Lock Picking and Physical Security

Tyler Nighswander

Lock Picking and Physical Security

Tyler Nighswander

Introduction

- Who I am:
  - PPP member (specializes in crypto and hardware interested in everything!)
  - CMU student in Computer Science and Physics

Before I Start...

- Some of the things I'll talk about are complicated
- I don't speak any Korean so it is hard for me to explain things to you
- If something I say is not clear, **stop me and ask!**

- After I'm done talking, a few people at a time can try picking some locks I have brought. I will also be happy to answer any other questions!

Why Lockpicking

- Picking locks is a good lesson in how not to do security!

  (important to learn common mistakes so you don't do them)

- A system is only as strong as the weakest link

  (breaking into a physical server room is a great way to get access)

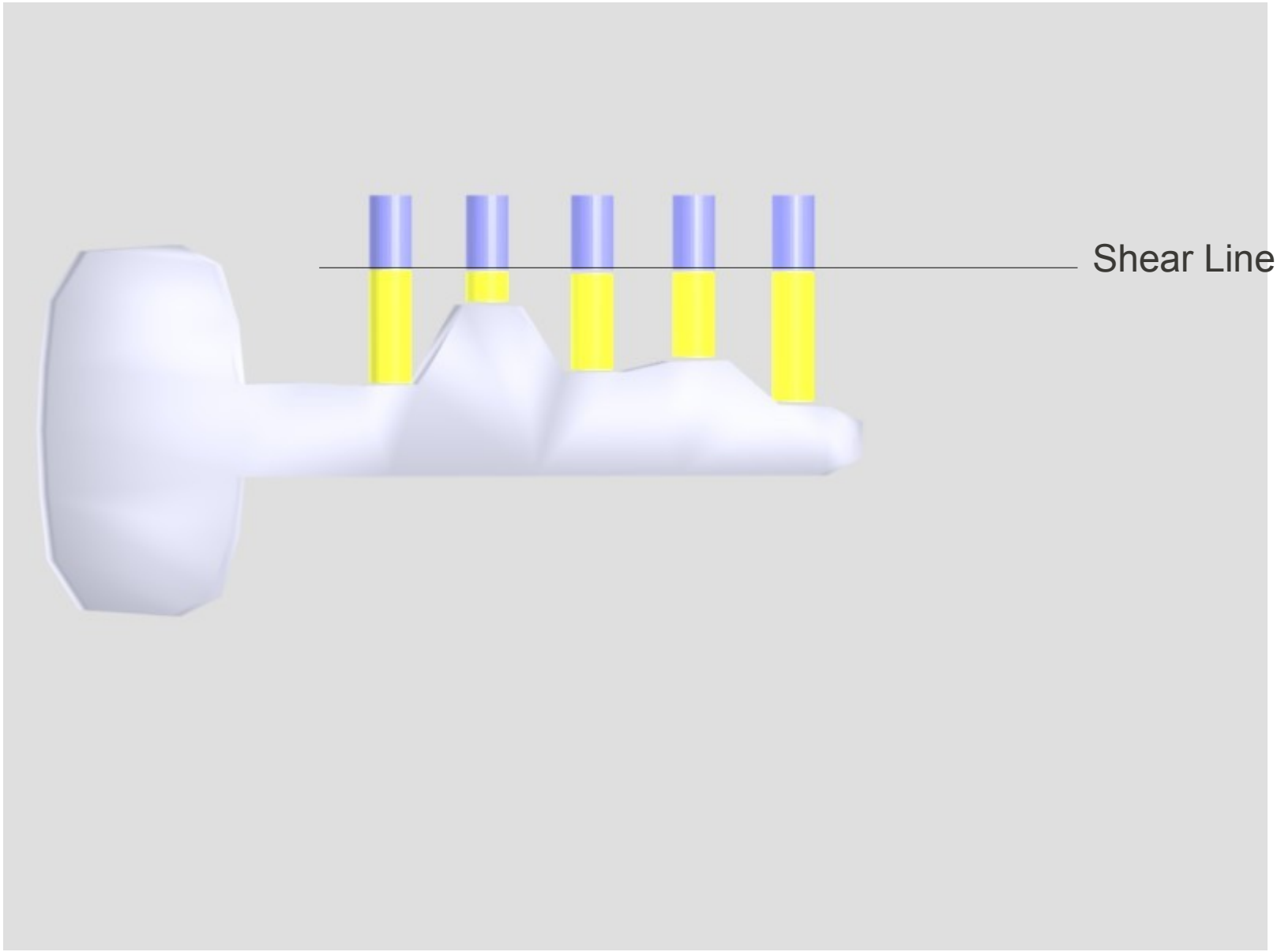
- Many relations to software security

  (especially cryptography, which I will talk about here)

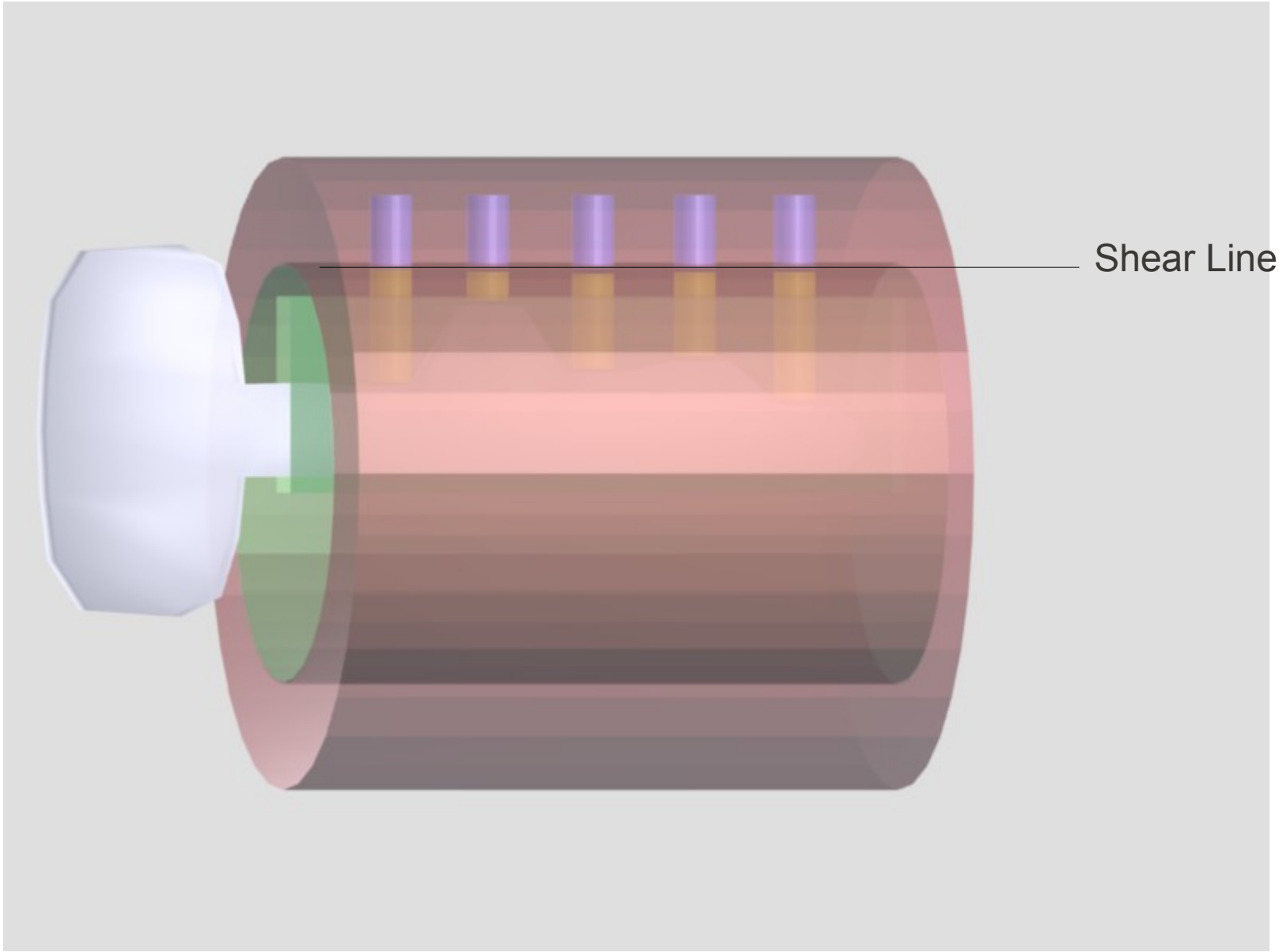
Disclaimer

- Breaking into places is illegal!
- In some areas, having lockpicks is illegal!
- Please be very careful and don't do anything you shouldn't!

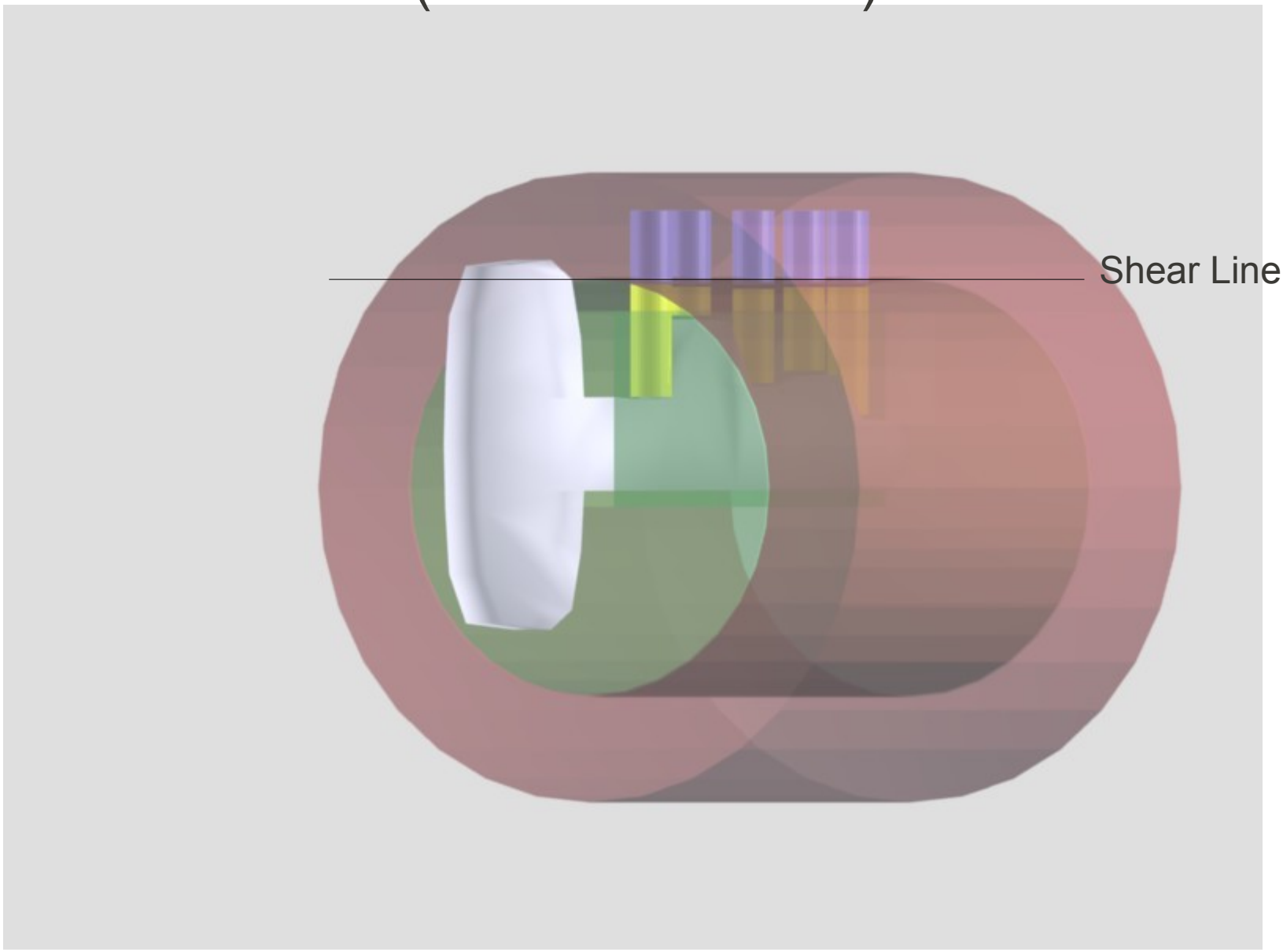
How locks work
(Pin and Tumbler)



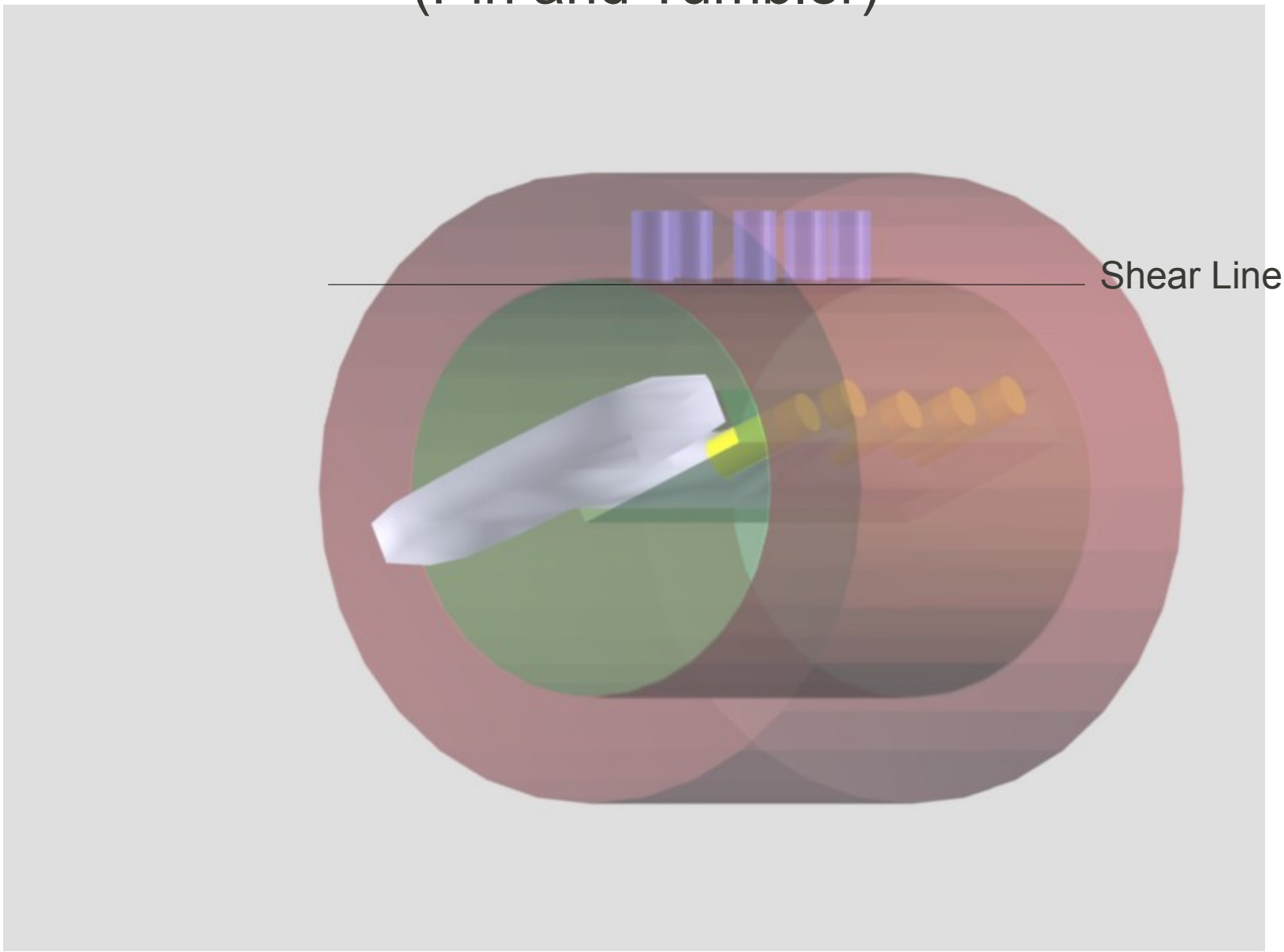
How locks work
(Pin and Tumbler)



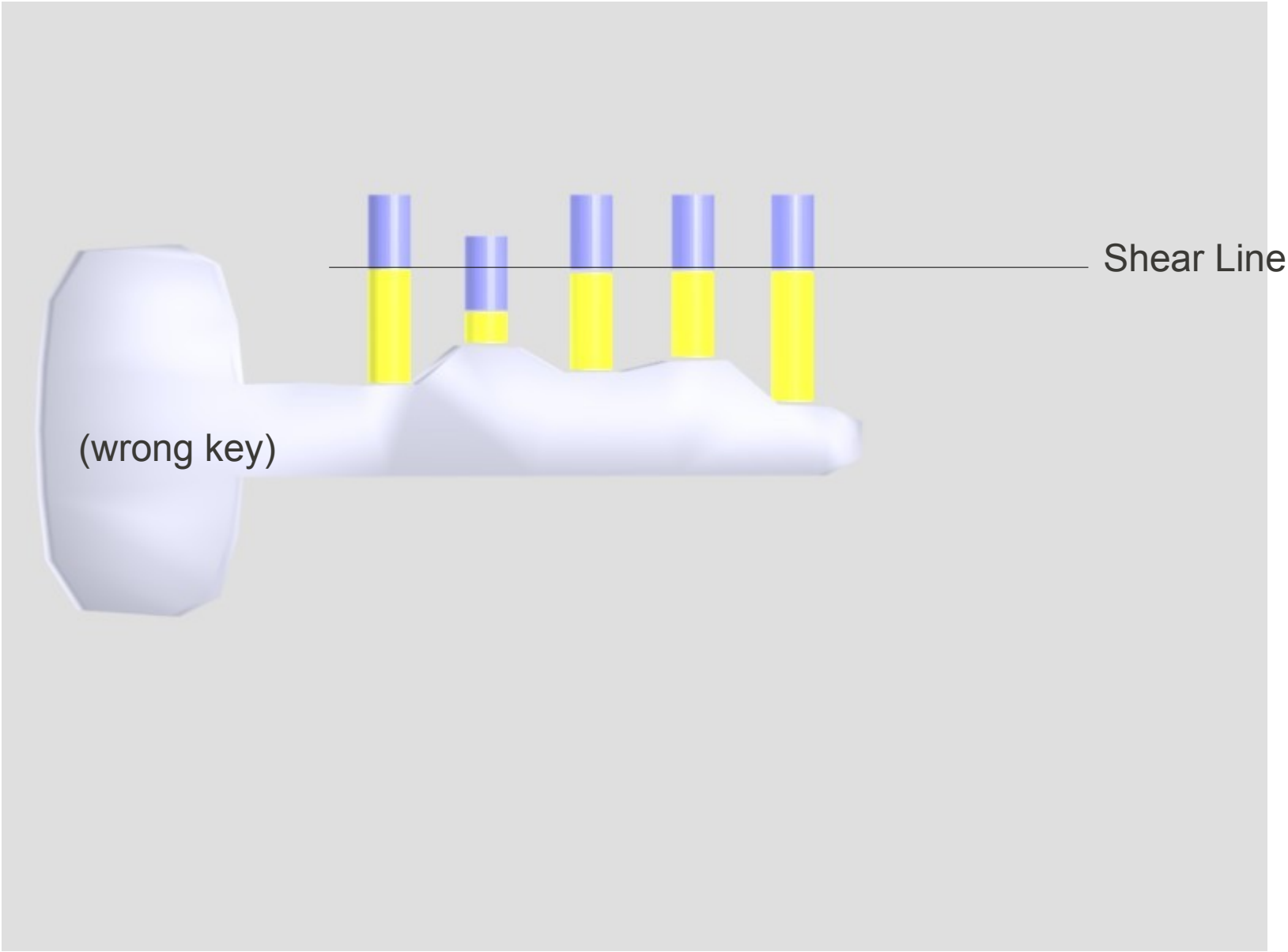
How locks work
(Pin and Tumbler)



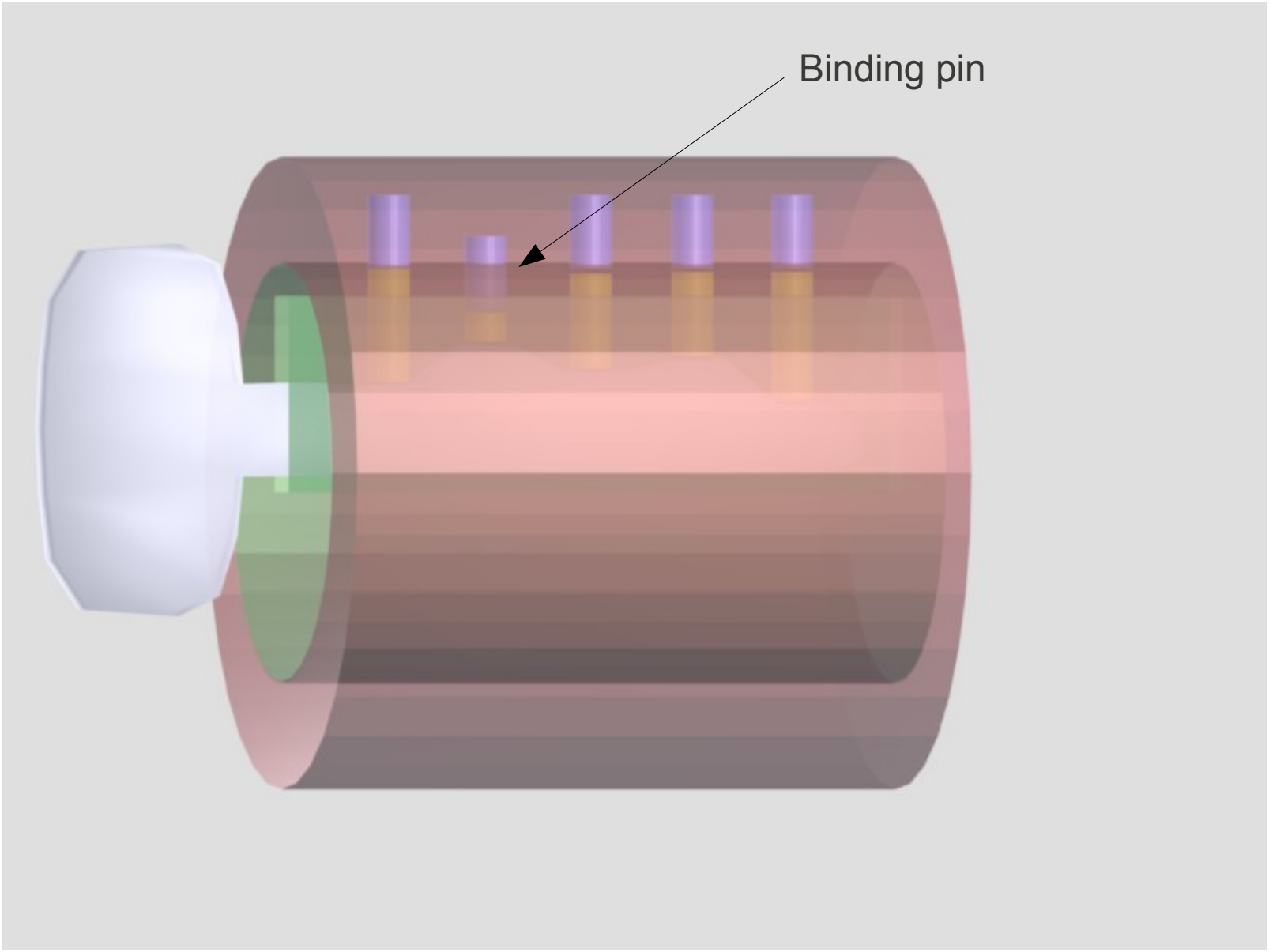
How locks work
(Pin and Tumbler)



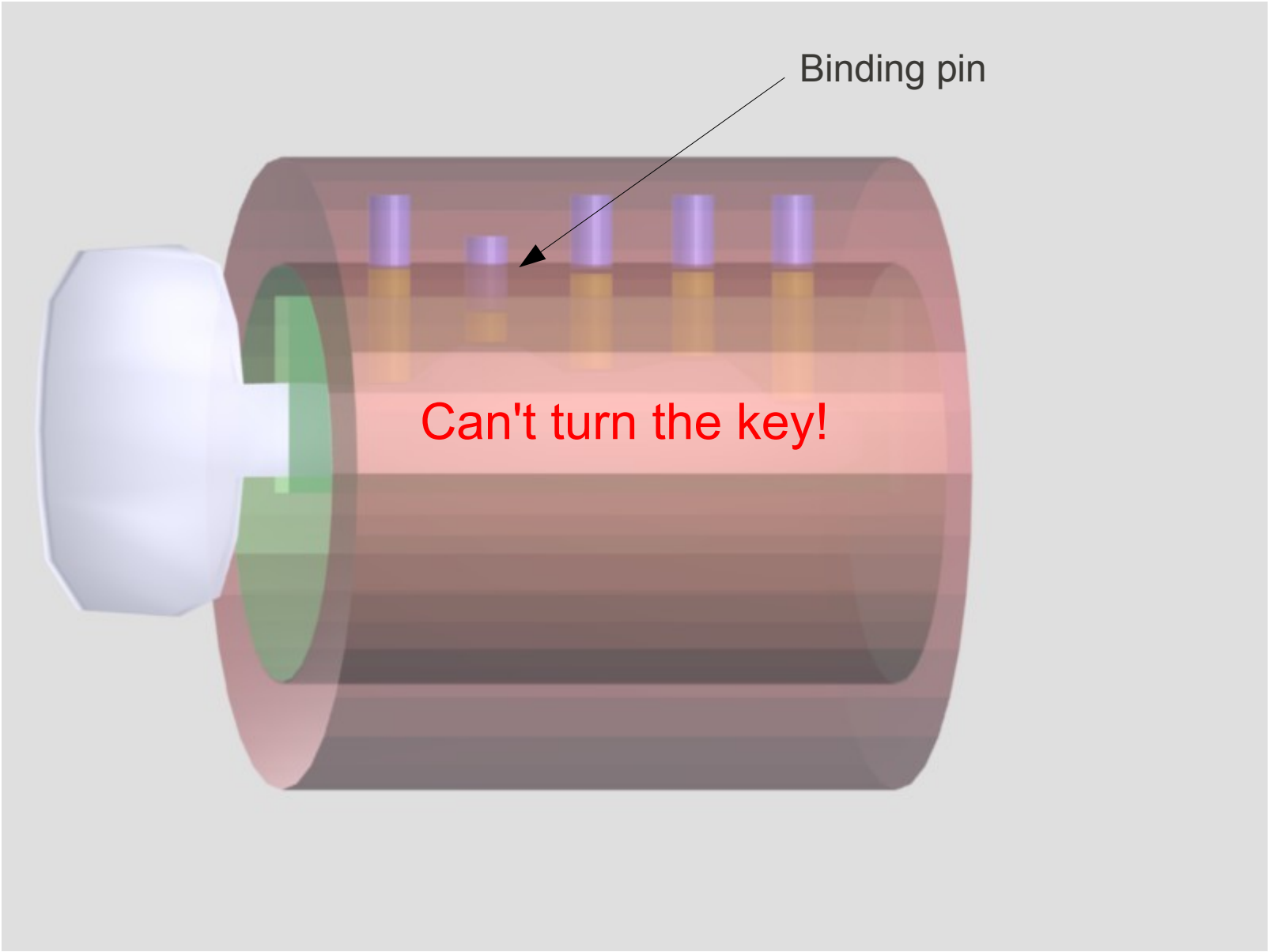
How locks work
(Pin and Tumbler)



How locks work
(Pin and Tumbler)

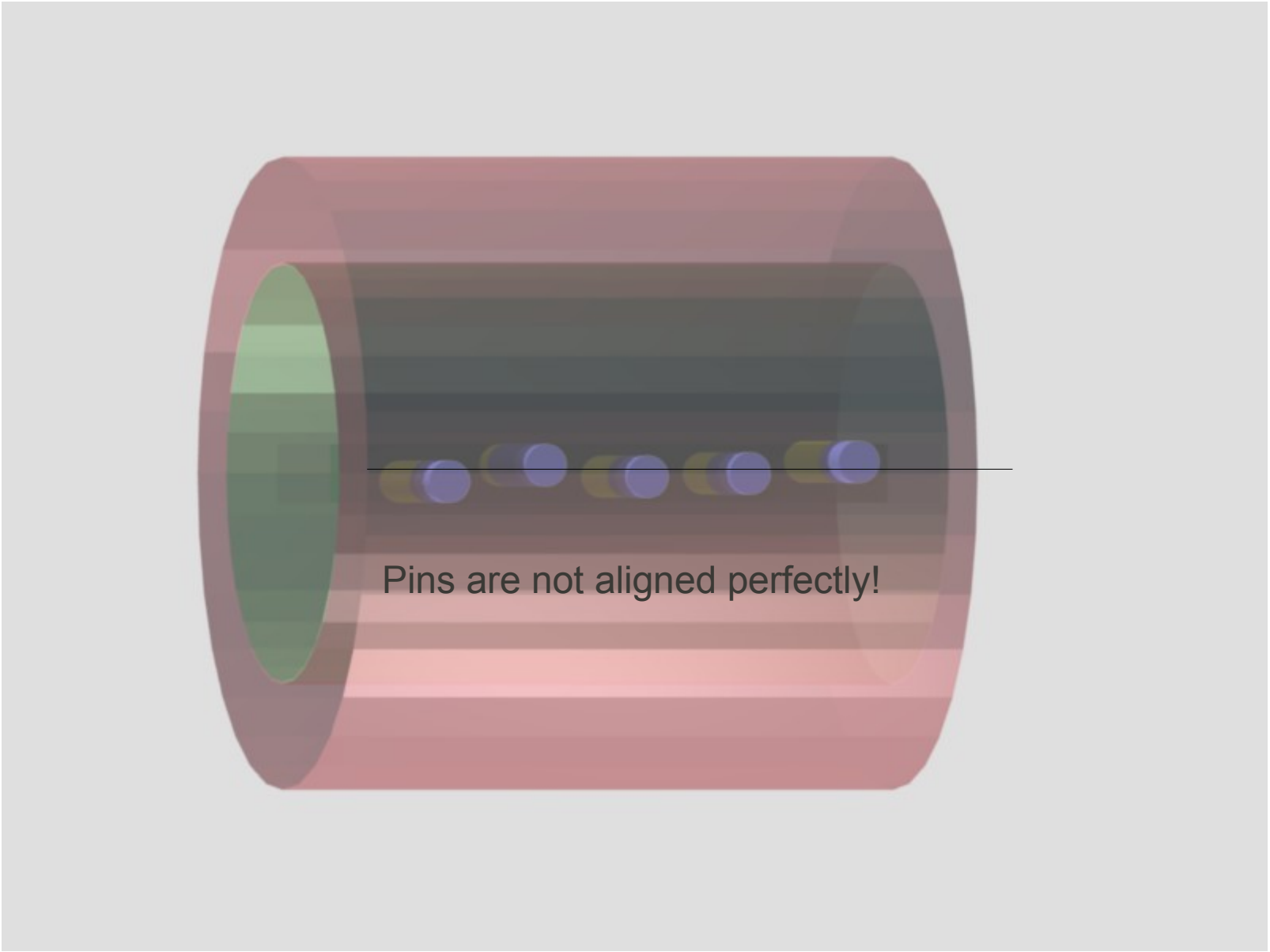


How locks work
(Pin and Tumbler)

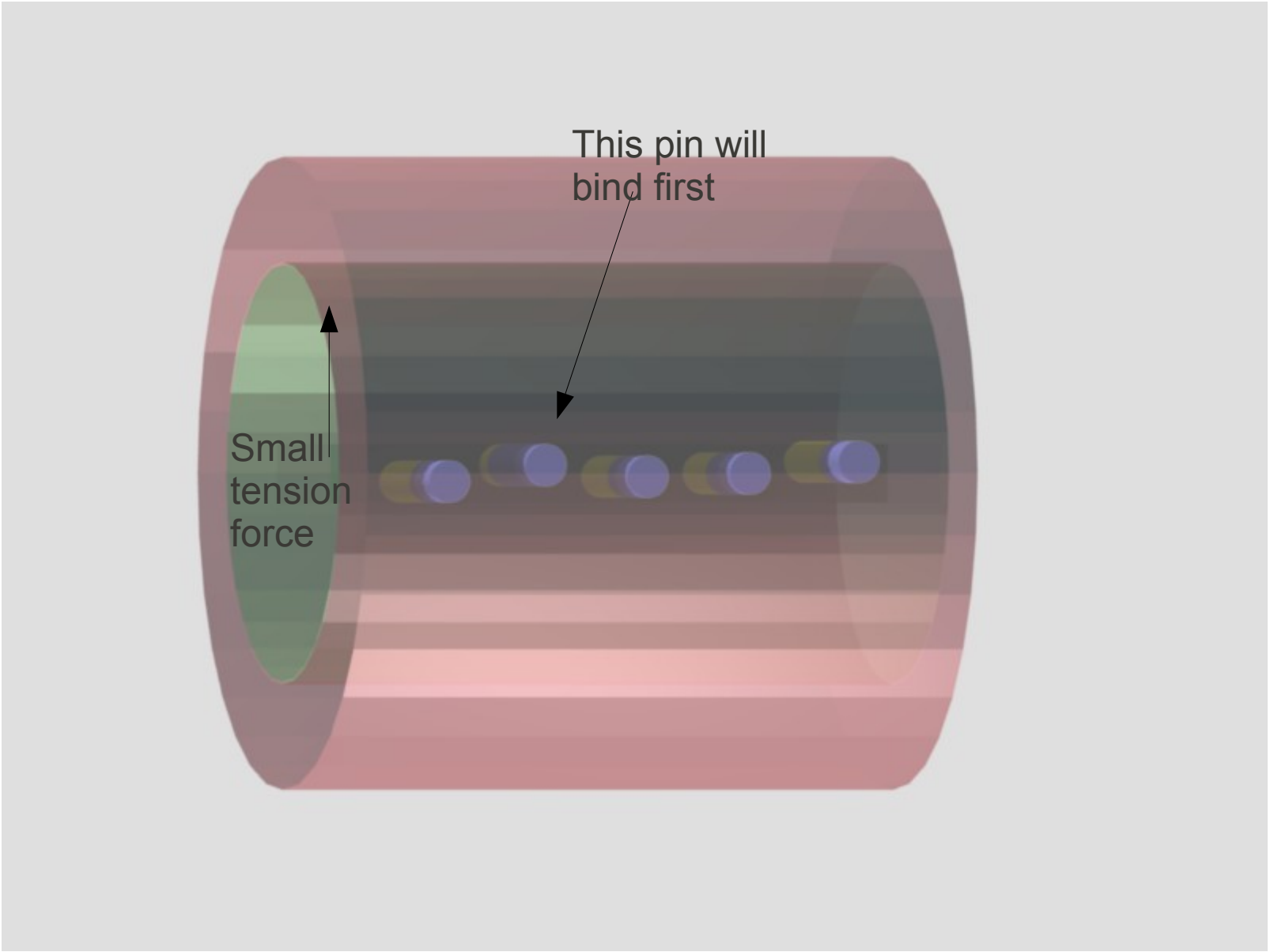


Questions so far?

Lockpicking

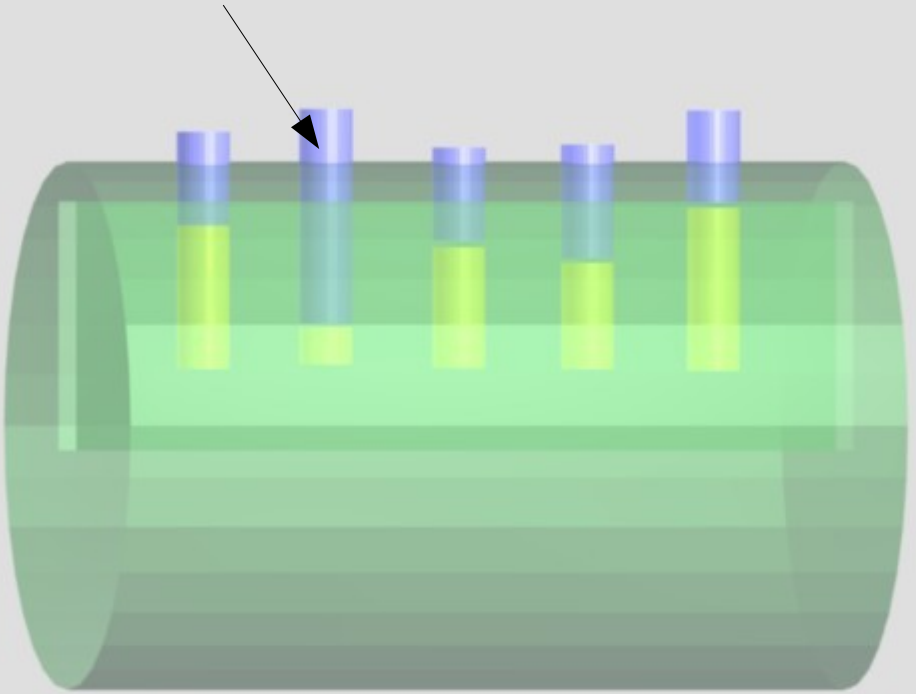


Lockpicking

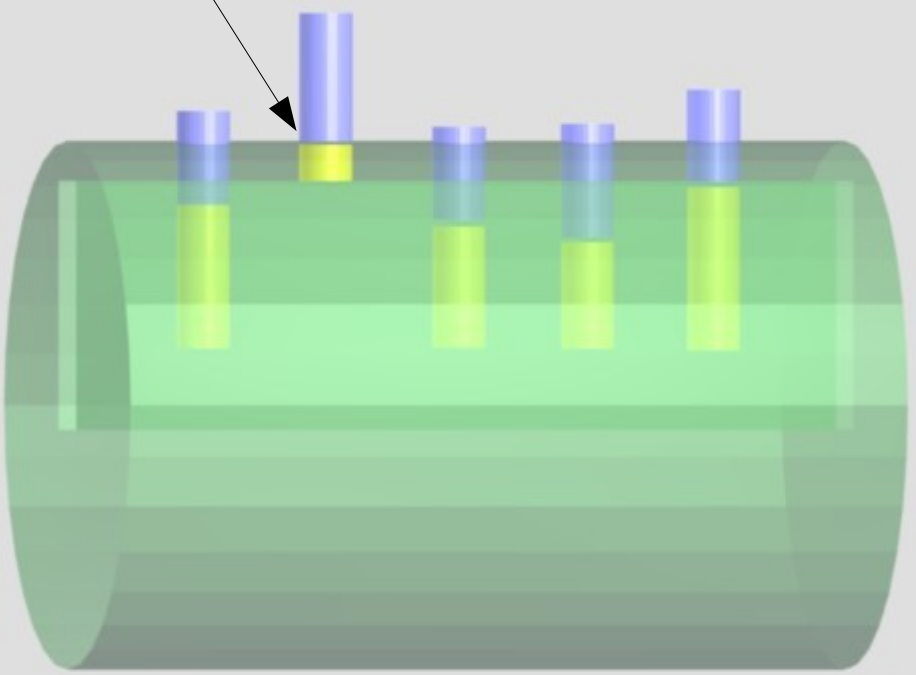


Lockpicking

Still putting tension on the cylinder, push up on that pin

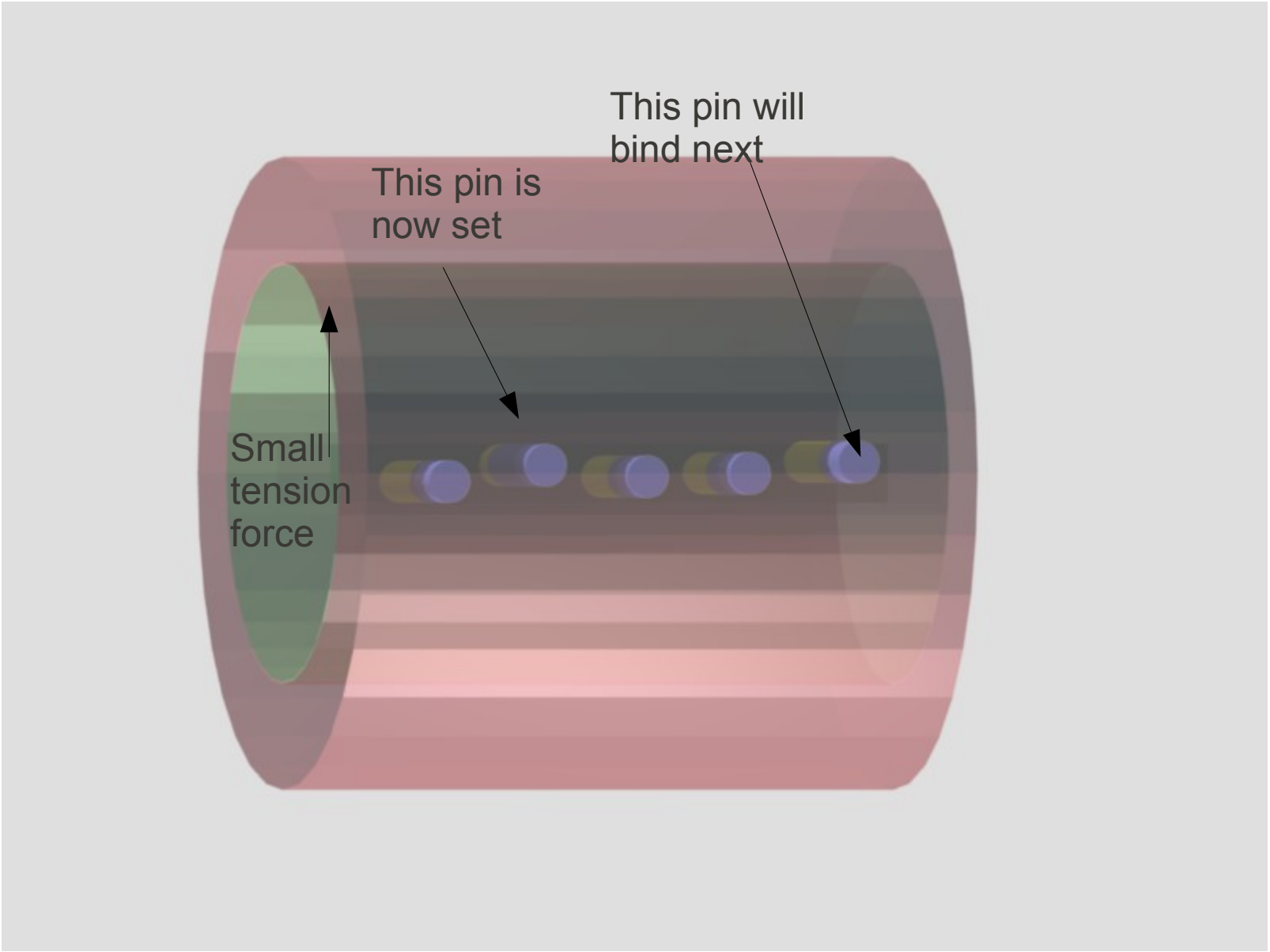


Lockpicking



When this happens, the cylinder should turn a tiny bit,
and you will hear a small click

Lockpicking



Lockpicking

L shaped tool is called “tension wrench”, this provides the turning force on the cylinder

Other tool is called the pick, use this to set the pins in the lock

Cryptography

- Just like in cryptography, only the “key” should be secret
  - Thief may possess the lock
  - Hacker may possess an encrypted file

Cryptography

- Just like in cryptography, only the “key” should be secret
  - Thief may possess the lock
  - Hacker may possess an encrypted file
- *Unlike* cryptography, finding “key” can usually be done in $O(n)$ tries vs $O(2^n)$
  - Makes physical locks much less secure than digital ones!

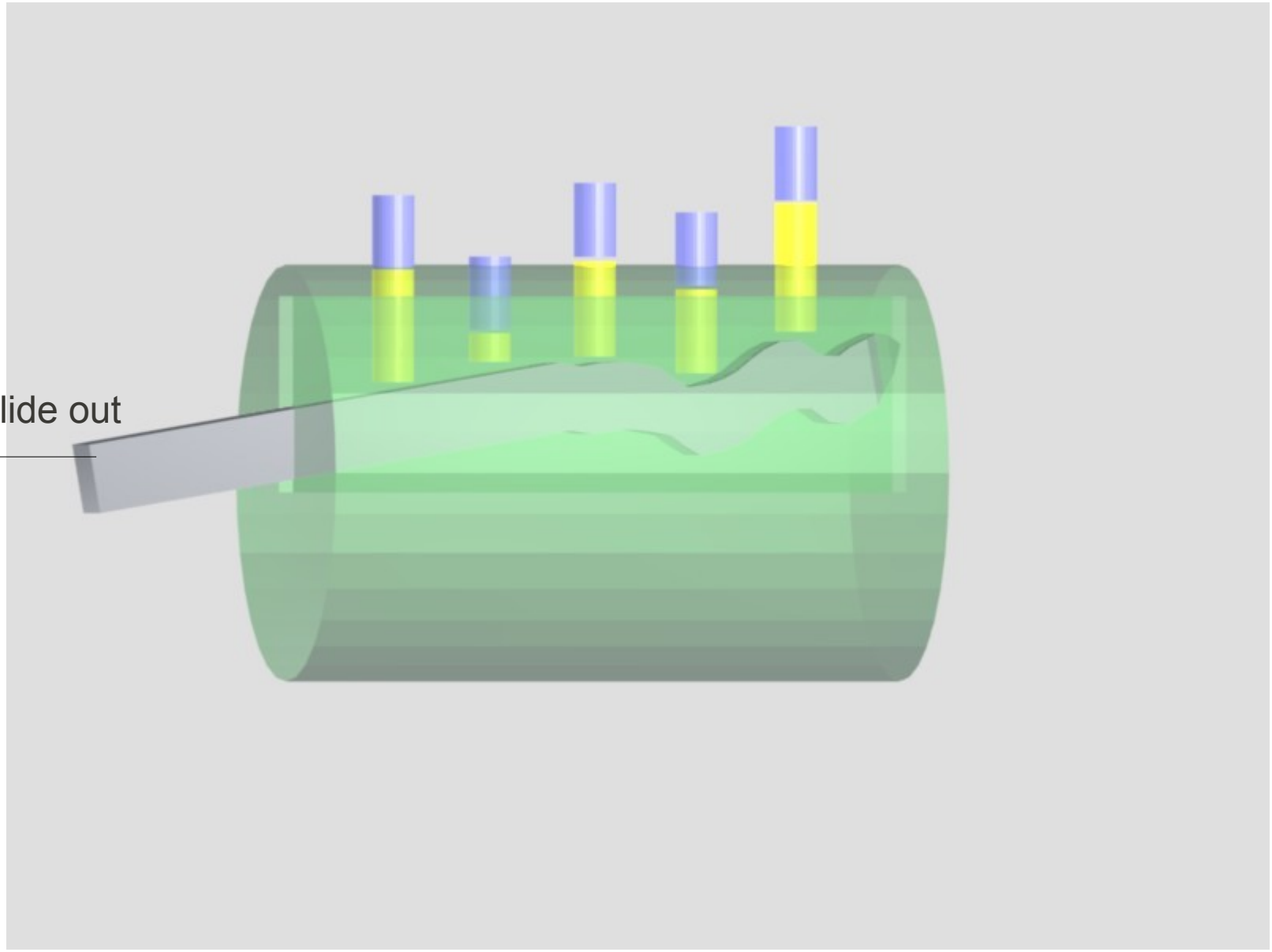
That sounds too easy!

It can be even easier!

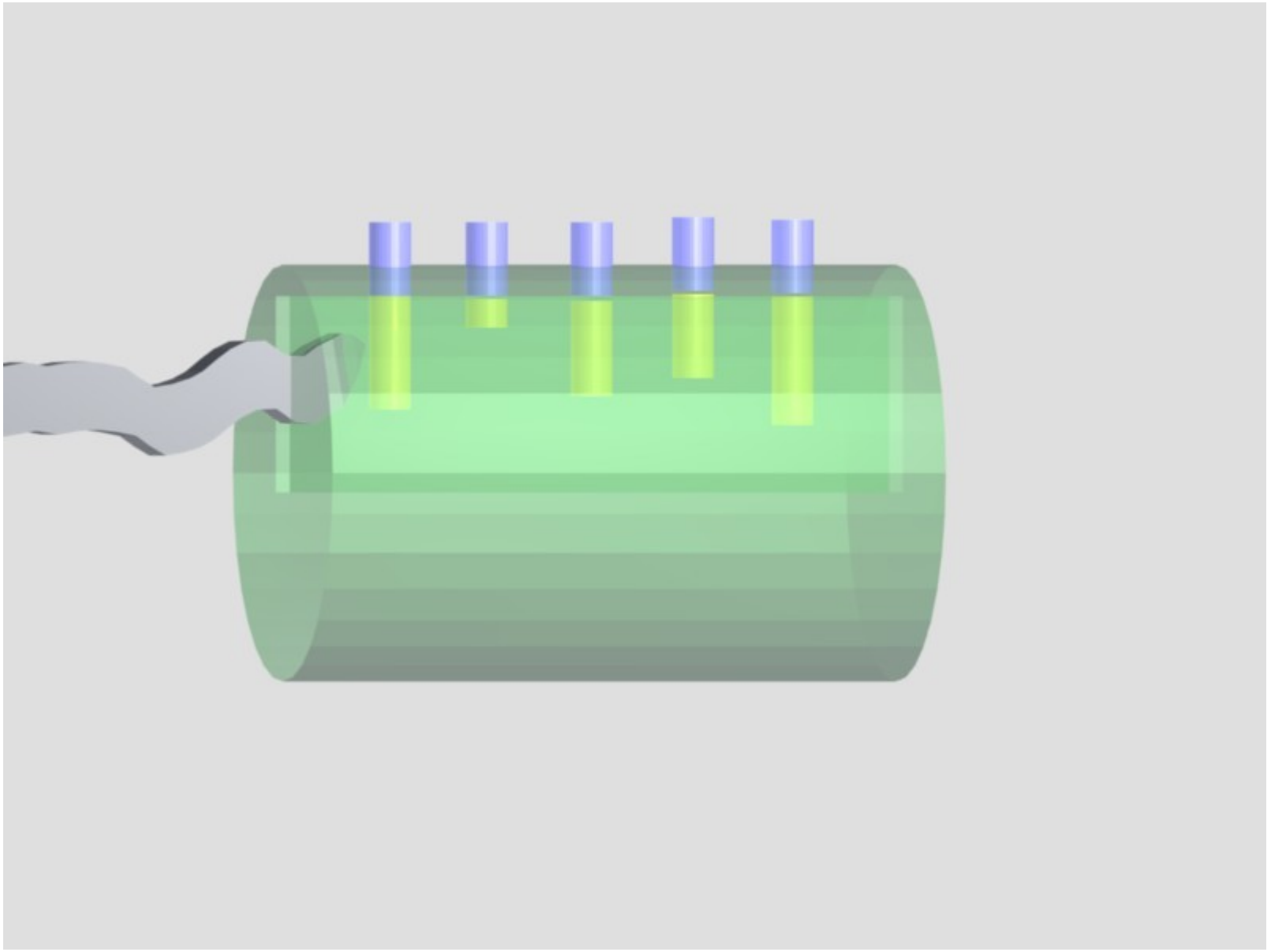
Raking

- Quickly slide across the pins while applying a small amount of tension
- All the pins will lift up, and as the pins fall back into place, they should get set one by one
- Takes practice to master, doesn't always work
- Usually one will make a few passes raking, and then proceed to set the pins that are left

Raking



Raking



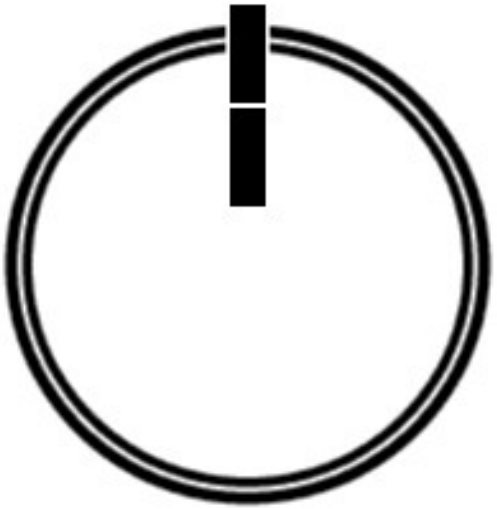
High security measures

(And countermeasures)

High Security

- “High security pins” (spool, mushroom, serrated)
  - Why are they hard to pick?
  - How can you tell if a lock is using them?
  - How can we defeat them?

High Security



Normal pins will not let cylinder turn

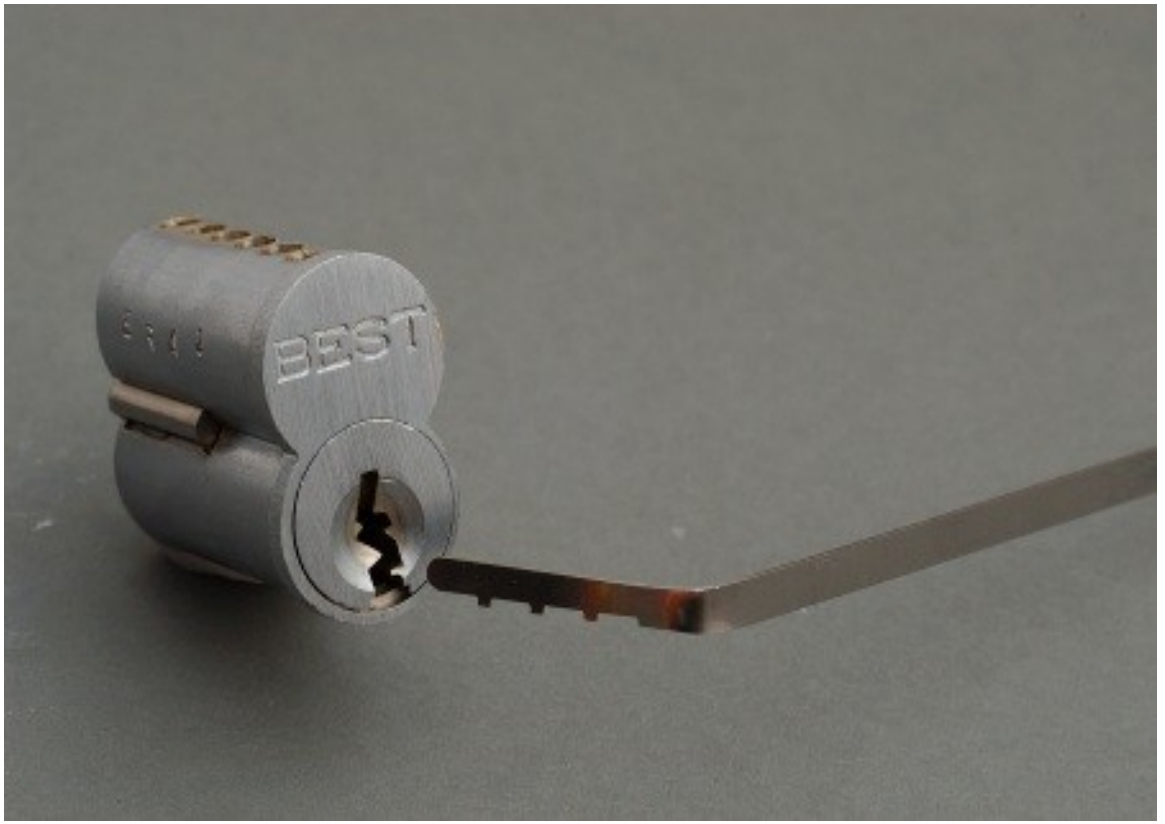
High security pins will let the cylinder turn, but will be set incorrectly!

High Security

- “Best” locks have two shear lines
  - One is for “control keys”, the other is for normal keys
  - Can't tell which is being set while picking the lock!

High Security

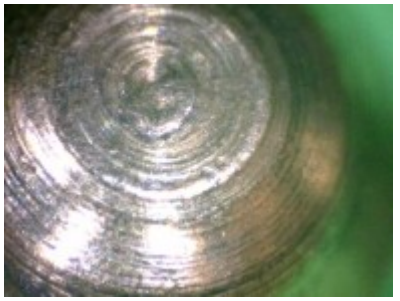
- Special torque wrench spins only one core

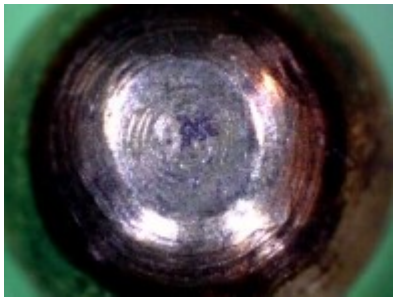


High Security

- In general “high security” just means you need a special tool to break it!

Forensics

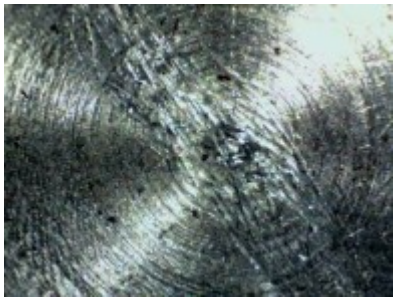





Normal usage

Attempted picking


Attempted raking



Forensics

- Physical evidence in lock is like digital evidence for computers
  - Brute forcing leads to evidence left behind
  - Careful checking leads to evidence of break-ins, or attempted break ins

Other bypass techniques

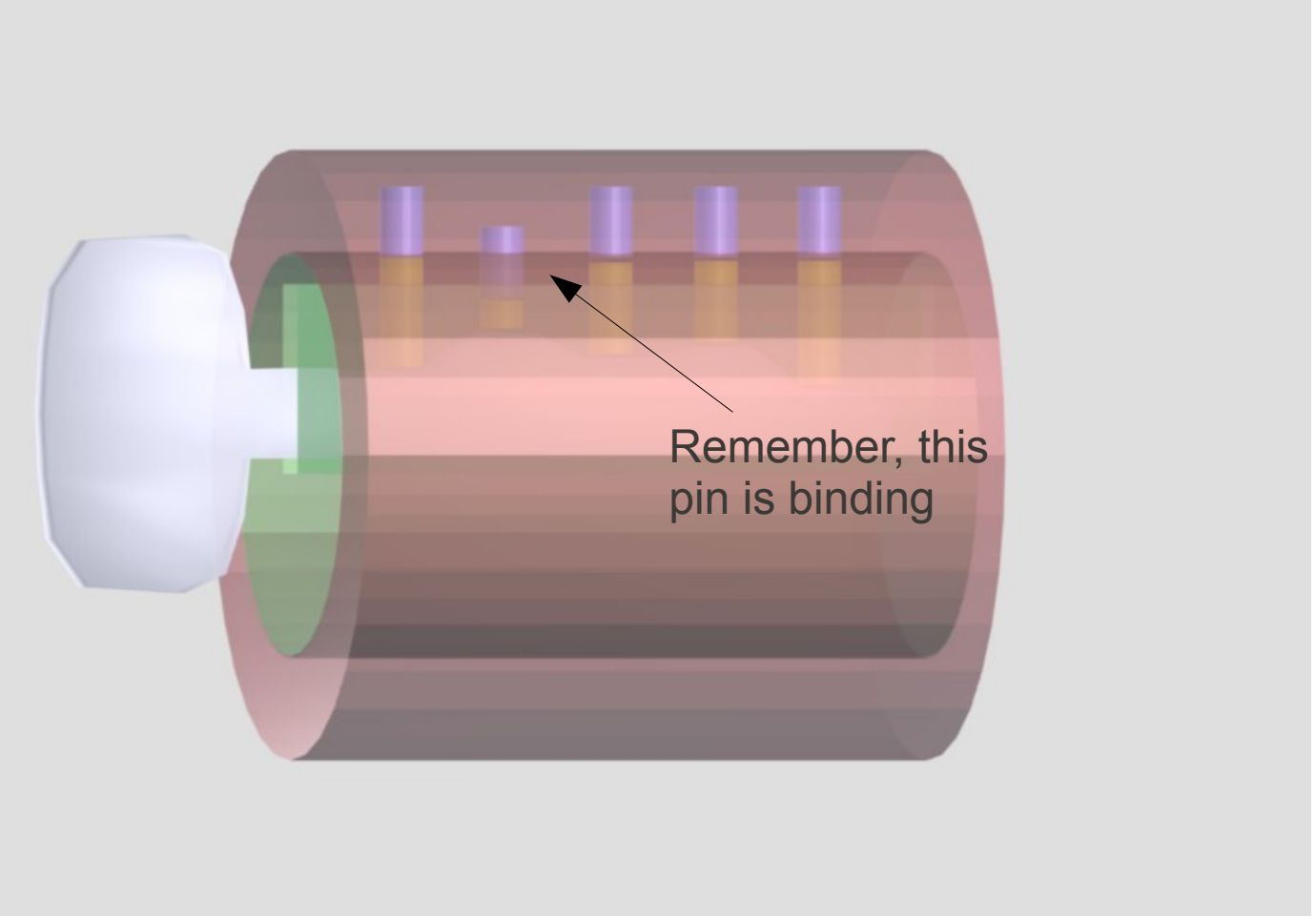
- “Pick style” techniques
  - Bump keys
  - Pick guns
  - Impressioning
- Other style
  - Shimming
  - Destructive entry

Bump keys and Pick guns

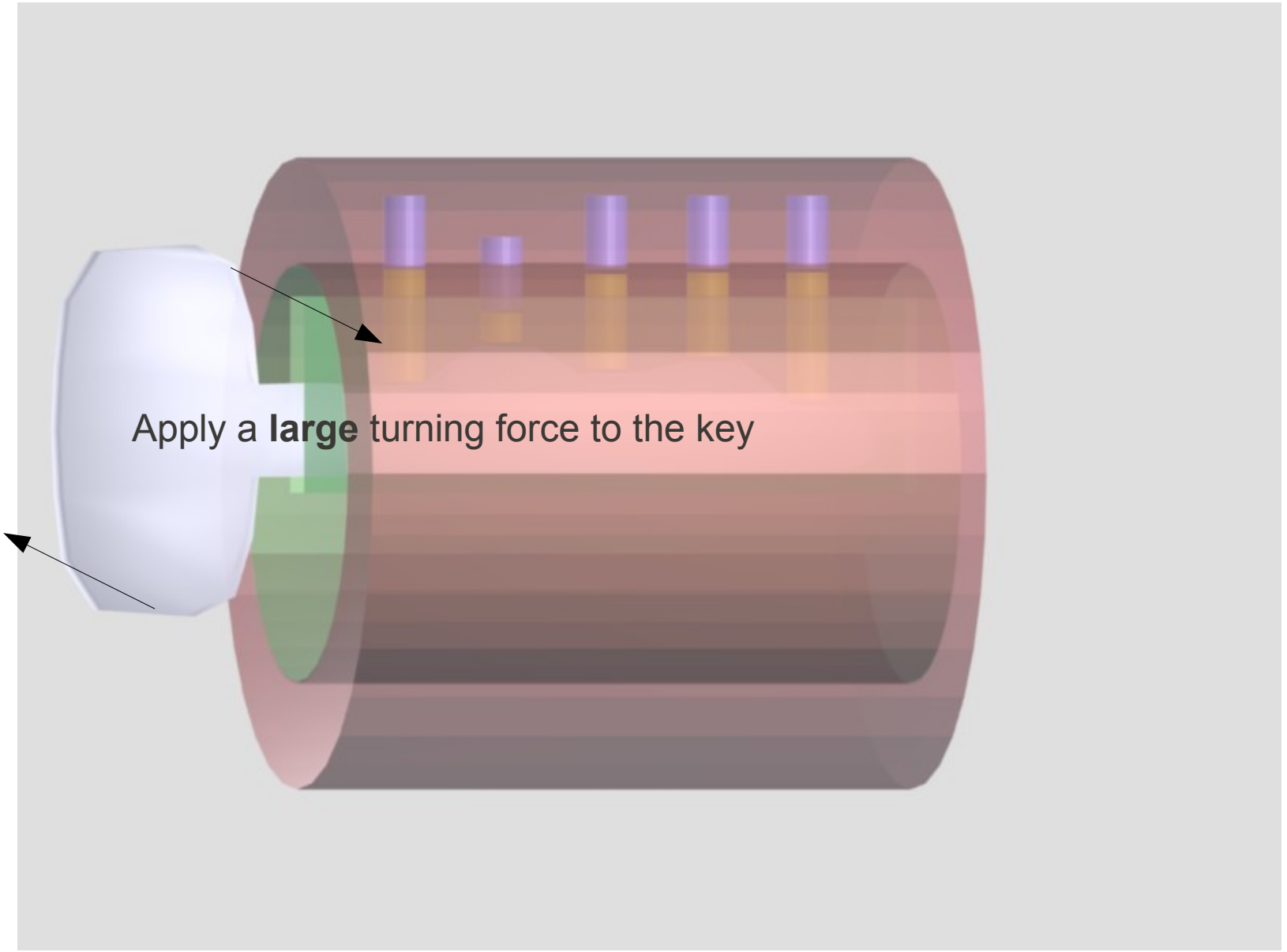
- Very similar to the raking technique!
- Hit the pins up very quickly
- Try turning the cylinder at the same time
- Hopefully the pins will settle correctly

Impressioning

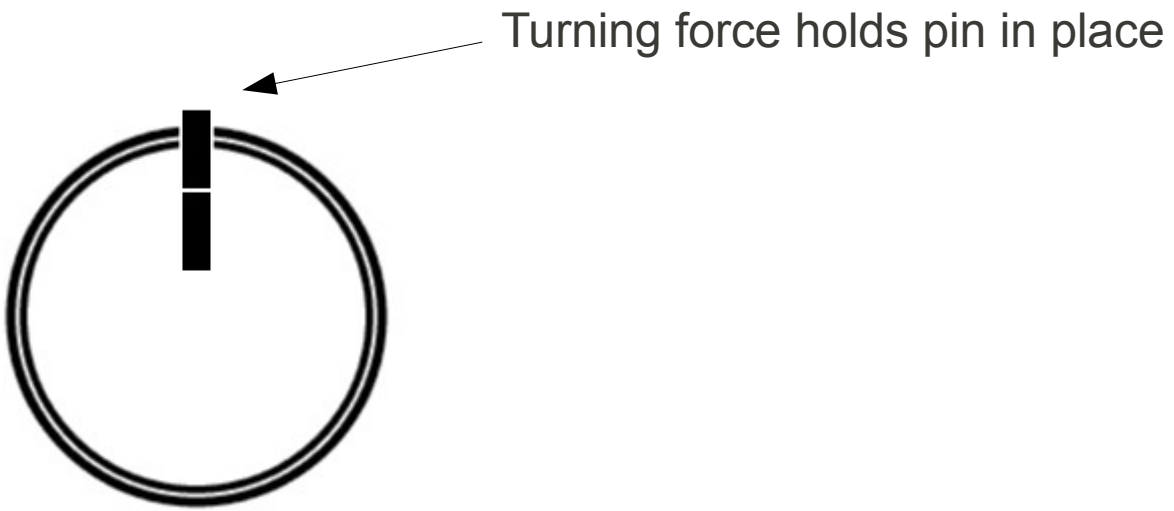
- Not only do you open the lock, but you actually get a key for the lock



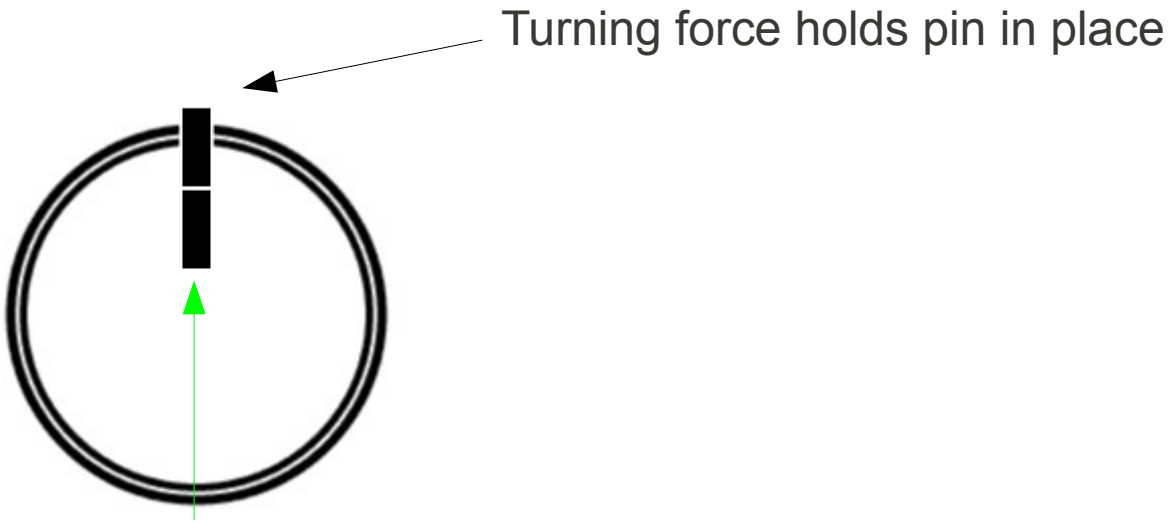
Impressioning



Impressioning

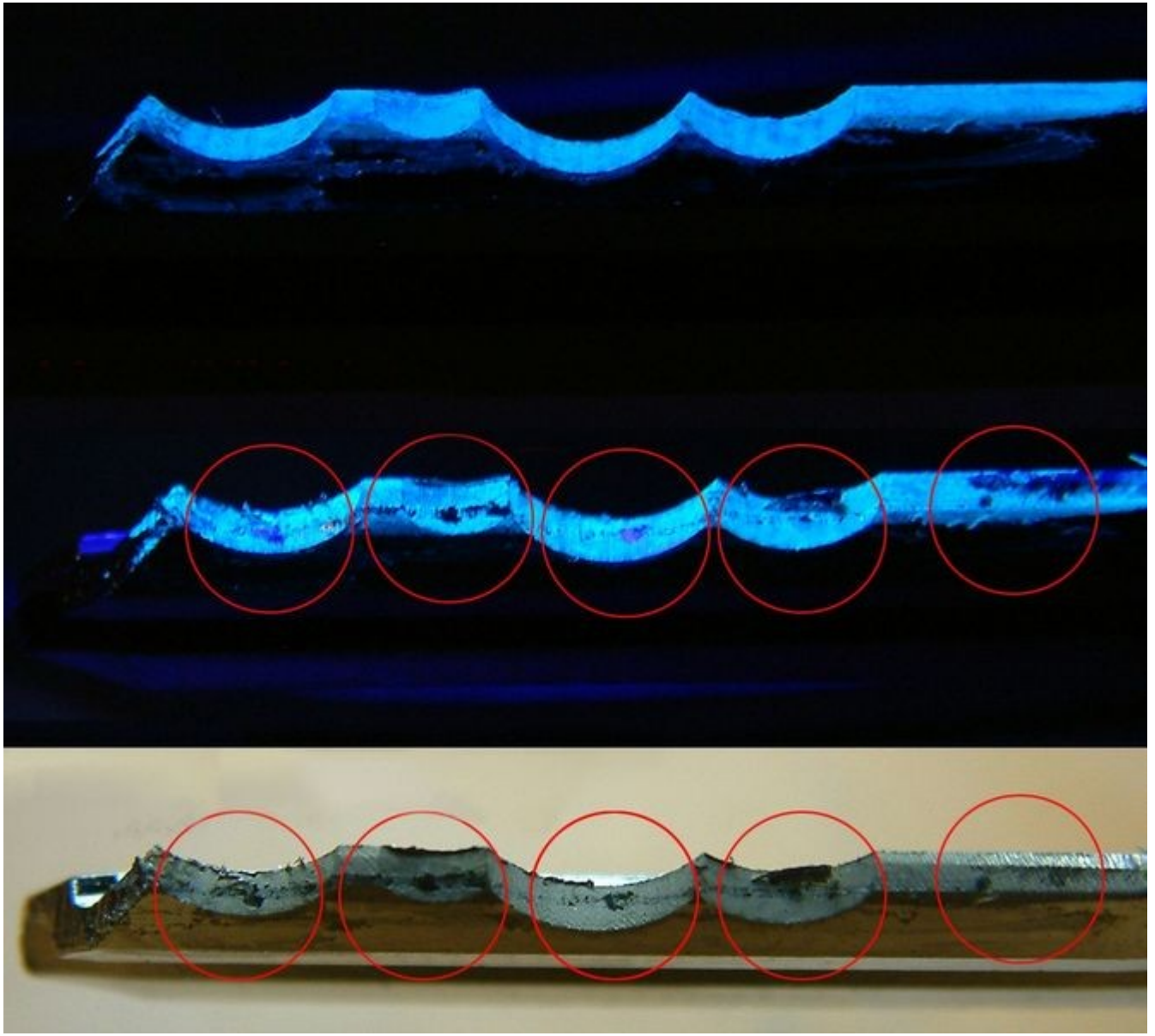


Impressioning



Push the key up against the pin and wiggle the key: it will scratch the key's surface because the pin cannot move!

Impressioning



Wherever a mark appears, that means that part of the key should be filed down

Impressioning

- Eventually no more scratches will appear on the key
- When that happens, the key should open the lock!

Cryptography

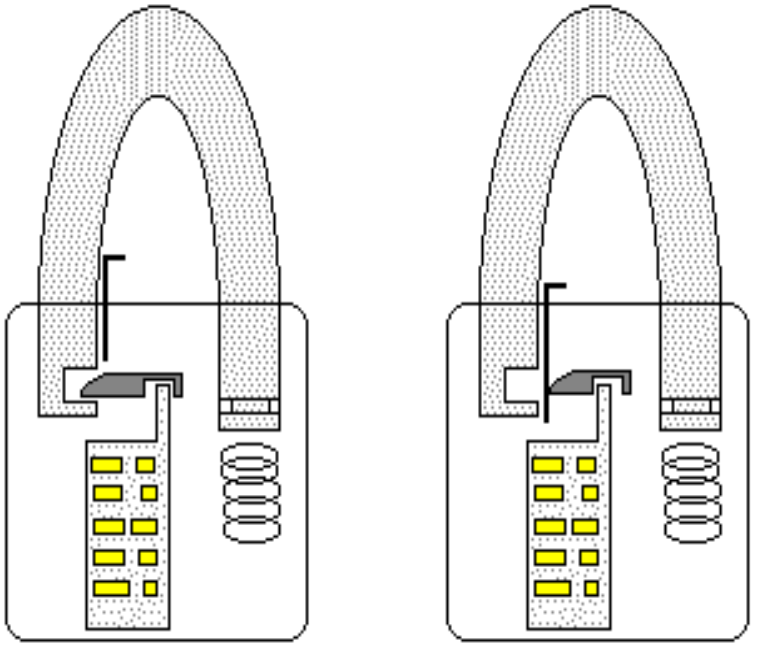
- Impressioning uses the lock as an “Oracle”
- Given a key and a lock, you can find out which pins are set and which are not
- This is like a computer which tells you which letters are wrong in a password!
- Oracles are a common way to reason about some cryptographic systems
  - Padding oracles tell whether or not an encrypted string has proper encoding
  - With a padding oracle, some crypto systems can be broken in linear time!

Other bypass techniques

- "Pick style" techniques
  - Bump keys
  - Pick guns
  - Impressioning
- Other style
  - Shimming
  - Destructive entry

Other techniques

- Shimming



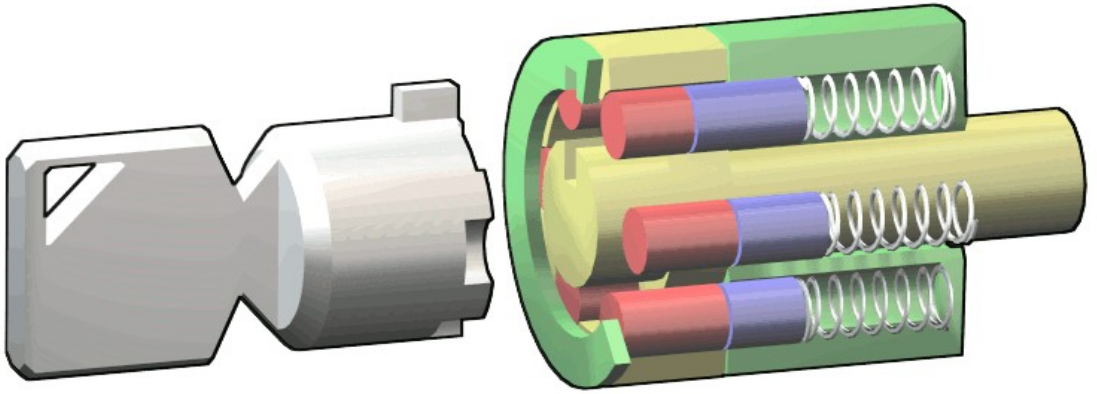
- Destructive entry
  - Just break the lock/door/window!

Cryptography

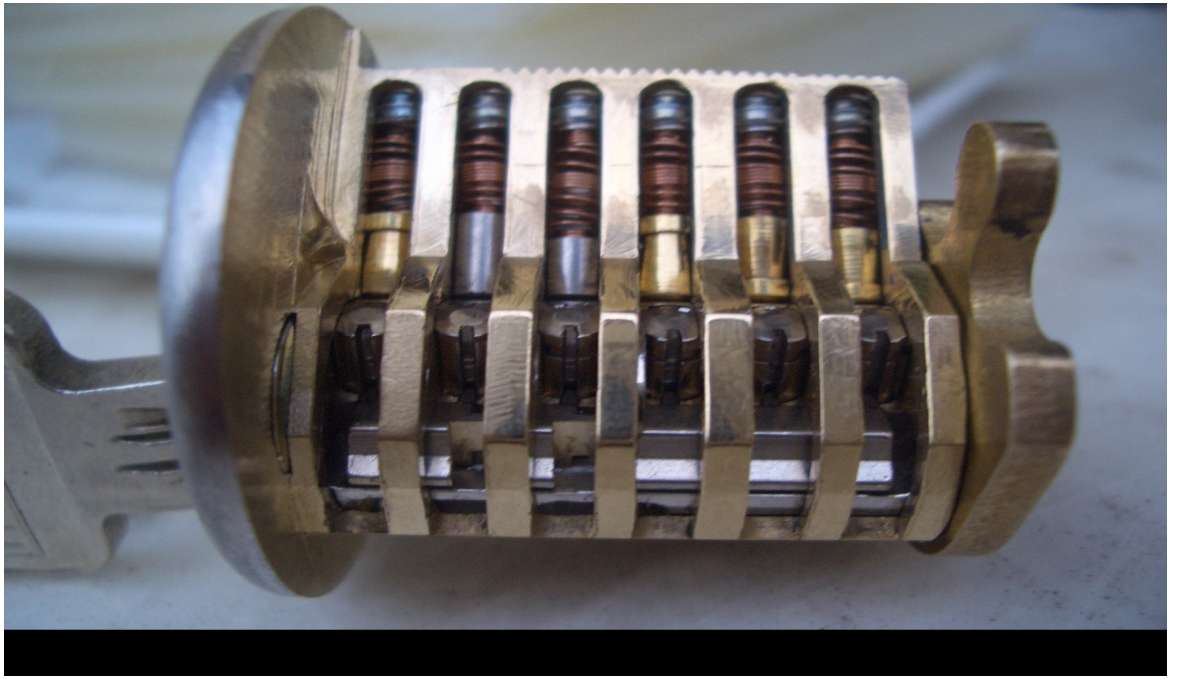
- The “other techniques” are really “side channel” attacks
  - In cryptography, this means attacking something other than the cryptographic algorithm itself (for example timing attacks or TEMPEST)
  - In lock picking this usually means “ignoring” the lock (for example, breaking down a door)
  - Many times these “side channel” attacks are the easiest to exploit, and the hardest to prevent

Other locks

- Tubular locks



- Medeco locks



Other locks

- Dimple pins

Your turn!

- I have some locks and picks, you can try opening some of the locks up here!

- If you have any questions, please ask them!