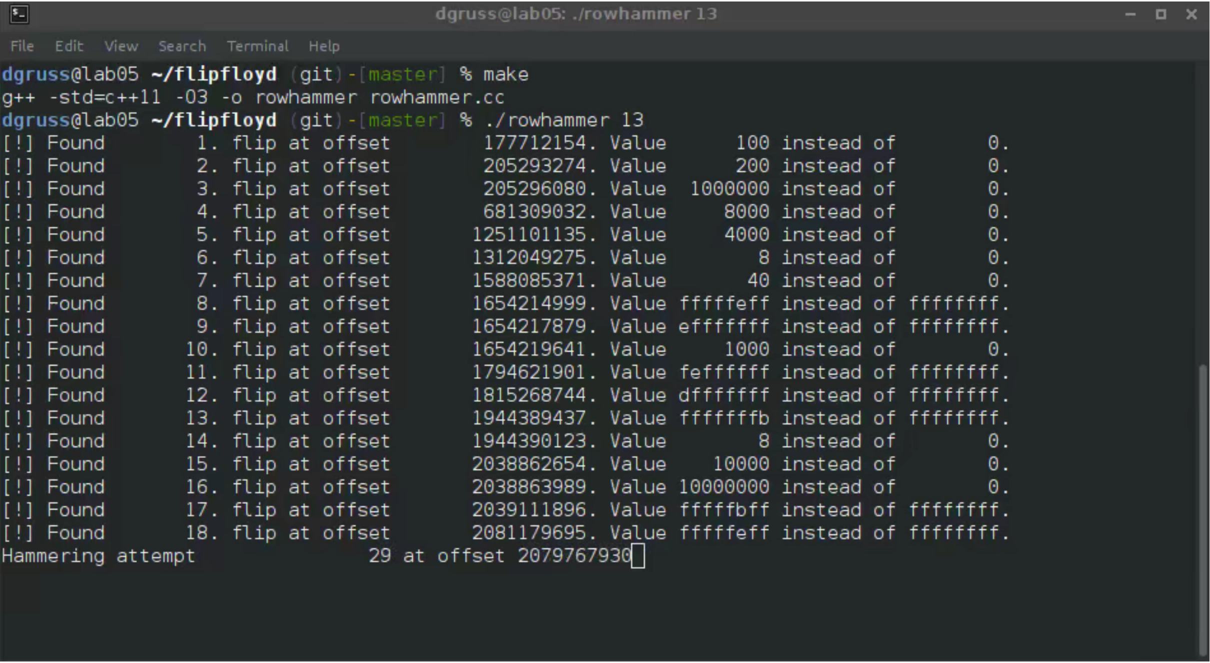
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset        177712154. Value      100 instead of        0.
[!] Found        2. flip at offset        205293274. Value      200 instead of        0.
[!] Found        3. flip at offset        205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset        681309032. Value     8000 instead of        0.
[!] Found        5. flip at offset       1251101135. Value     4000 instead of        0.
[!] Found        6. flip at offset       1312049275. Value        8 instead of        0.
[!] Found        7. flip at offset       1588085371. Value       40 instead of        0.
[!] Found        8. flip at offset       1654214999. Value fffffeff instead of ffffffff.
[!] Found        9. flip at offset       1654217879. Value efffffff instead of ffffffff.
[!] Found       10. flip at offset       1654219641. Value     1000 instead of        0.
[!] Found       11. flip at offset       1794621901. Value feffffff instead of ffffffff.
[!] Found       12. flip at offset       1815268744. Value dfffffff instead of ffffffff.
[!] Found       13. flip at offset       1944389437. Value fffffffb instead of ffffffff.
[!] Found       14. flip at offset       1944390123. Value        8 instead of        0.
```



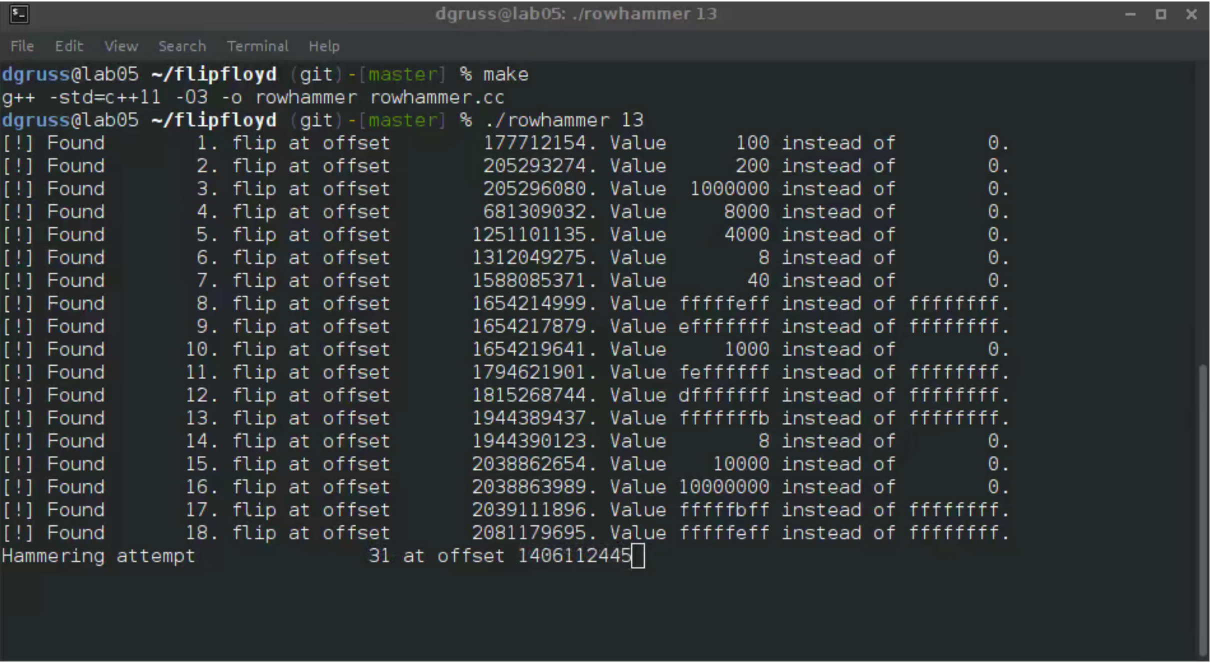
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset        177712154. Value      100 instead of        0.
[!] Found        2. flip at offset        205293274. Value      200 instead of        0.
[!] Found        3. flip at offset        205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset        681309032. Value     8000 instead of        0.
[!] Found        5. flip at offset       1251101135. Value     4000 instead of        0.
[!] Found        6. flip at offset       1312049275. Value        8 instead of        0.
[!] Found        7. flip at offset       1588085371. Value       40 instead of        0.
[!] Found        8. flip at offset       1654214999. Value  ffffeff instead of  fffffff.
[!] Found        9. flip at offset       1654217879. Value  effffff instead of  fffffff.
[!] Found       10. flip at offset       1654219641. Value     1000 instead of        0.
[!] Found       11. flip at offset       1794621901. Value  fefffff instead of  fffffff.
[!] Found       12. flip at offset       1815268744. Value  dffffff instead of  fffffff.
[!] Found       13. flip at offset       1944389437. Value  ffffffb instead of  fffffff.
[!] Found       14. flip at offset       1944390123. Value        8 instead of        0.
[!] Found       15. flip at offset       2038862654. Value    10000 instead of        0.
[!] Found       16. flip at offset       2038863989. Value 10000000 instead of        0.
[!] Found       17. flip at offset       2039111896. Value  ffffbff instead of  fffffff.
[!] Found       18. flip at offset       2081179695. Value  ffffeff instead of  fffffff.
```



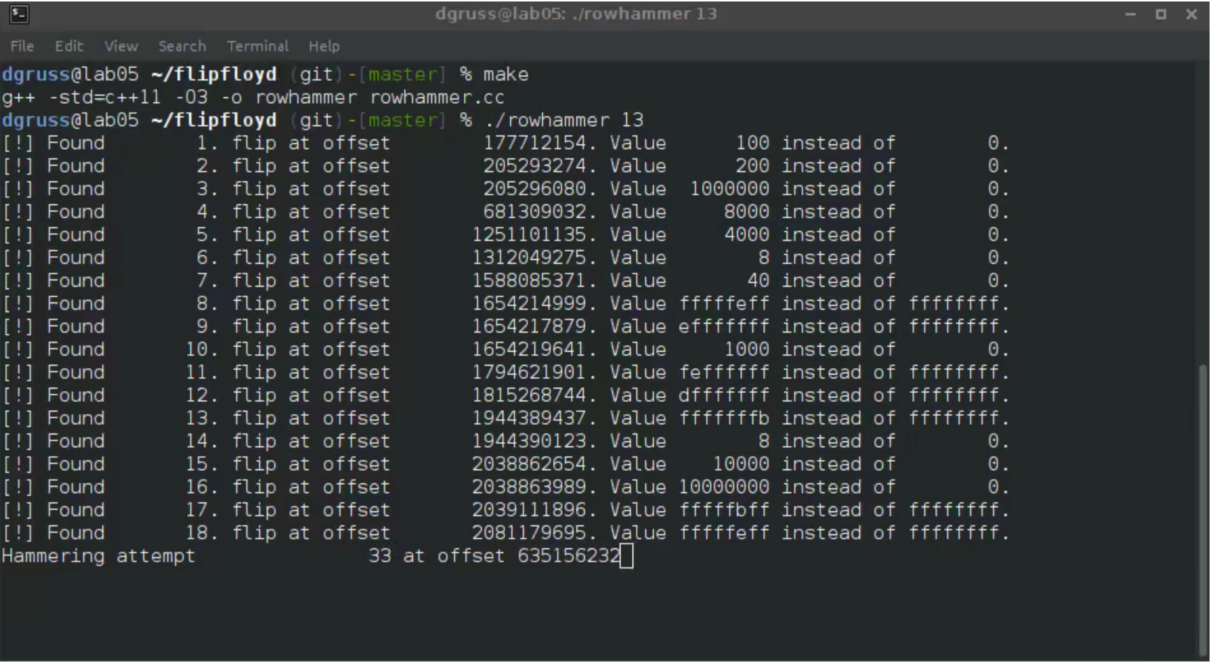
```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset         177712154. Value      100 instead of        0.
[!] Found        2. flip at offset         205293274. Value      200 instead of        0.
[!] Found        3. flip at offset         205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset         681309032. Value     8000 instead of        0.
[!] Found        5. flip at offset        1251101135. Value     4000 instead of        0.
[!] Found        6. flip at offset        1312049275. Value        8 instead of        0.
[!] Found        7. flip at offset        1588085371. Value       40 instead of        0.
[!] Found        8. flip at offset        1654214999. Value fffffeff instead of ffffffff.
[!] Found        9. flip at offset        1654217879. Value efffffff instead of ffffffff.
[!] Found       10. flip at offset        1654219641. Value     1000 instead of        0.
[!] Found       11. flip at offset        1794621901. Value feffffff instead of ffffffff.
[!] Found       12. flip at offset        1815268744. Value dfffffff instead of ffffffff.
[!] Found       13. flip at offset        1944389437. Value fffffffb instead of ffffffff.
[!] Found       14. flip at offset        1944390123. Value        8 instead of        0.
[!] Found       15. flip at offset        2038862654. Value    10000 instead of        0.
[!] Found       16. flip at offset        2038863989. Value 10000000 instead of        0.
[!] Found       17. flip at offset        2039111896. Value fffffbff instead of ffffffff.
[!] Found       18. flip at offset        2081179695. Value fffffeff instead of ffffffff.
Hammering attempt               27 at offset 498816397
```



```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset         177712154. Value      100 instead of        0.
[!] Found        2. flip at offset         205293274. Value      200 instead of        0.
[!] Found        3. flip at offset         205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset         681309032. Value     8000 instead of        0.
[!] Found        5. flip at offset        1251101135. Value     4000 instead of        0.
[!] Found        6. flip at offset        1312049275. Value        8 instead of        0.
[!] Found        7. flip at offset        1588085371. Value       40 instead of        0.
[!] Found        8. flip at offset        1654214999. Value fffffeff instead of ffffffff.
[!] Found        9. flip at offset        1654217879. Value efffffff instead of ffffffff.
[!] Found       10. flip at offset        1654219641. Value     1000 instead of        0.
[!] Found       11. flip at offset        1794621901. Value feffffff instead of ffffffff.
[!] Found       12. flip at offset        1815268744. Value dfffffff instead of ffffffff.
[!] Found       13. flip at offset        1944389437. Value fffffffb instead of ffffffff.
[!] Found       14. flip at offset        1944390123. Value        8 instead of        0.
[!] Found       15. flip at offset        2038862654. Value    10000 instead of        0.
[!] Found       16. flip at offset        2038863989. Value 10000000 instead of        0.
[!] Found       17. flip at offset        2039111896. Value fffffbff instead of ffffffff.
[!] Found       18. flip at offset        2081179695. Value fffffeff instead of ffffffff.
Hammering attempt               29 at offset 2079767930
```



```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset        177712154. Value      100 instead of        0.
[!] Found        2. flip at offset        205293274. Value      200 instead of        0.
[!] Found        3. flip at offset        205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset        681309032. Value     8000 instead of        0.
[!] Found        5. flip at offset       1251101135. Value     4000 instead of        0.
[!] Found        6. flip at offset       1312049275. Value        8 instead of        0.
[!] Found        7. flip at offset       1588085371. Value       40 instead of        0.
[!] Found        8. flip at offset       1654214999. Value fffffeff instead of ffffffff.
[!] Found        9. flip at offset       1654217879. Value efffffff instead of ffffffff.
[!] Found       10. flip at offset       1654219641. Value     1000 instead of        0.
[!] Found       11. flip at offset       1794621901. Value feffffff instead of ffffffff.
[!] Found       12. flip at offset       1815268744. Value dfffffff instead of ffffffff.
[!] Found       13. flip at offset       1944389437. Value fffffffb instead of ffffffff.
[!] Found       14. flip at offset       1944390123. Value        8 instead of        0.
[!] Found       15. flip at offset       2038862654. Value    10000 instead of        0.
[!] Found       16. flip at offset       2038863989. Value 10000000 instead of        0.
[!] Found       17. flip at offset       2039111896. Value fffffbff instead of ffffffff.
[!] Found       18. flip at offset       2081179695. Value fffffeff instead of ffffffff.
Hammering attempt               31 at offset 1406112445
```



```
dgruss@lab05 ~/flipfloyd (git)-[master] % make
g++ -std=c++11 -O3 -o rowhammer rowhammer.cc
dgruss@lab05 ~/flipfloyd (git)-[master] % ./rowhammer 13
[!] Found        1. flip at offset        177712154. Value      100 instead of        0.
[!] Found        2. flip at offset        205293274. Value      200 instead of        0.
[!] Found        3. flip at offset        205296080. Value  1000000 instead of        0.
[!] Found        4. flip at offset        681309032. Value     8000 instead of        0.
[!] Found        5. flip at offset       1251101135. Value     4000 instead of        0.
[!] Found        6. flip at offset       1312049275. Value        8 instead of        0.
[!] Found        7. flip at offset       1588085371. Value       40 instead of        0.
[!] Found        8. flip at offset       1654214999. Value fffffeff instead of  fffffff.
[!] Found        9. flip at offset       1654217879. Value efffffff instead of  fffffff.
[!] Found       10. flip at offset       1654219641. Value     1000 instead of        0.
[!] Found       11. flip at offset       1794621901. Value feffffff instead of  fffffff.
[!] Found       12. flip at offset       1815268744. Value dfffffff instead of  fffffff.
[!] Found       13. flip at offset       1944389437. Value fffffffb instead of  fffffff.
[!] Found       14. flip at offset       1944390123. Value        8 instead of        0.
[!] Found       15. flip at offset       2038862654. Value    10000 instead of        0.
[!] Found       16. flip at offset       2038863989. Value 10000000 instead of        0.
[!] Found       17. flip at offset       2039111896. Value fffffbff instead of  fffffff.
[!] Found       18. flip at offset       2081179695. Value fffffeff instead of  fffffff.
Hammering attempt               33 at offset 635156232
```

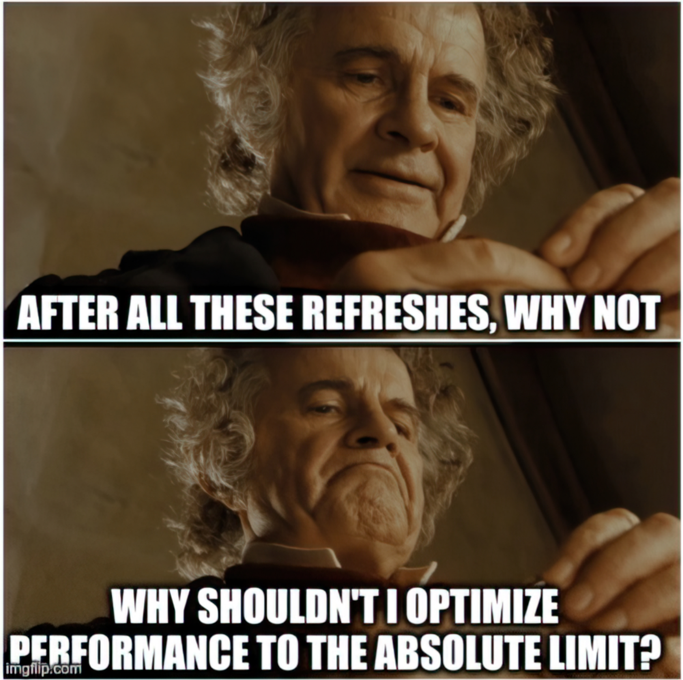
What do vendors do against it?

Mobile vendors since 2018: let’s add ECC by default, then it is more security!

What do vendors do against it?

Mobile vendors since 2018: let’s add ECC by default, then it is more security!

Also vendors: Let’s squeeze out the last bit of efficiency for battery runtime


AFTER ALL THESE REFRESHES, WHY NOT
WHY SHOULDN'T I OPTIMIZE PERFORMANCE TO THE ABSOLUTE LIMIT?
imgflip.com

OH NOES, A NEW ROWHAMMER ATTACK

Principled Cryptographic Security and Integrity

Make bit flips degrade performance **without** impacting security

Principled Cryptographic Security and Integrity

Make bit flips degrade performance **without** impacting security

- Cryptographic MAC

Principled Cryptographic Security and Integrity

Make bit flips degrade performance **without** impacting security

- Cryptographic MAC
- Detect **any** number of bit flips

Principled Cryptographic Security and Integrity

Make bit flips degrade performance **without** impacting security

- Cryptographic MAC
- Detect **any** number of bit flips
- Correction by **brute-force** search for correct data

CSI:Rowhammer Security Guarantees

CSI:Rowhammer Security Guarantees

CSI:Rowhammer Security Guarantees

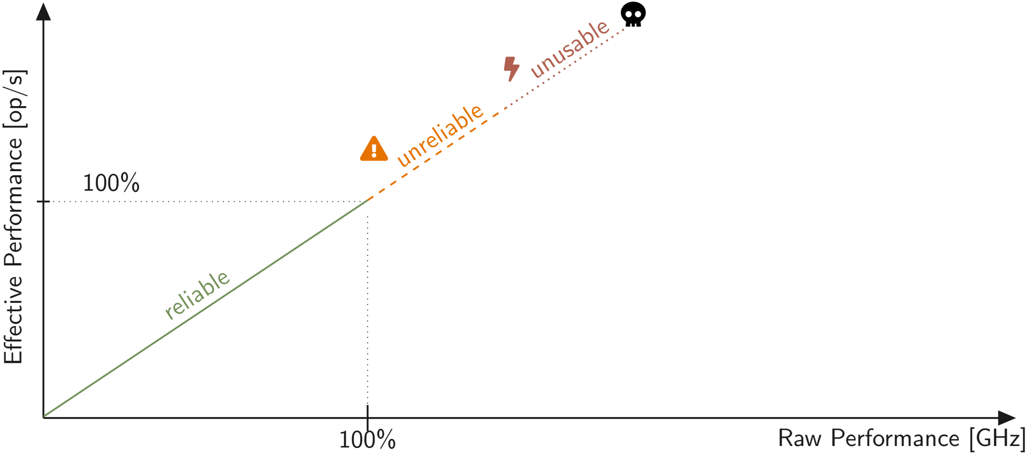
- Silent data corruption less than once per 10^9 billion years

CSI:Rowhammer Security Guarantees

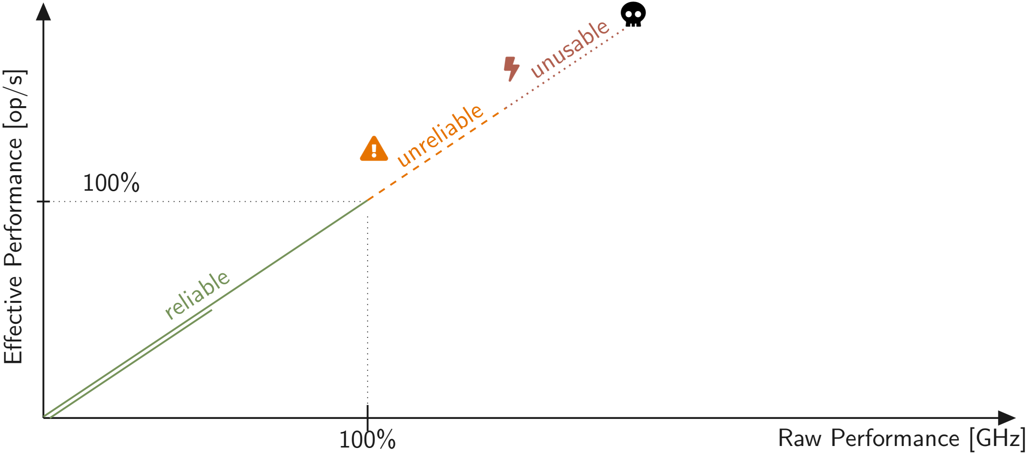
- Silent data corruption less than once per 10^9 billion years
- Second preimage after hammering for one year: $9.75 \cdot 10^{-5}\,\%$

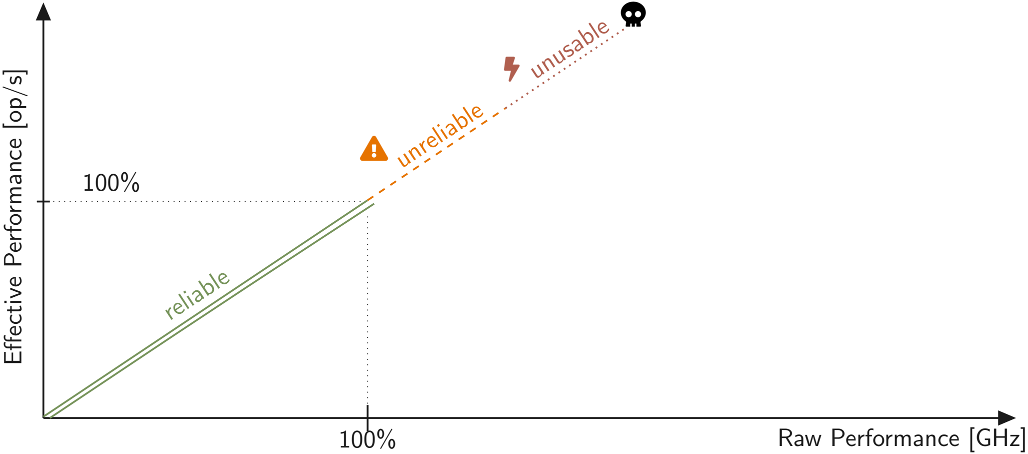
CSI:Rowhammer Security Guarantees

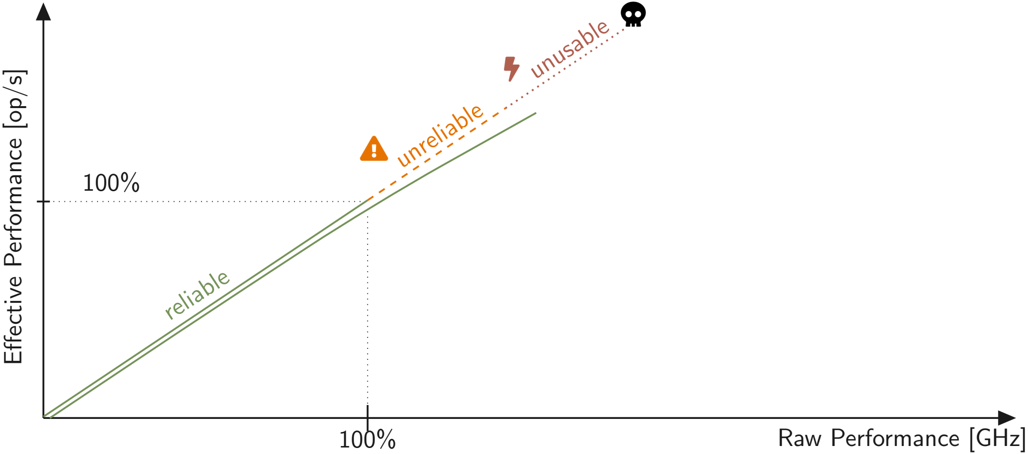
- Silent data corruption less than once per 10^9 billion years
- Second preimage after hammering for one year: $9.75 \cdot 10^{-5}\,\%$
- Erroneous correction of 8-bit errors: $0.0161\,\%$

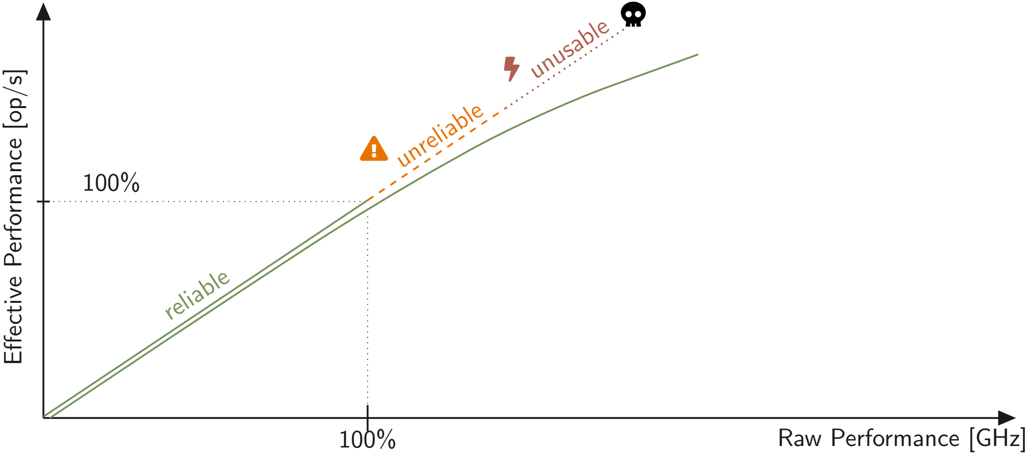


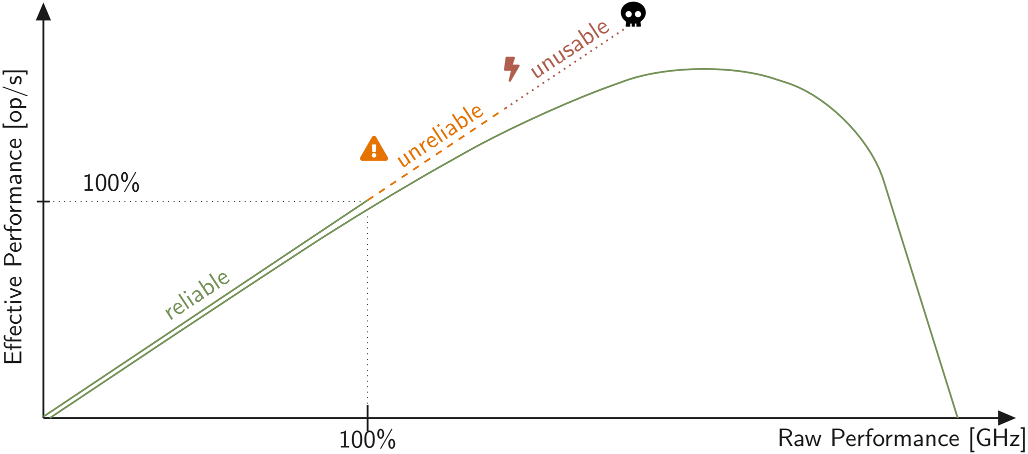
Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]

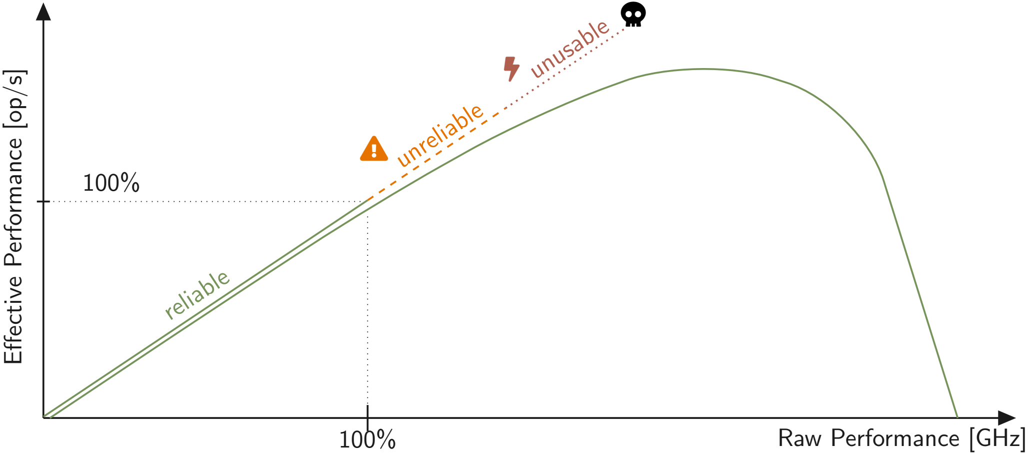

Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]

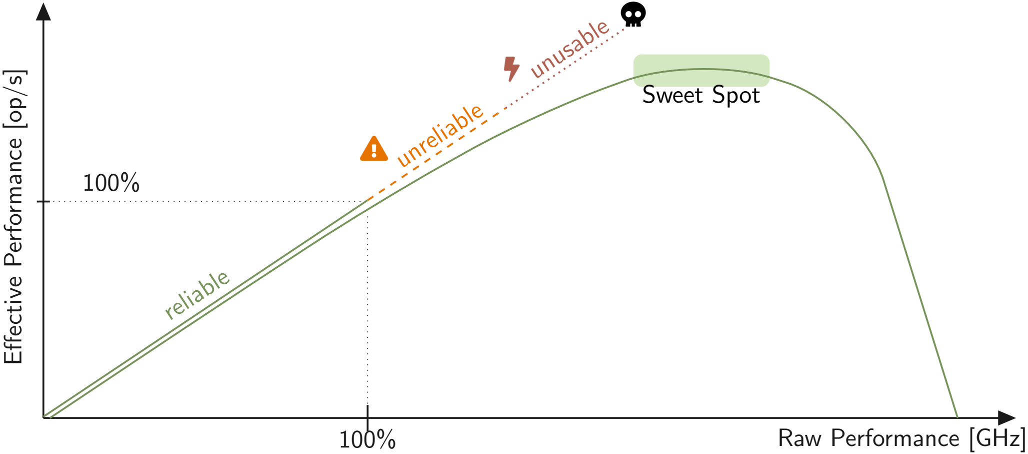

Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]


Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]


Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]


Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]


Effective Performance [op/s]
100%
reliable
unreliable
unusable
100%
Raw Performance [GHz]


Effective Performance [op/s]
100%
reliable
⚠ unreliable
unusable
Sweet Spot
100%
Raw Performance [GHz]

Conclusion

~~Conclusion~~ Road to Success

1. Add principled security

~~Conclusion~~ Road to Success

1. Add principled security
2. Bump up efficiency A LOT!

~~Conclusion~~ Road to Success

1. Add principled security
2. Bump up efficiency A LOT!
3. ...

~~Conclusion~~ Road to Success

1. Add principled security
2. Bump up efficiency A LOT!
3. ...
4. Profit!

~~Conclusion~~ Road to Success

1. Add principled security
2. Bump up efficiency A LOT!
3. Security just eats up some of the efficiency **we gained anyway**
4. Profit!

Mit Sicherheit effizient?

Daniel Gruss

TU Graz