Safe lock manipulation 101

Hackerhotel 2024

Introduction

- Why are we here?
- Safe lock overview
- Safe Manipulation
- Final thoughts

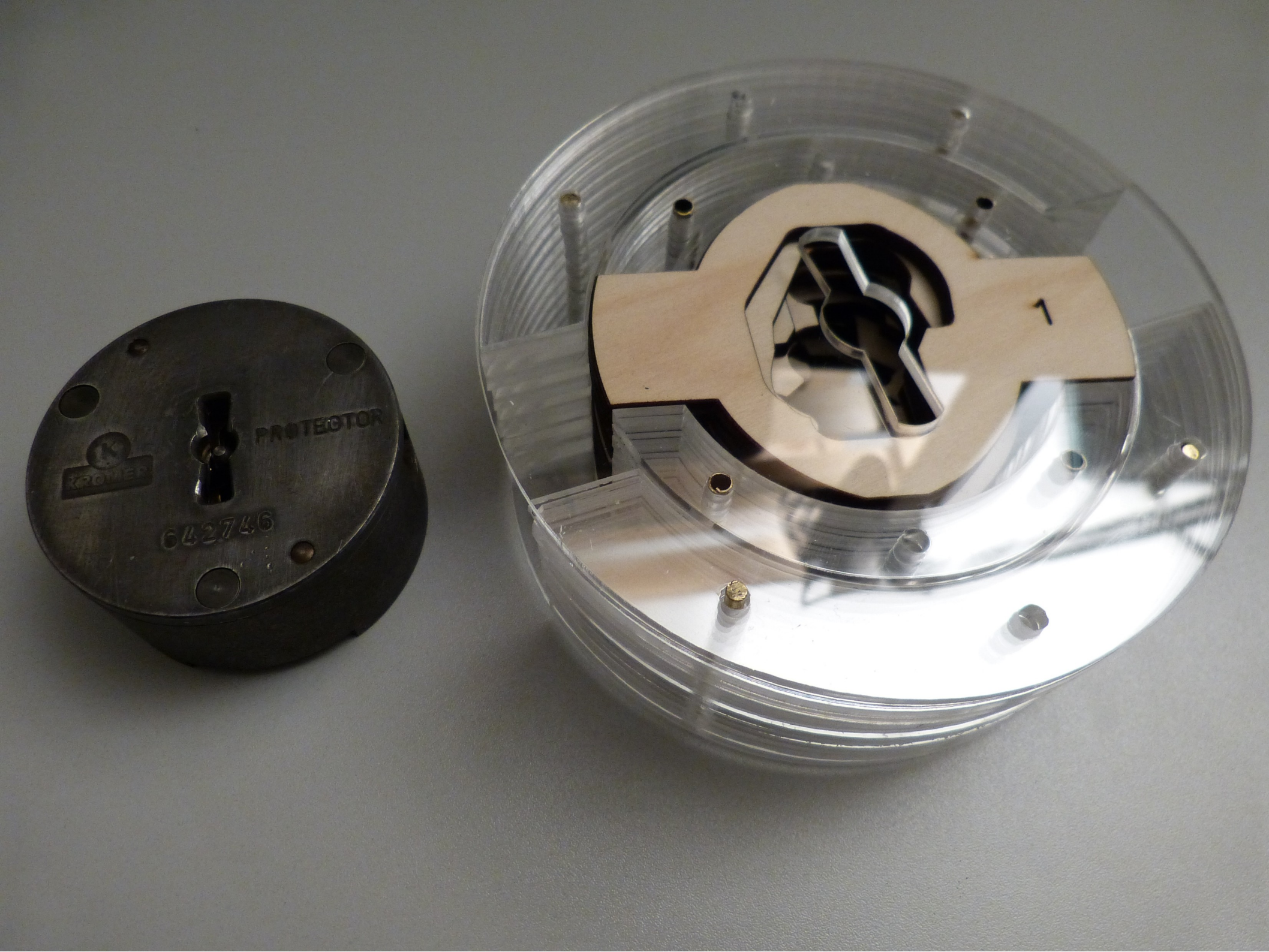
Introduction

- Disclaimer:
  - I’m not a safe technician
  - Locks are a puzzle
  - Non Destructive Entry (NDE)
  - Sources:
    - The National Locksmith Guide to Manipulation
    - Safecracker: A Chronicle of the Coolest Job in the World
    - www.lockpicking101.com

Introduction

- Your trainer
  - Jan-Willem Markus
  - Security Analyst & trainer
  - President of The open Organisation of lockpickers NL

PCF8566T
60547
TSM97361
TAIWAN
X07.02
373597
470µF 6.3V


PROTECTOR
KROMEX
642746
1

Introduction

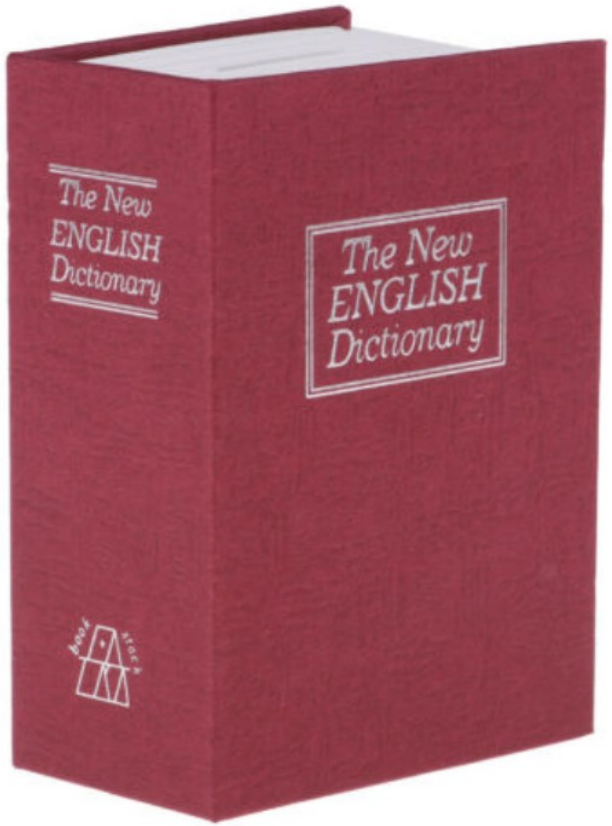
- Now it’s your turn:
  - What are your **interests**?
  - What do you want to **learn**?
  - What do you think of the words **safe**, **vault**, and **safe lock**?

Introduction

- The words **safe** and **vault** are used for many things, but one of these is not like the other.


YORK SAFE & LOCK CO.
YORK, PA.
THE HERMAN SAFE CO.
AGENTS
SAN FRANCISCO, CAL.

SAVE UP TO 9% See all eligible items and terms ▸



$ Have one to sell? Sell now

Safe Lock Key Book Hide Money Jewelry Stash Diversion Dictionary

Condition: New

Sale ends in: 01d 20h 26m

Color: - Select -

Quantity: 1 More than 10 available / 16 sold

Price: **US $14.31**

~~US $15.72~~ Save 9%

Buy It Now

Add to cart

♡ Add to Watchlist

A seller you've bought from	Free shipping	30-day returns

Shipping: FREE Standard SpeedPAK from Greater China | See details

International shipment of items may be subject to customs processing and additional charges.

Located in: Shenzhen, China

Delivery: Estimated between Thu. Oct. 28 and Wed. Nov. 10

Seller ships within 1 day after receiving cleared payment.

Please note the delivery estimate is **greater than 7 business days.**

Please allow additional time if international delivery is subject to customs processing.

Returns: 30 day returns. Buyer pays for return shipping | See details

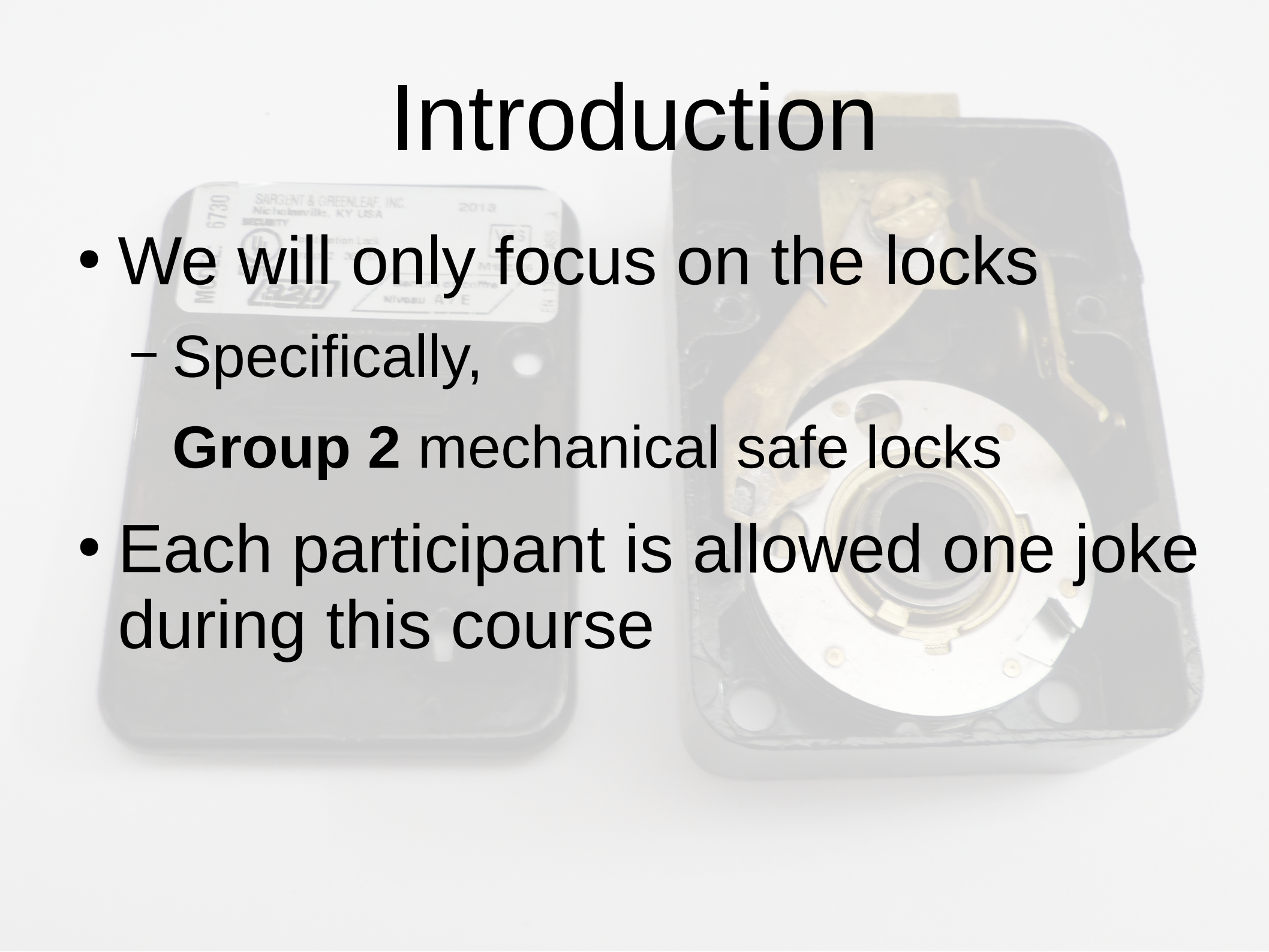
Payments: PayPal G Pay VISA

Introduction

- We will only focus on the locks
  - Specifically,

    Group 2 mechanical safe locks

Introduction



- We will only focus on the locks
  - Specifically,

    Group 2 mechanical safe locks
- Each participant is allowed one joke during this course

Virtual lock to practice

Virtual lock to practice

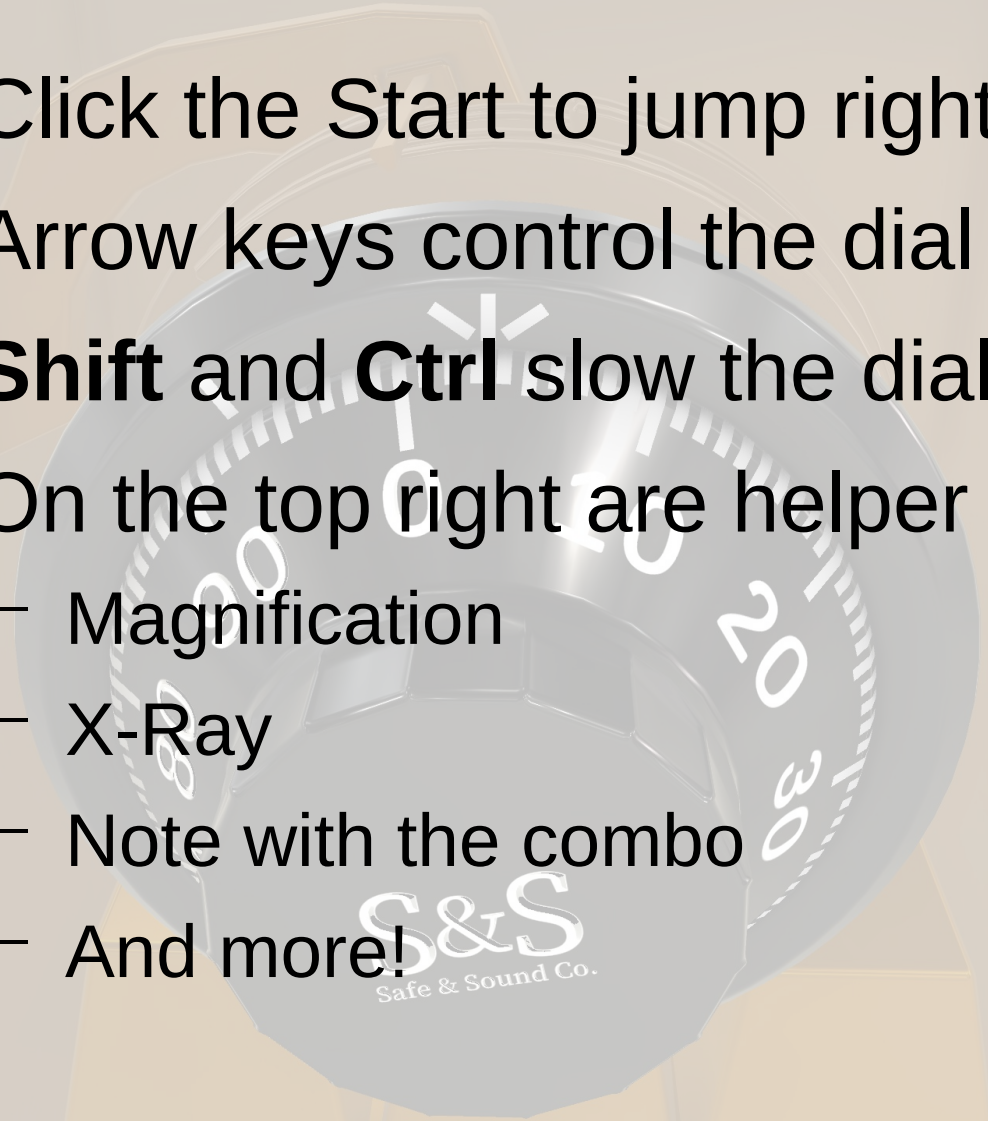
- This is a note to the people playing along at home:
  - Get the **Sophies Safecracking Simulator** at $3
  - https://sophieh.itch.io/sophies-safecracking-simulator

Virtual lock to practice

Virtual lock to practice

- Click the Start to jump right in
- Arrow keys control the dial
- **Shift** and **Ctrl** slow the dialing down
- On the top right are helper functions:
  - Magnification
  - X-Ray
  - Note with the combo
  - And more!

L81, R96, L28




36,400
0
10
20
30
40
06
Wi-Fi-GyBro

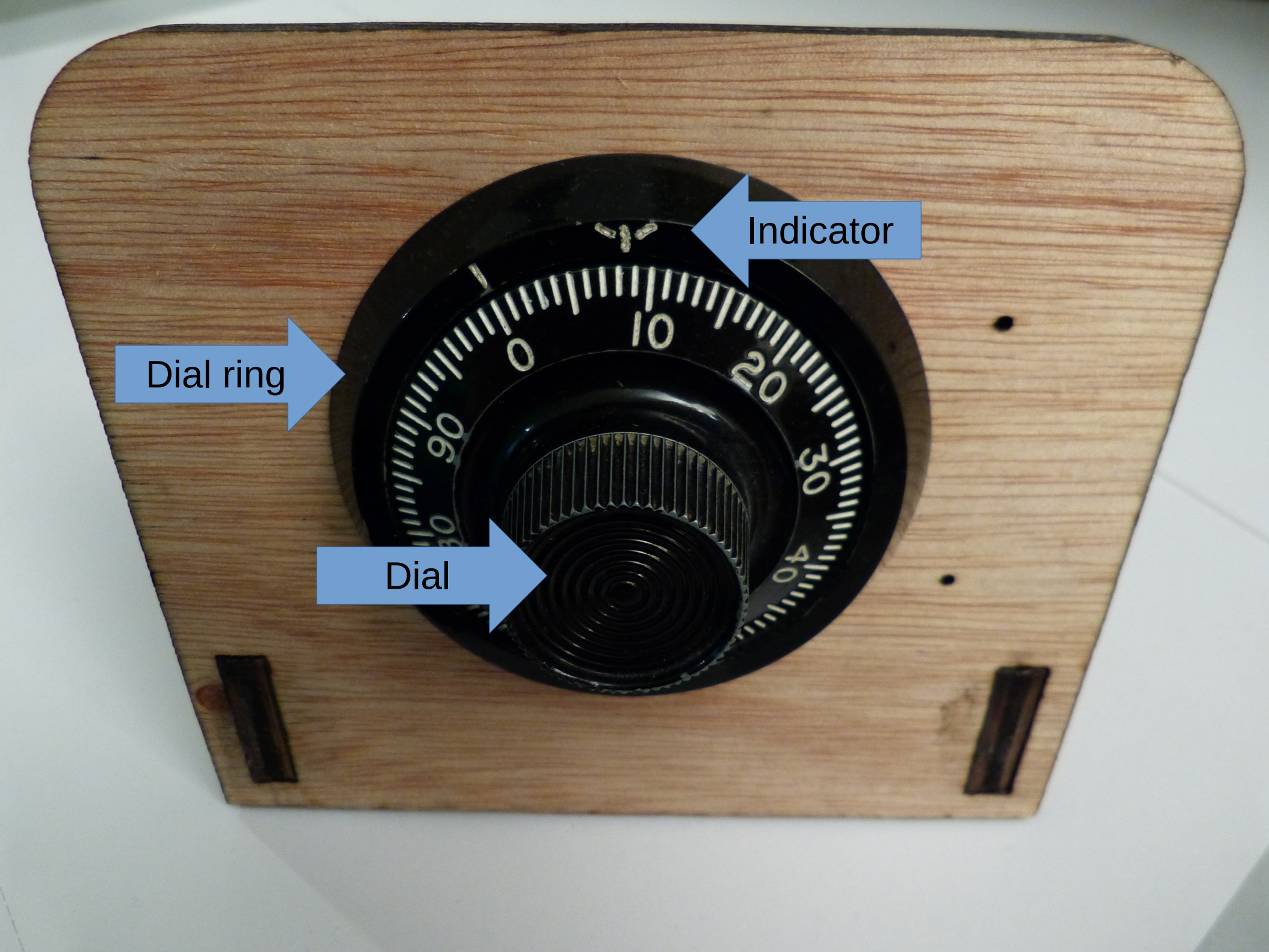
Mechanical Safe Lock

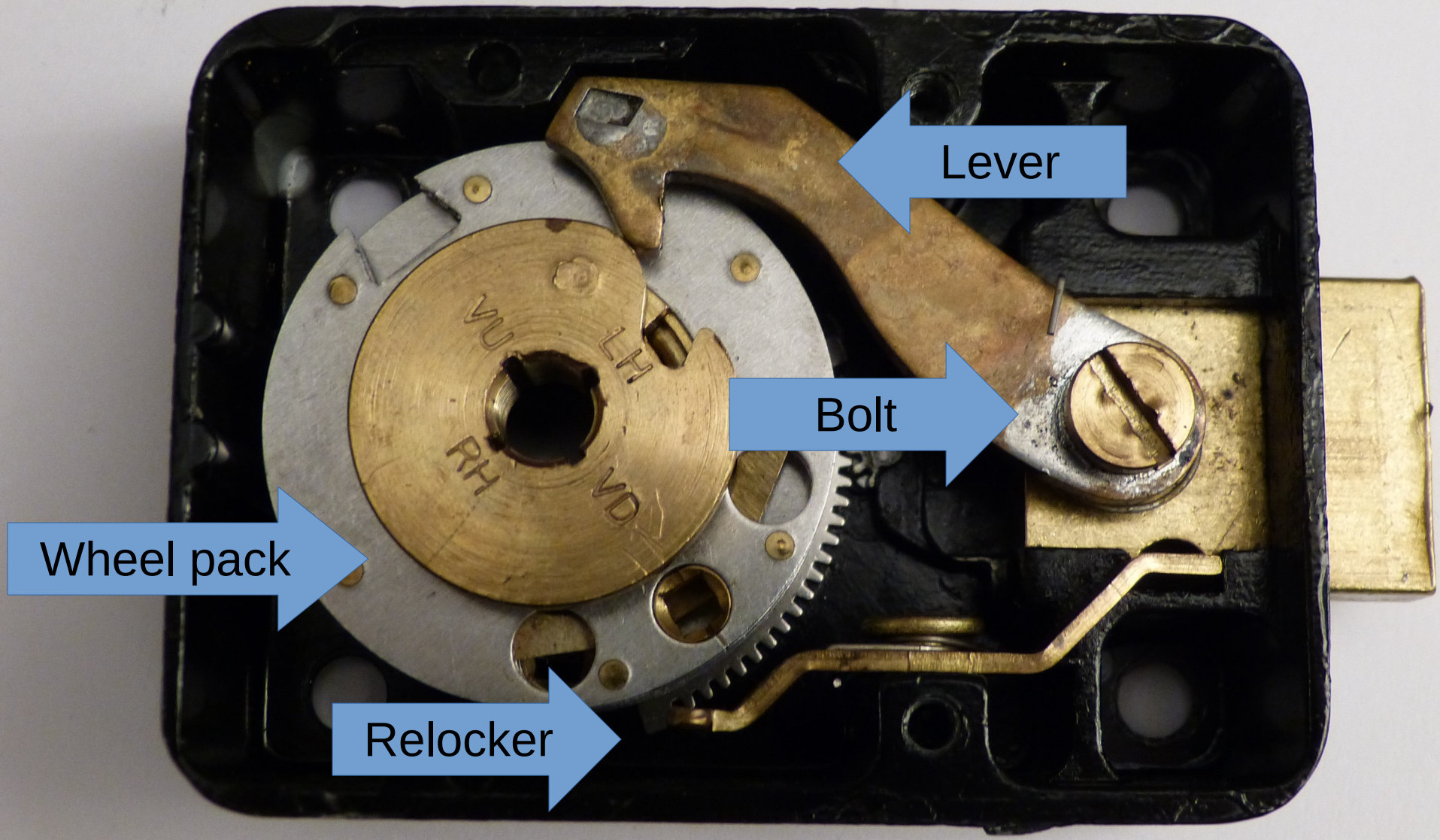
Mechanical Safe Lock

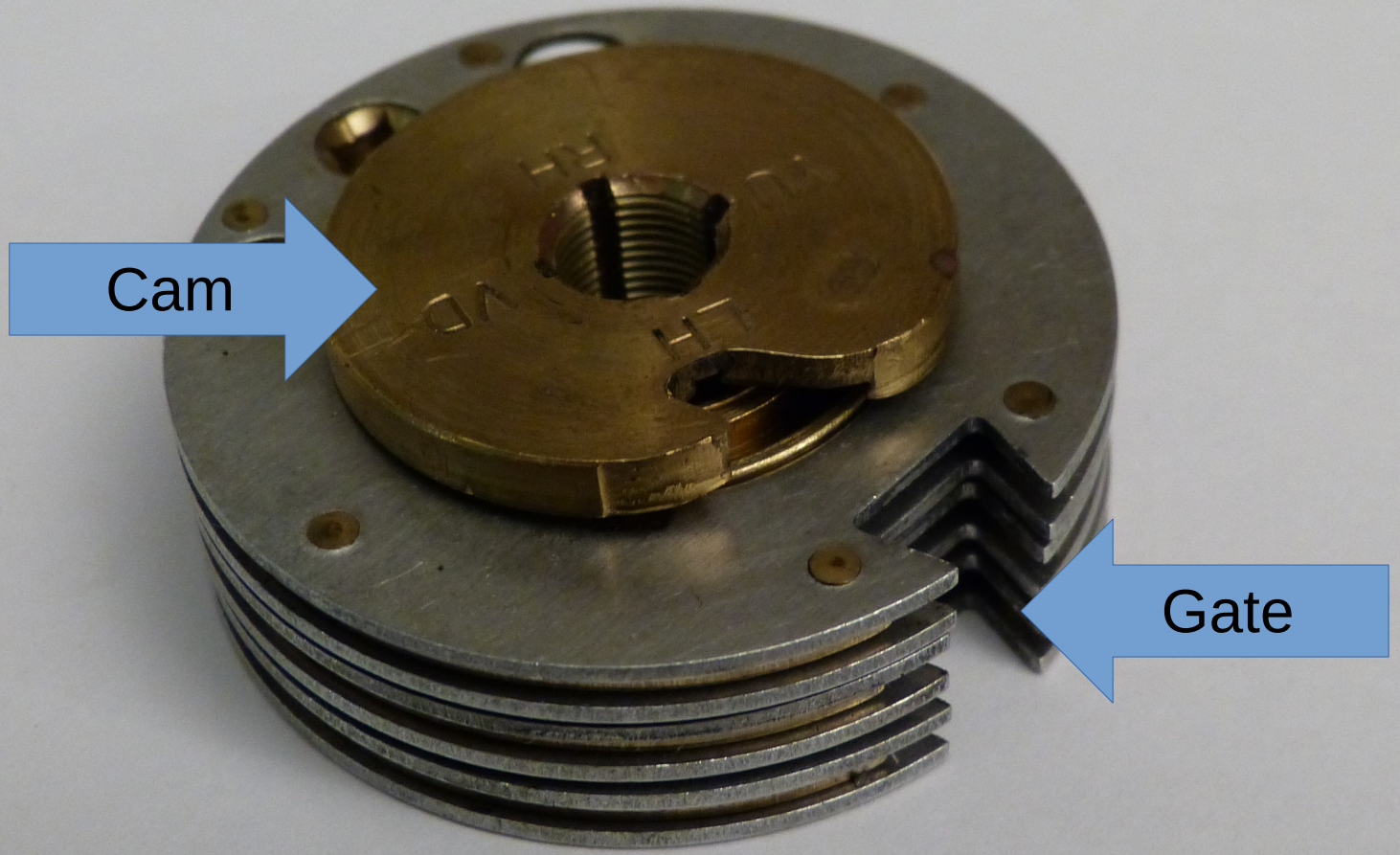
- Spring lever combination lock
  - **Group 2**
    - 2h manipulation resistant
  - **Group 1**
    - Effectively manipulation resistant
  - **Group 1R**
    - X-ray resistant

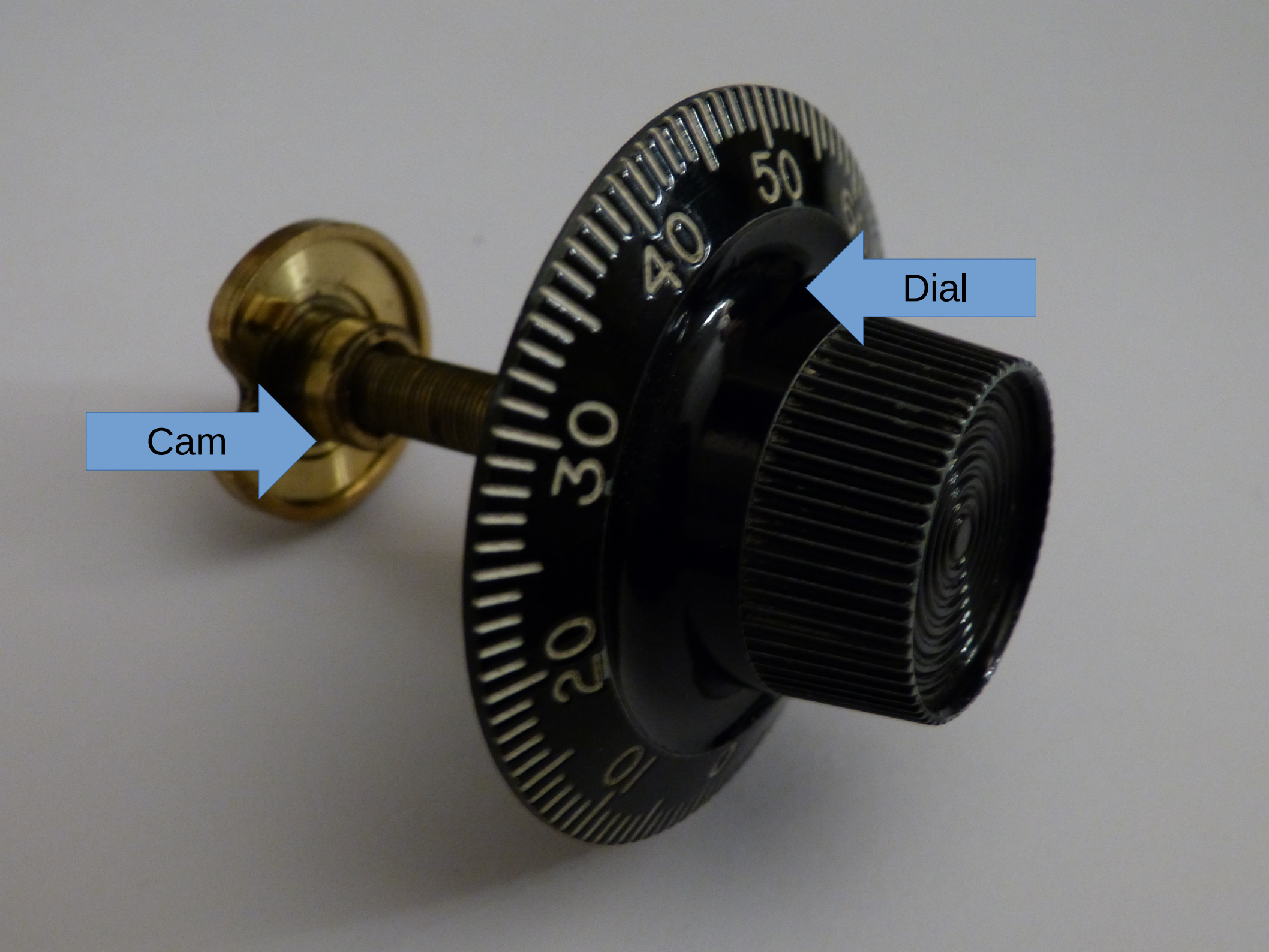
Mechanical Safe Lock

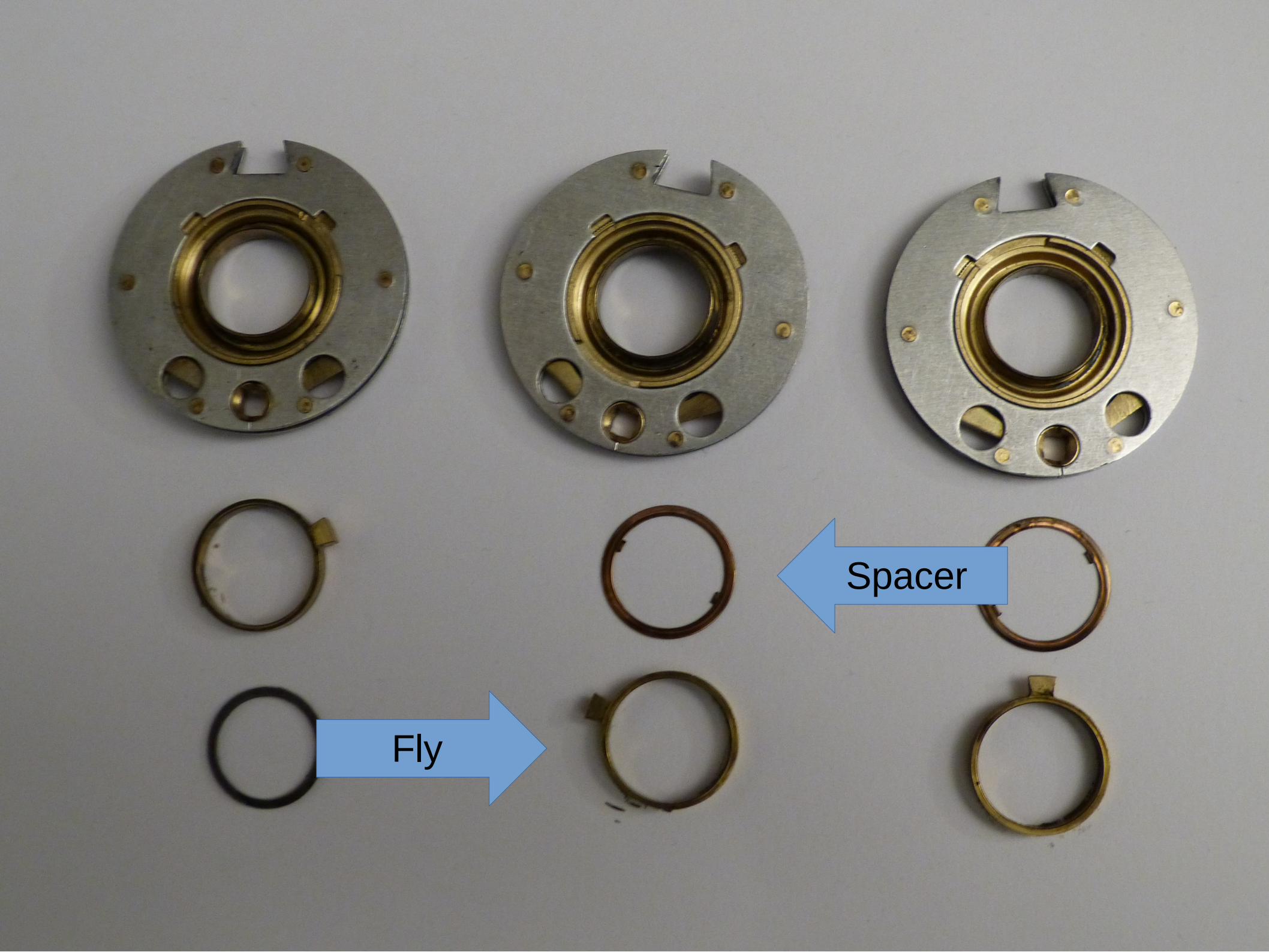
- Target for today:
  - **Sargent Greenleaf 6730**
  - Group 2 safe lock
  - Three wheels
    - Theoretically a million combinations
    - Practically ~400k combinations

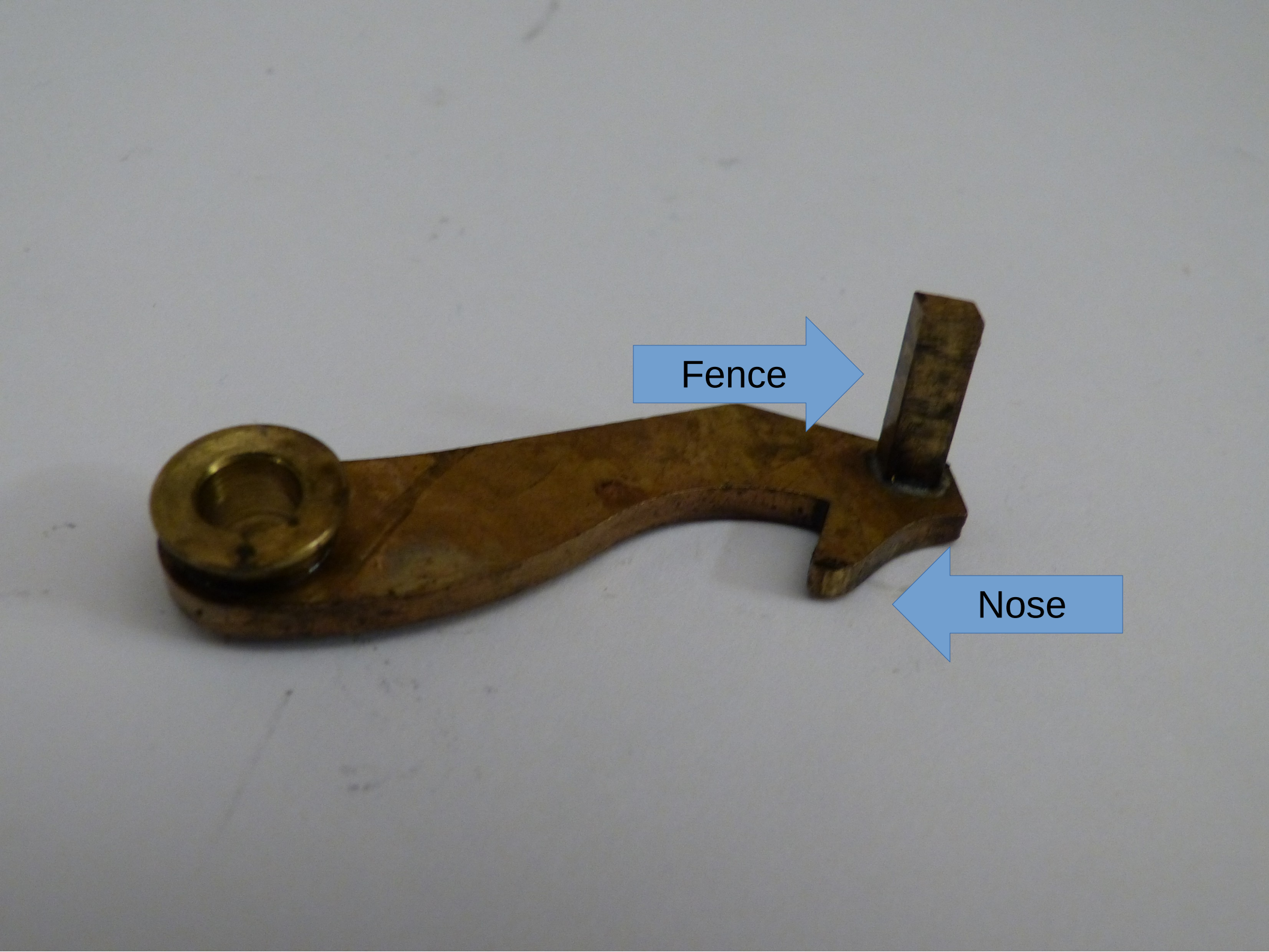

Indicator
Dial ring
Dial
1
0
10
20
30
40
90
80


Lever
Bolt
Wheel pack
Relocker
VU
LH
RH
VD


Cam
Gate


Cam
Dial
50
40
30
20

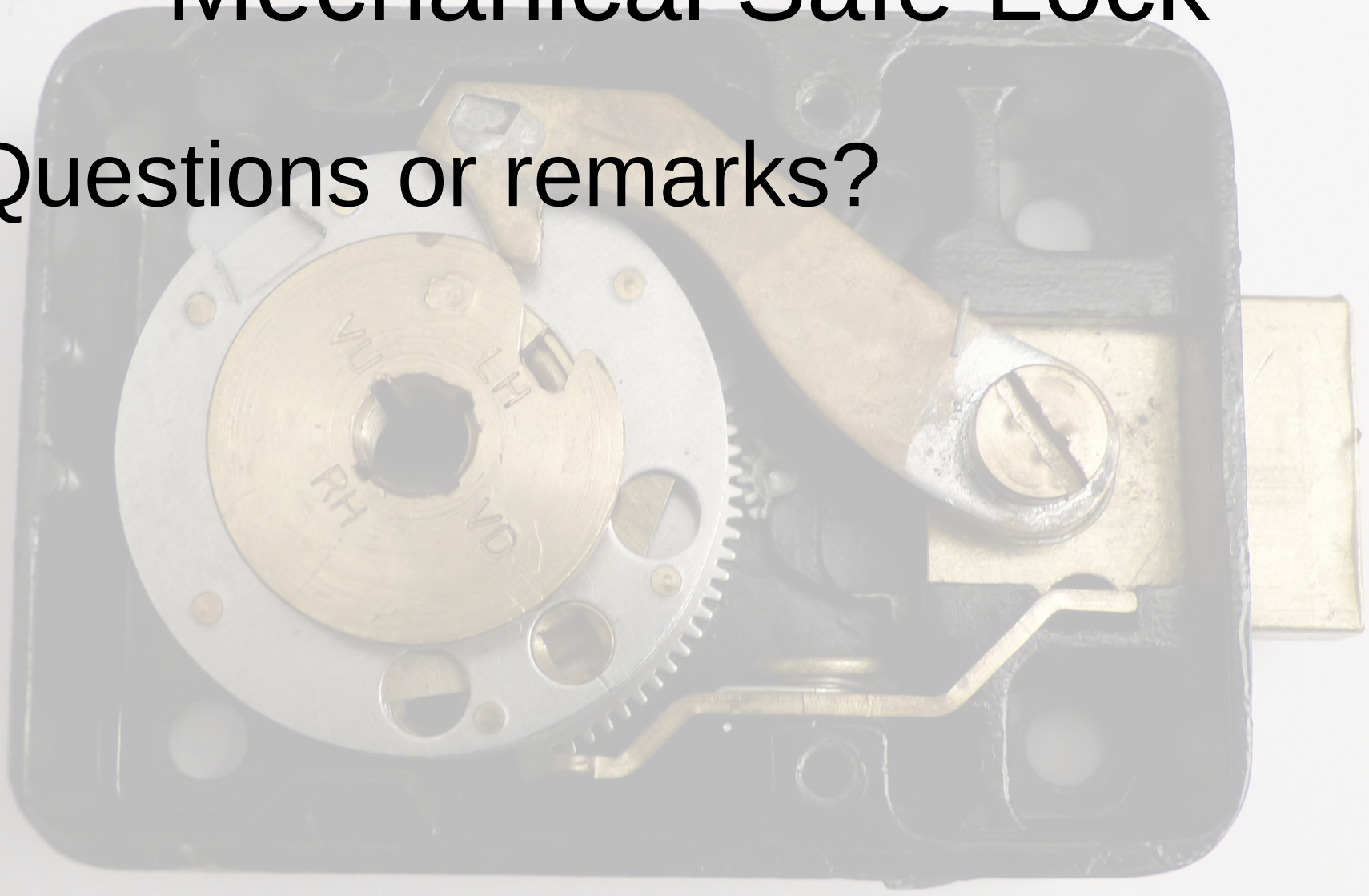

Spacer
Fly


Fence
Nose

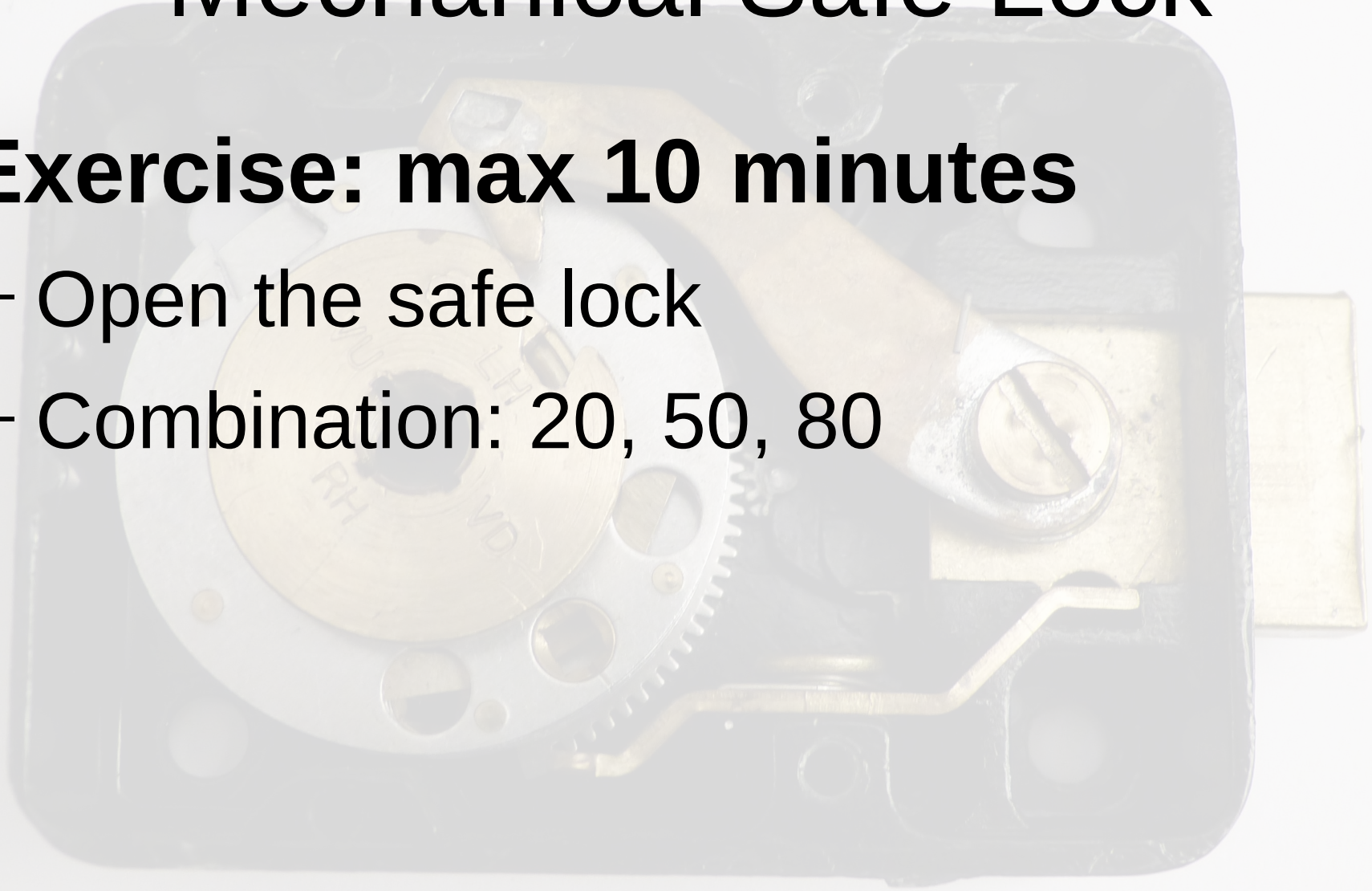

LH
VU
VD
RH

Mechanical Safe Lock

- Questions or remarks?



Mechanical Safe Lock



- **Exercise: max 10 minutes**
  - Open the safe lock
  - Combination: 20, 50, 80

Exercise

- Dialing sequence:
  - Left **four times** to the **first** number
  - Right **three times** to the **second** number
  - Left **twice** to the **last** number
  - Right **past zero** to open the lock

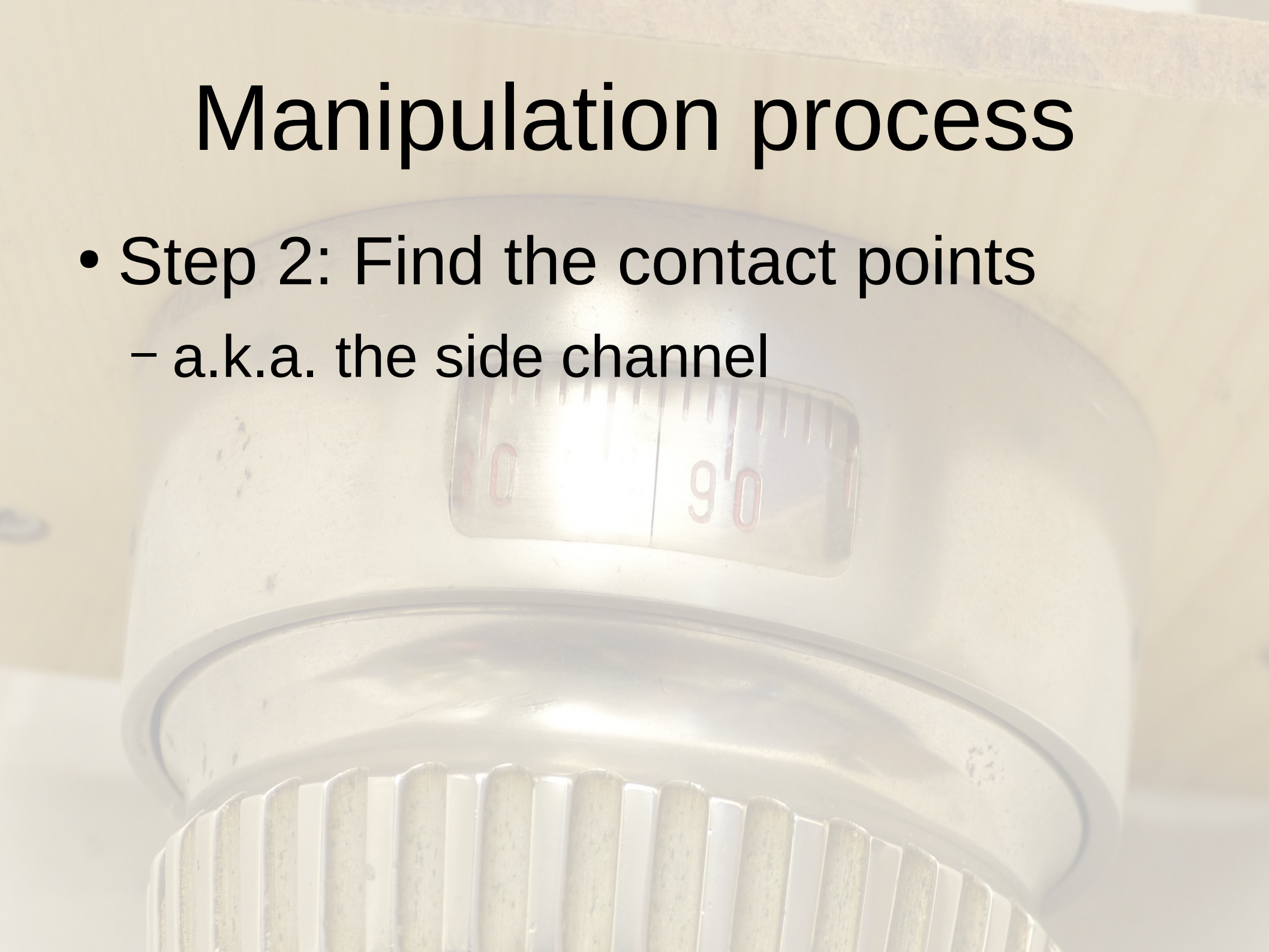
  - Combo reminder: 20, 50, 80

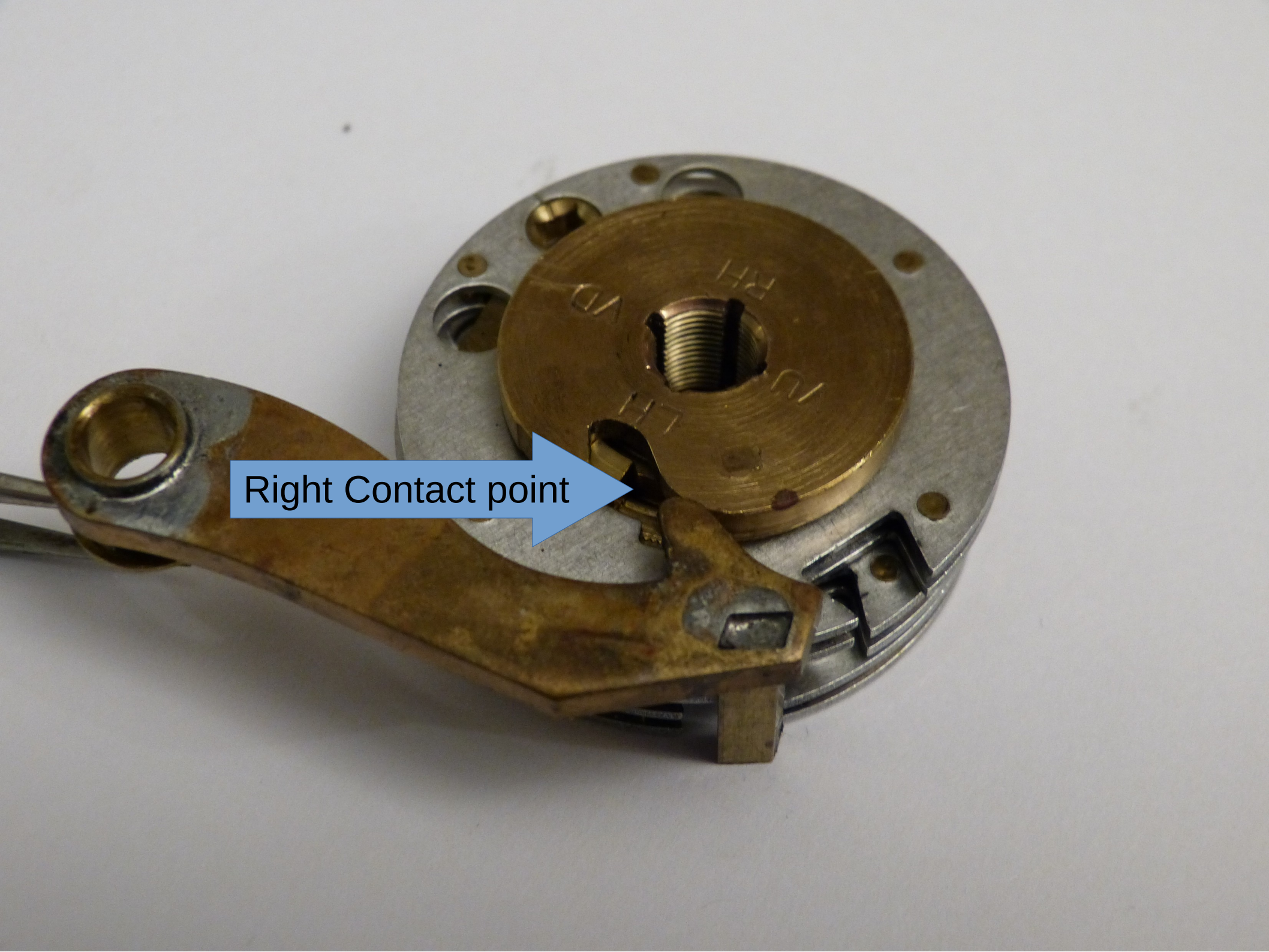
Manipulation process

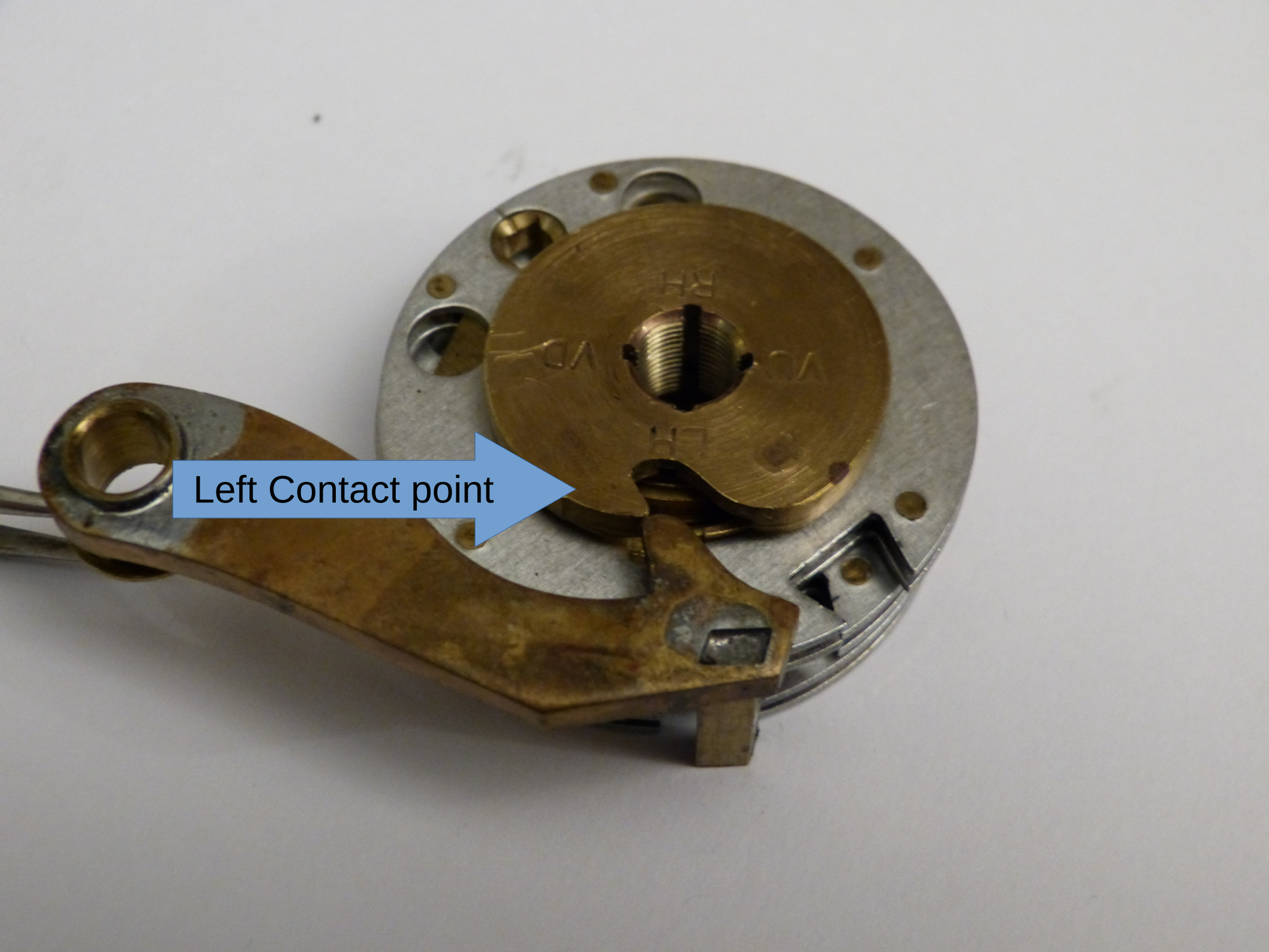
Manipulation process

Manipulation process

- Step 2: Find the contact points
  - a.k.a. the side channel

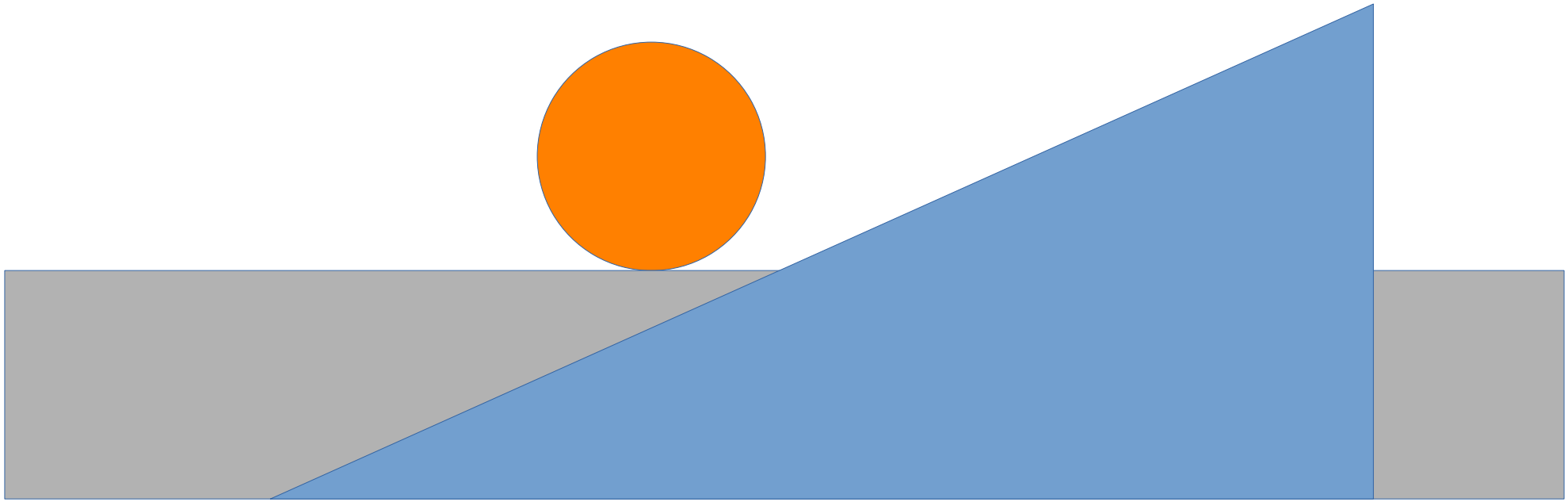



Right Contact point


Left Contact point

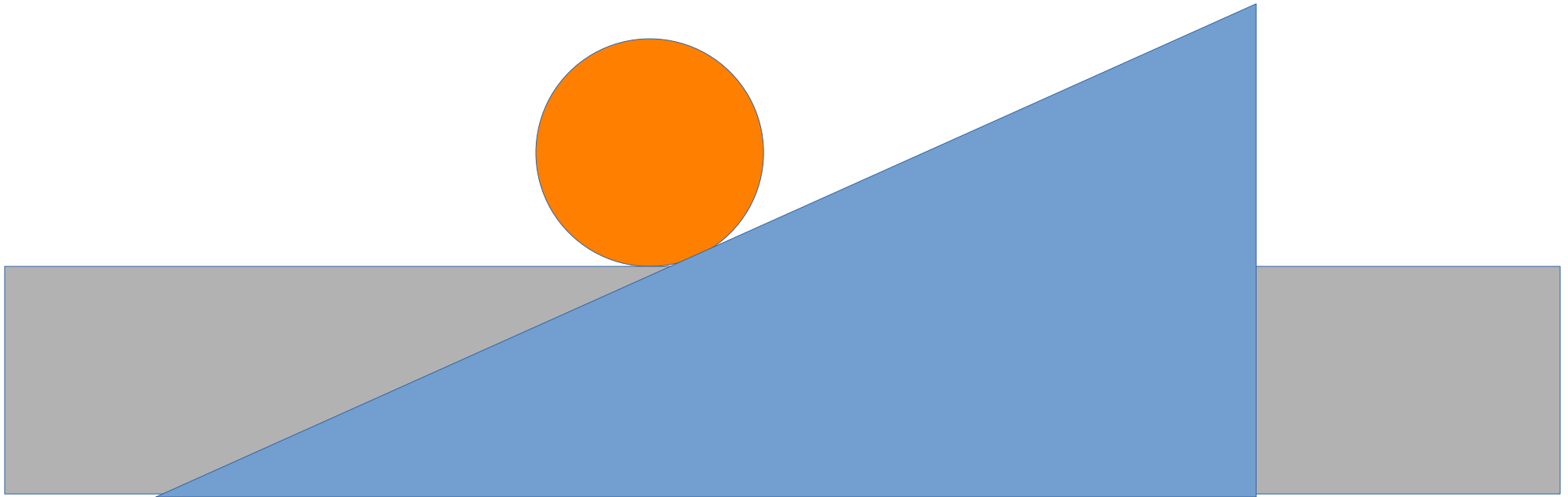
Manipulation process

- Let me illustrate
  - Gray: Wheel
  - Ball: lever nose
  - Ramp: contact point



Manipulation process

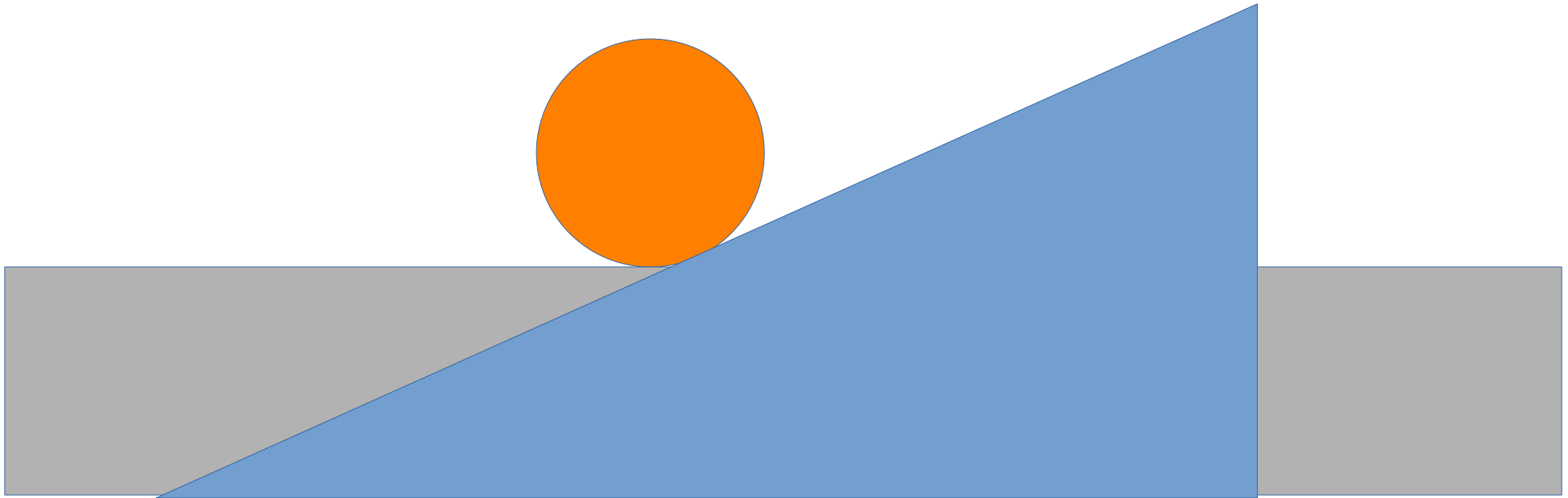
- The fence rests on the wheel
  - With the contact point we can measure it’s position



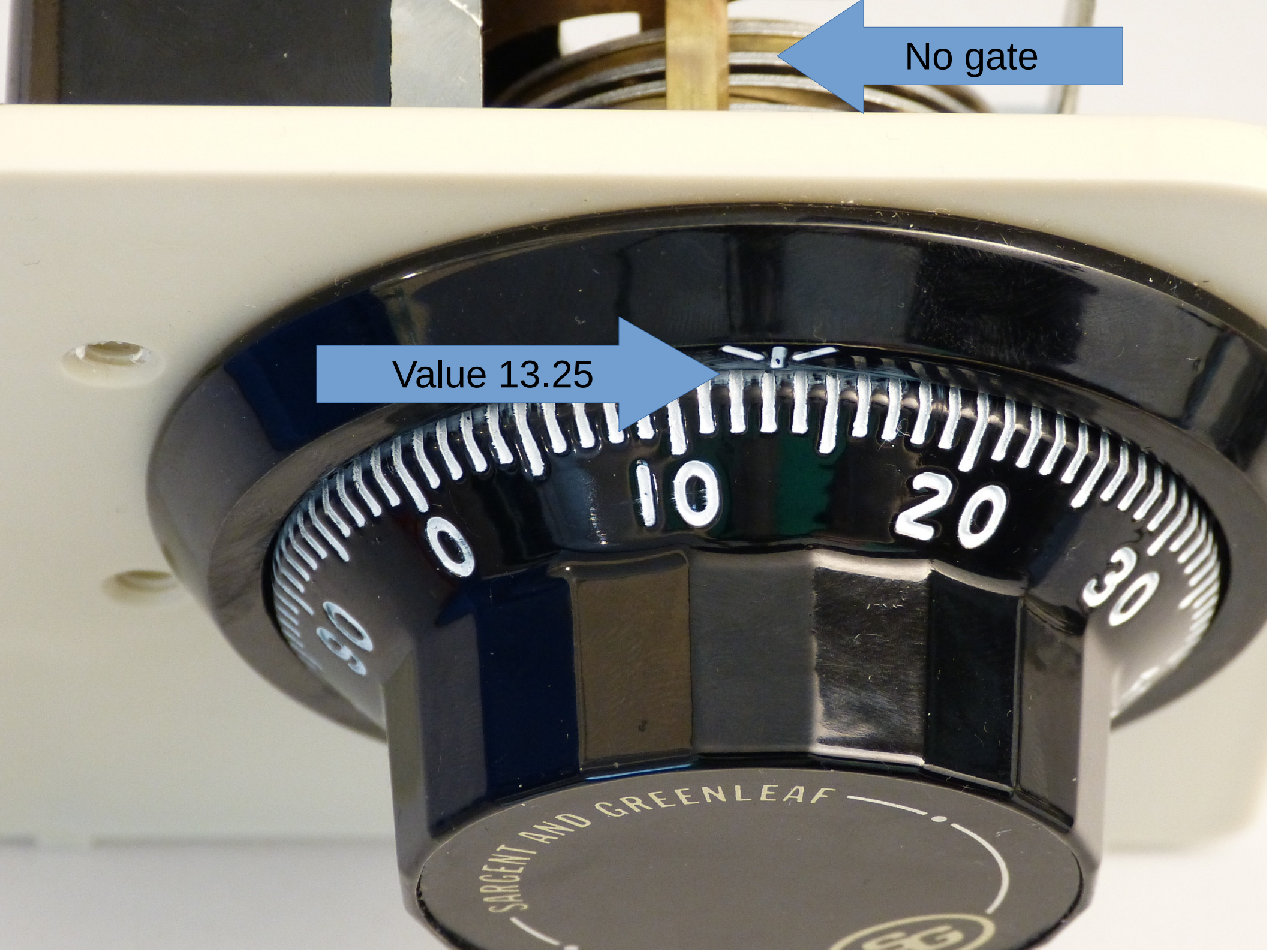
Manipulation process

Indirectly we measure the height of the wheels

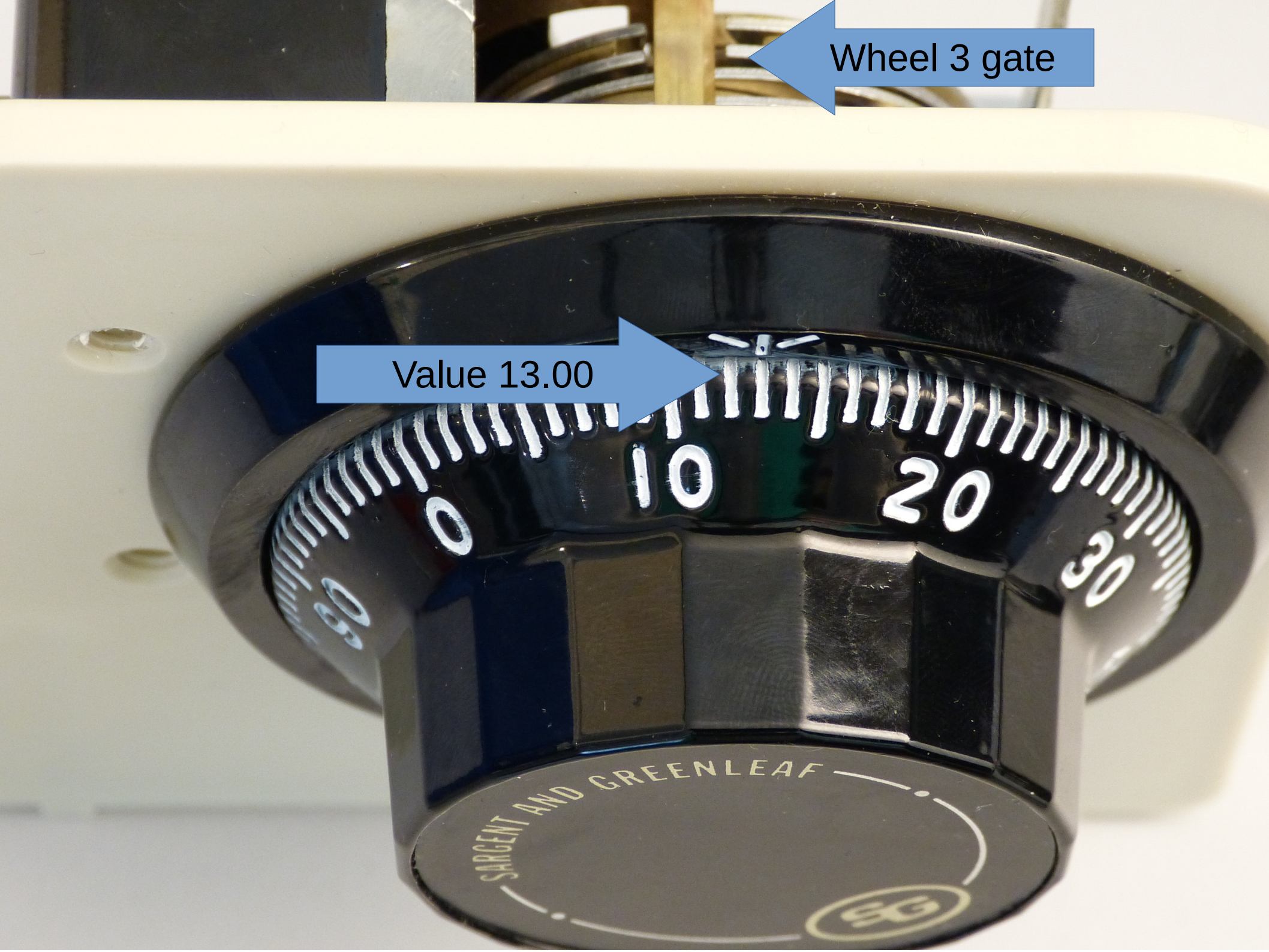
- **Lower point = closer to open**




No gate
0
10
20
30
SARGENT AND GREENLEAF


No gate
Value 13.25
0
10
20
30
SARGENT AND GREENLEAF


Gate of wheel 3
0
10
20
30
80
SARGENT AND GREENLEAF


Wheel 3 gate
Value 13.00
0
10
20
30
40
SARGENT AND GREENLEAF
SG

Manipulation process

- Did you spot the difference?
  - With one gate under the fence the contact point shifted.
  - We want to be very precise
    - Traditionally 0.125 of a digit

Manipulation process

- Questions or remarks?

Manipulation process

- Exercise: 10 minutes
  - find the contact points on your lock
    - They should be around 5 and 15
    - 5 is a hard stop while 15 is on a slope
  - Dial different combinations and observe the contact point value change slightly

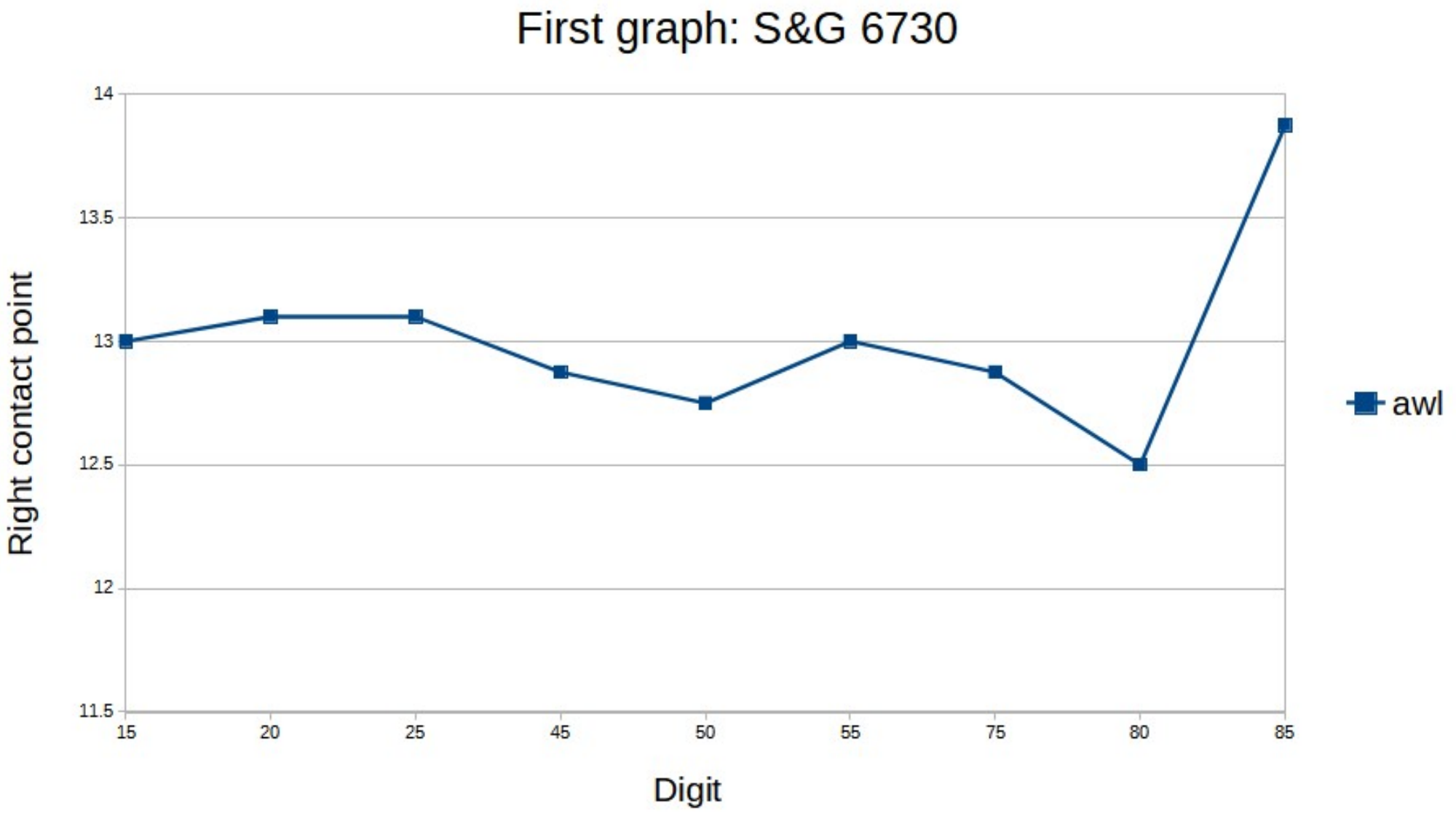
Manipulation process

- Step 3: Graph the wheels shape
  - All wheels left

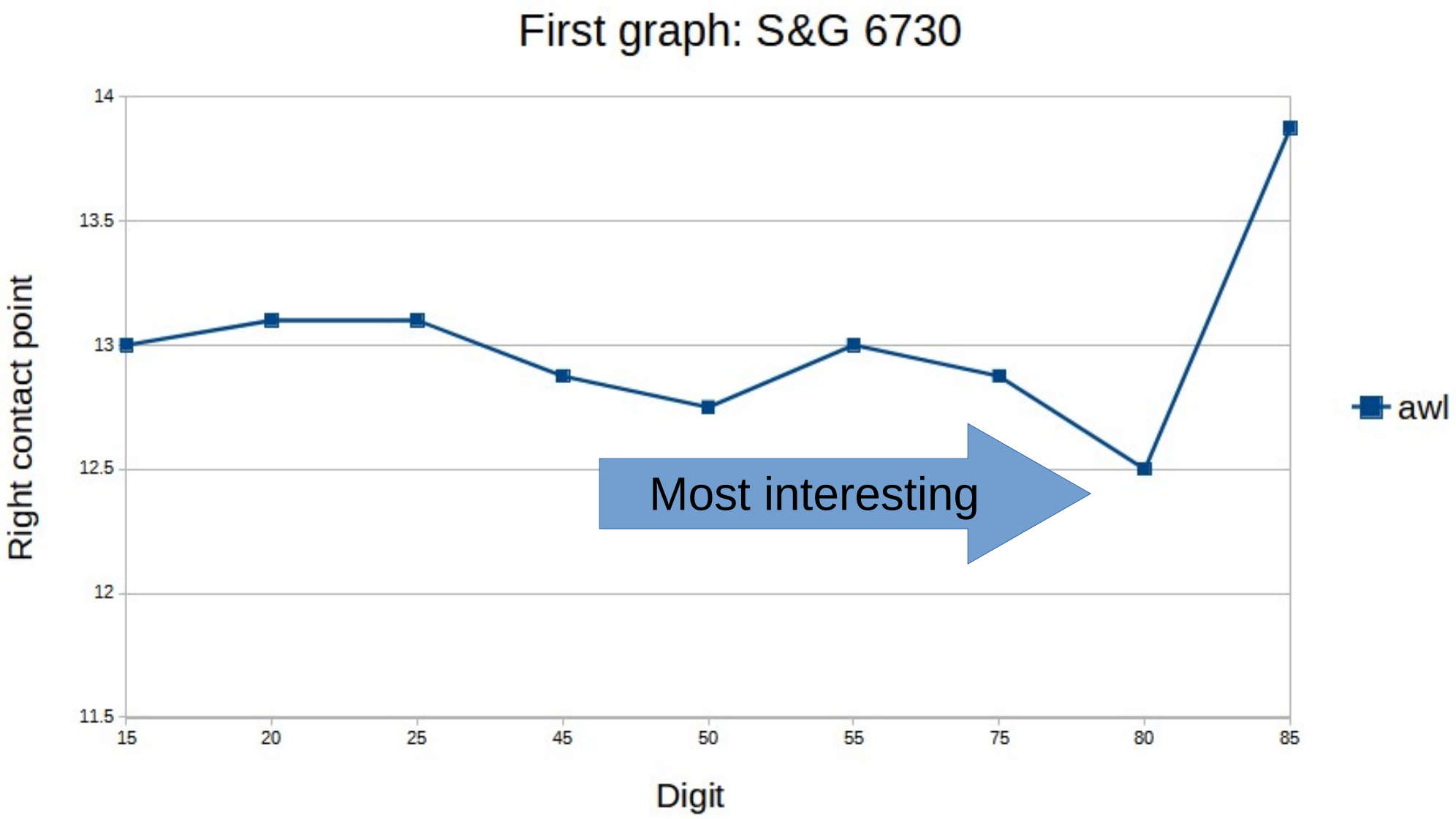
Manipulation process

- All wheels left:
  - Dial four times left and stop at 0
  - Dial back to 15 and note the contact point
  - Dial left to 2.5
  - Dial back to 15 and take a reading
  - Incrementing the number by 2.5, again
  - Take a reading
  - Repeat until back to the beginning

Manipulation process



Manipulation process



Manipulation process

- We need to test which wheel is the lowest point is
  - We dial:
    - 80L 80L 70R and take a reading
    - 70R 80L 80L and take a reading
    - 80L 70R 80L and take a reading

Manipulation process

- We need to test which wheel is the lowest point is
  - We dial:
    - 80L 80L 70R
      - 4 Left to 80, 2 Right to 70, R to 15
    - 70R 80L 80L
      - 4 Right to 70, 3 Light to 70, R to 15
    - 80L 70R 80L
      - 4L 80, 3R 70, 2L 80, R to 15

Manipulation process

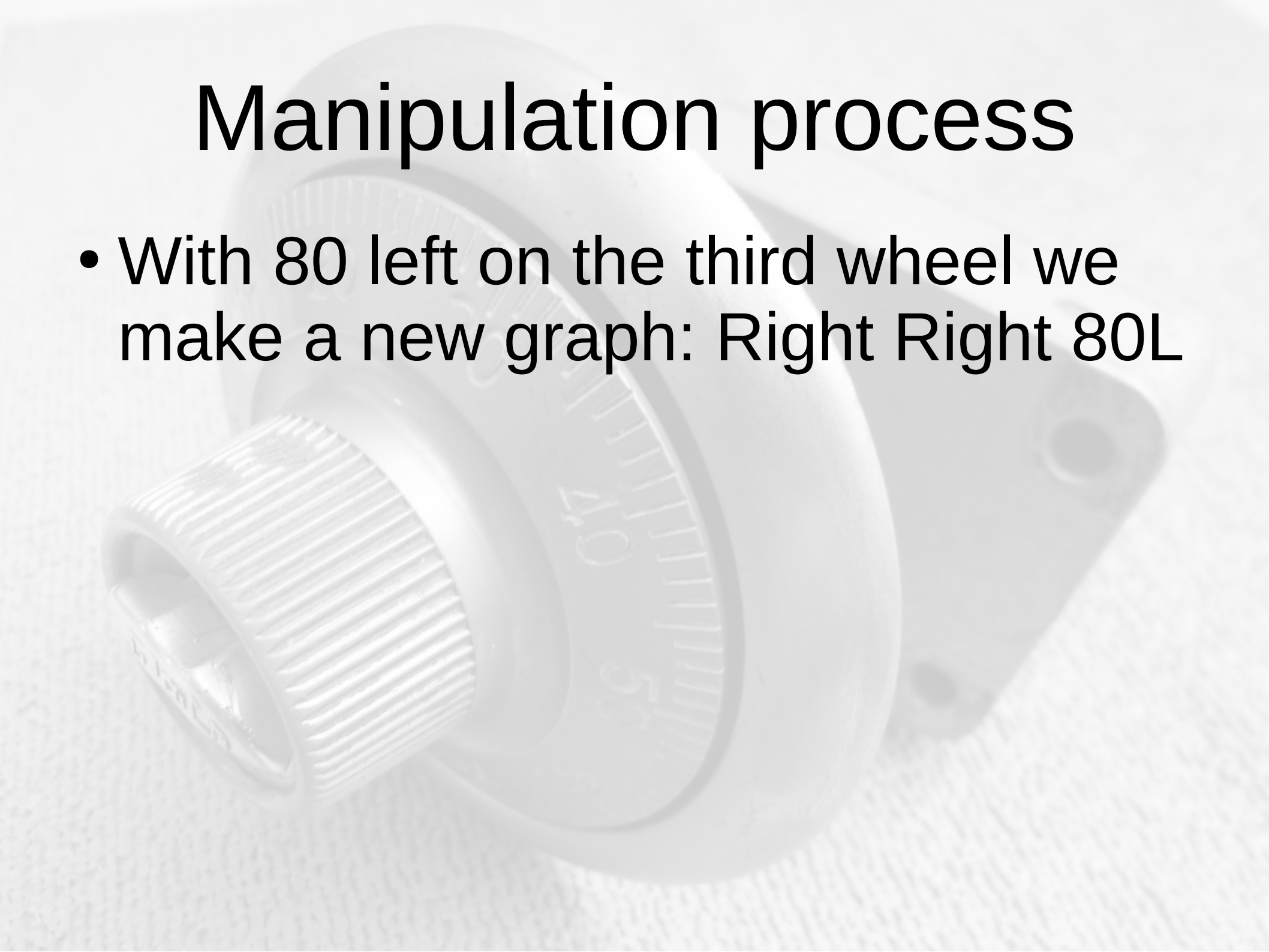
- We need to test which wheel is the lowest point is
  - We dial:
    - 80L 80L 70R 13
    - 70R 80L 80L 12.5
    - 80L 70R 80L 12.5

Manipulation process

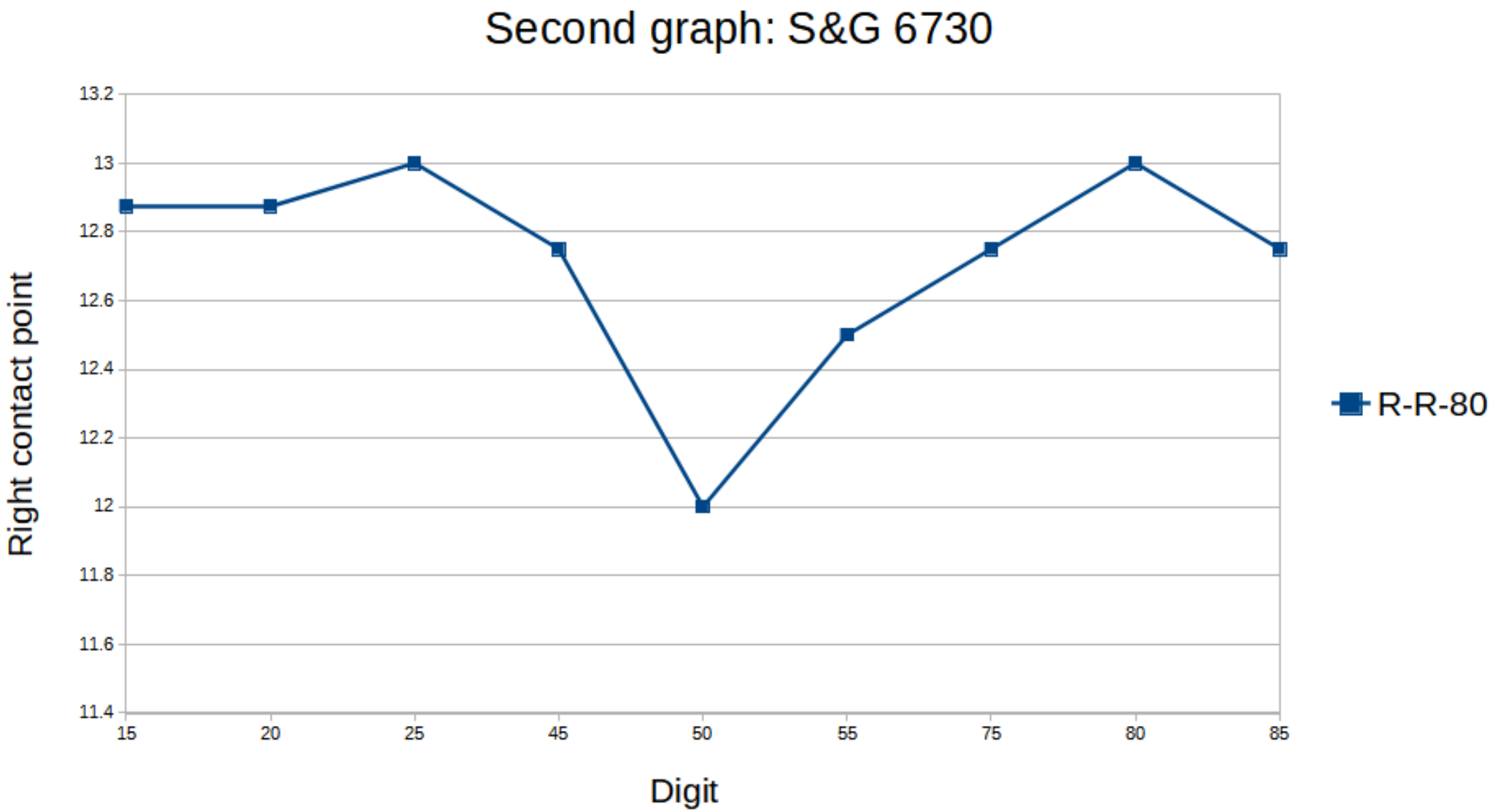
- We need to test which wheel is the lowest point is
  - We dial: (note the dialing direction)
    - 80L 80L 70R 13
    - 70R 80L 80L 12.5
    - 80L 70R 80L 12.5
  - 80L on the last wheel is our new lower bound

Manipulation process

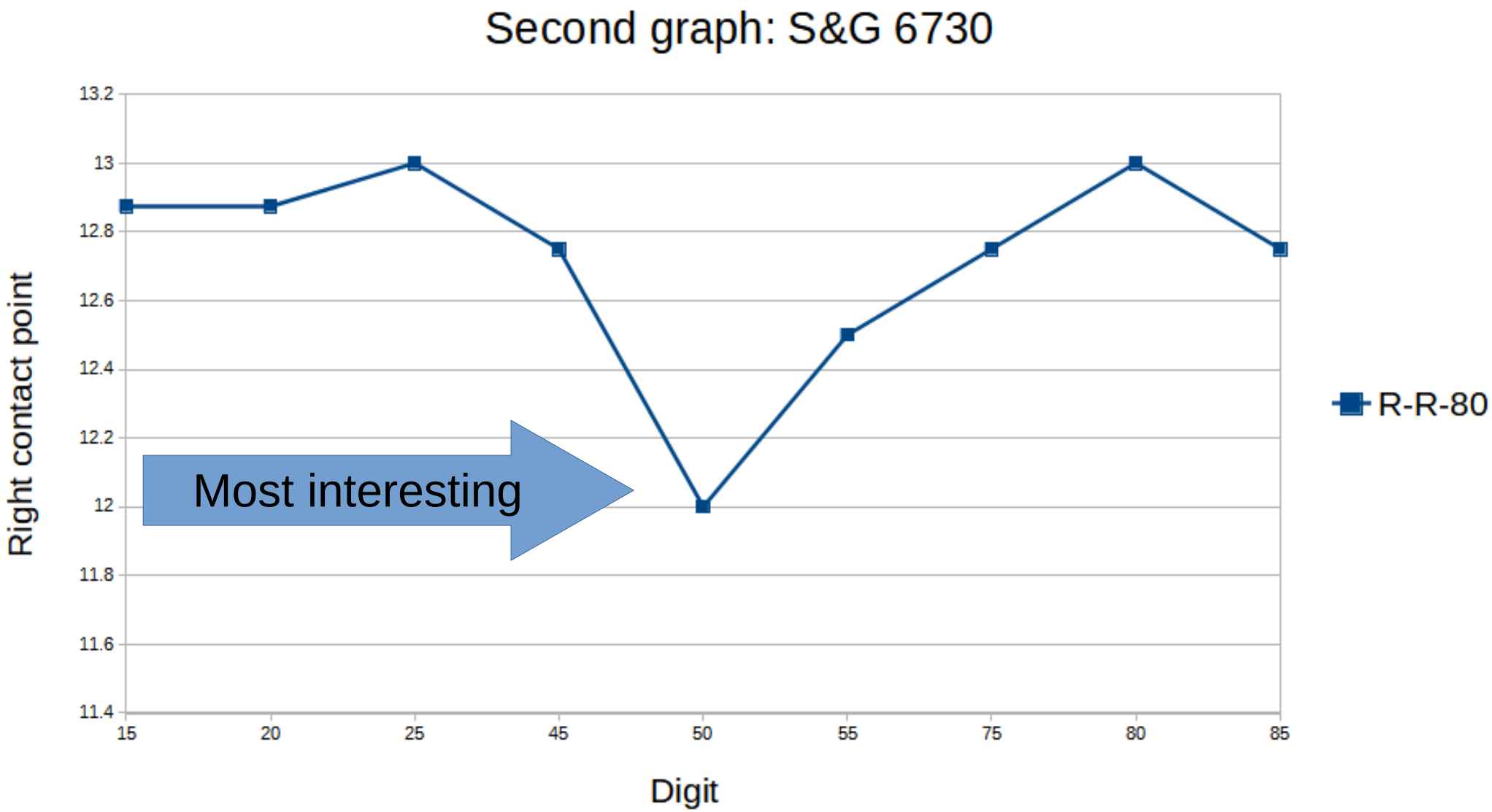
- With 80 left on the third wheel we make a new graph: Right Right 80L



Manipulation process



Manipulation process



Manipulation process

- We need to test which wheel is the lowest point is
  - We dial:
    - 50L 40R 80L 13
    - 40L 50R 80L 12

Manipulation process

- We need to test which wheel is the lowest point is
  - We dial:
    - 50L 40R 80L 13
    - 40L 50R 80L 12
  - Low point is on ?L 50R 80L

Manipulation process

- Brute force the last number or make another graph.
- Brute forcing **L 50R 80L** the lock opened at **20**, giving us the solution **20L 50R 80L**.

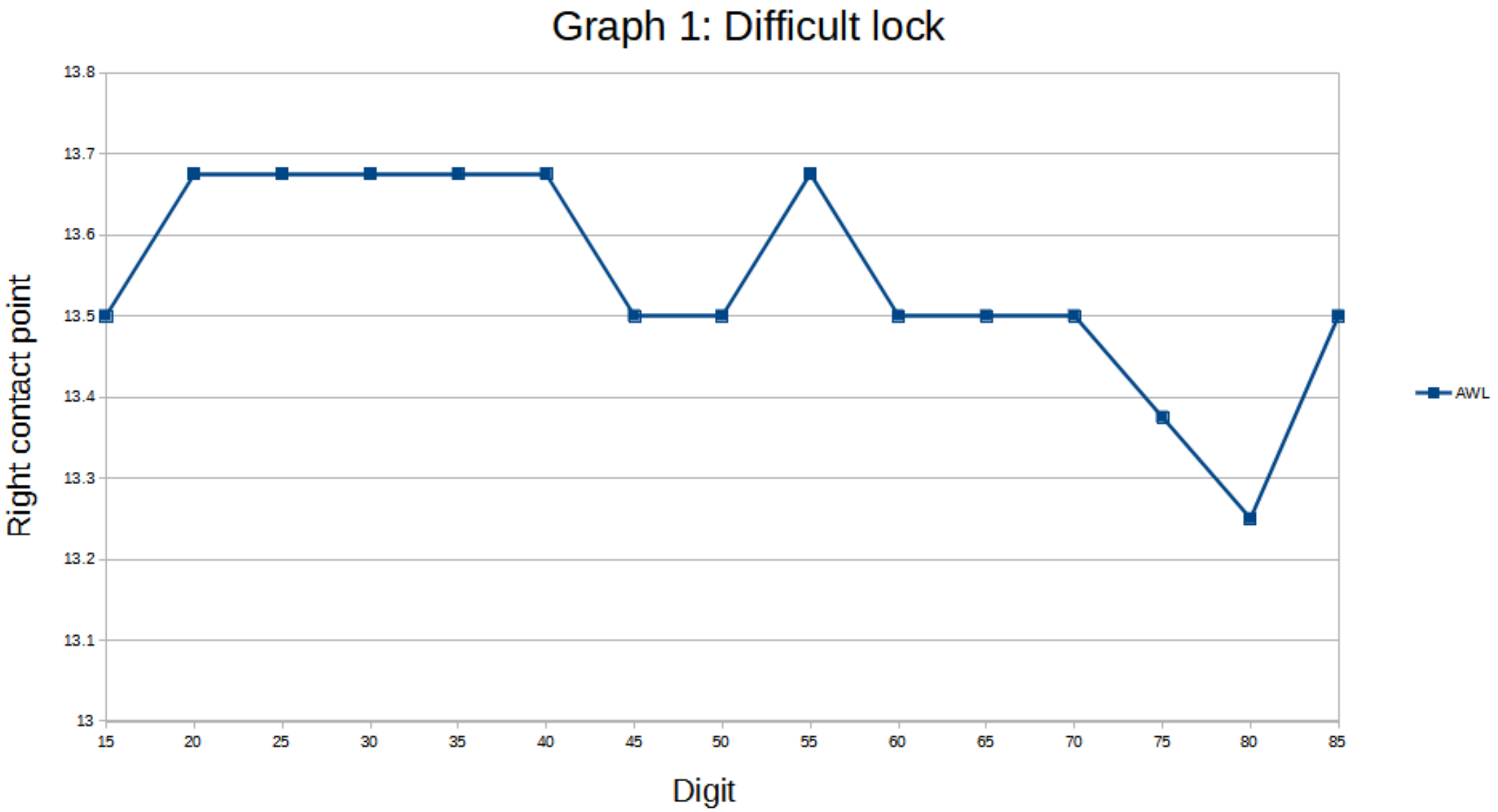
Manipulation process

- Note the dialing rotation
- Check every **2.5** numbers
- Be very precise when dialing/graphing
- The goal is to find a new low reading, this does not have to be a gate.

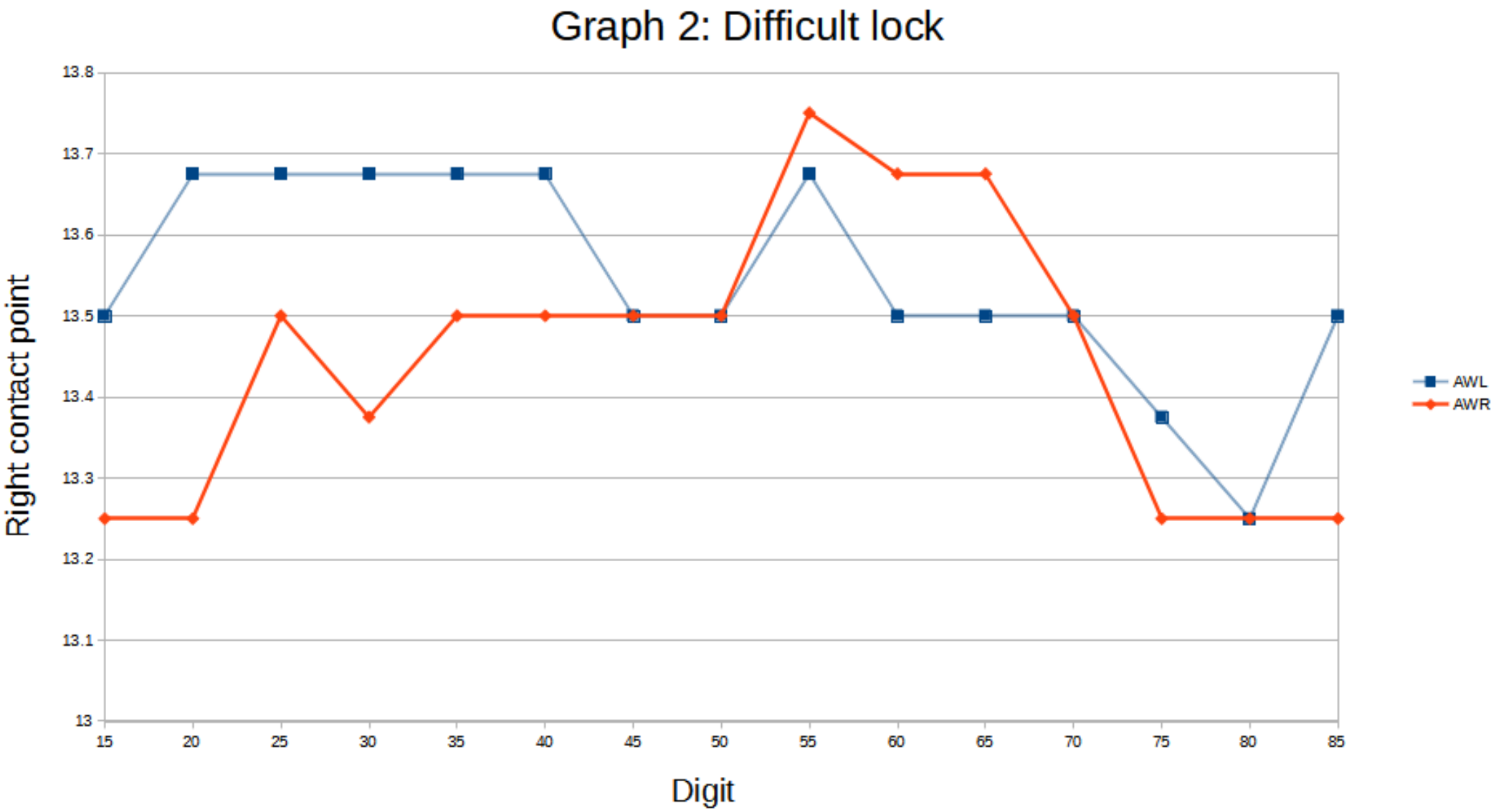
Manipulation process

- Example graph of a harder lock.

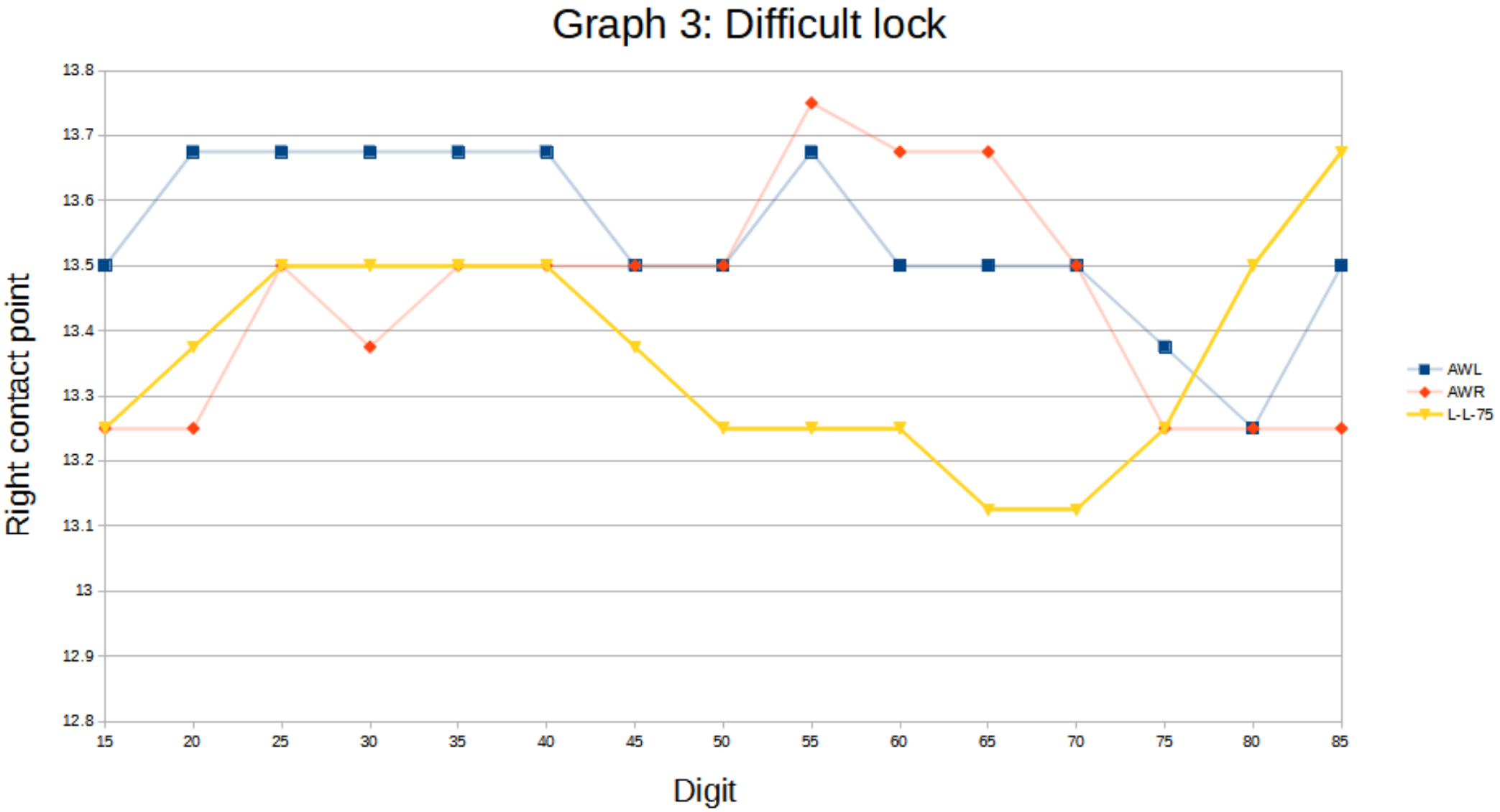
Manipulation process



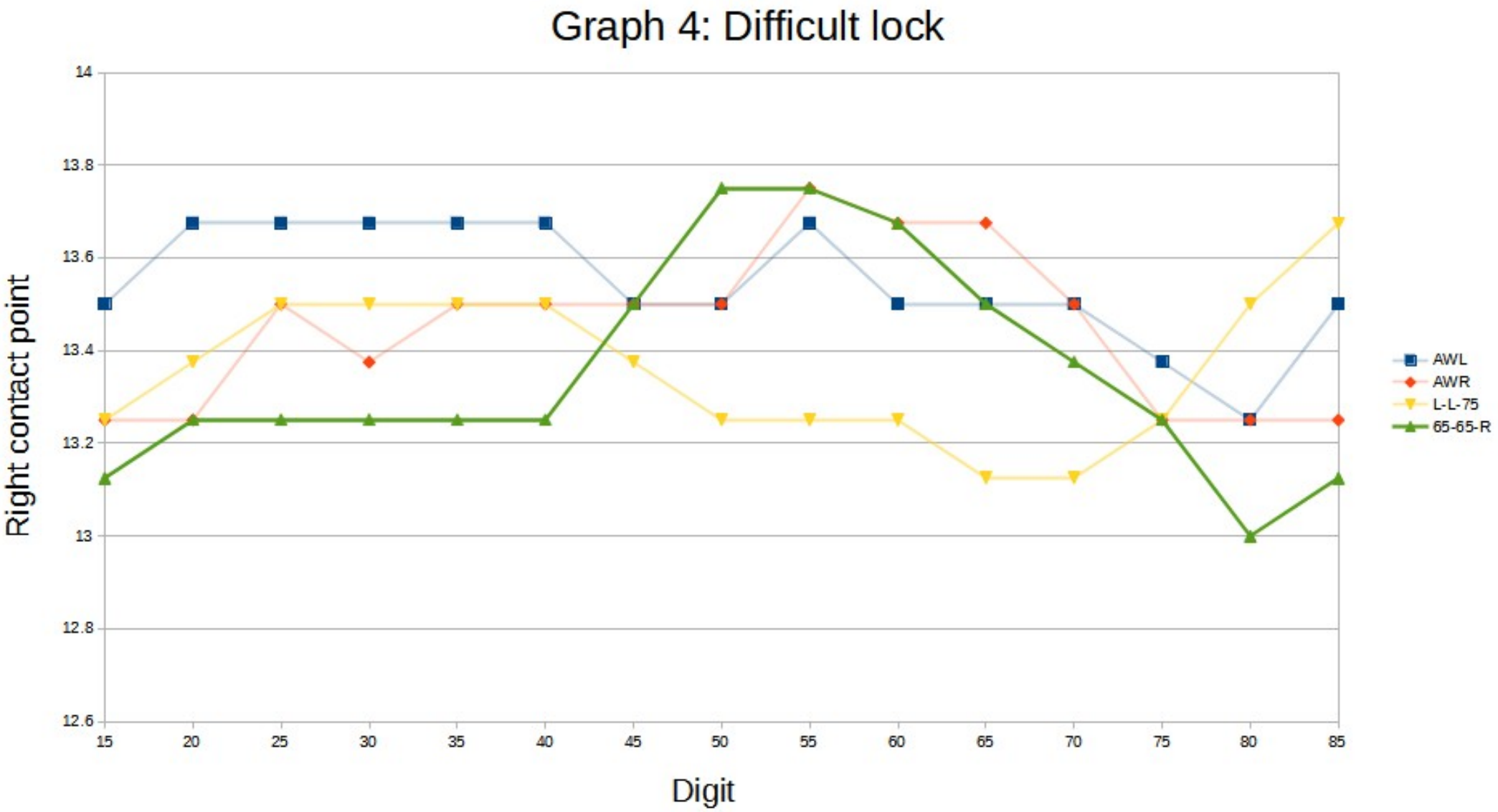
Manipulation process



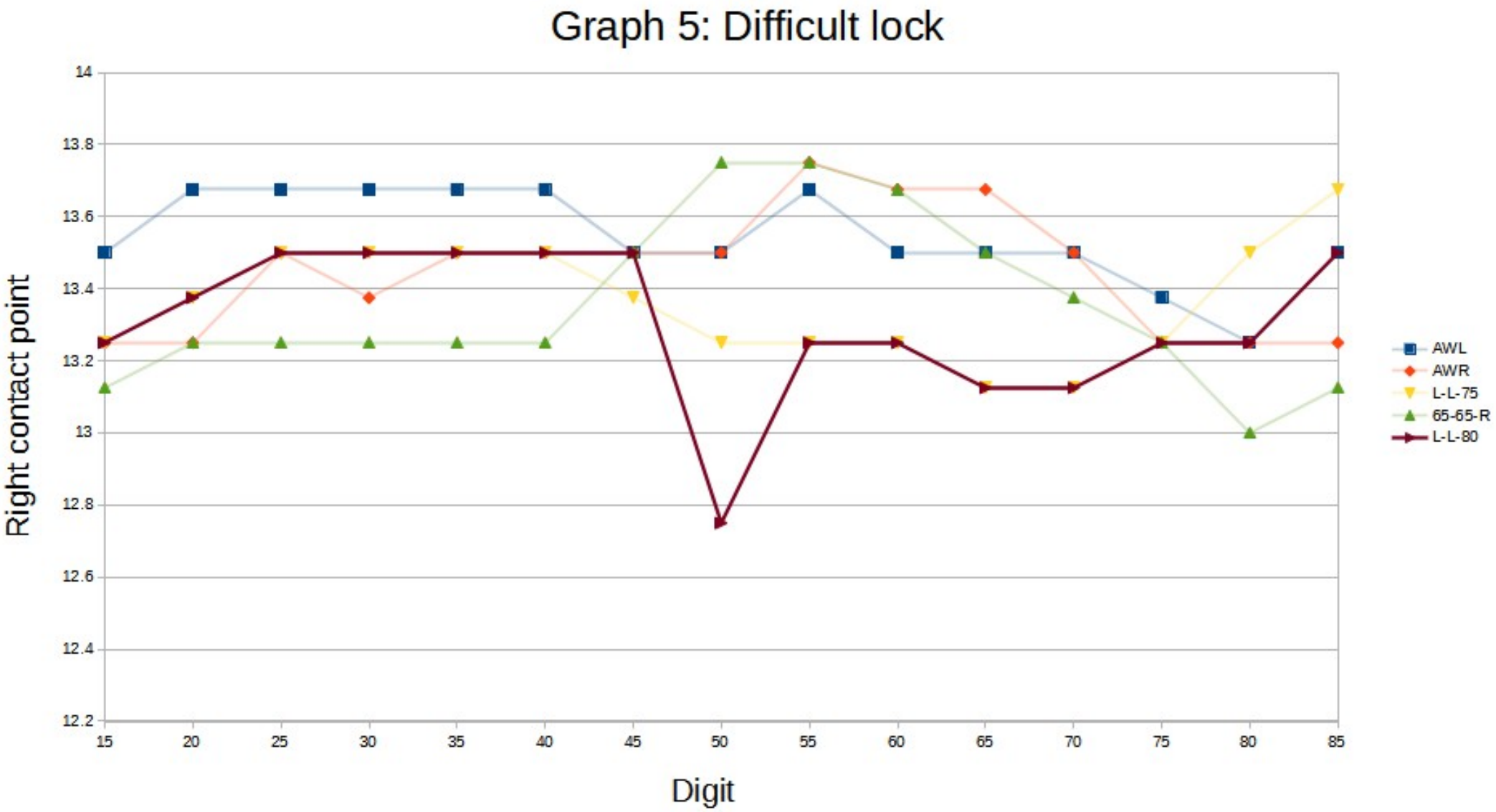
Manipulation process



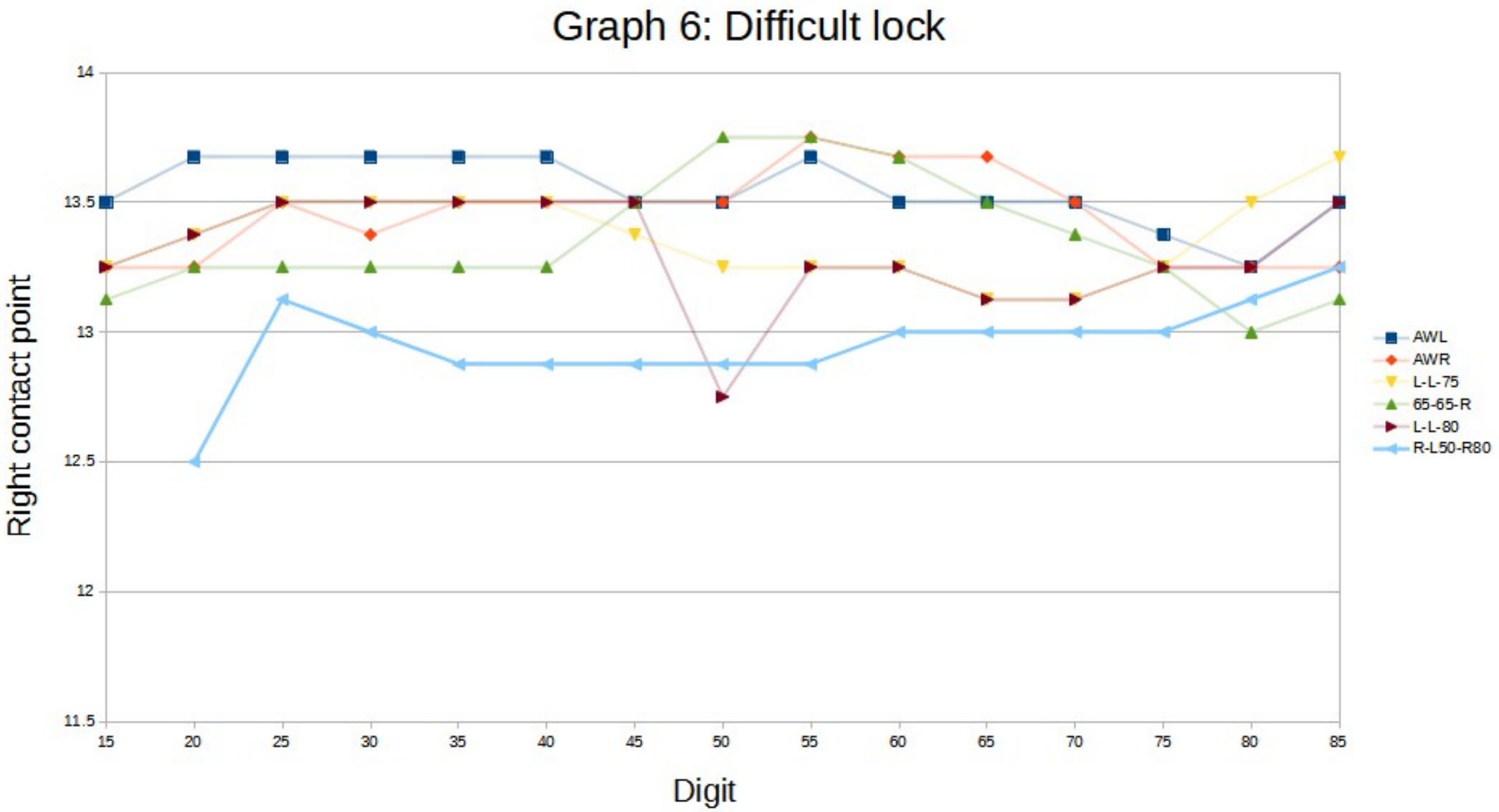
Manipulation process



Manipulation process



Manipulation process



Manipulation process

- This lock took an hour to graph but each graph got us closer to open

Manipulation process

- **Exercise: Max 30min**
  - Use the graph paper to graph AWL between 0 and 100 with 2.5 increments
  - Preform the high-low test
  - Show the trainer.

Manipulation process

- **Exercise: Max ??min**
  - Graph the remaining wheels
  - Preform the high-low test
  - Show the trainer.

Manipulation process

- **Exercise: Max ??min**
  - Graph the remaining wheels
  - Preform the high-low test
  - Show the trainer.
- We can reset the combo for you

Final thoughts

- If you are considering picking up the hobby:
  - **S&G 6730** are usually the easiest locks but the hardest to get
  - The locks sell for around €100
  - A lot of knowledge available online