Madison Gurkha
Your Security is Our Business

Lockpicking 101

Walter Belgers
walter@ehv.toool.nl

About me

- Walter Belgers
- Partner, Principal Security Consultant at Madison Gurkha (Netherlands)

- 10+ years lockpicking experience
- Founder of the Eindhoven chapter of TOOOL, The Open Organisation of Lockpickers

Outline

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

LOCKS!

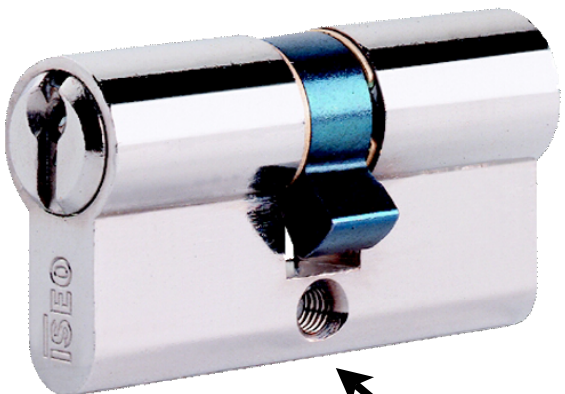
Opening a lock

- Normal entry
  - Using the key and/or codes
- Forced entry
  - Using destructive techniques
- Covert/surreptitious entry
  - Not leaving obvious traces

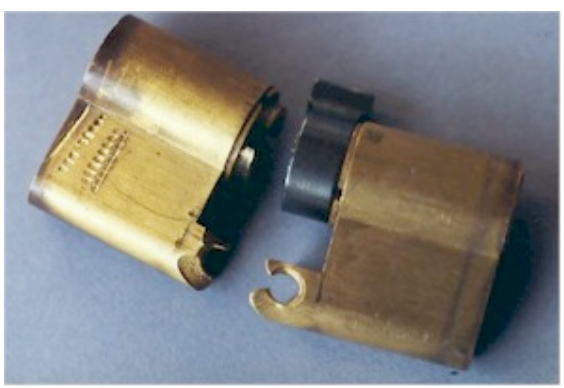
Forced entry

- Attacking not the locking mechanism itself

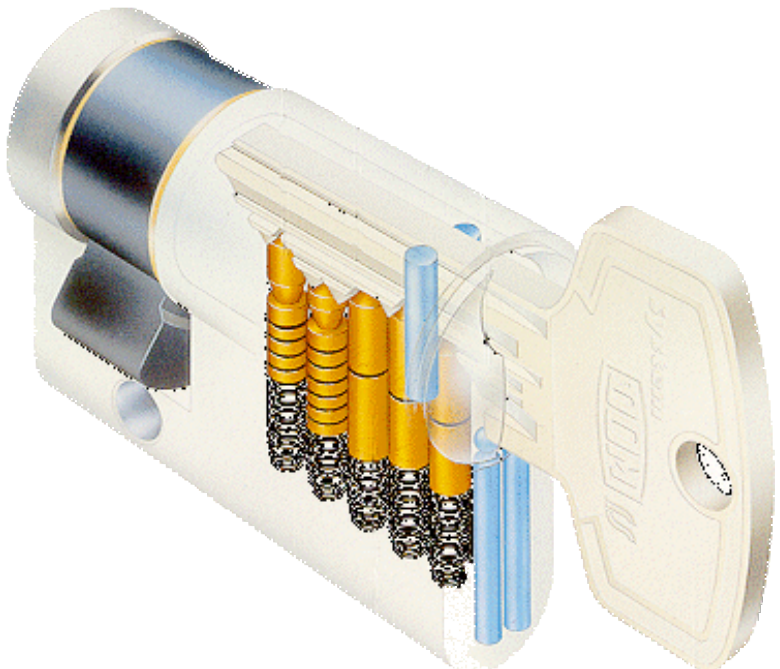
Forced entry

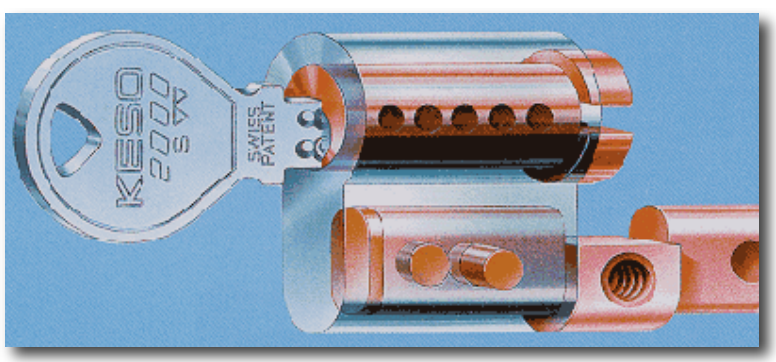


weak spot



Forced entry, protection





Covert/surreptitious entry

- Opening a lock without using the key/ knowing the correct code
- Without breaking the lock
- Without leaving (obvious) traces behind
  - Traces may be found upon close examination

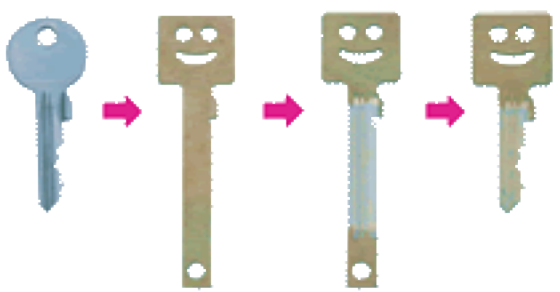
Lockpicking

"The sport of opening locks covertly, with permission of the owner."

TOOOL
The Open Organisation Of Lockpickers

Copying the key

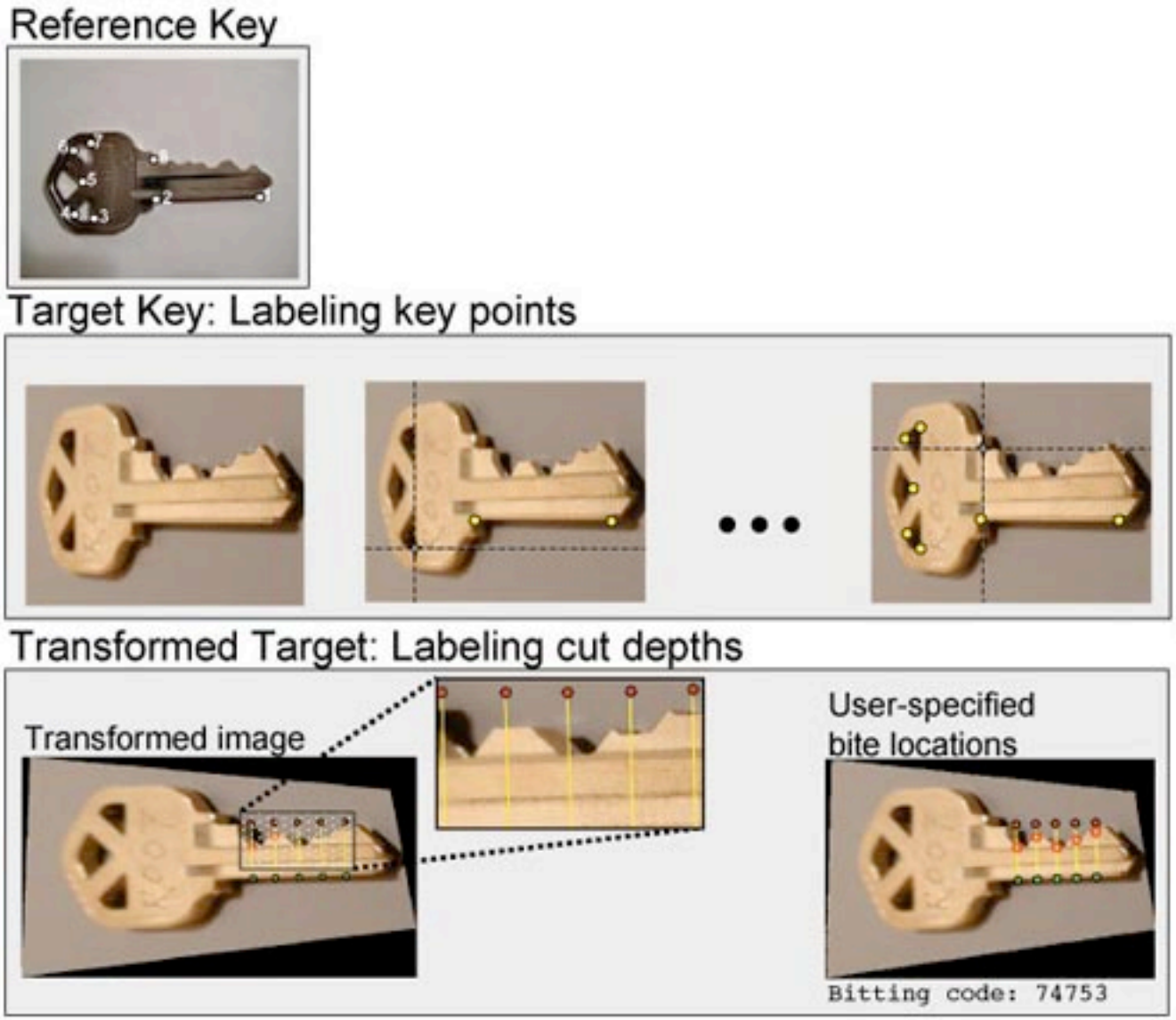
- Of course, if you have the key, you can copy it



Copying the key

Copying the key

Copying the key



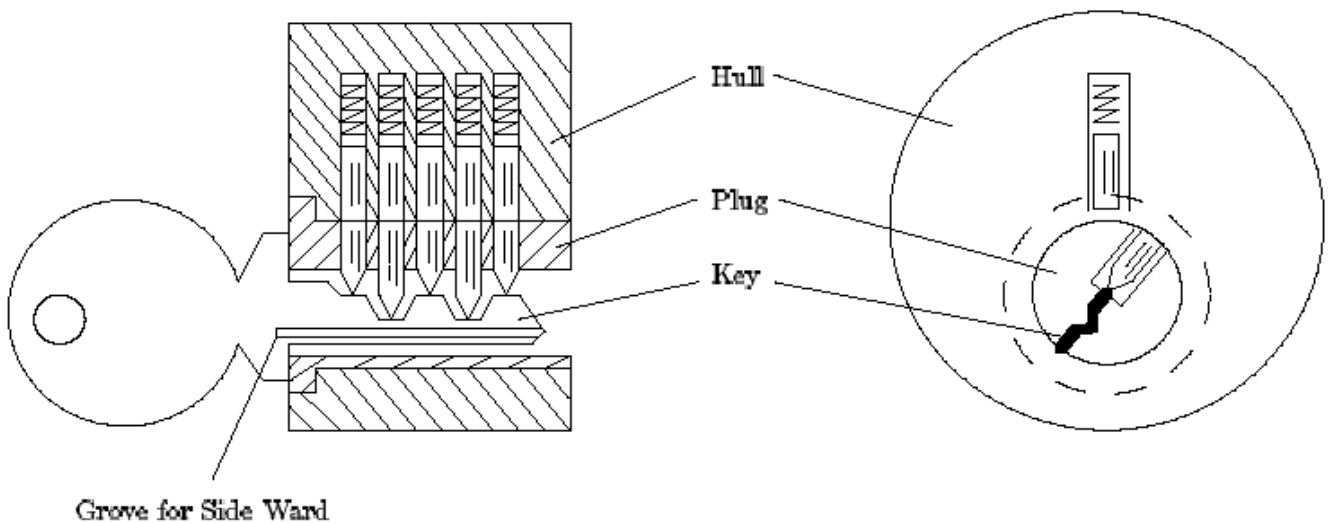
http://vision.ucsd.edu/~blaxton/sneakey.html

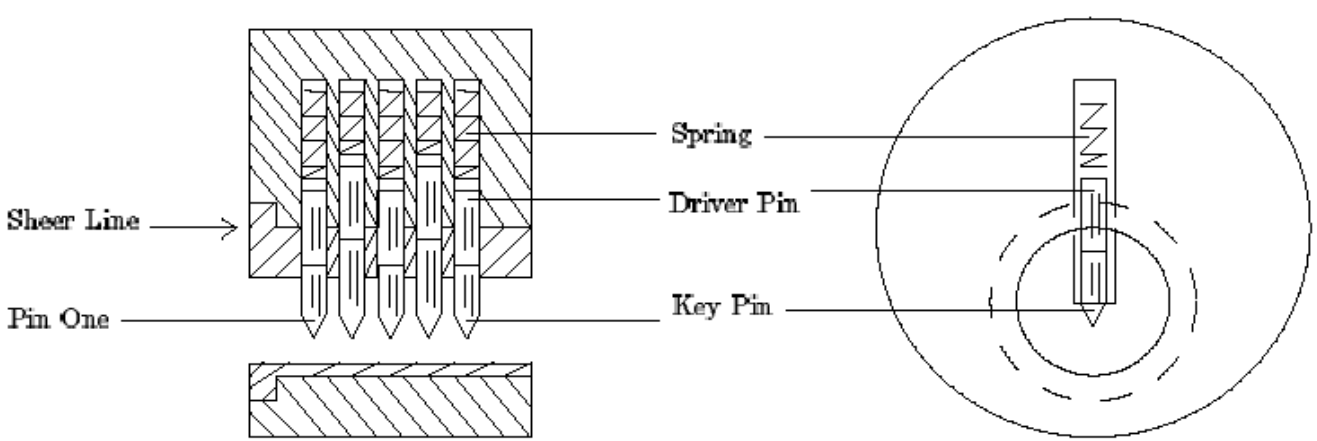
Lockpicking

- Understand how a lock works
- Think of ways to circumvent security

- This is actually "hacking"
- Circumventing security by thinking out of the box

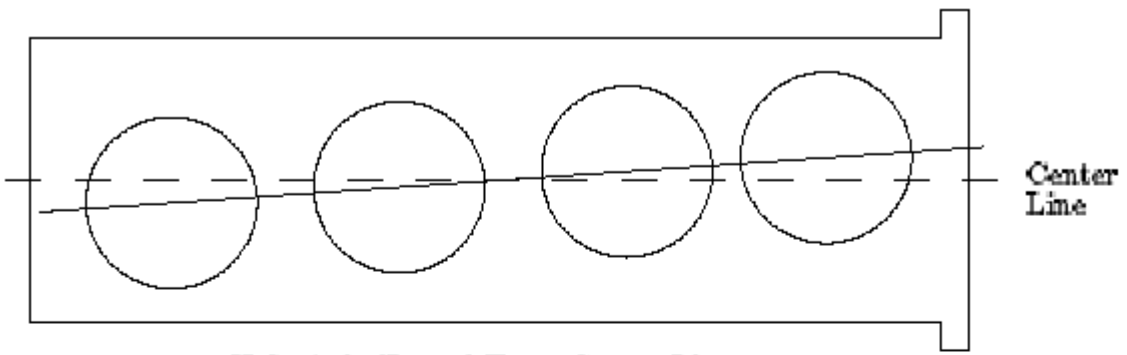
Standard cylinder



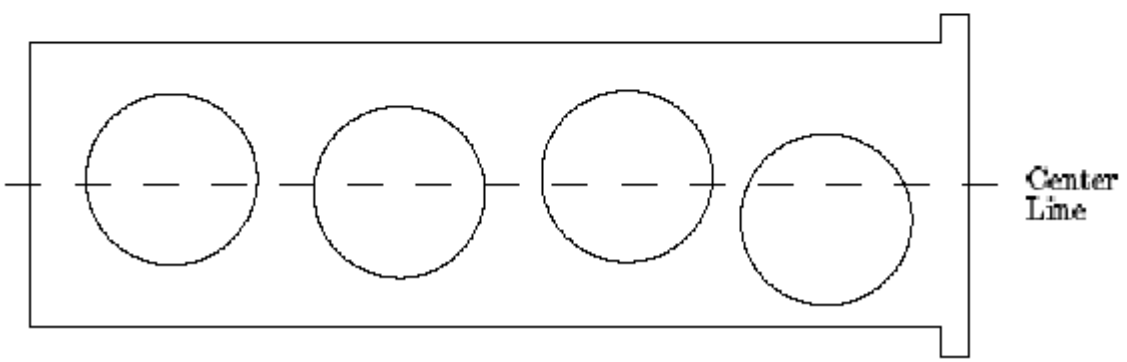


Alignment of plug holes

- Misalignment of plug holes makes it possible to open a lock by lifting the pins one at a time
- Applying shear force will hold pins in position
- Mechanical/economical limitation



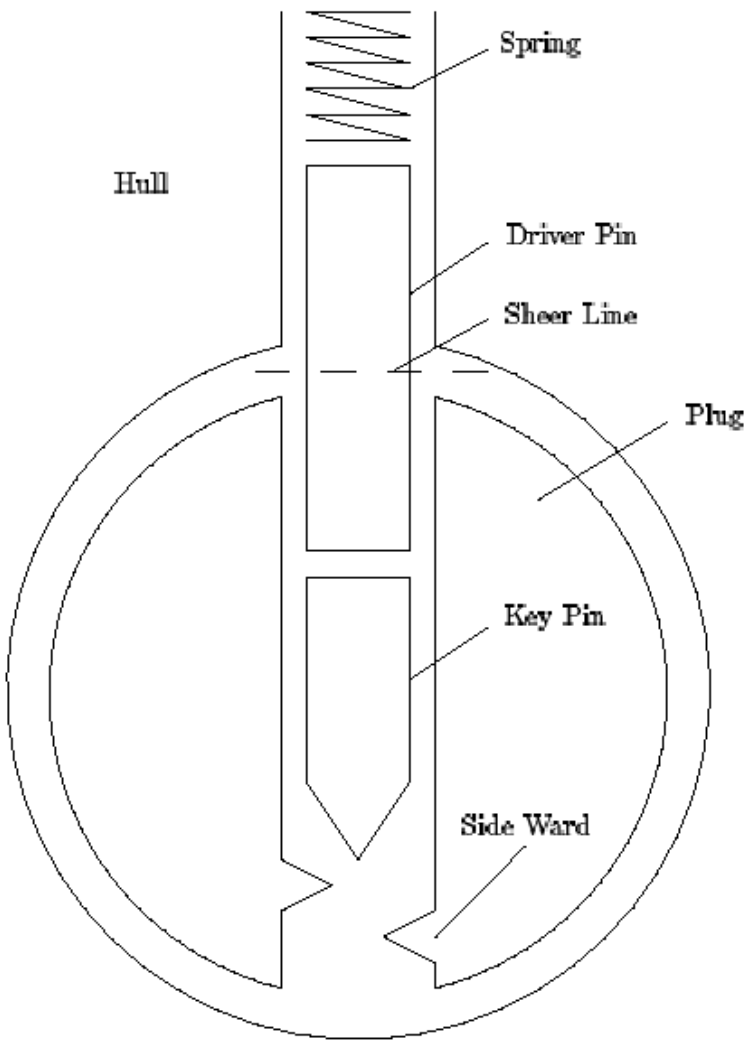
Hole Axis Skewed From Center Line



Random Hole Alignment

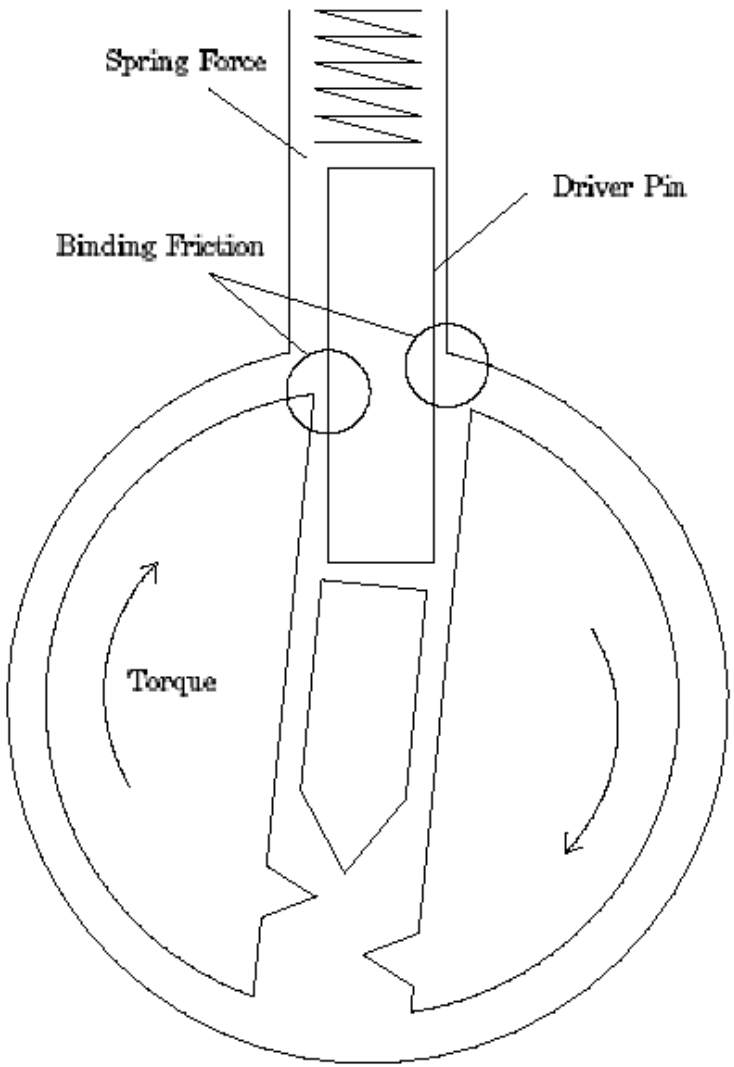
Pin column model

- Frontal view of one pin column in the standard cylinder
- Only the key pin and the plug can be easily manipulated from the outside

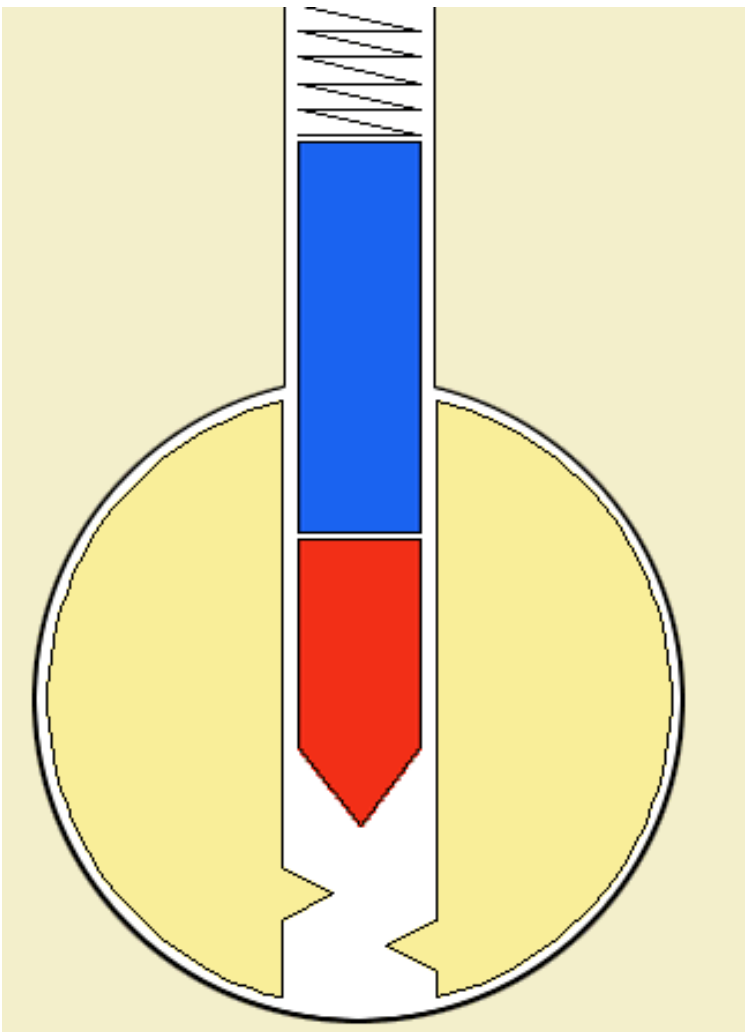


Binding

- Torque is applied using the tension wrench
- Binding friction at the shear line:
  - Keeps the plug from turning
  - Provides feedback on which pin is blocking the plug
  - Can be used to hold a pin in place

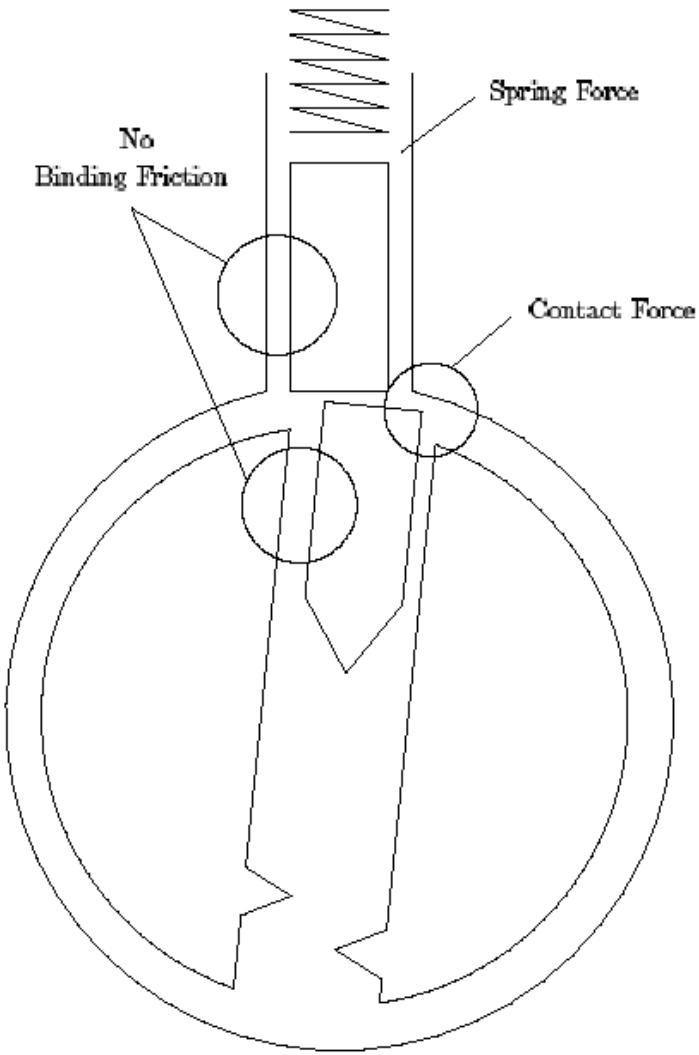


Binding

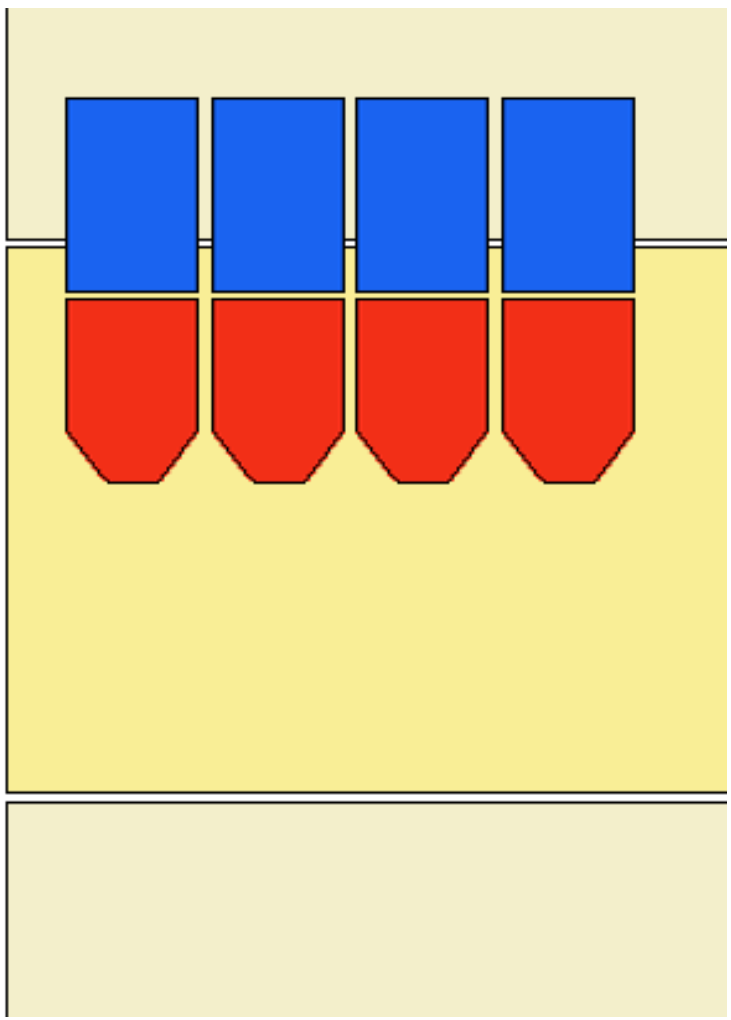


Pins at the sheer line

- Once the holding driver pin enters the hull, the plug can be turned (slightly) due to the alignment defect mentioned before
- Now the search is on for the next pin keeping the plug from turning



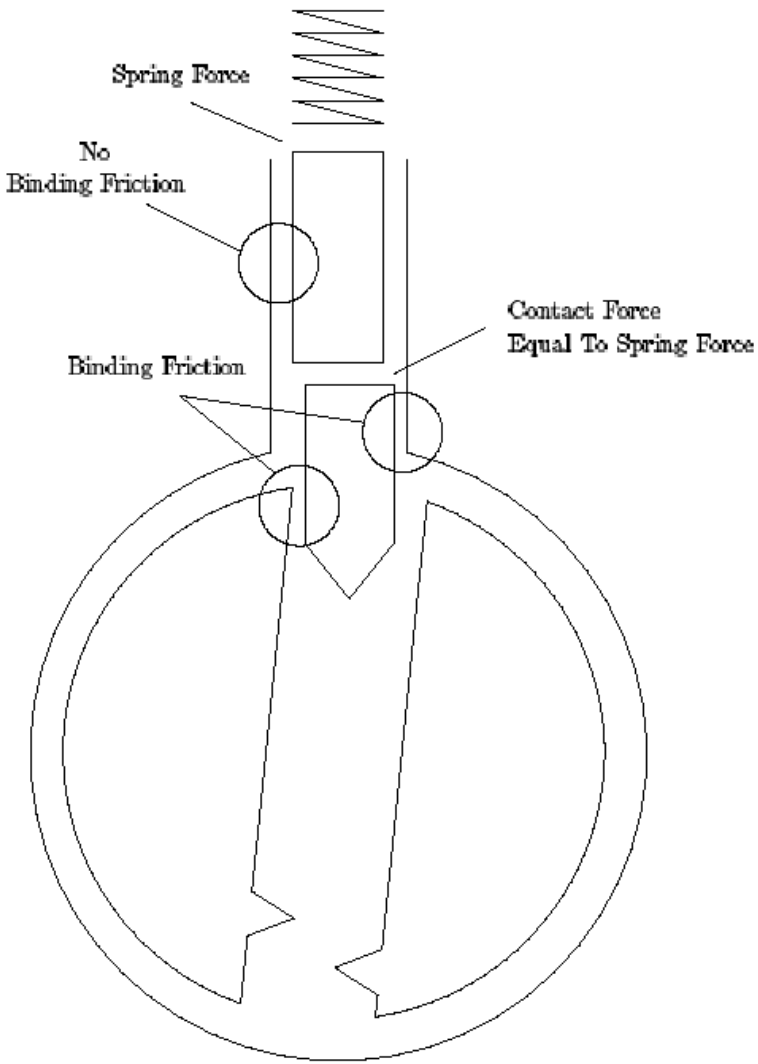
Binding



Tools used

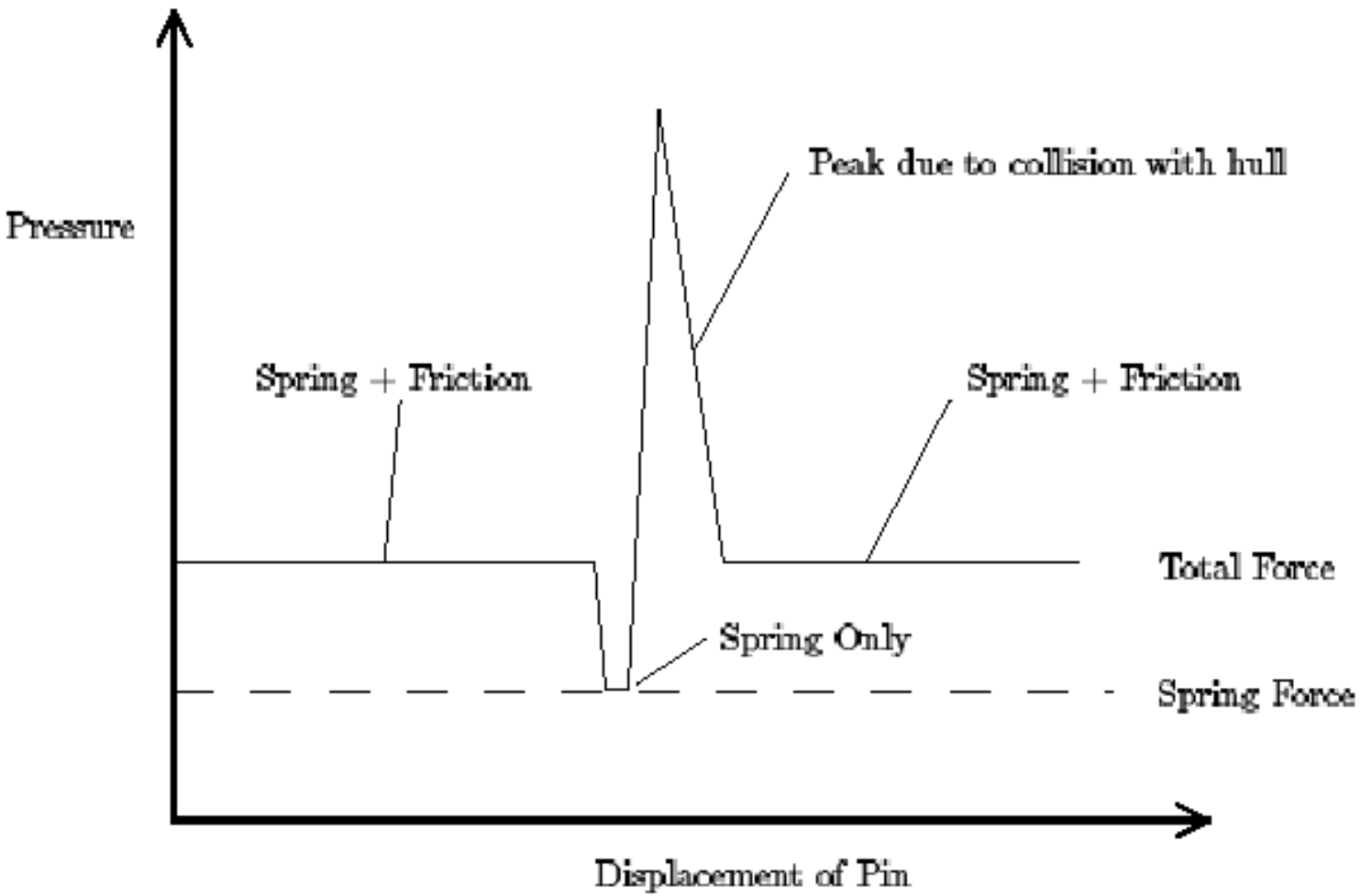
Key pin enters hull

- Here, the key pin is holding the plug from turning
- Some locks allow both driver and key pins to enter the hull, this will also allow the plug to turn
(combing a lock)



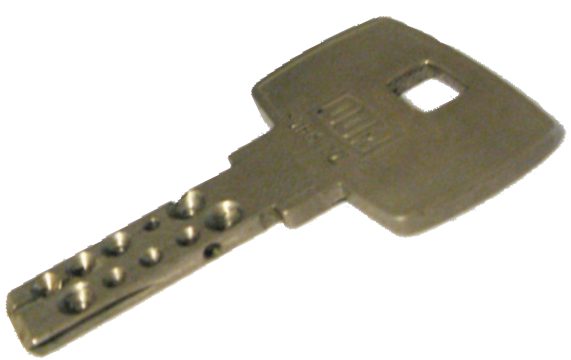
Combing

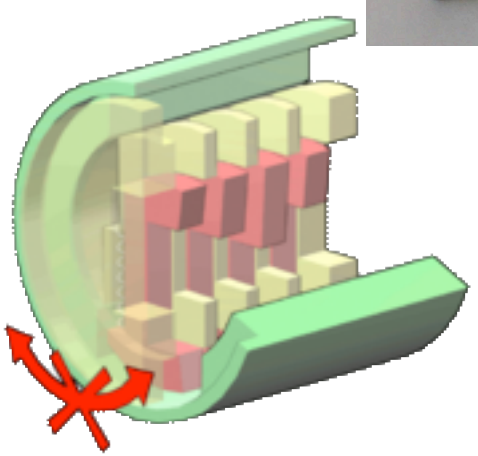
Pressure graph

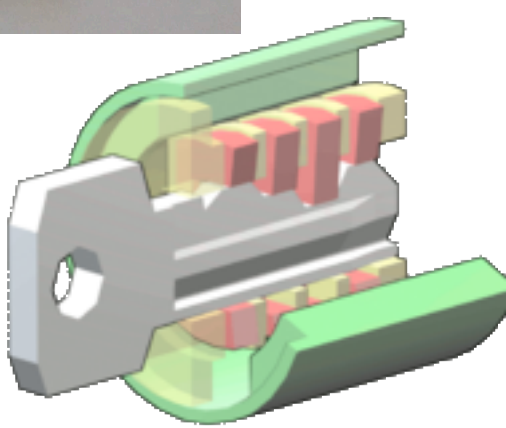


Lockpicking

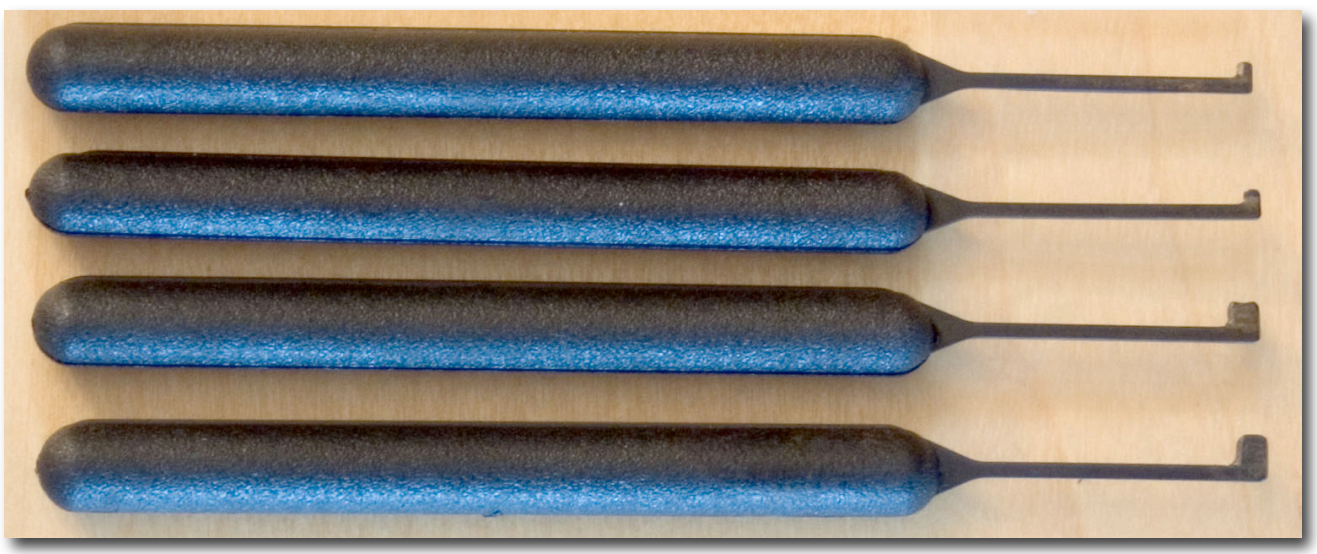
- This technique works with:
  - Pin-tumbler locks (including padlocks)
  - Wafer tumbler locks
  - Dimple locks
  - Tubular locks







Dimple locks



Raking: a shortcut

- Using a technique called raking, we can try to set more than one pin at the same time
- With cheap locks, raking is all that is needed to open them
- With better locks, raking can still be useful
  - Rake 2, 3, 4 pins
  - Set the last one(s) using standard picking techniques

Raking tools

Padlock shortcuts

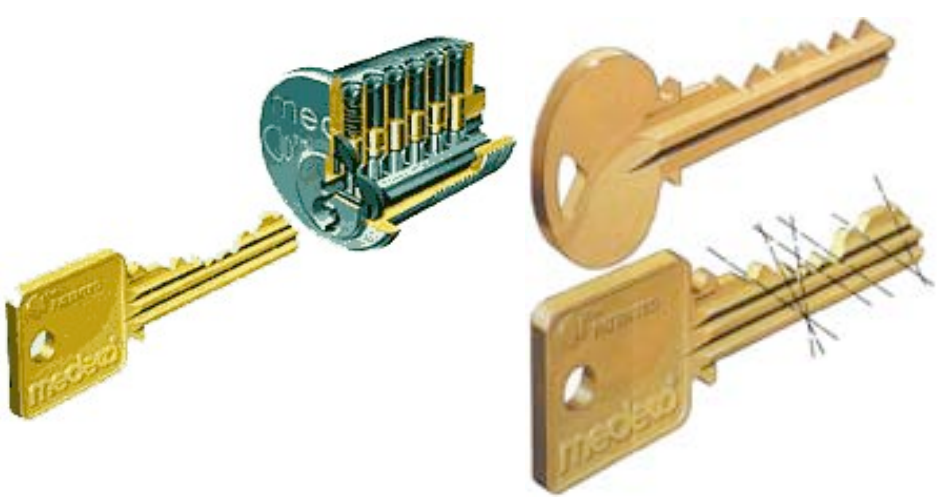
- Padlock shims: unlock the shackle without opening the lock
- On older locks: operate the shackle locking mechanism with a pick tool

Countermeasures

- Drilling and pulling:
  - Harder materials
  - Special pins
- Key duplication:
  - Certificates
  - Specially formed keys
  - Patents

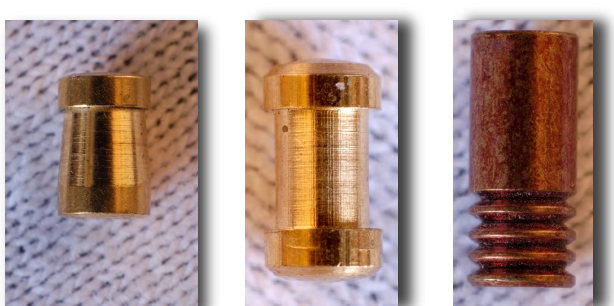
Countermeasures

- Picking:
  - Mushroom pins
  - Awkward keyways
  - New designs/technologies



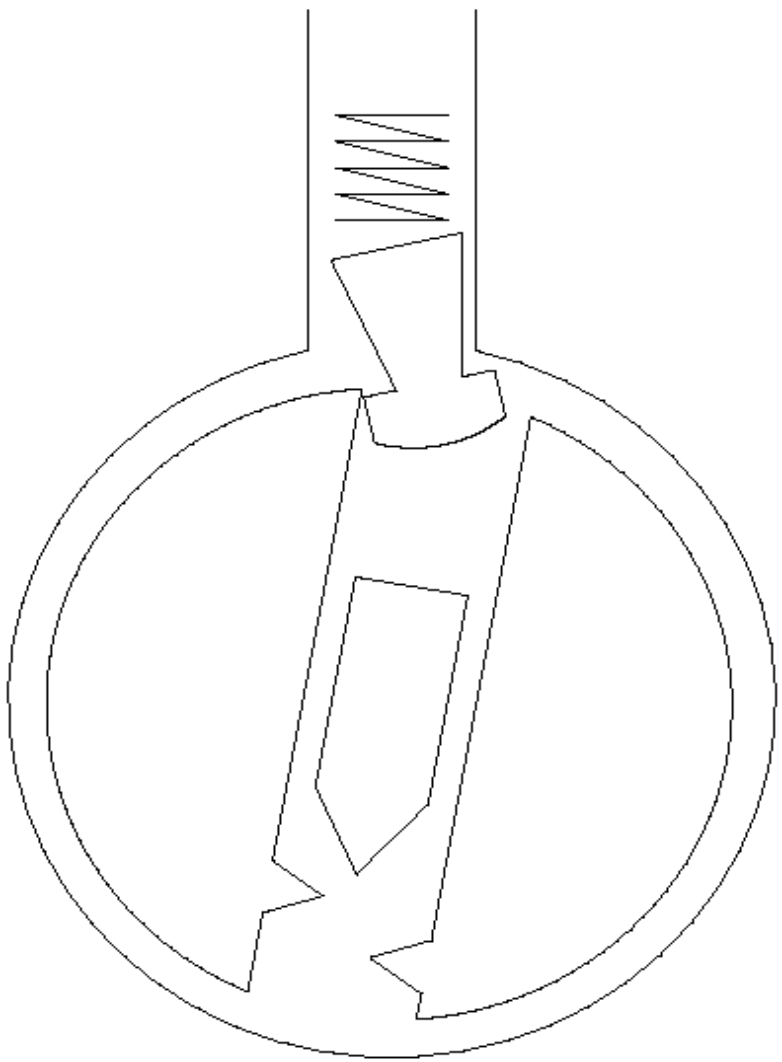
Mushroom pins

- Makes it harder (not impossible) to pick a lock
- The pressure graph no longer holds
- Mostly a few pins, sometimes all pins

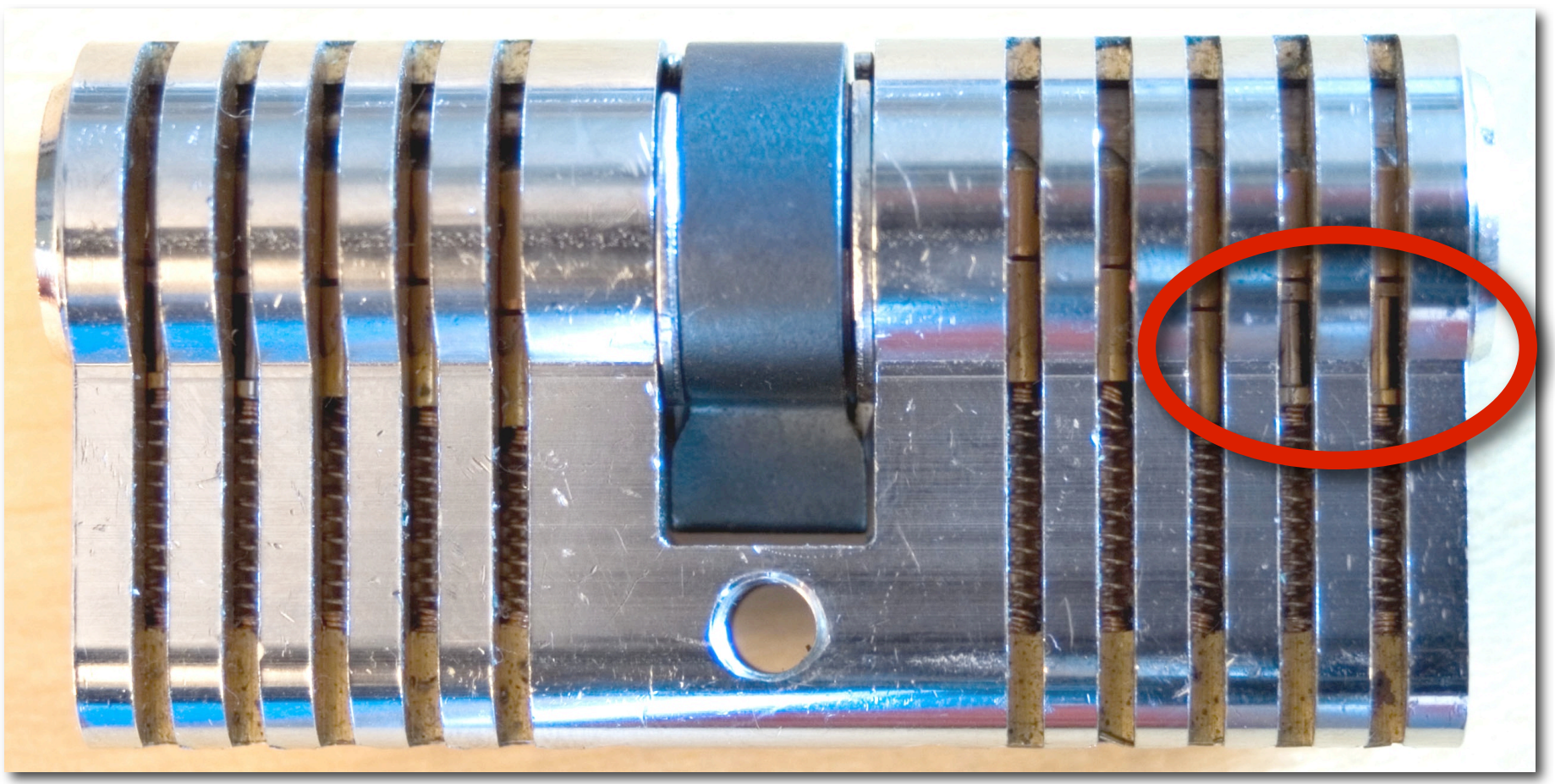


Pictures: Matt Blaze

Mushroom, Spool, Serrated

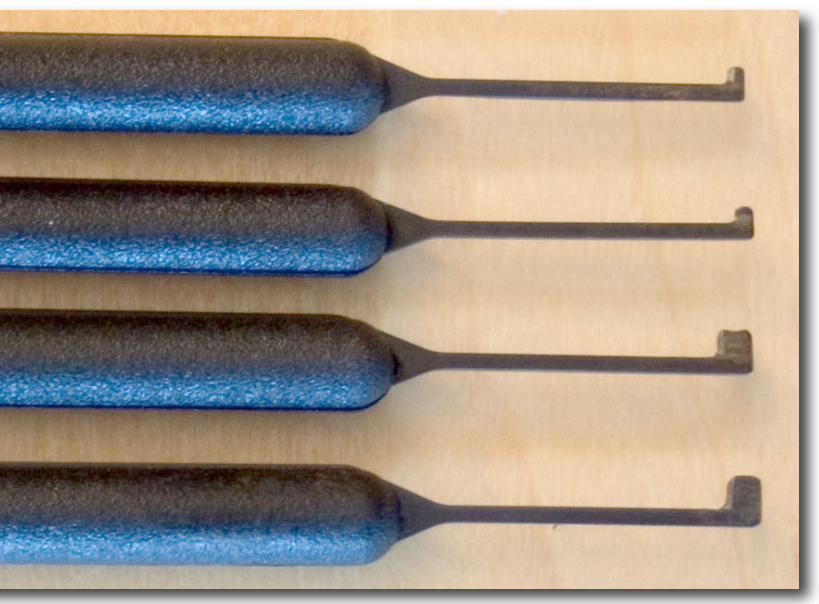


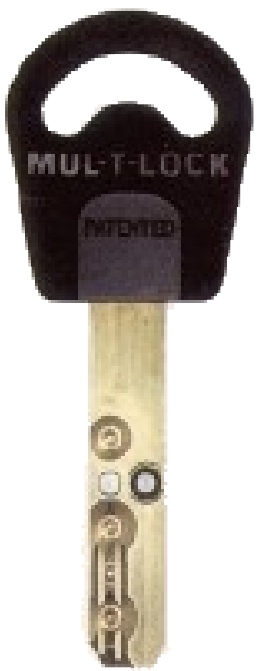
Spool pins

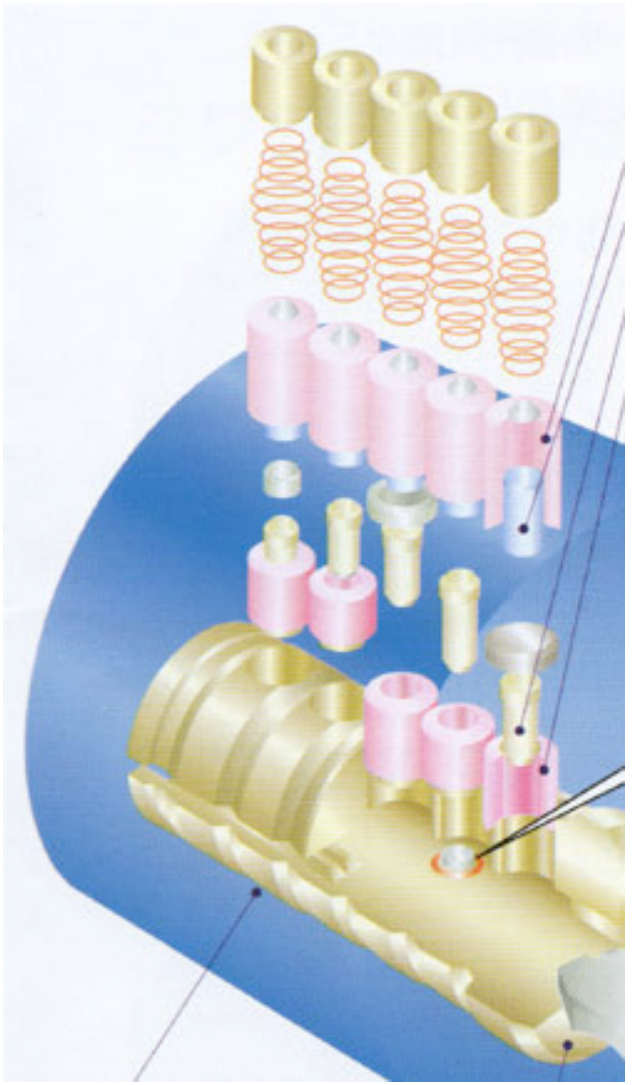


Mul-T-Lock

- Pin-in-pin system
- Only twice as hard

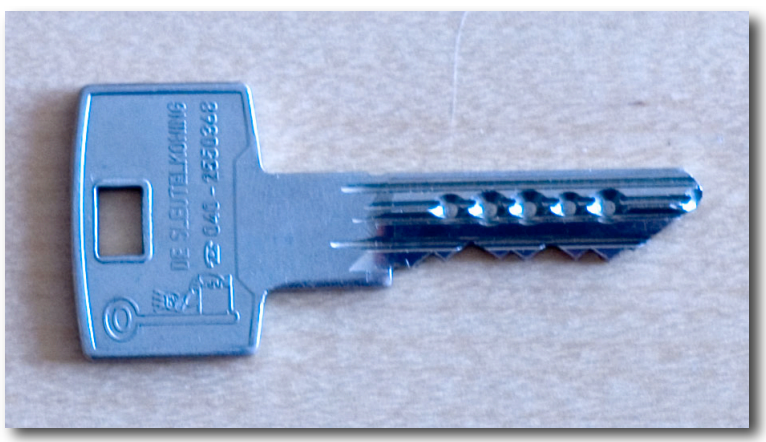




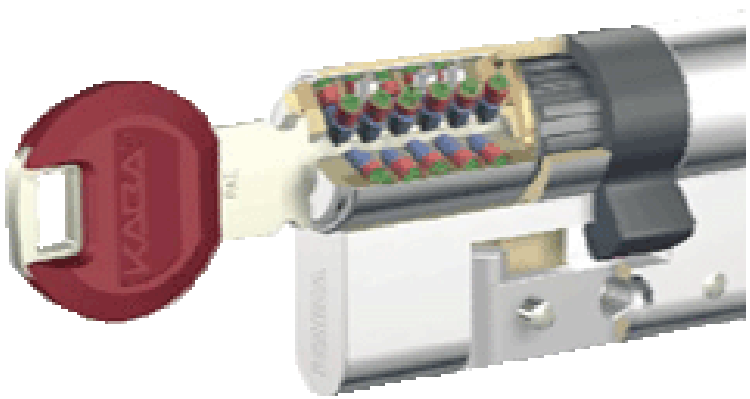


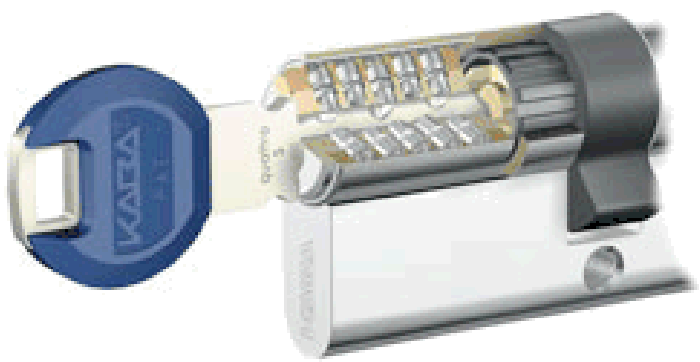
ABUS/Pfaffenhein

- Multiple rows of pins
- Second row on the side
- Awkward keyway



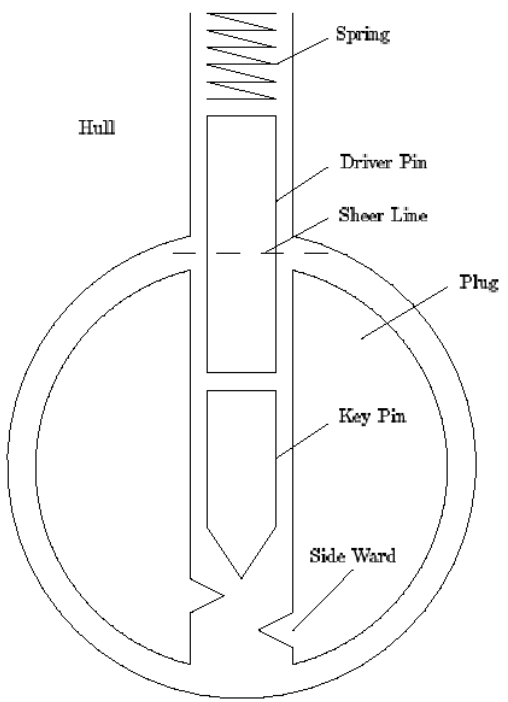
Kaba Gemini/Quattro/ Penta





Pick gun

- Different technique
- Transfer the energy like with billiard balls



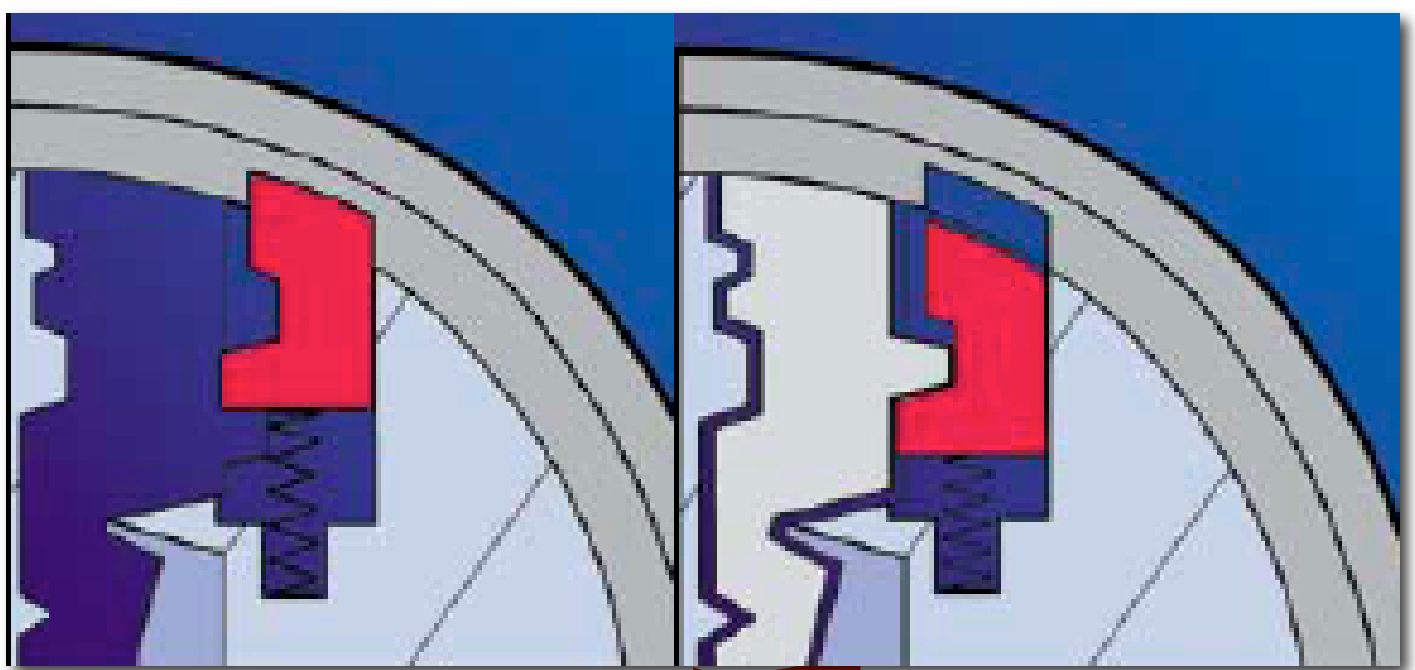
Pick gun

Bumping

- Pick gun on steroids
- Use a key as “pick gun”, so awkward keyways are no problem (also works on dimple locks)

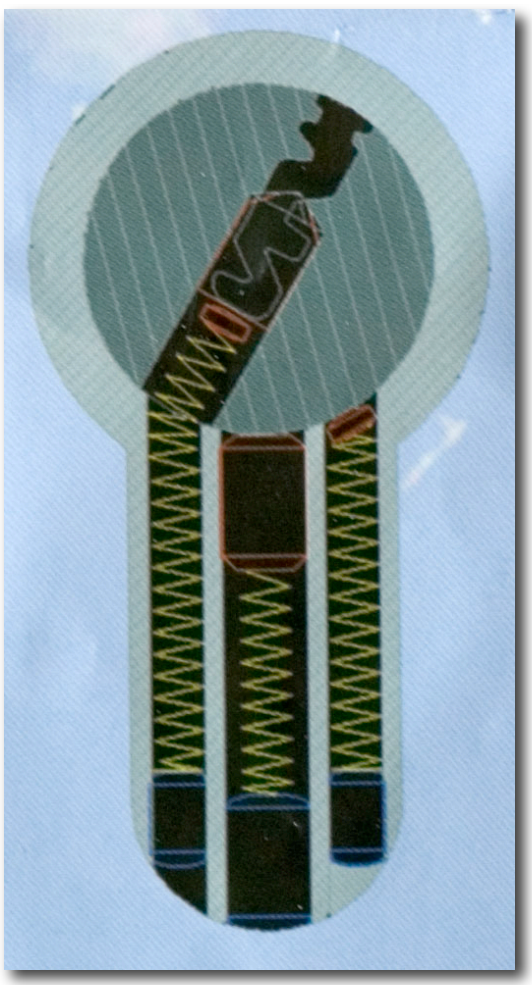
Defeating pick guns

- Defeating pick guns
  - Awkward keyways (no use against bumping)
  - New designs/technologies

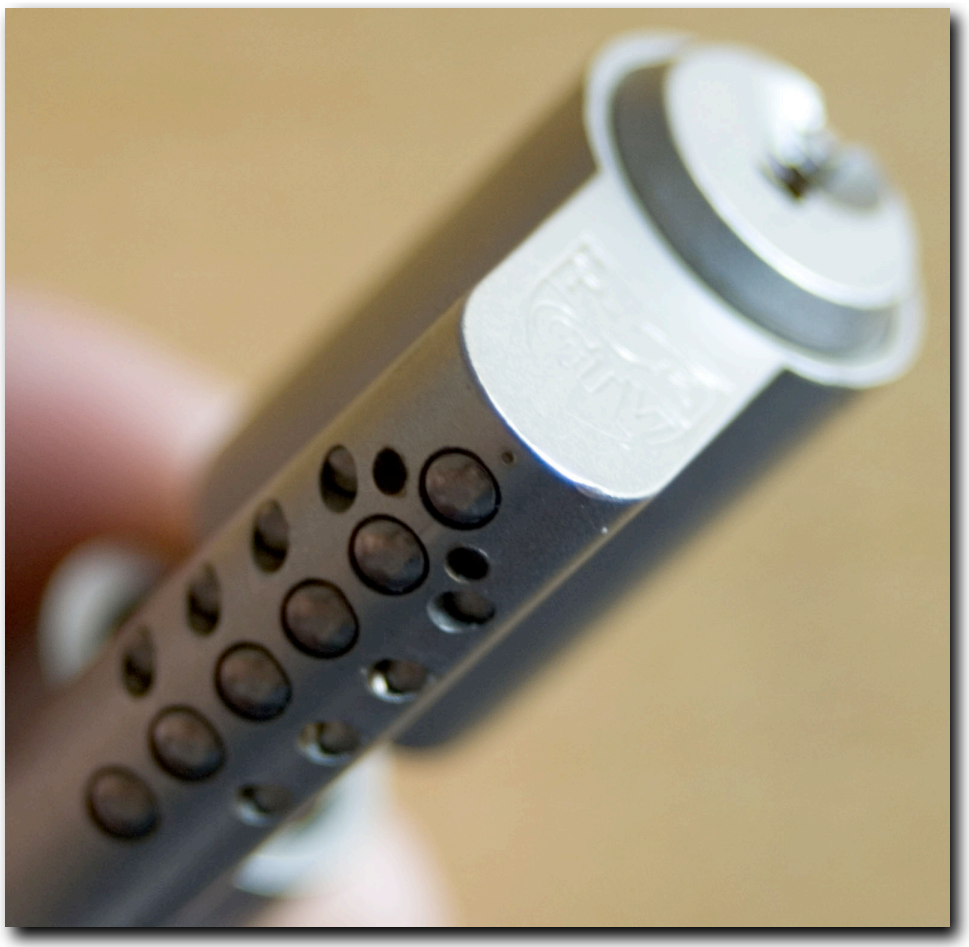


Defeating bumping

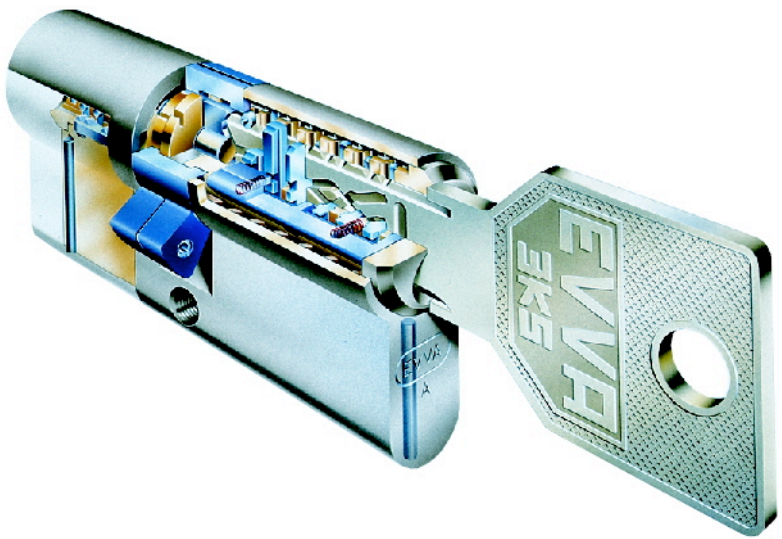
- Three rows with pins
- Normal lock (pickable)
- Extra rows are passive if correct key is used
- Key + pins fill up the plug, preventing small pins entering the plug, even using a spinner

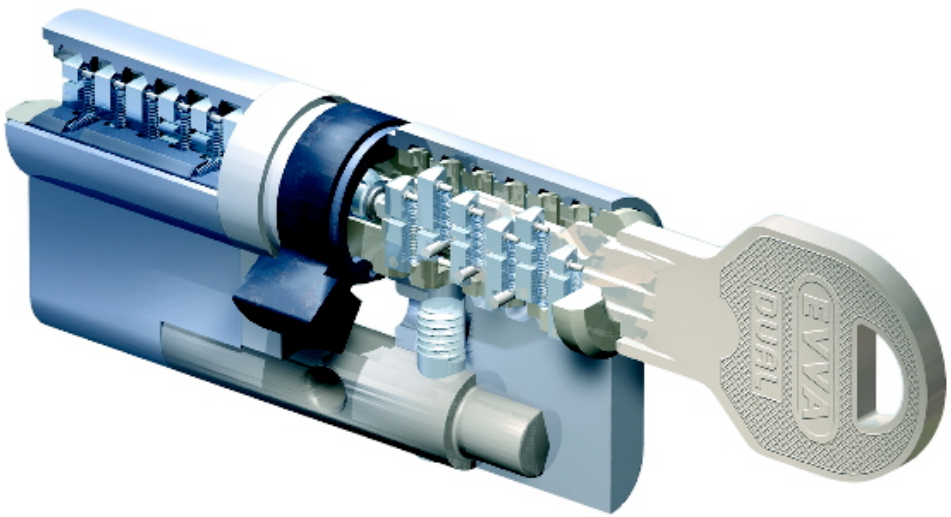


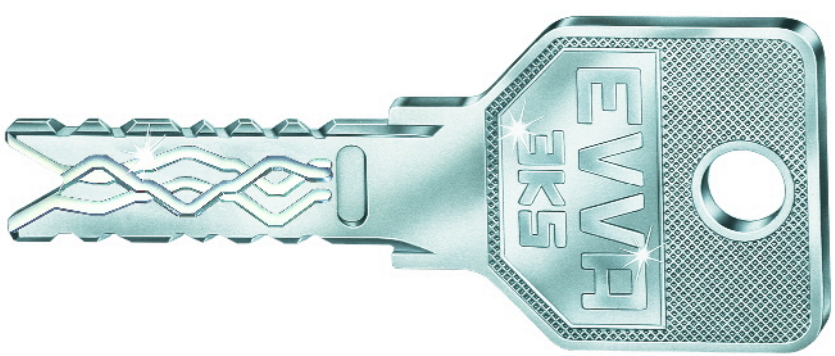
GTV



EVVA

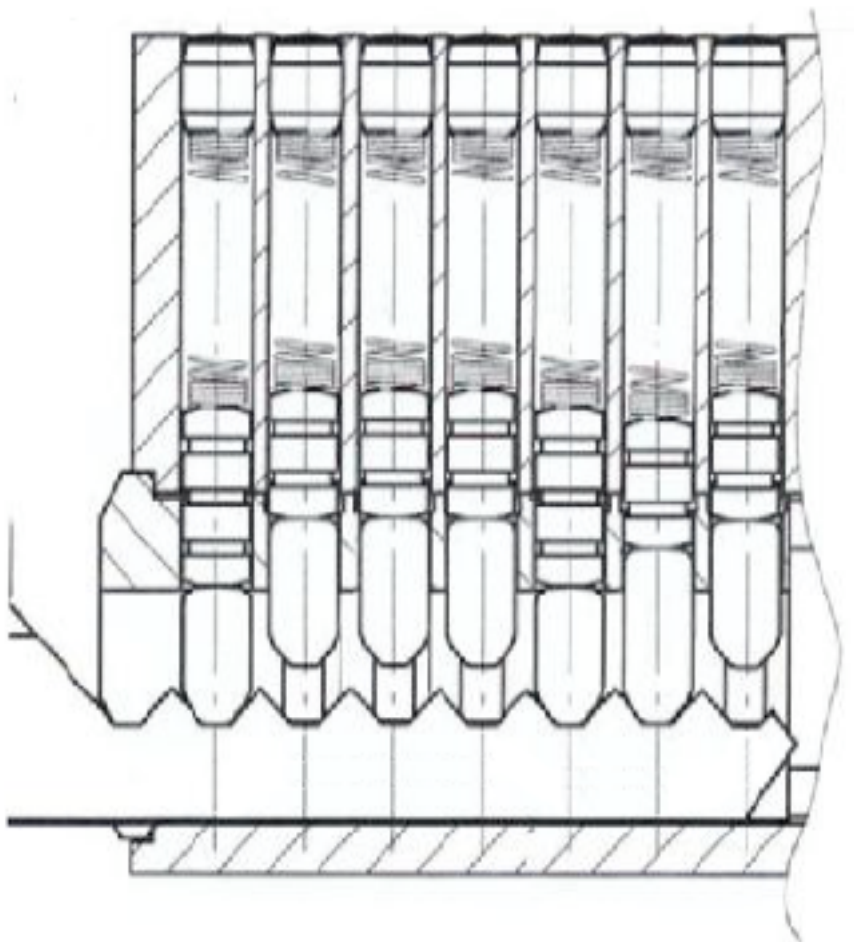






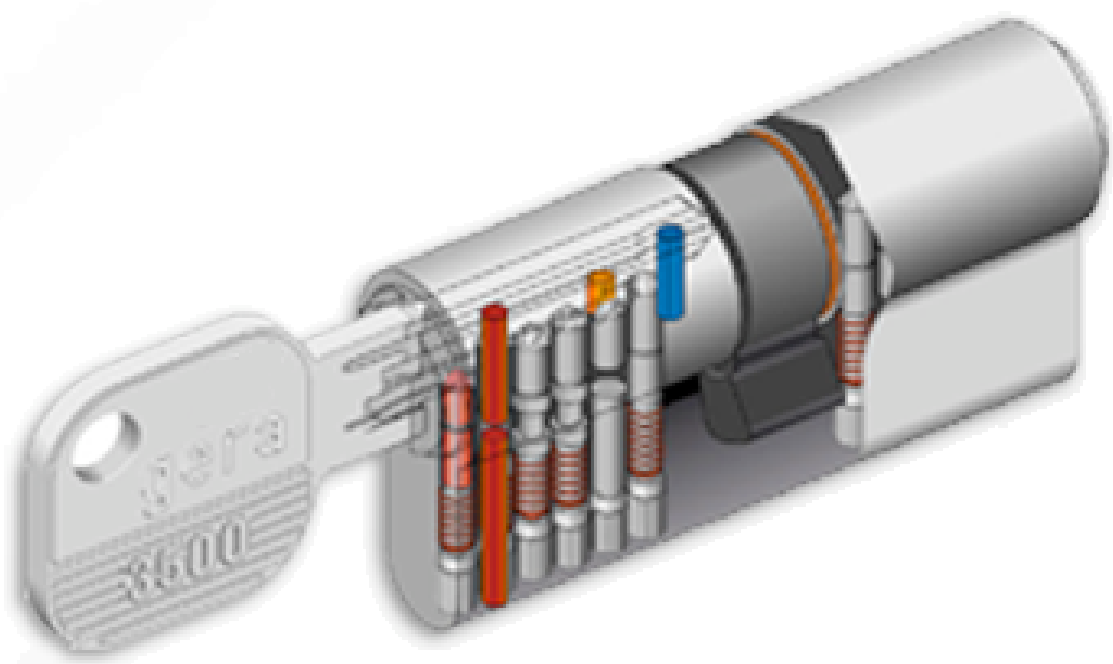
CES

- Bump key does not touch all pins

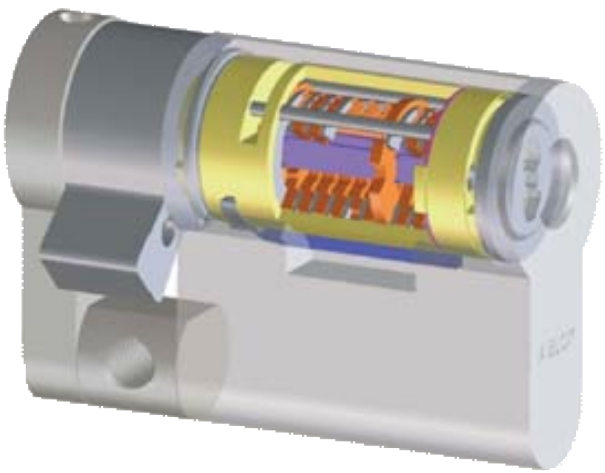


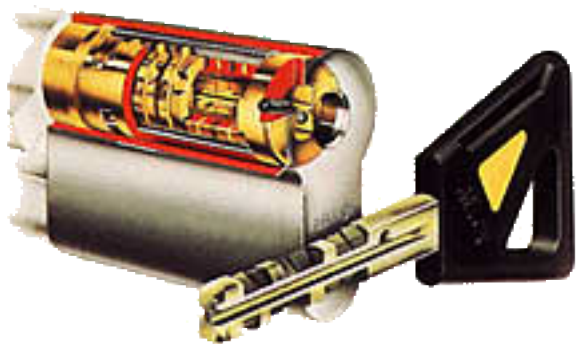
GERA

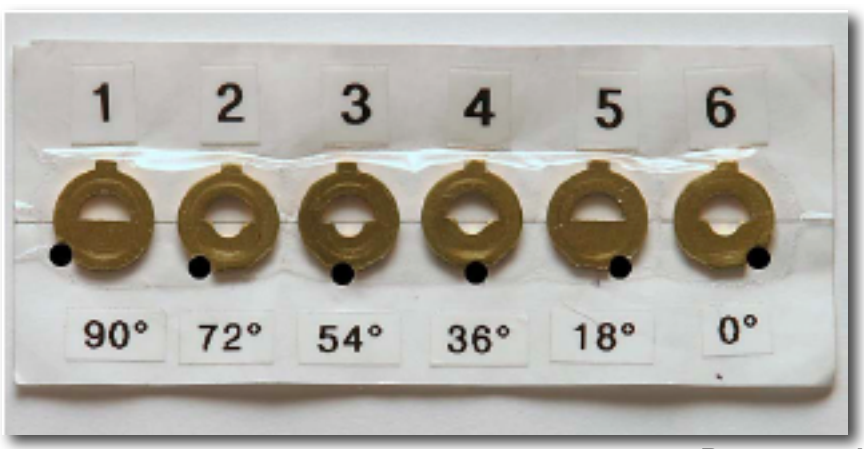
- Magnet in the key pulls one pin up



Rotating disc locks

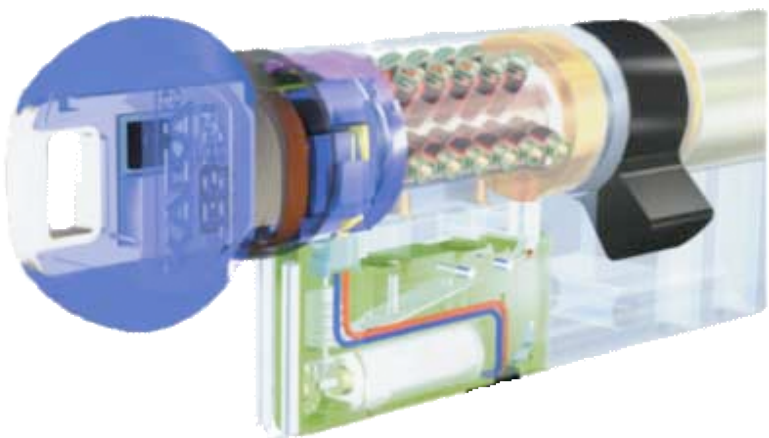






Pictures: Han Fey

Magnetic/electronic

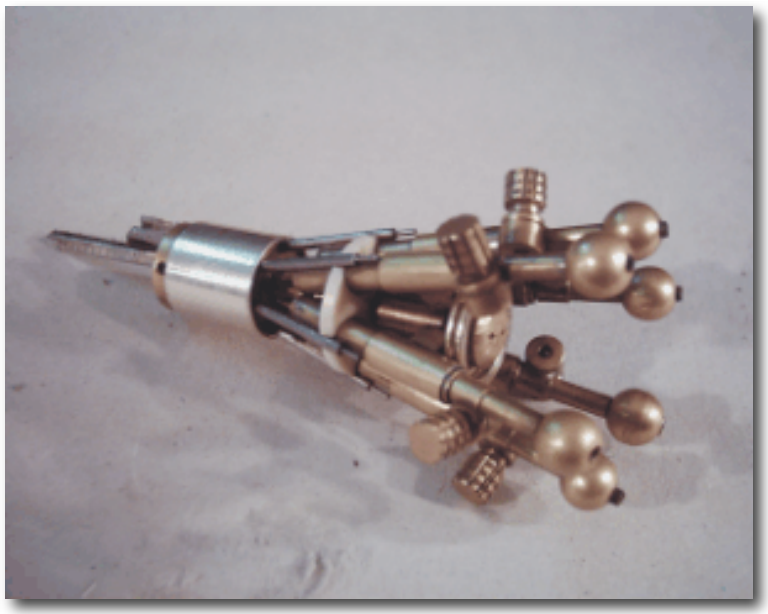


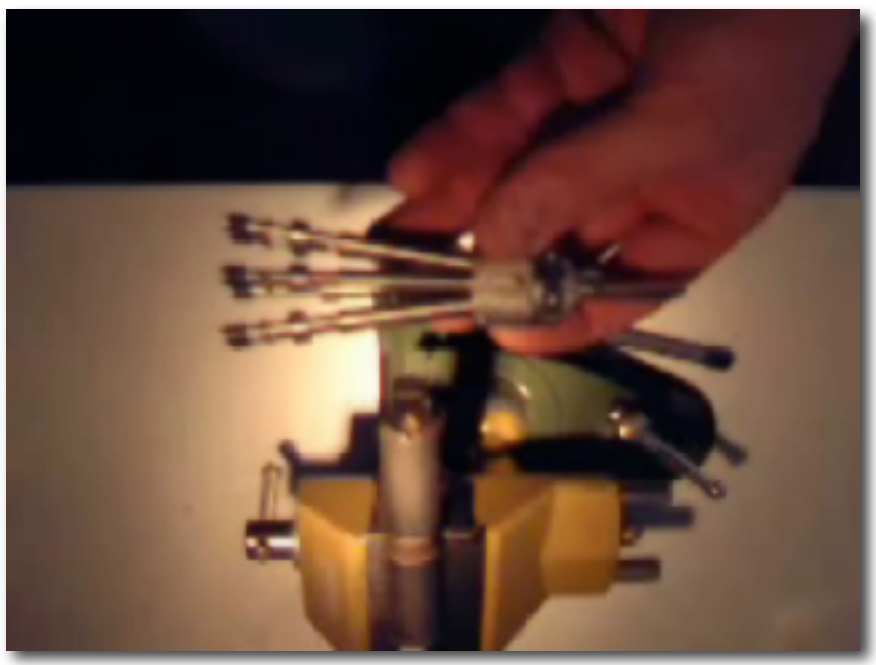
Magnetic/electronic

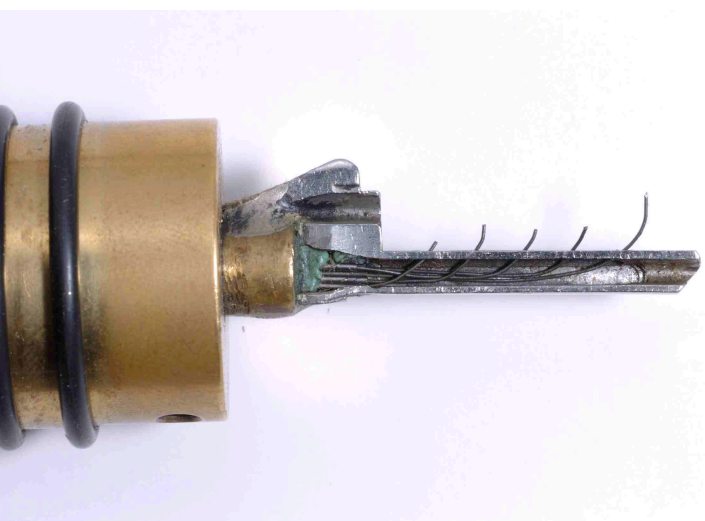
Decoding

- Lockpicking, bumping, will open the lock only once
- *Decoding* is finding out what the key looks like
  - And maybe opening at the same time

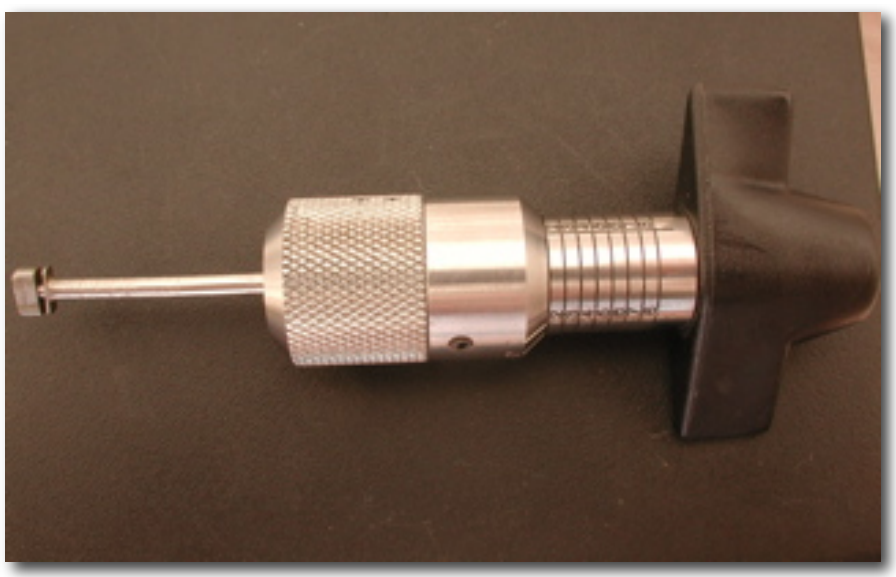
Decoding - Sputnik



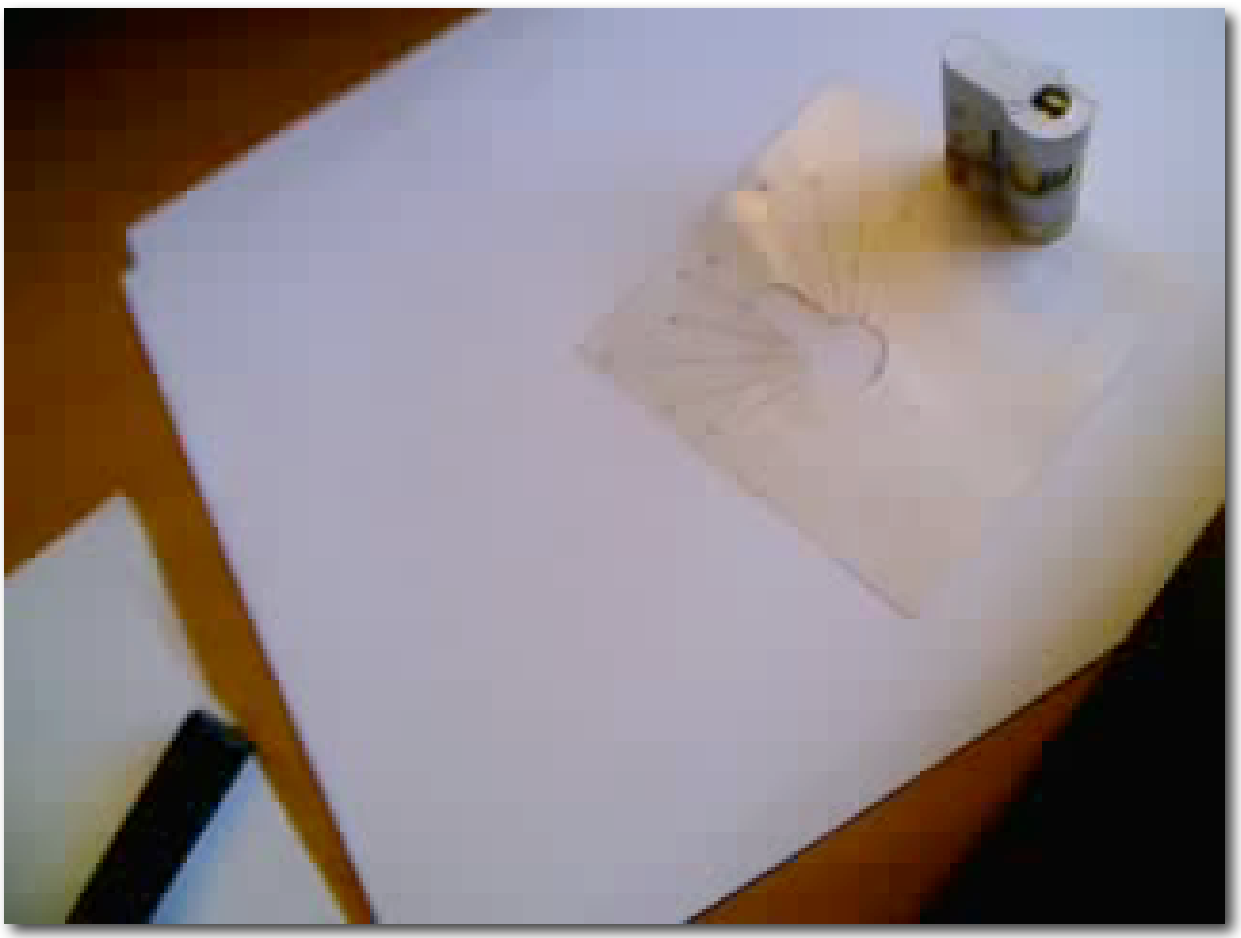




Decoding - ABUS

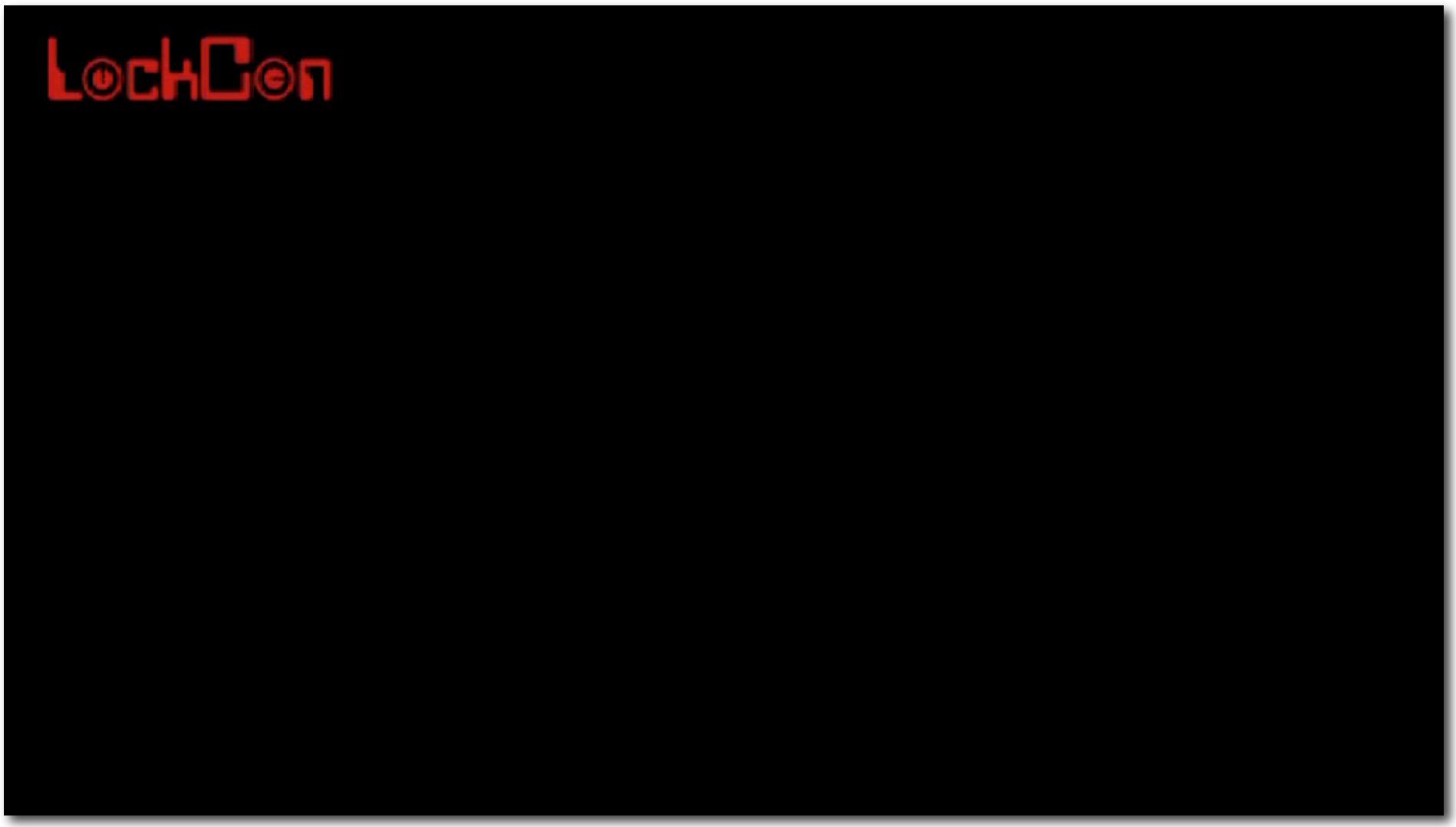


Decoding - Abloy Protec



Impressioning

Impressioning



Lessons learned

- Locks can combine characteristics but must stay within space and money limitations
- Lock manufacturer chooses from his bag of tricks to build a lock with certain characteristics w.r.t.:
  - Price
  - Key duplication and lock copying
  - Resistance to force, lockpicking, bumping, decoding

Dziekuje!

walter@ehv.toool.nl

Note: some of the pictures I do not know of where they came from. If they are yours, please send me an e-mail so I can credit you or remove them.