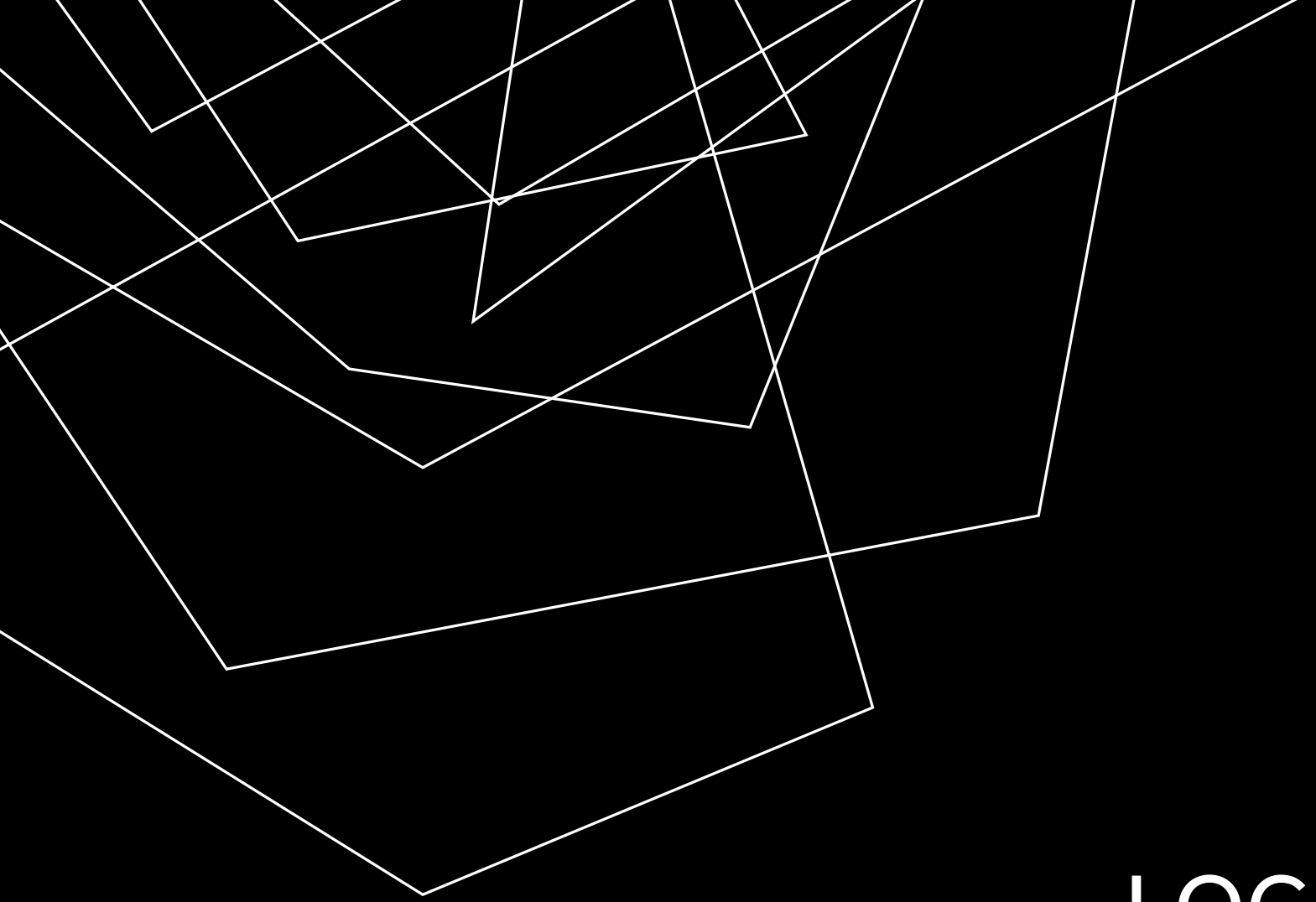


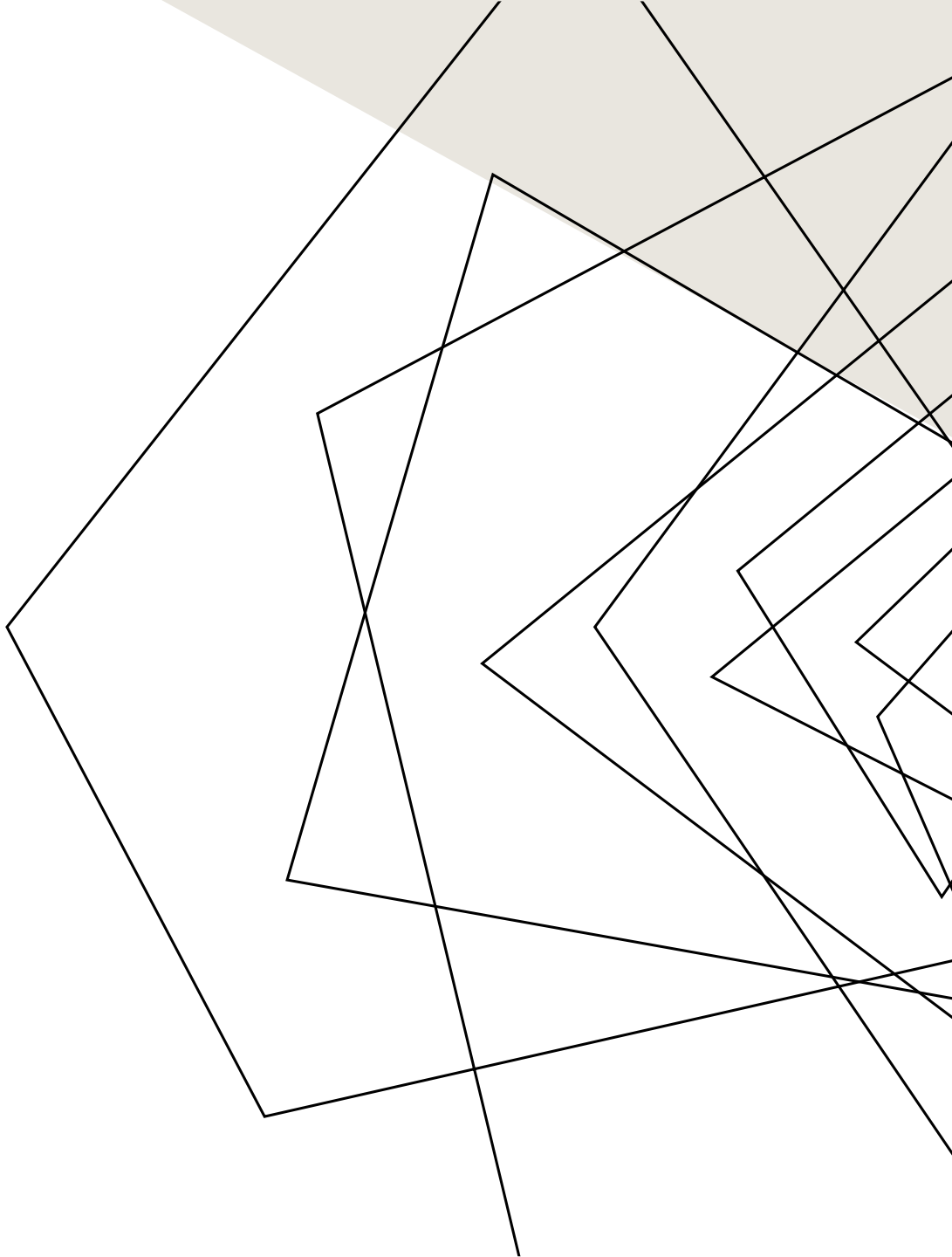
LOCKPICKING 101

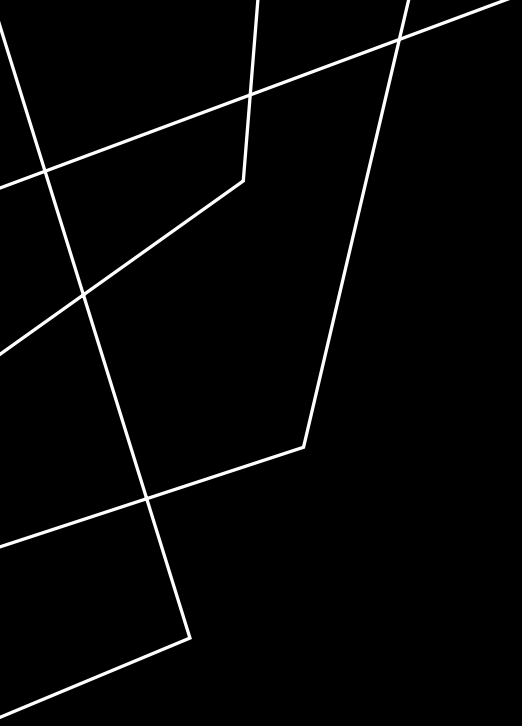
BRIDGEFEST – 25 MAY 2024

ABOUT US

Fotis Dilaris - Penetration Tester

Evgenios Anastasiadis – Penetration Tester

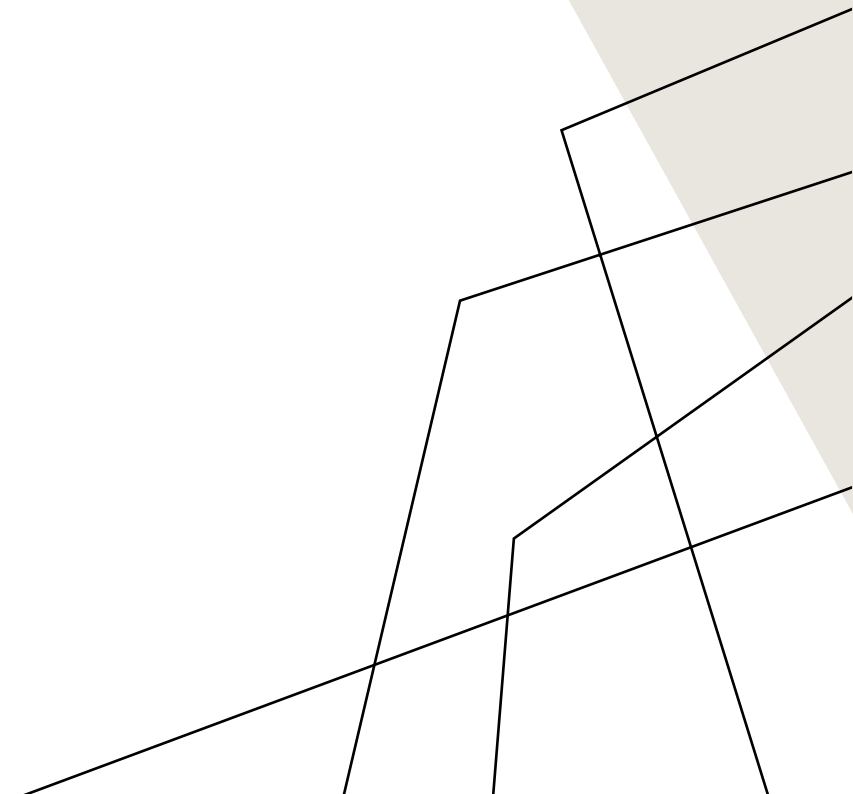




UNDERSTANDING LOCKS

TYPES OF LOCKS

- Wafer locks
- Tubular
- Disc-detainer locks
- Pin tumbler locks
- Cam Locks
- Etc



Wafer Locks

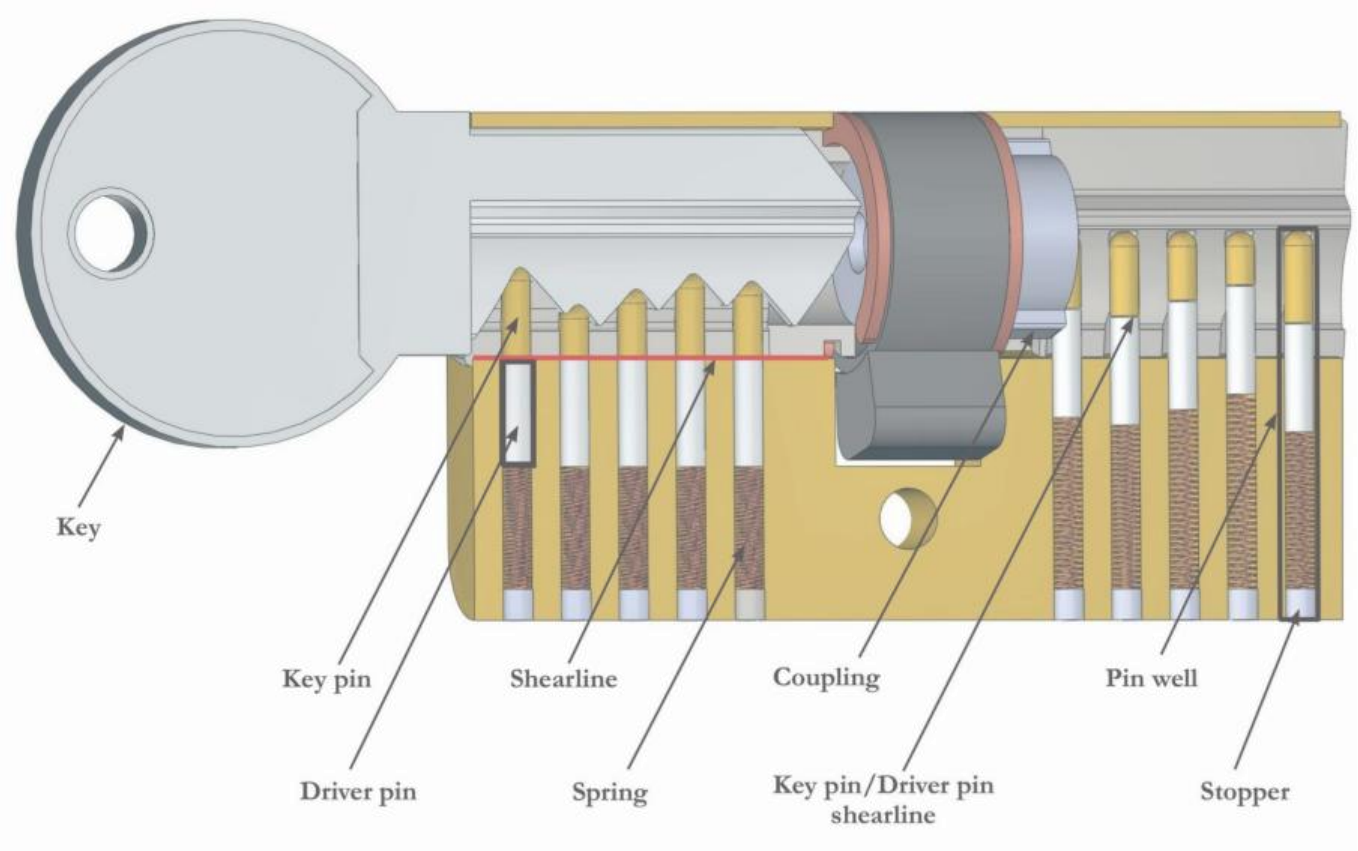
Pin tumbler locks

Tubular locks

Cam Locks

Disc-detainer locks

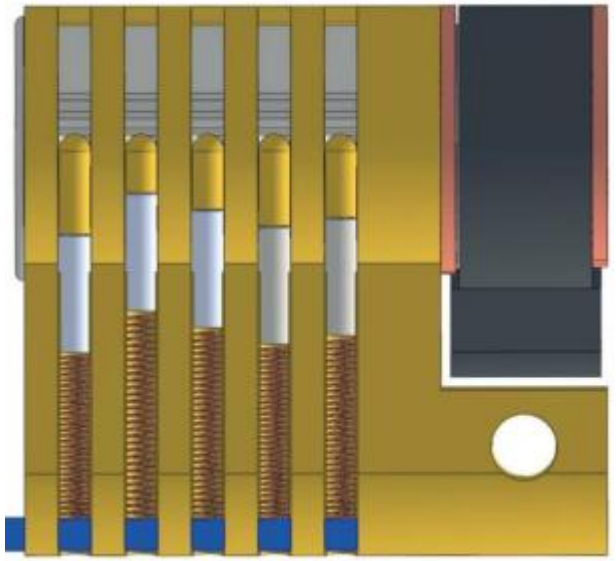
ANATOMY OF A STANDARD LOCK



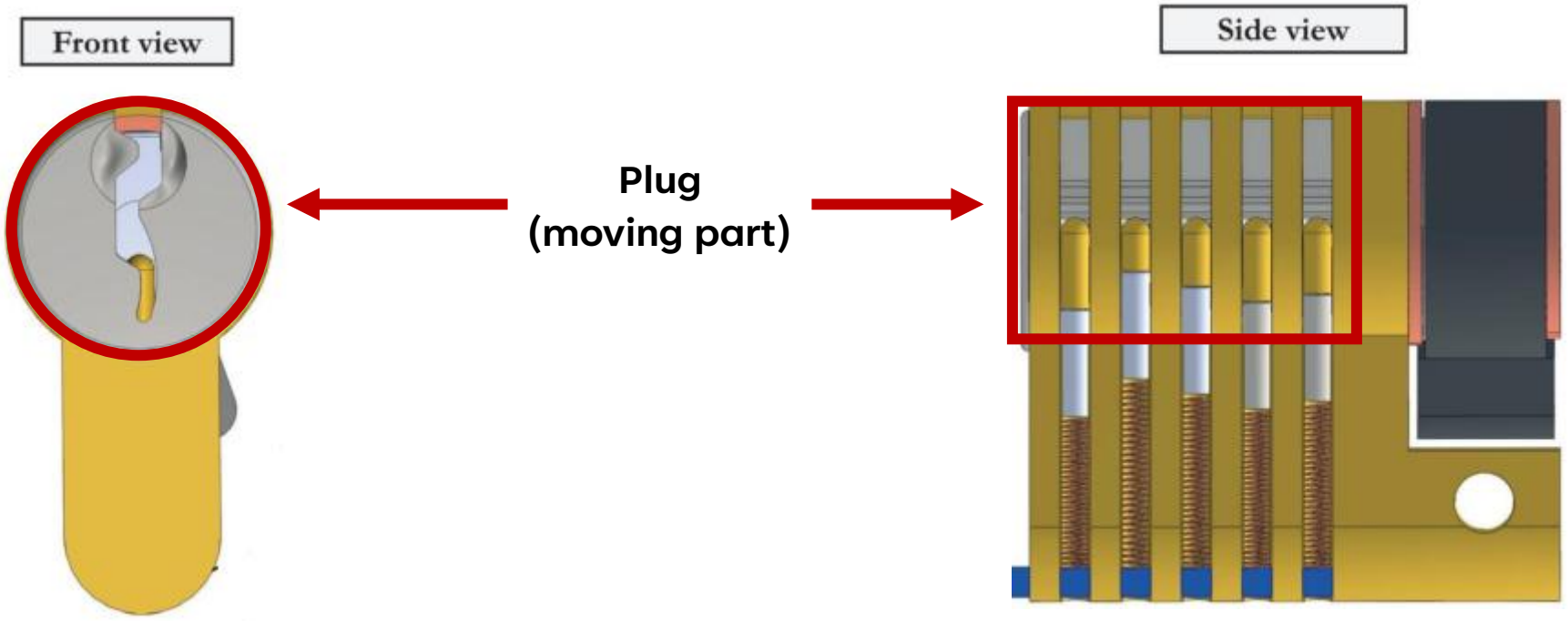
ANATOMY OF A STANDARD LOCK

Front view

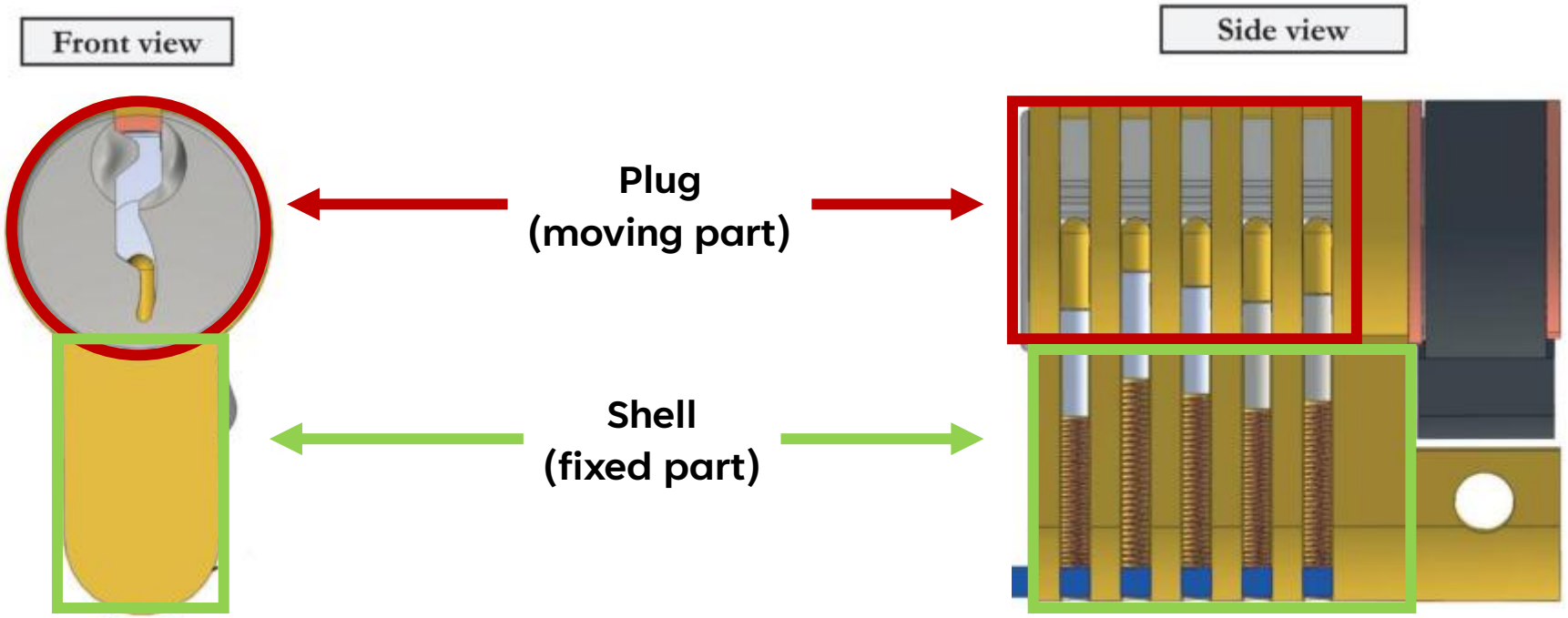
Side view



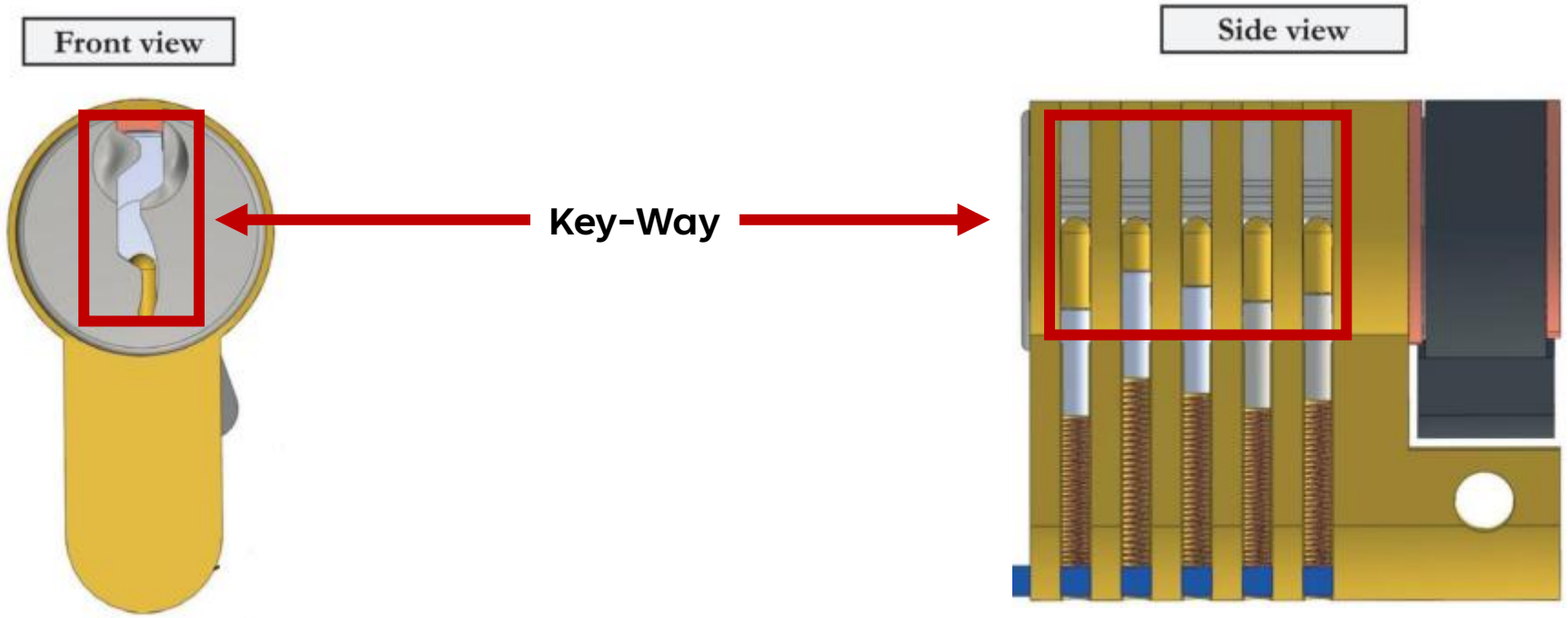
ANATOMY OF A STANDARD LOCK



ANATOMY OF A STANDARD LOCK



ANATOMY OF A STANDARD LOCK

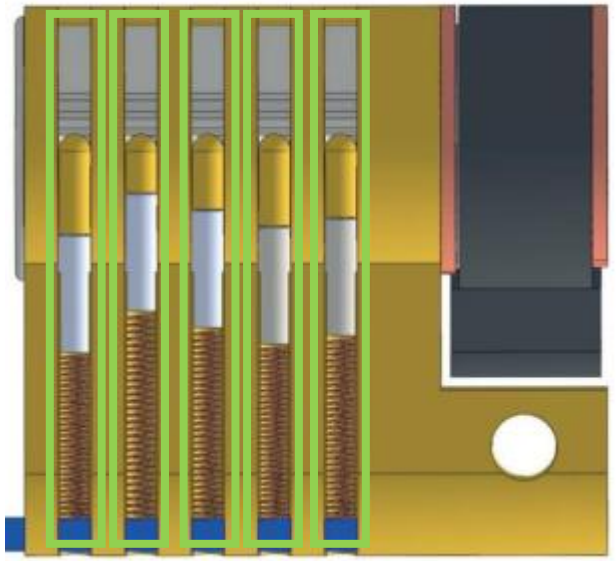


ANATOMY OF A STANDARD LOCK

Front view

Pin wells/guides

Side view

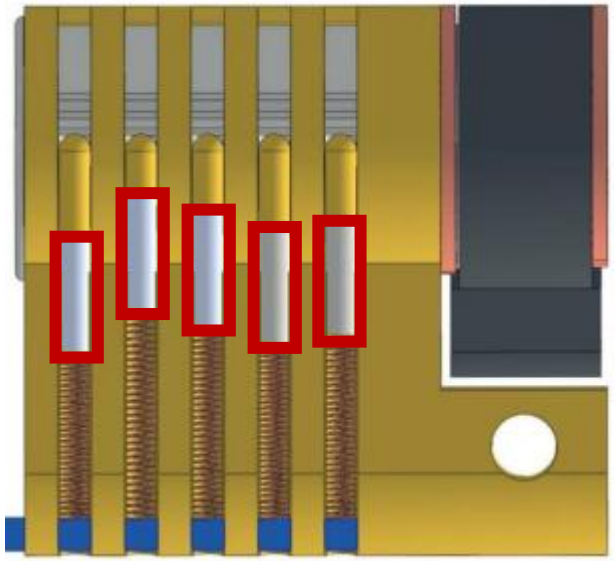


ANATOMY OF A STANDARD LOCK

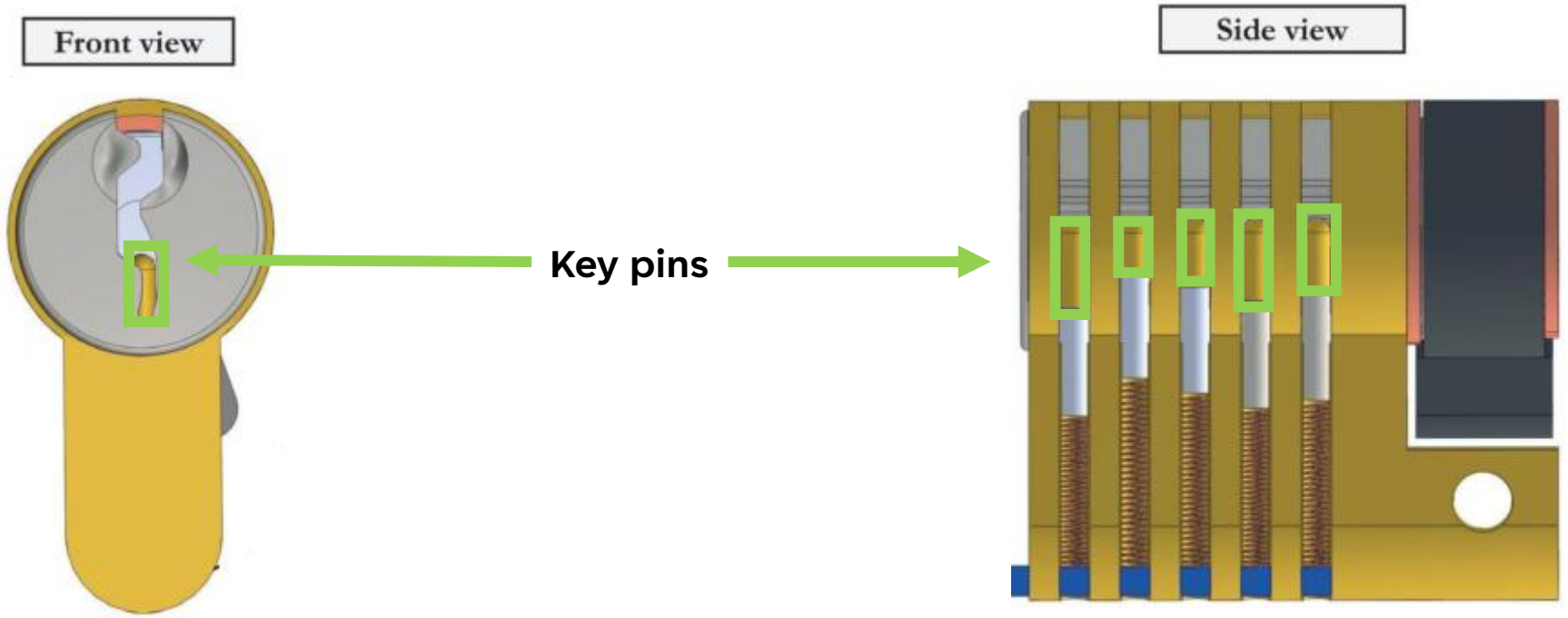
Front view

Side view

Driver pins



ANATOMY OF A STANDARD LOCK

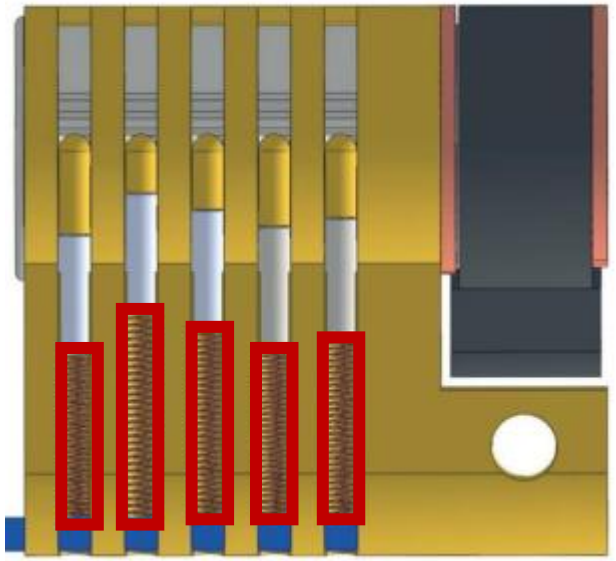


ANATOMY OF A STANDARD LOCK

Front view

Side view

Springs

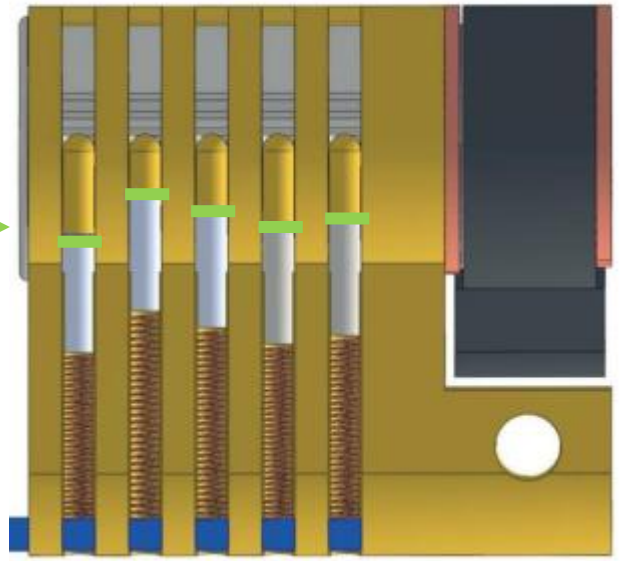


ANATOMY OF A STANDARD LOCK

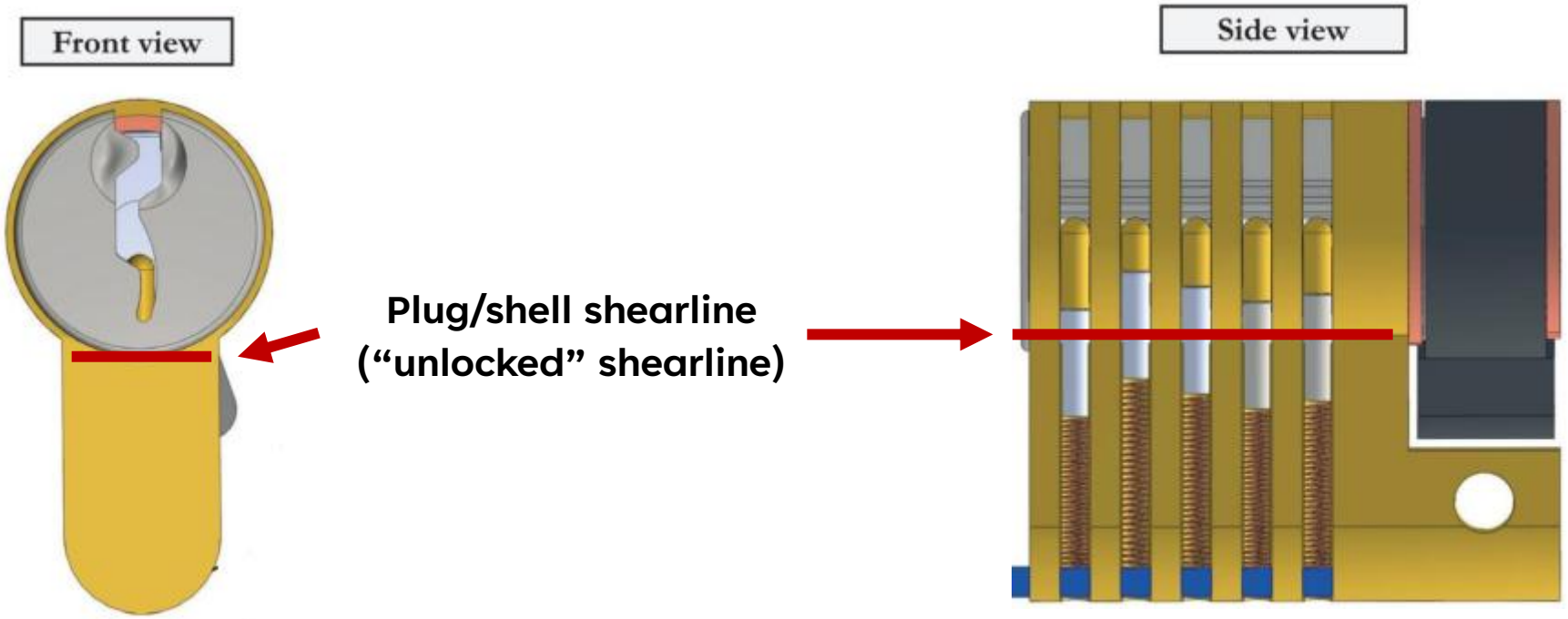
Front view

Key-pin/driver-pin shearline ("locked" shearline)

Side view



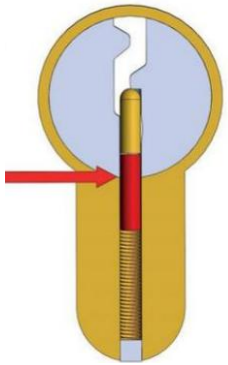
ANATOMY OF A STANDARD LOCK

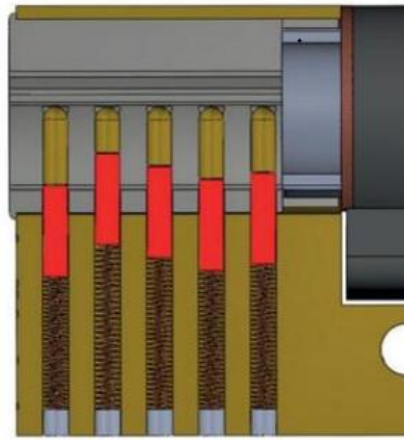


ANATOMY OF A STANDARD LOCK

LOCKED

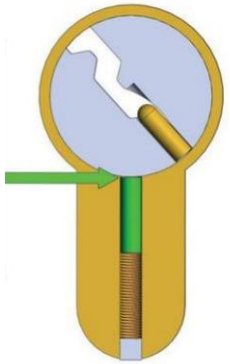
If **no key** is inserted, the **plug cannot rotate**, as its rotation is **blocked** by the driver pins.

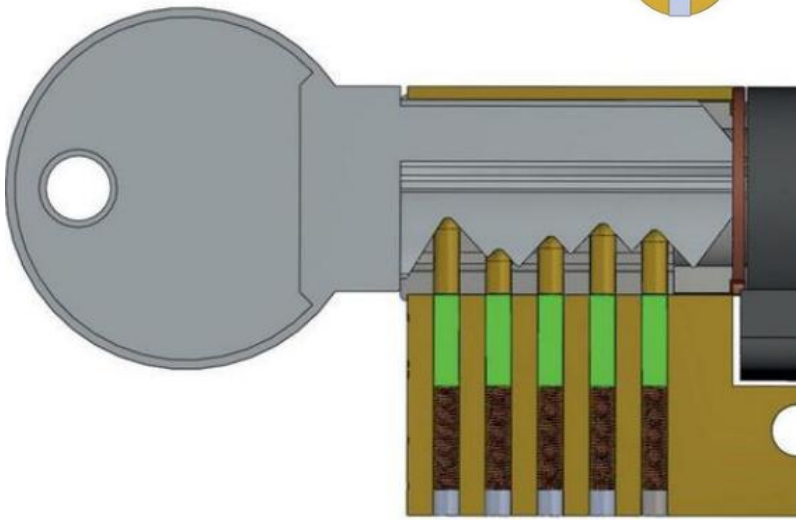




UNLOCKED

If **correct key** is inserted, the **key-pin/driver-pin shearline** is **aligned** with the **plug/shell shearline** and the plug is **free to rotate**.

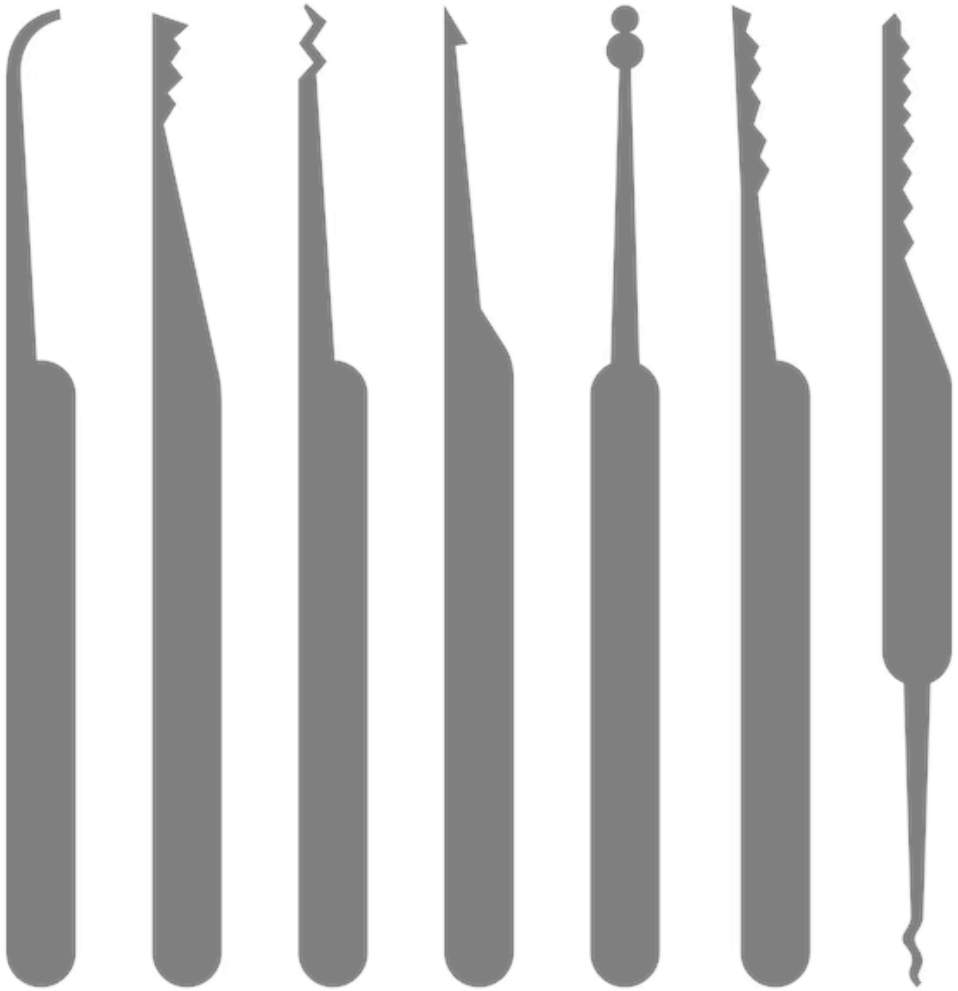




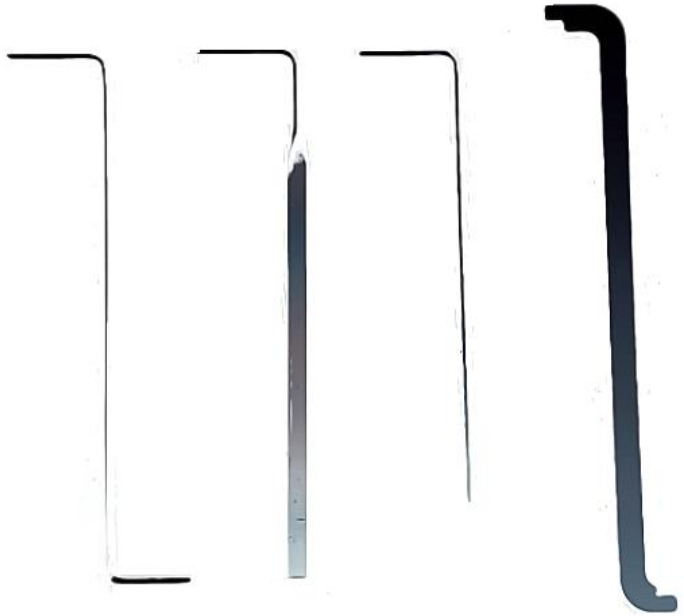
BASIC TOOLS

TOOLS

- **Tension wrenches**
- **Pick rakes**
- **Single-pin picks**
- **Bump keys**
- **Etc**

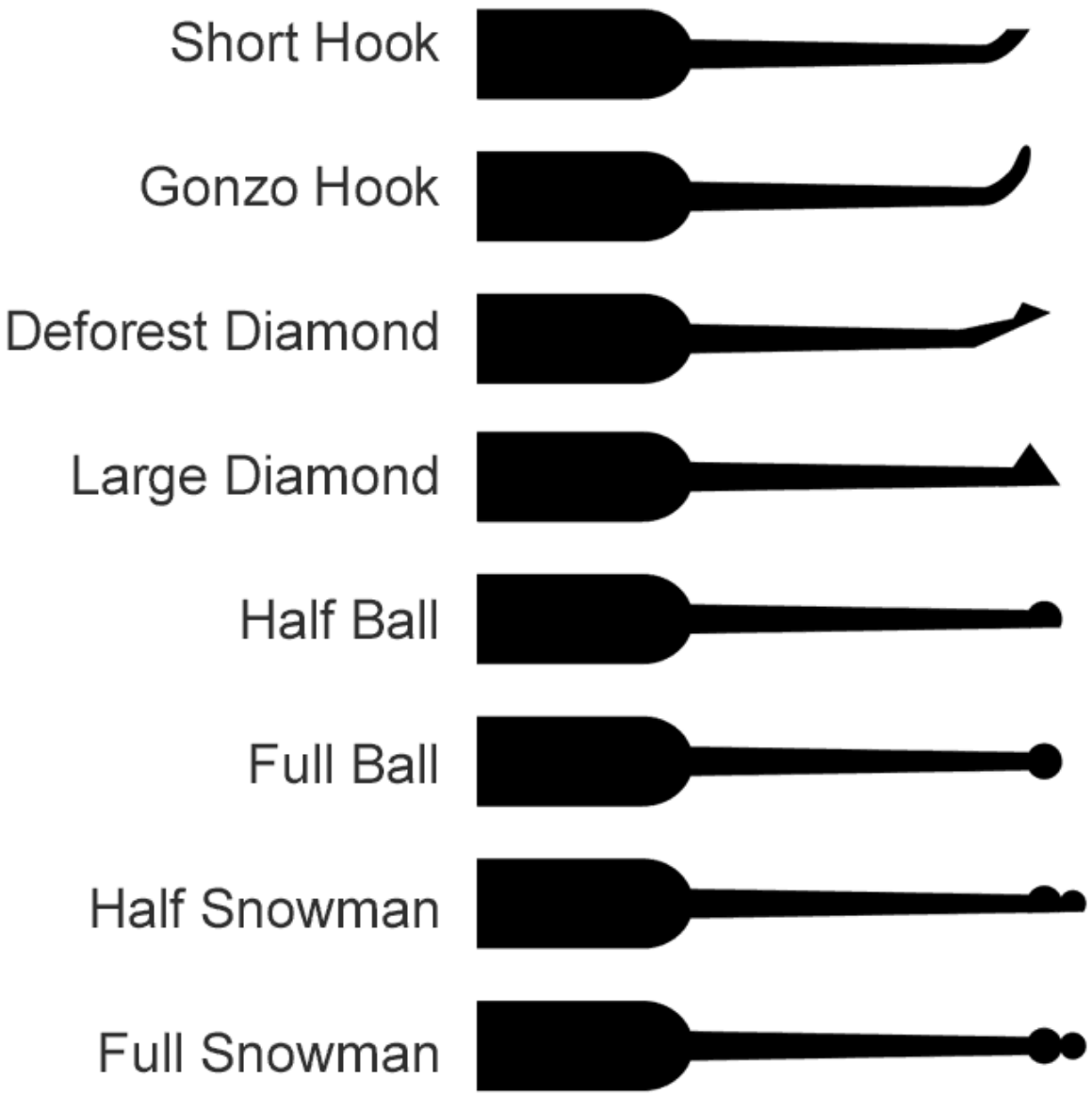


BASIC TOOLS



FEELER PICK

Just like the name implies, feeler picks are small picks designed to let you feel the pins inside a lock and apply pressure to them one by one.



LOCK PICKING RAKE

There’s another tool called a lock picking rake, and instead of attempting to set each pin individually, you can “rake” back and forth over them more or less randomly. This often works faster, but not all locks will be tripped by raking.

TENSION WRENCH

Tension wrenches come in a few different sizes and styles, based on your ergonomic preference, but also for different sizes and types of locks.

BASIC LOCKPICKING TECHNIQUES

FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

IDEAL WORLD

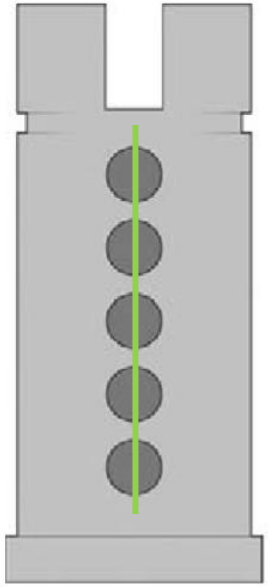
- **Pin guides** would be **aligned perfectly**
- **All pins** would have the exact **same diameter**
- The **plug** would allow only a **perfect rotation** on the center axis

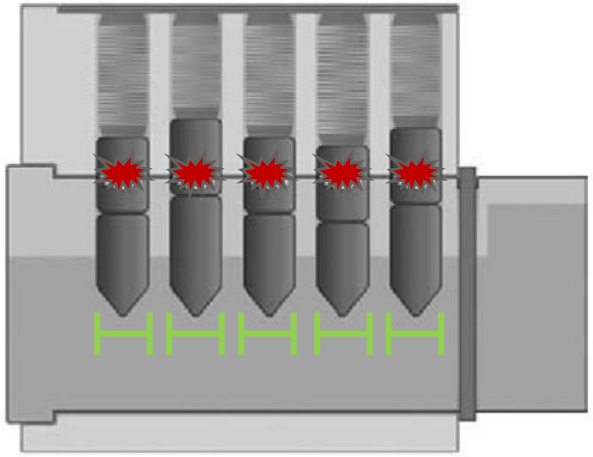
REAL WORLD

- **Pin guides** are NOT **aligned perfectly**
- **All pins** does NOT have **same diameter**
- The **plug** does NOT allow only a **perfect rotation** on the center axis

FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

LOCK IN IDEAL WORLD

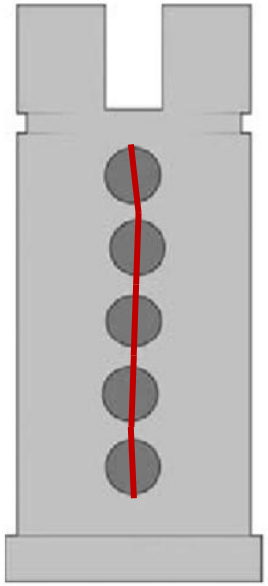


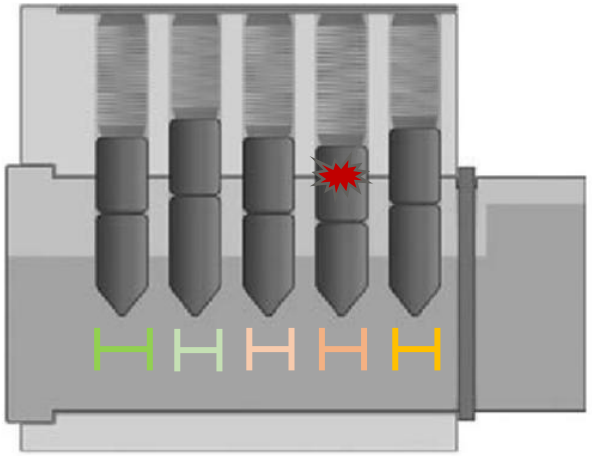


- When **rotational force** is applied to the plug of a lock **ALL the pins would evenly bind** in the shear line.

FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

LOCK IN REAL WORLD

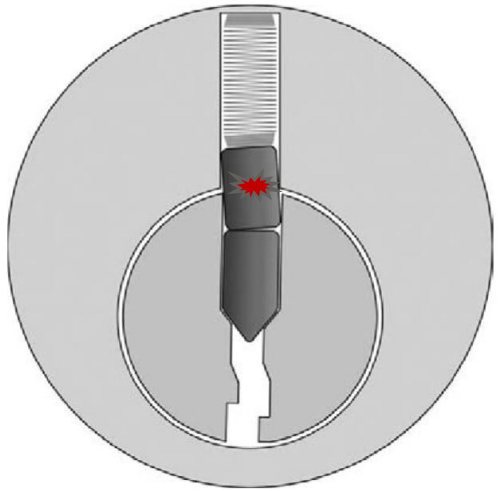




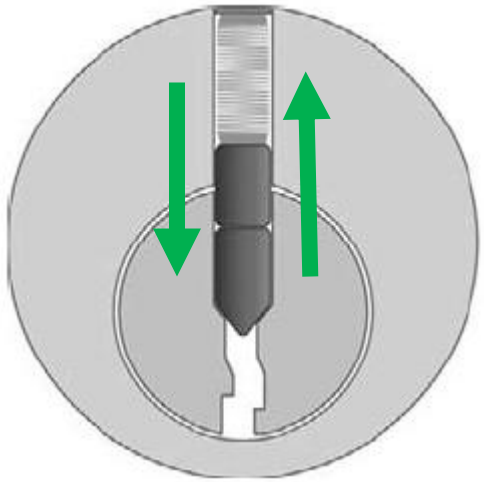
- When **rotational force** is applied to the plug of a lock the pins do **NOT** all experience the same degree of force.
- In many cases, only **ONE single pin** is **binding**.
- The **other pins** simply sit in their chambers **without making significant contact** with any surfaces at the shear line.

FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

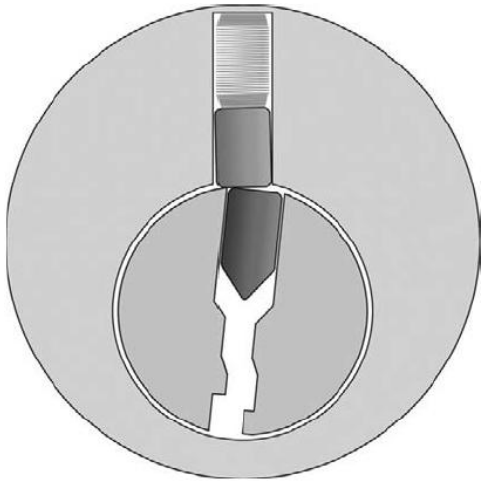
Binding



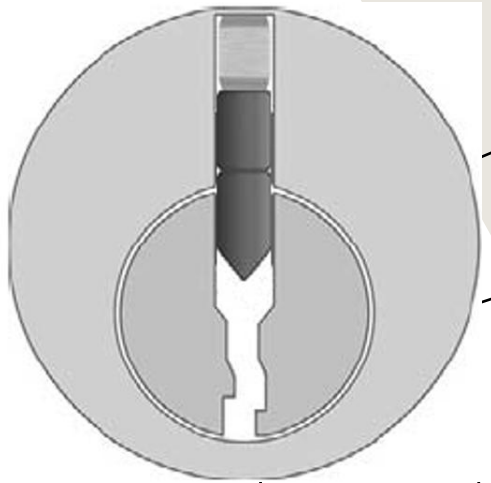
Springy



Set

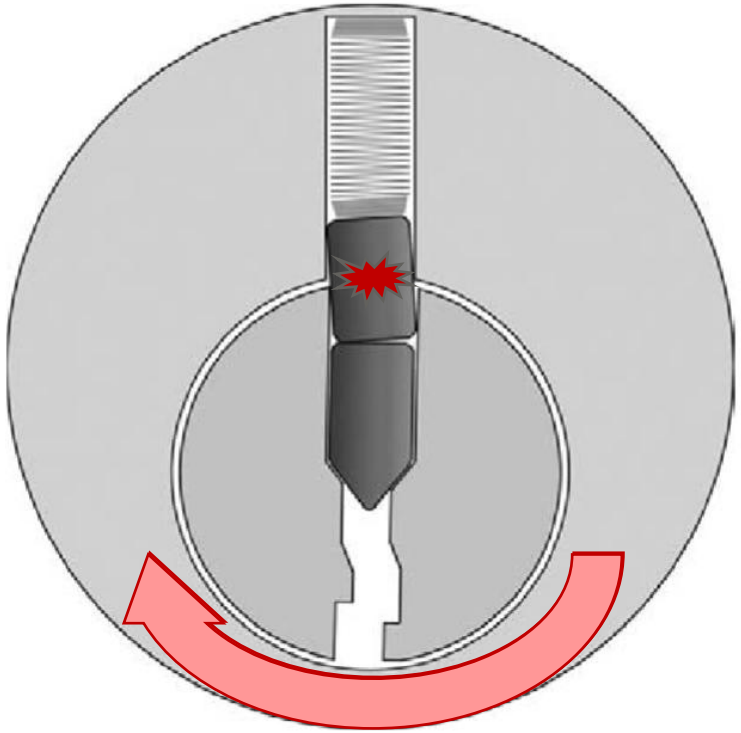


Over-Set



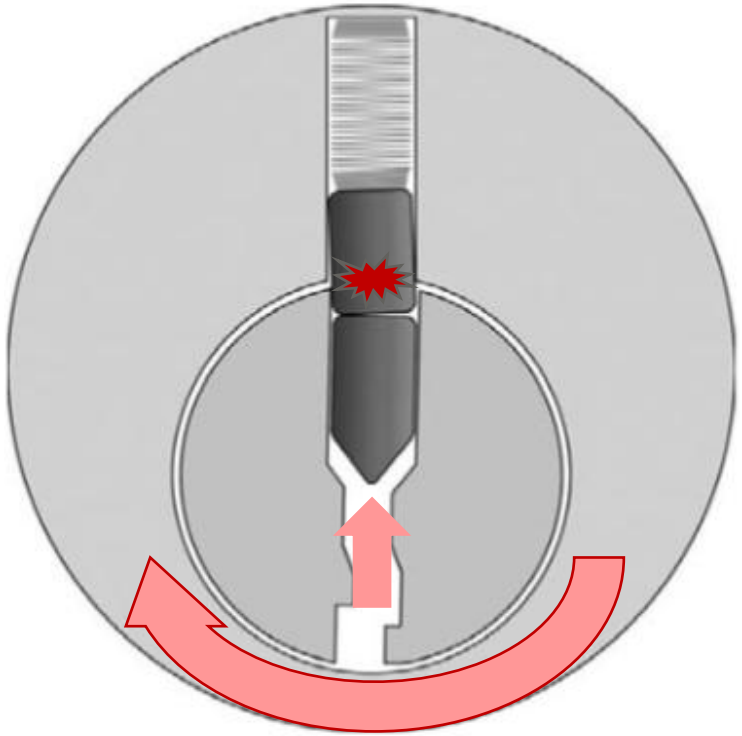
FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

BINDING PIN



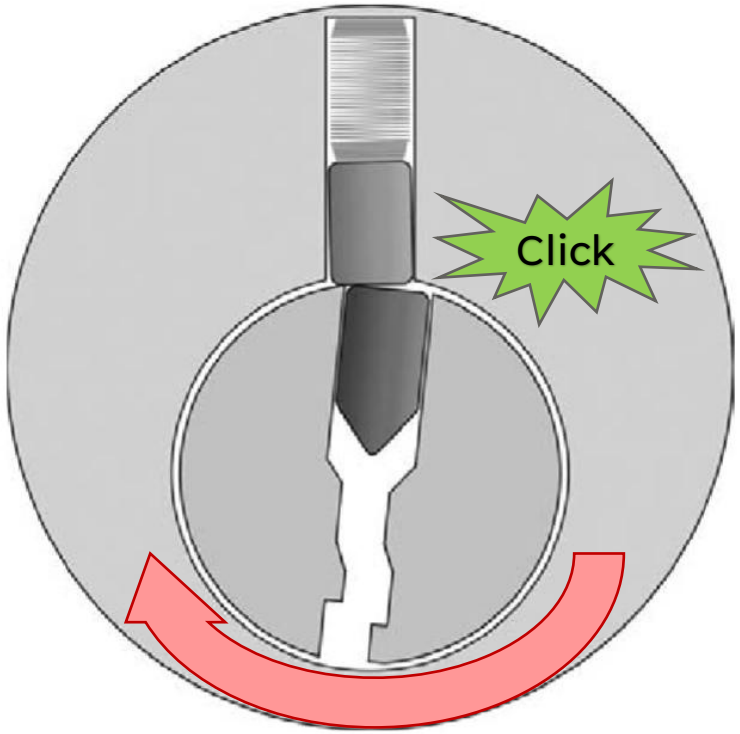
FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

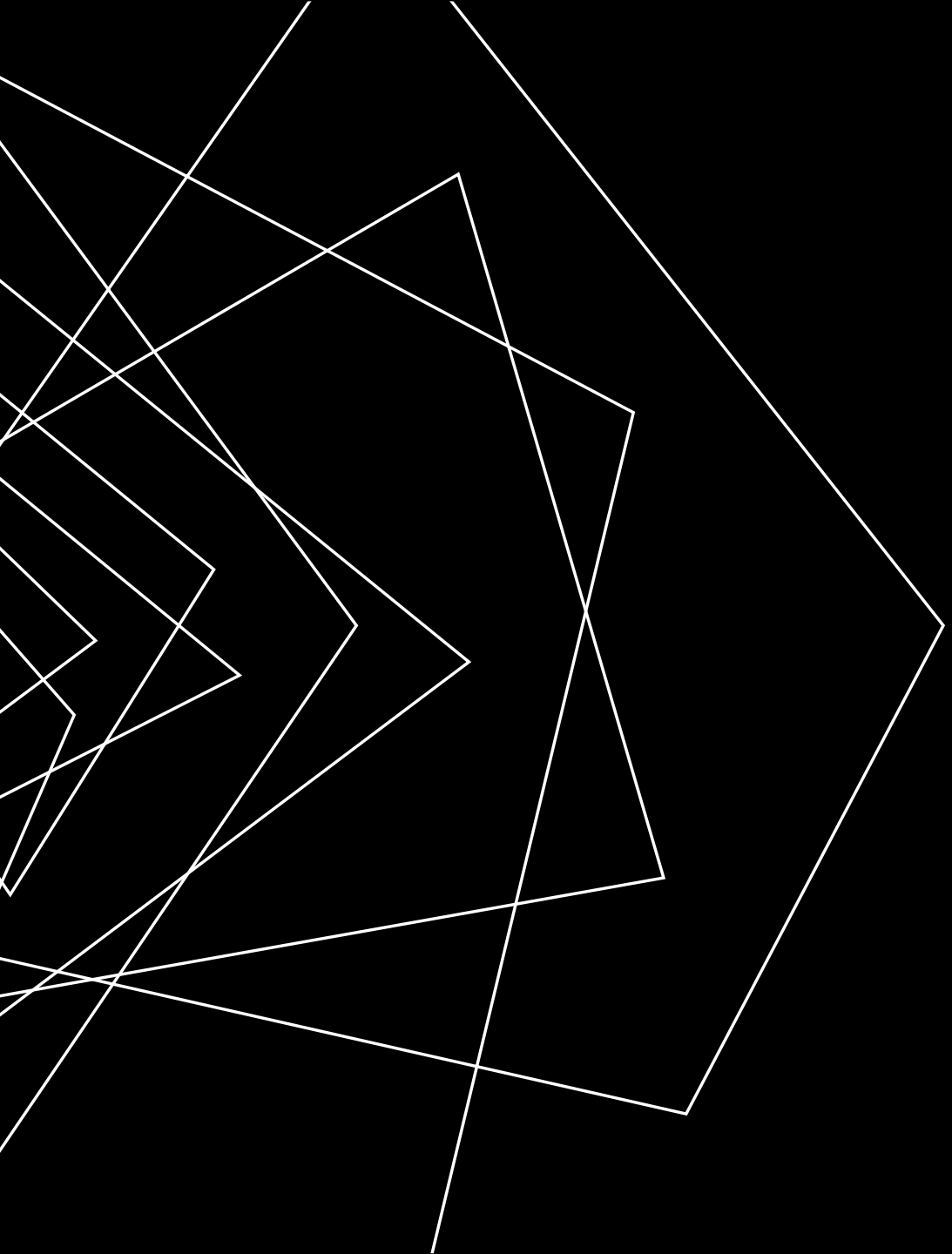
BINDING PIN



FUNDAMENTALS OF NON-DESTRUCTIVE OPENING

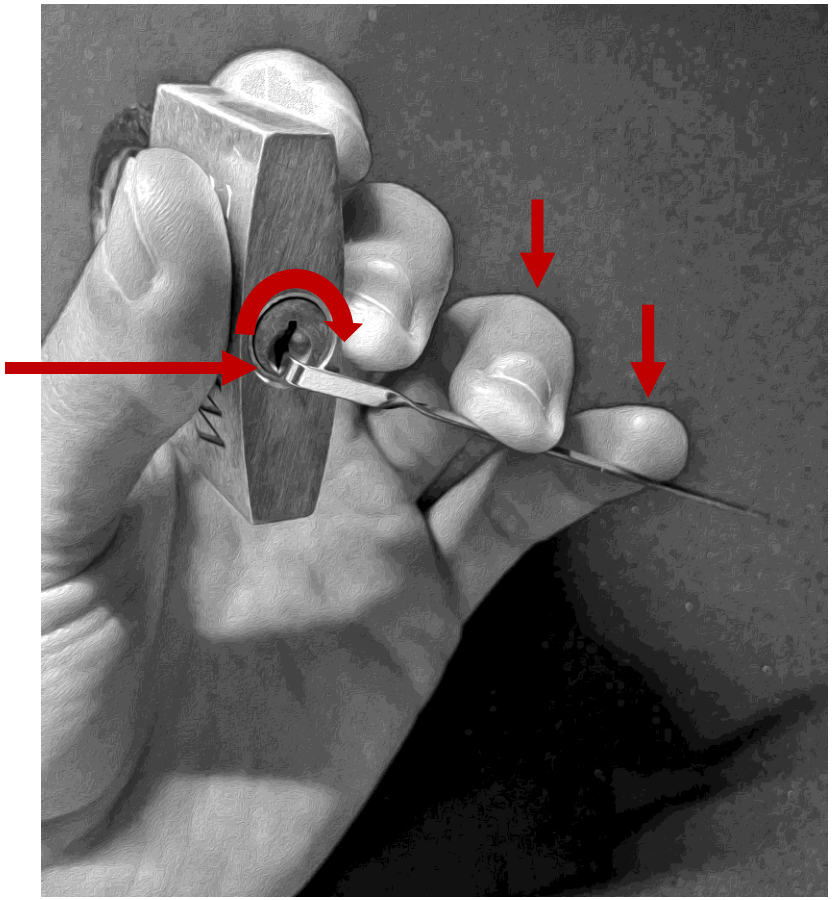
SET PIN





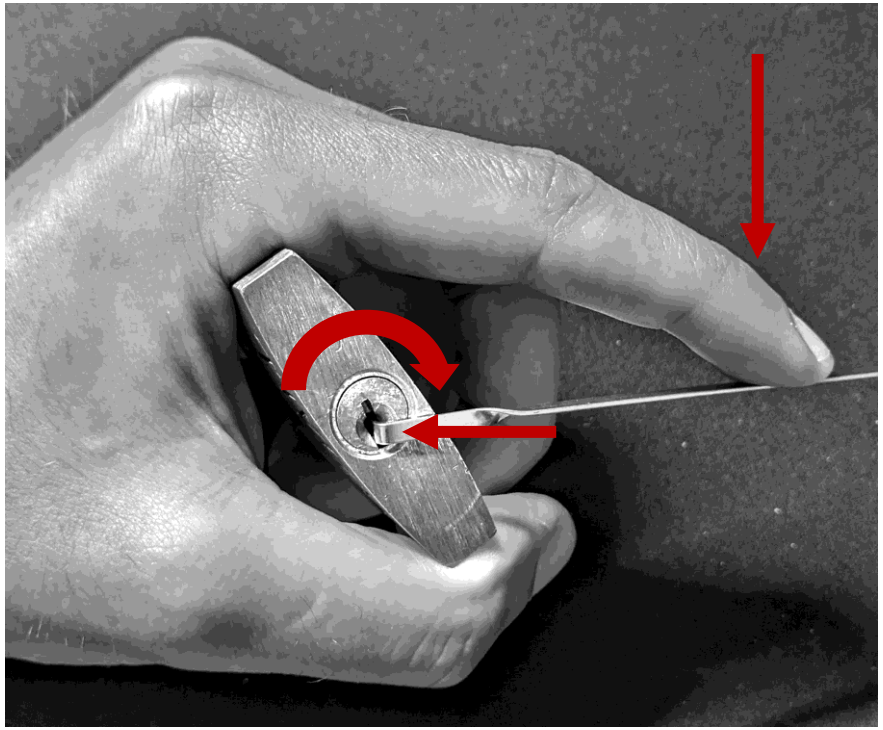
TENSIONING

USING TENSION WRENCH – METHOD 1



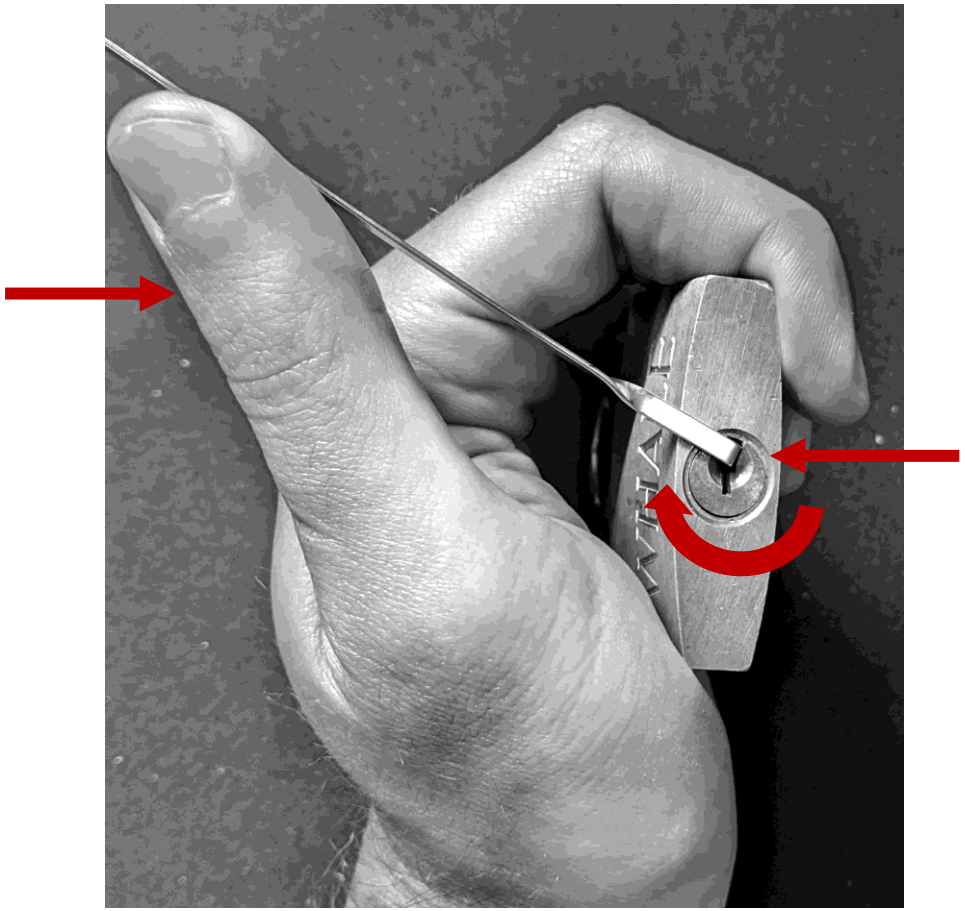
- Use an L-shape tension wrench
- Insert tension wrench at the **edge** of the plug
- Use **pinky** and **ring finger**
- Put a small amount of pressure and push **clockwise**

USING TENSION WRENCH – METHOD 2



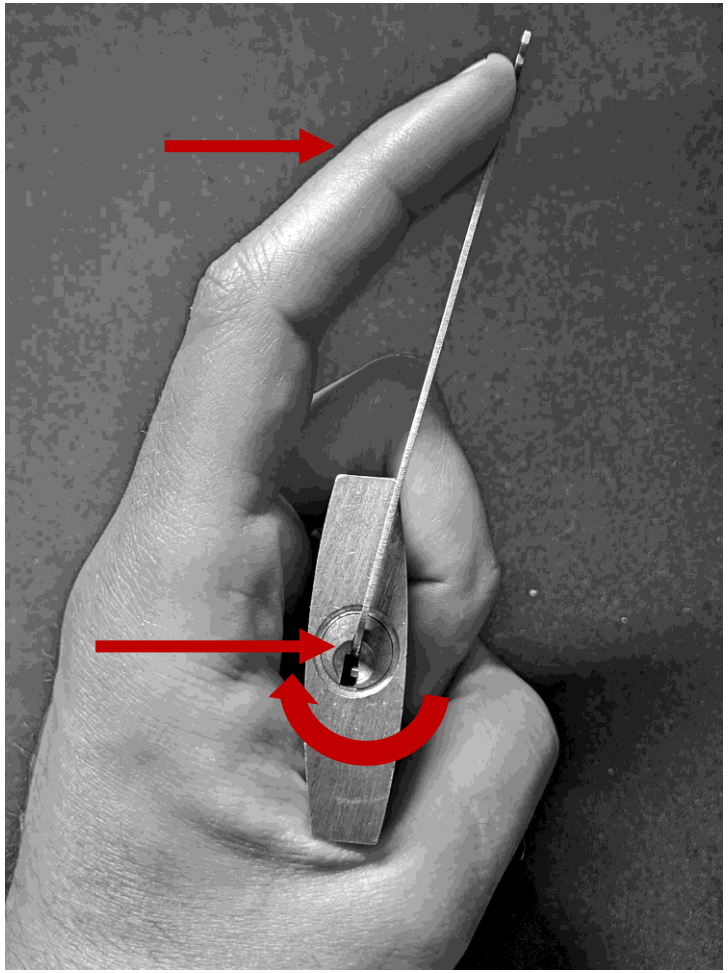
- Use an L-shape tension wrench
- Insert tension wrench at the **edge** of the plug
- Use your **index finger**
- Put a small amount of pressure and push **clockwise**

USING TENSION WRENCH – METHOD 3



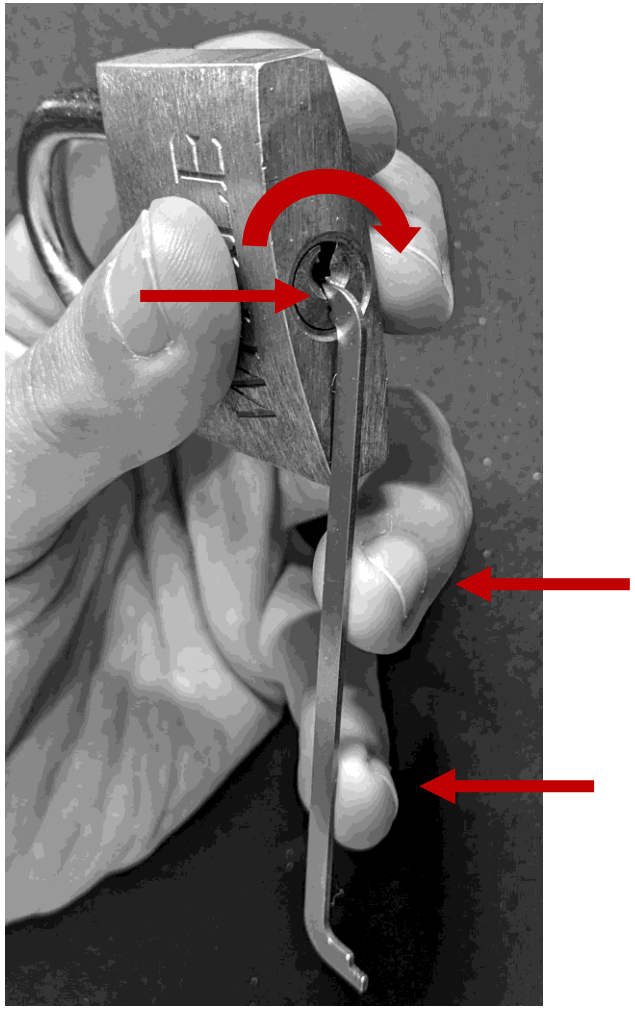
- Use an L-shape tension wrench
- Insert tension wrench at the **edge** of the plug
- Use your **thumb**
- Put a small amount of pressure and push **clockwise**

USING TENSION WRENCH – METHOD 4



- Use **center of keyway** tension wrench
- Insert tension wrench at the **center** of the plug
- Use your **index finger**
- Put a small amount of pressure and push **clockwise**

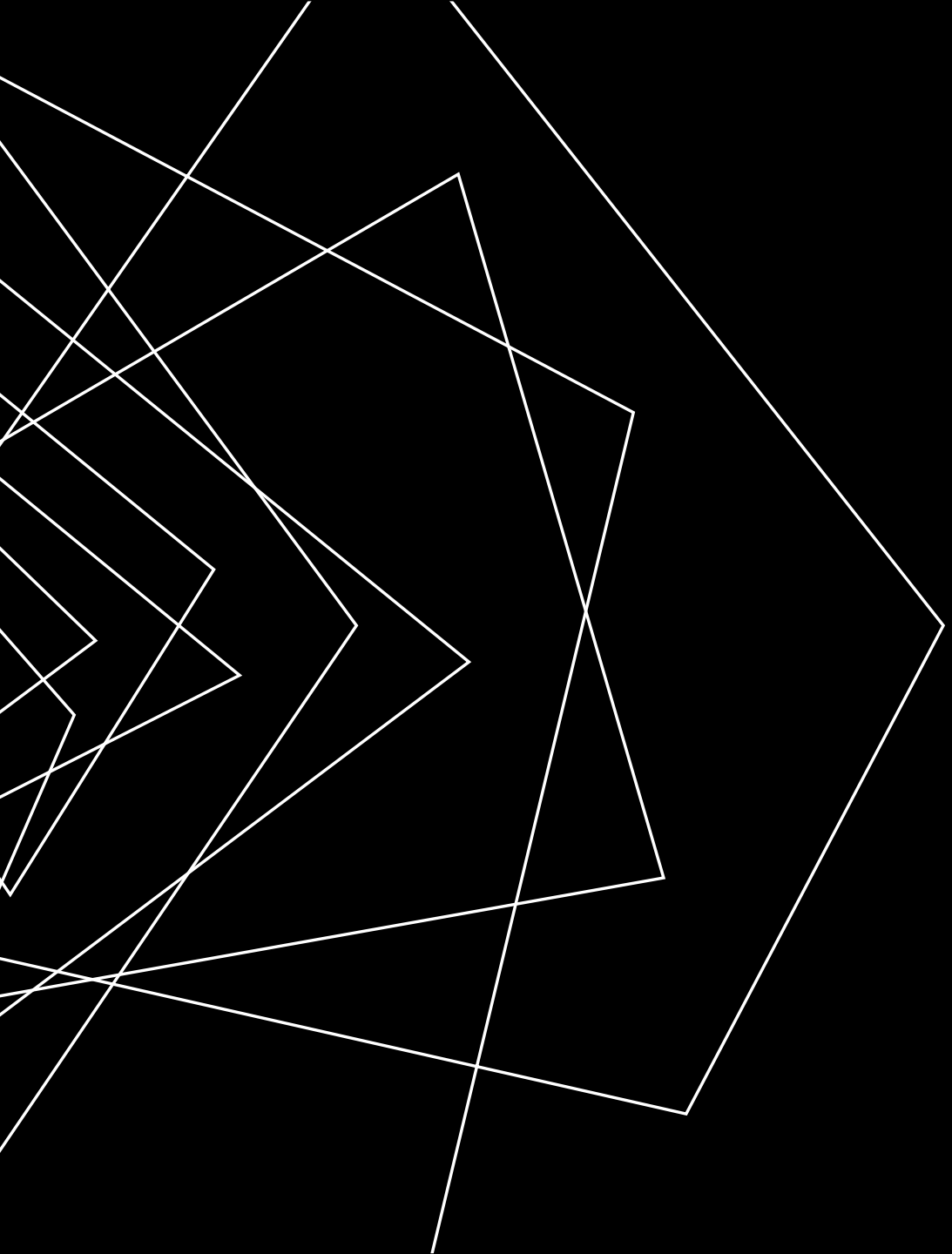
USING TENSION WRENCH – METHOD 5



- Use **center of keyway** tension wrench
- Insert tension wrench at the **center** of the plug
- Use **pinky** and **ring finger**
- Put a small amount of pressure and push **clockwise**

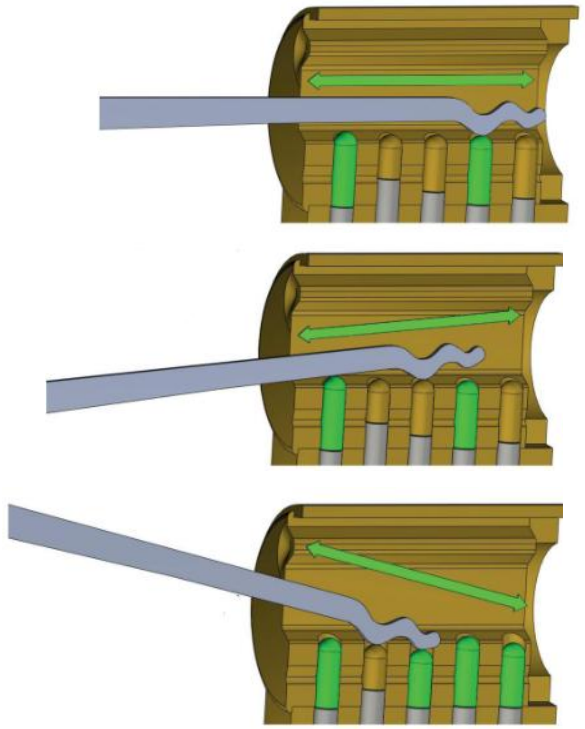
TENSIONING TIPS

“Use less tension than you expect to need”



RAKING

USING RAKES



- Use an **L-Shape** tension wrench
- Gently tension the plug
- Insert the rake into the keyway **till the end**, without touching the pins
- **Pull out** the rake in one **quick** movement
- Repeat 10 to 20 times.
- Vary:
  1. Amount of rotating tension
  2. Amount of force pushing the pins
  3. Angle of raking tool
  4. Speed
  5. Raking tools

USING RAKES

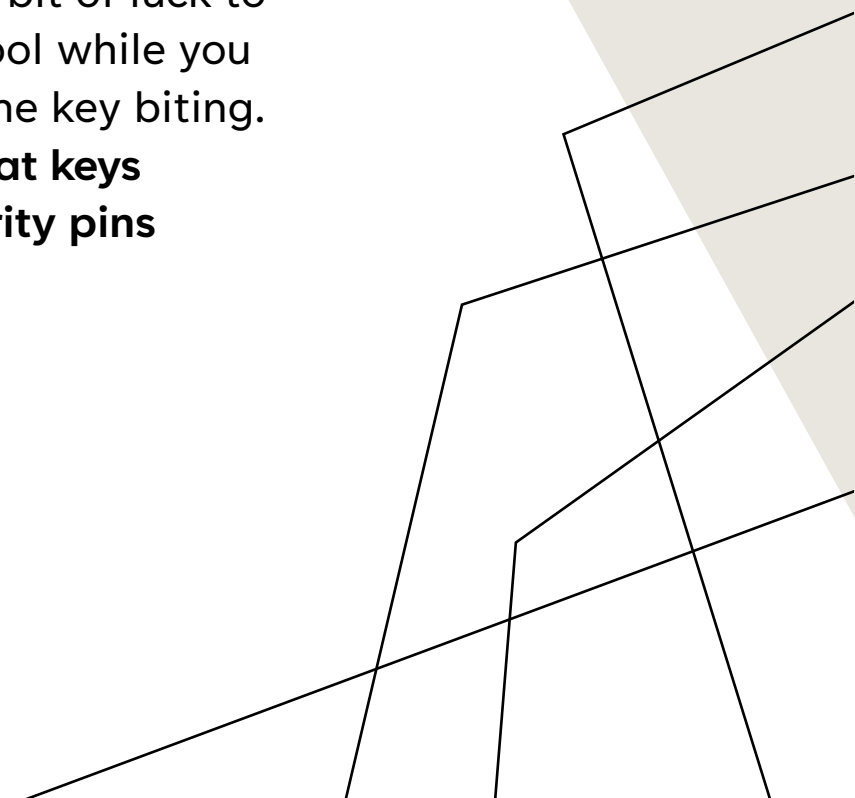
USING RAKES

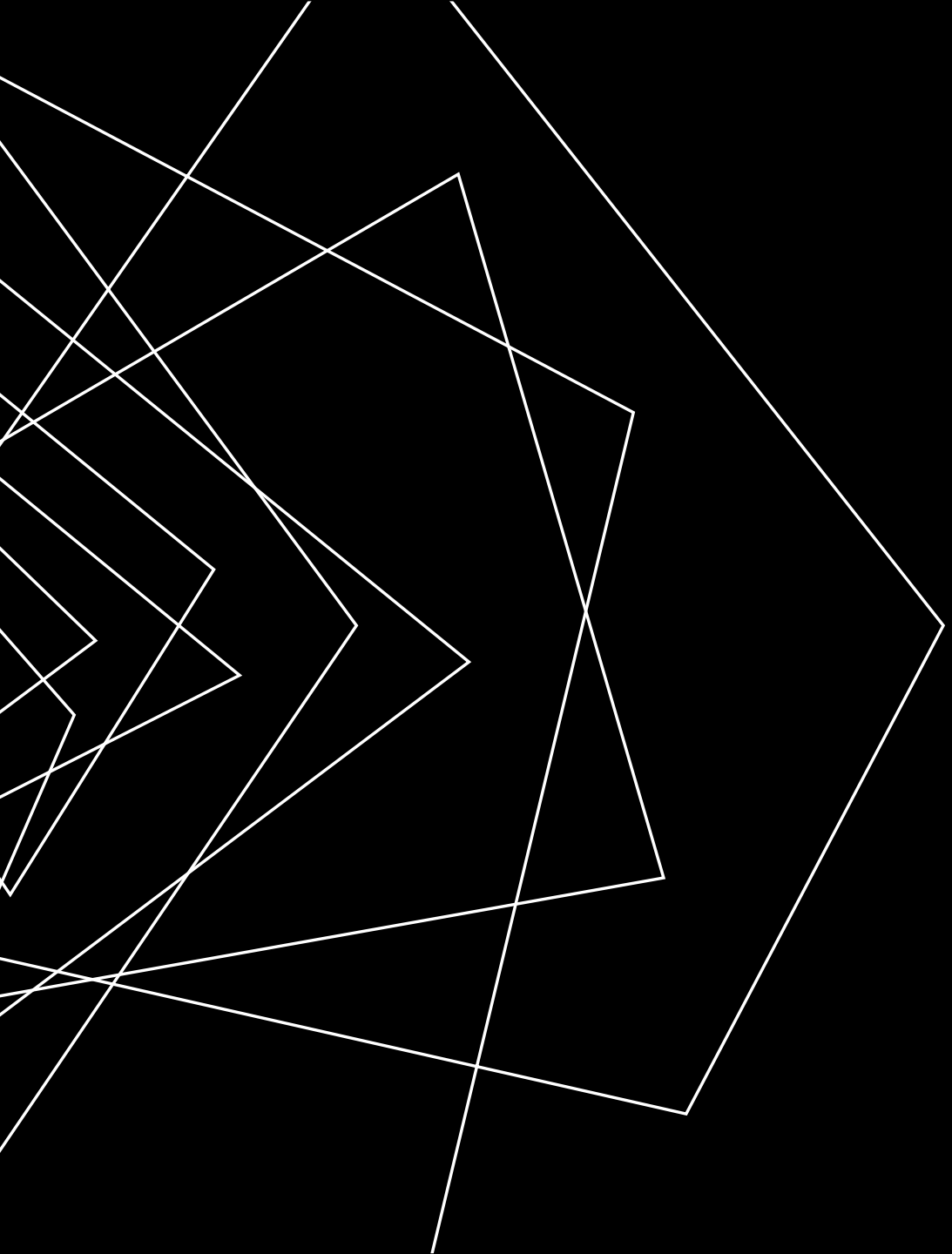
Advantages of raking:

- It can be **quick** if works

Disadvantages of raking:

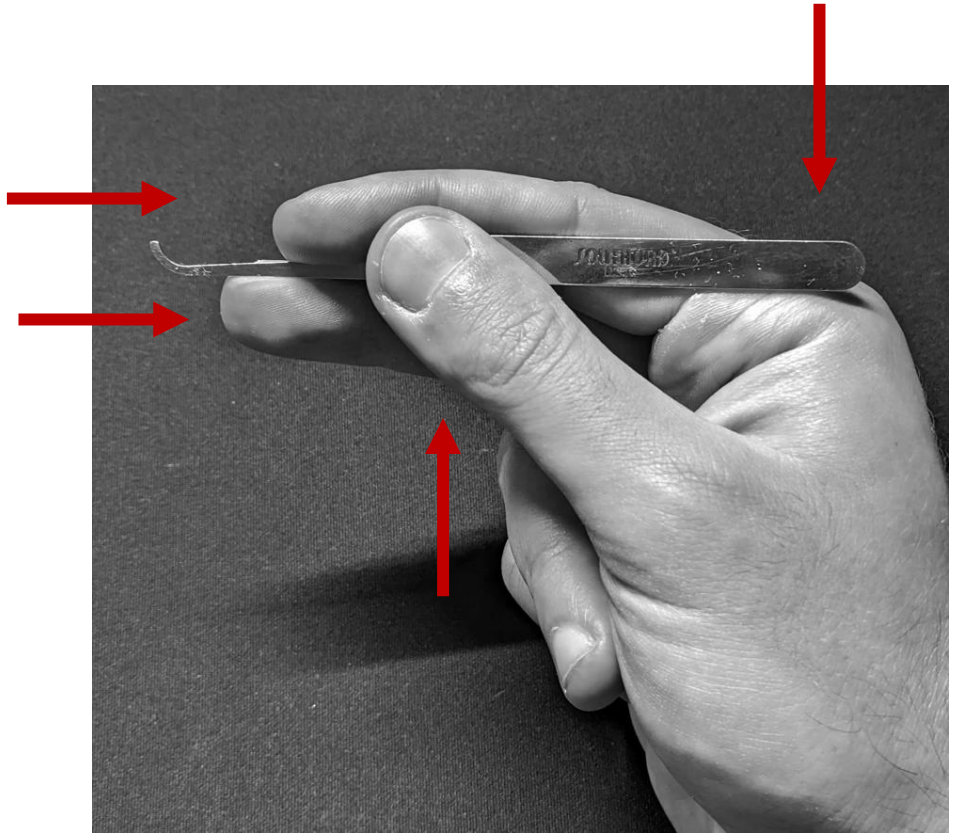
- Not all locks can be raked. It depends on the **biting of the lock's key** and it requires a bit of luck to choose the correct tool while you have no info about the key biting. Requires relatively **flat keys**
- Cannot bypass **security pins**





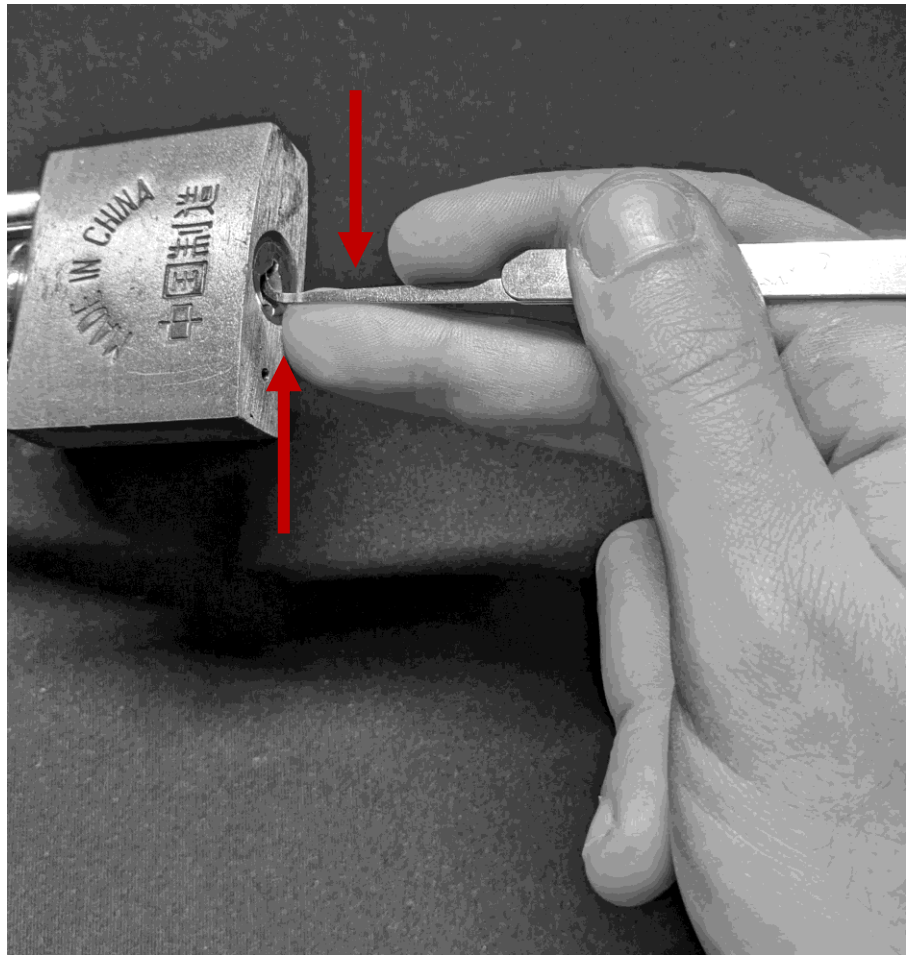
SINGLE-PIN PICKING

USING HOOKS



- Place the hook between your **index** and your **middle finger**
- Hold it with your **thumb**
- Rest in your **index knuckle**

USING HOOKS

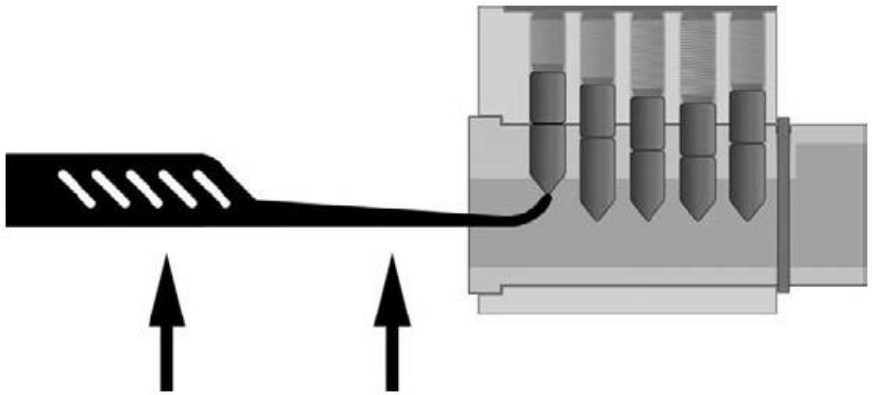


For better accuracy:

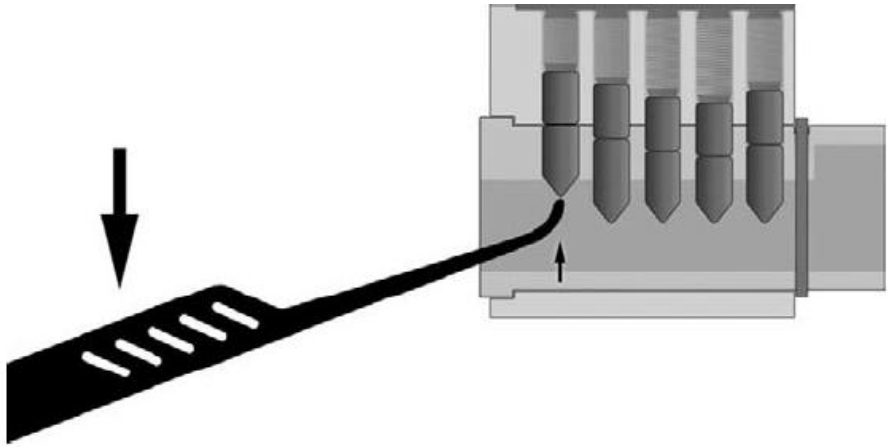
- The **hook** should touch on your **middle finger.**
- And your **middle finger** should touch the **lock**.

USING HOOKS

Raising



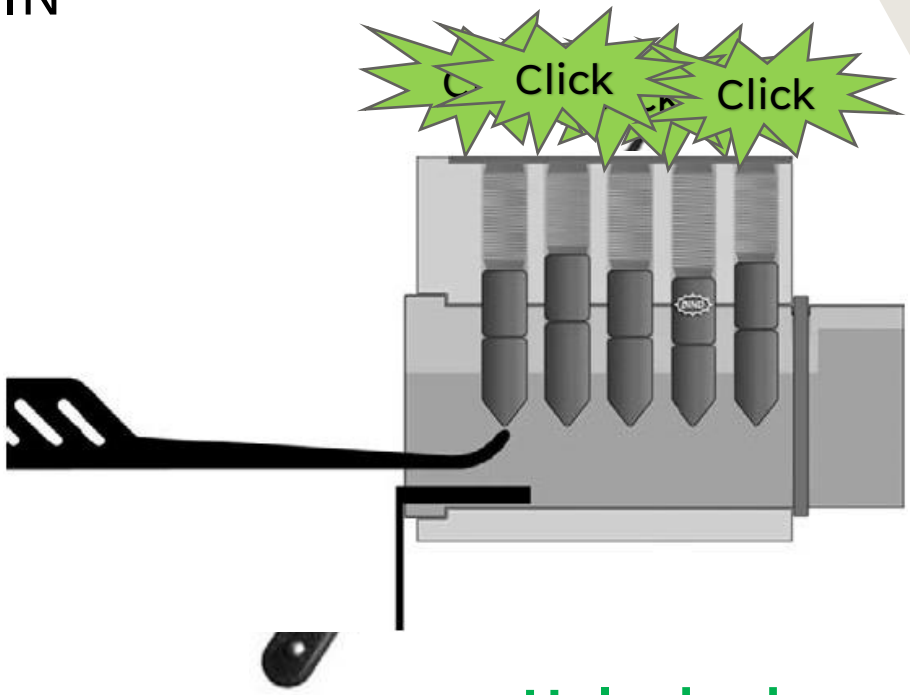
Rocking



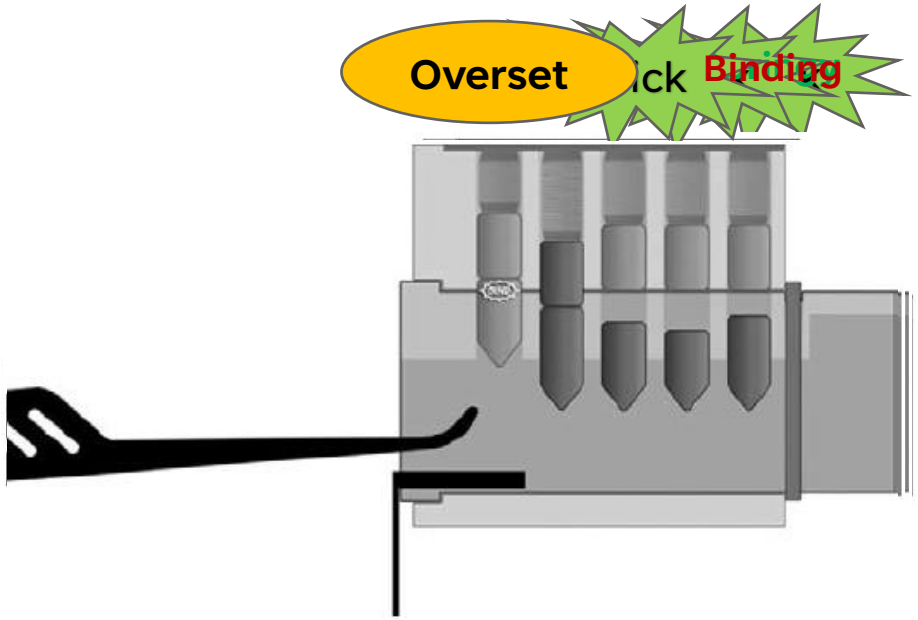
SINGLE PIN PICKING

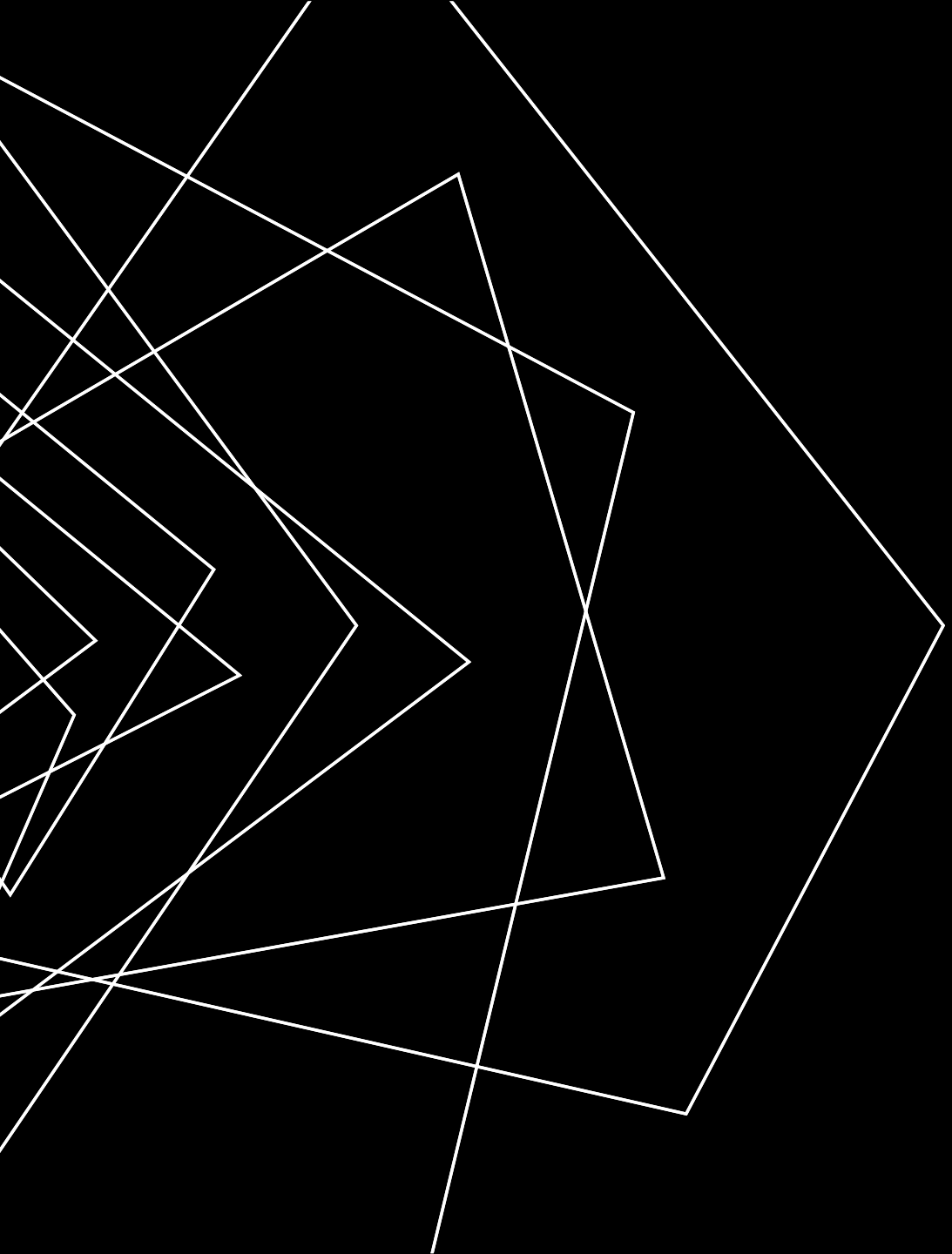
OR SEARCHING FOR THE BINDING PIN

- Use a **tensioner** and
- A **single-pin picking hook**
- Apply rotational force to the plug and insert the hook
- Use picking hook to navigate to each one of the pins
- Search for the binding pin among springy pins
- When it is set go through the rest and search for the next binding pin
- Continue until all the pins are in set position



SINGLE PIN PICKING
OVERSET SCENARIO





THANK YOU

REFERENCES

1. **Practical Lock Picking** – A physical penetration tester's training guide, Deviant Ollam, Syngress 2010
2. **Locksport** – A hacker's guide to lockpicking, impressioning and safe cracking, Jos Weyers, Matt Burrough, Walter Belgers, BandEAtoZ, and Nigel K. Tolley, NoStarchPress 2024
3. **Little black book of Lockpicking** – Lock opening and bypass techniques for Security Professionals, Alexandre Triffault, ATSecurity 2021