Voltage Glitch using ChipWhisperer

ECE 559 – Project (Part 4)

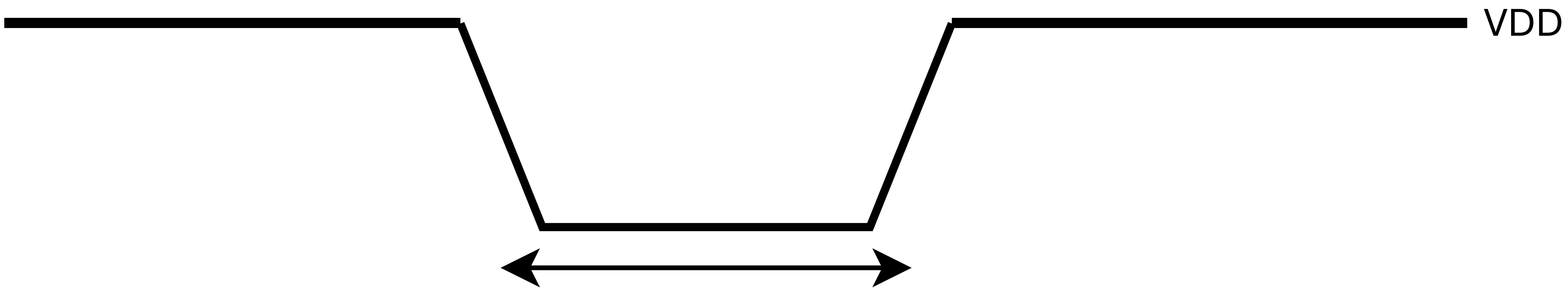
Sk Hasibul Alam

Md Mazharul Islam

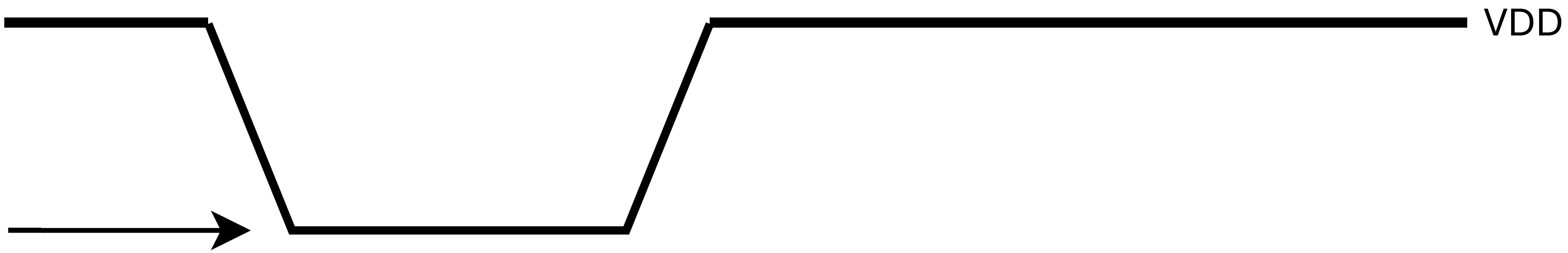
THE UNIVERSITY OF TENNESSEE KNOXVILLE

Preliminaries

- repeat



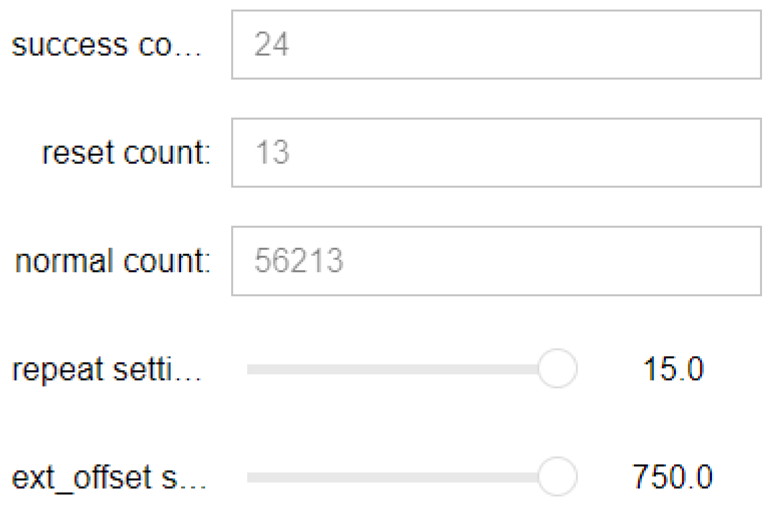
- ext_offset



Too short → No effect
Too long → Target crash

Part A: Glitching the for-loop

(a)



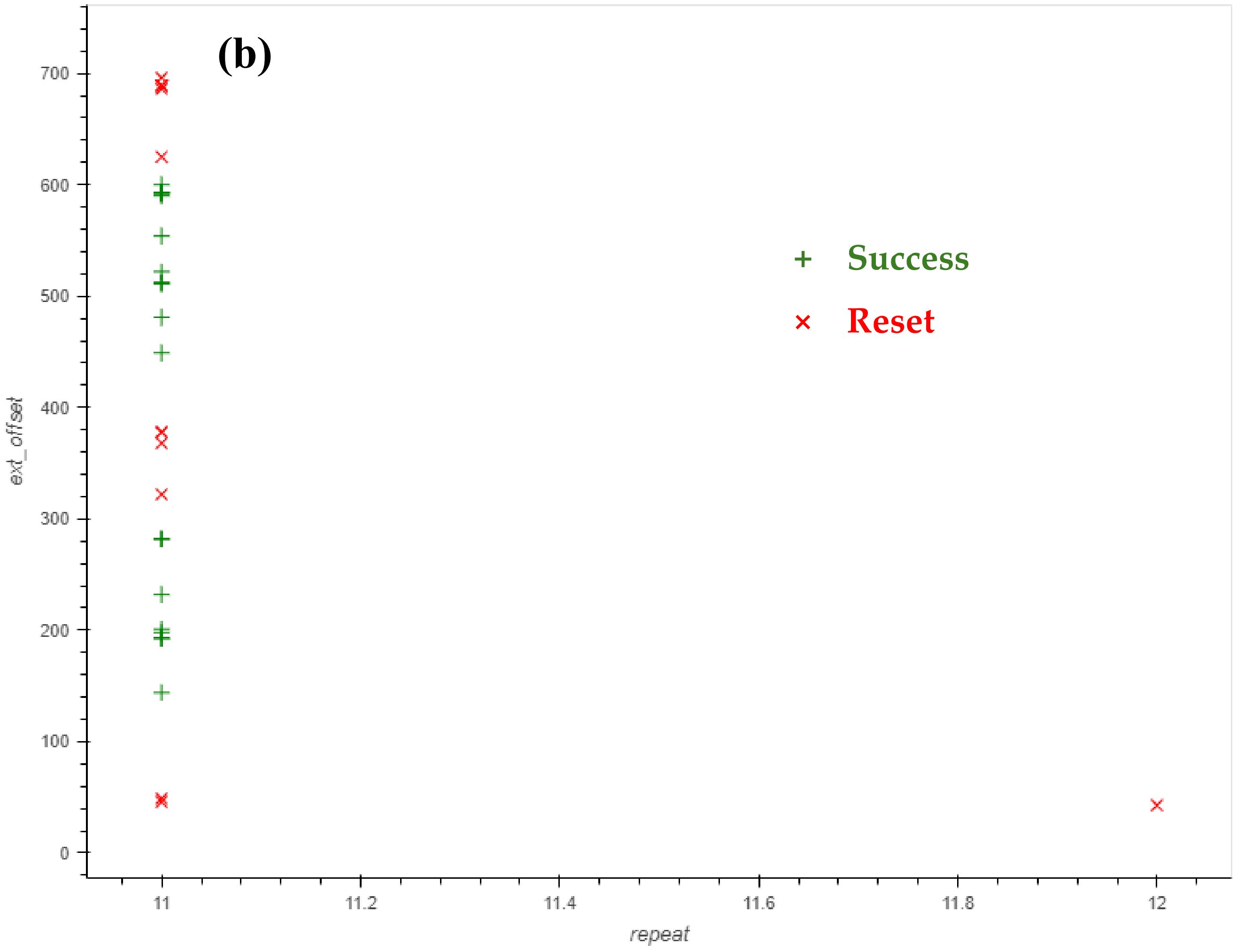
success co... 24

reset count: 13

normal count: 56213

repeat setti... 15.0

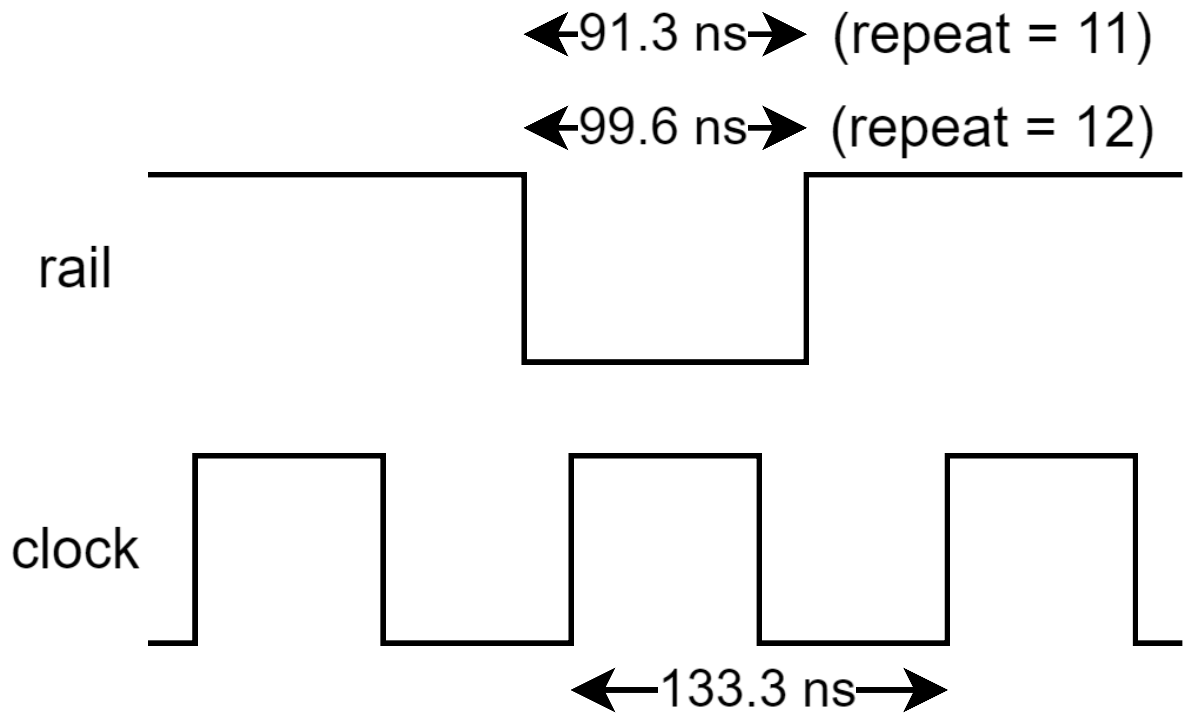
ext_offset s... 750.0



Speculation (*from* Part A)

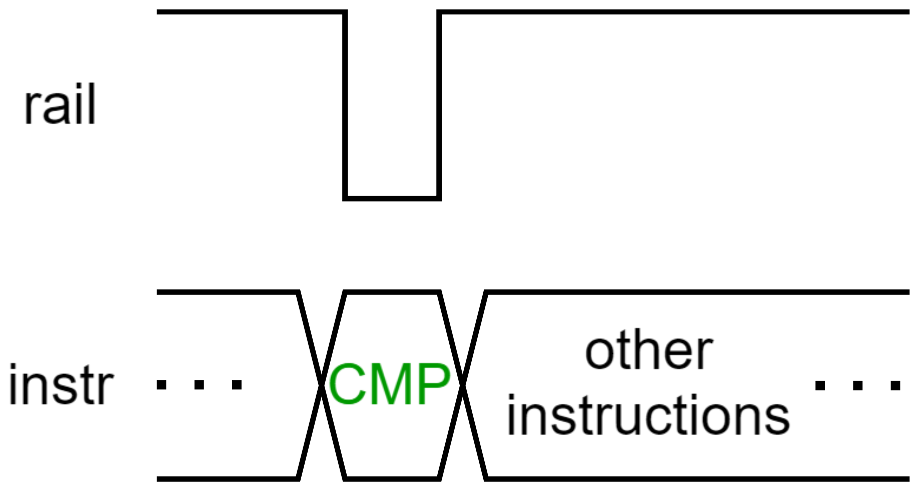
repeat

Typically, **11** or **12**



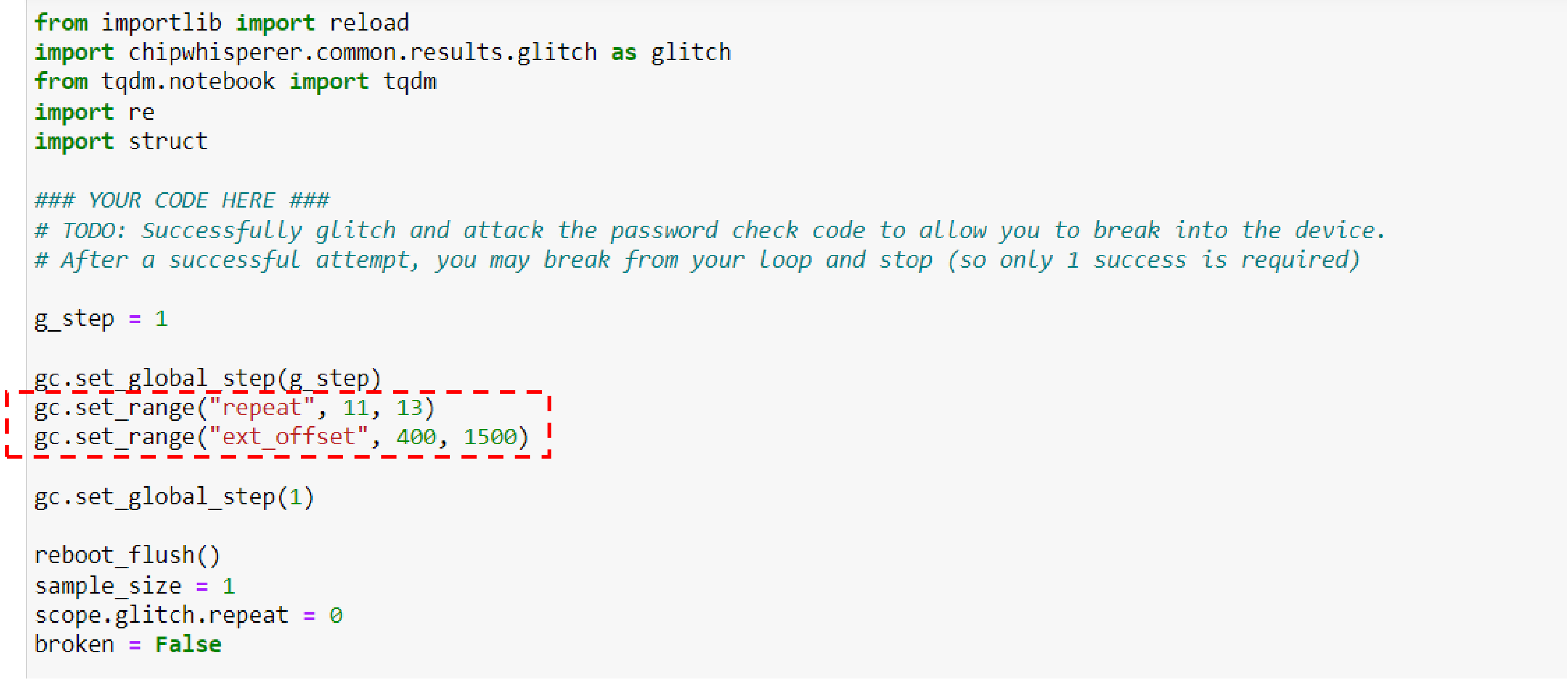
ext_offset

Wild range, between **50** and **950**



Part B: Bypassing the password

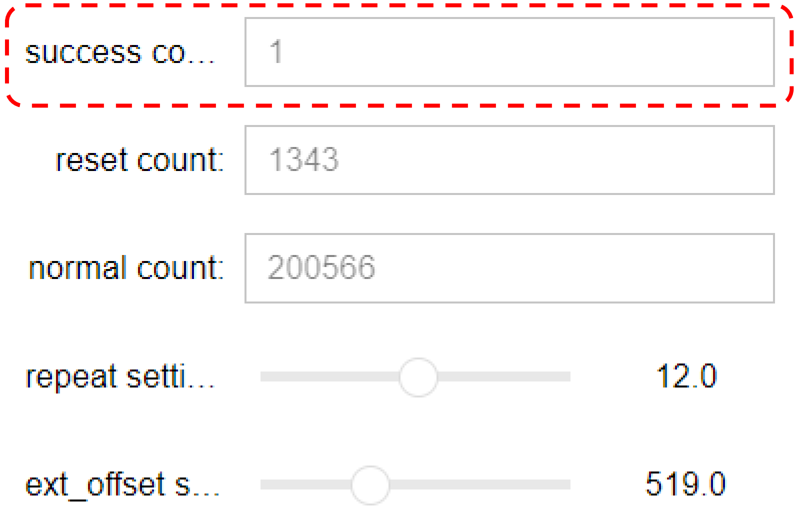
```
gc.set_range("repeat", 11, 13)
gc.set_range("ext_offset", 500, 600)
```



```
from importlib import reload
import chipwhisperer.common.results.glitch as glitch
from tqdm.notebook import tqdm
import re
import struct

### YOUR CODE HERE ###
# TODO: Successfully glitch and attack the password check code to allow you to break into the device.
# After a successful attempt, you may break from your loop and stop (so only 1 success is required)

g_step = 1

gc.set_global_step(g_step)
gc.set_range("repeat", 11, 13)
gc.set_range("ext_offset", 400, 1500)

gc.set_global_step(1)

reboot_flush()
sample_size = 1
scope.glitch.repeat = 0
broken = False
```

Success (Part B)

Only one success: Break after successful glitching



success co… 1

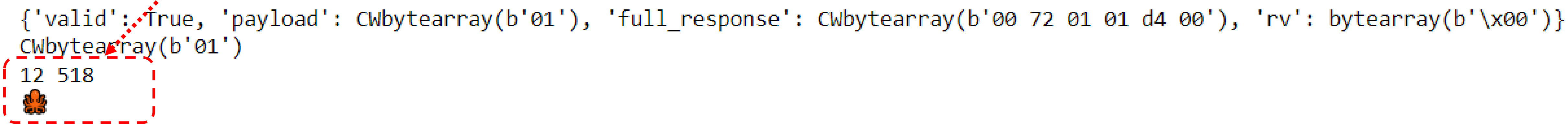
reset count: 1343

normal count: 200566

repeat setti… 12.0

ext_offset s… 519.0

Successful Glitching at Repeat : 12, External Offset : 518



```
{'valid': True, 'payload': CWbytearray(b'01'), 'full_response': CWbytearray(b'00 72 01 01 d4 00'), 'rv': bytearray(b'\x00')}
CWbytearray(b'01')
12 518
🐙
```

Questions?
Comments?
Concerns?