Locksport journey with Abloy disc detainer locks

newbie

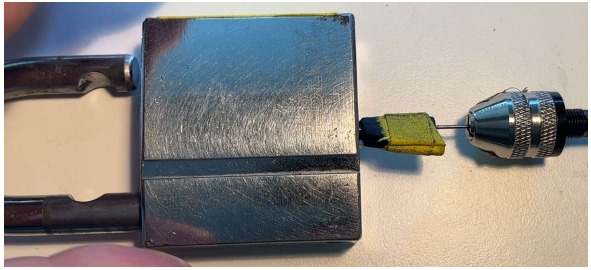
midbie

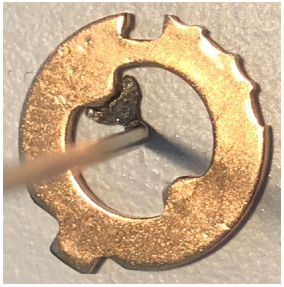
Lockcon 13.10.2023

Idanhurja

Contents of the presentation

- Introduction
- Abloy disc detainer lock: what is this guy and how it function
- Basics of Abloy lock picking
- Things I have tested because can / by accident
- Learnings & used steps to develop pick for Abloy Easy (for locksport purposes)





Live audience is -52% for my lock picking -skill

Disclaimer: This presentation in based on speaker own understanding, can be completely incorrect

Idanhurja, who is this Finnish guy?

yeah I just can't be bothered to spell that

August 2020

Oct 2020

This is absolutely the best success feeling in this scene so far!

locksport: Abloy classic PL341/25 picked

locksport: S&G 6731 autodialer build 0.4

locksport: Abloy Sento PL330 picked & gutted...

Locksport: Abloy Easy picked & gutted with pick...

1st place of 6108 hackers!

LOCKCON

?

Abloy locks are really robust

tori.fi: “old Abloy lock, no key.
To be used as a decoration item”

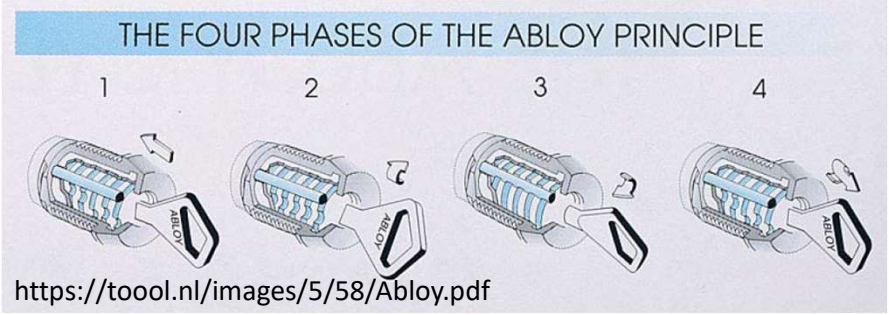
Picked, decoded, made a key. Functions just perfectly

Accidentally delivery package got broken during the postal delivery,
and the lock has dropped to floor/ground

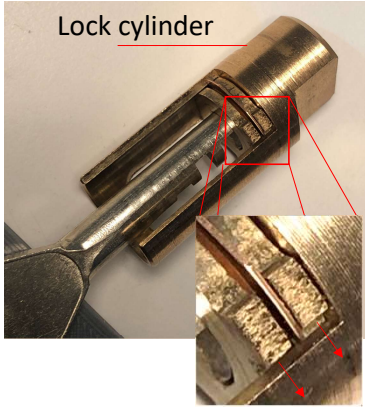
Operation of Abloy lock (for them all types)

- Phase1: Key is entered into the lock

- Phase2: Key turned 90deg clockwise. code discs turn based on cuttings in entered key (cuttings in 18deg steps). Lock cylinder not moving. If correct key in use the side bar enters the gates in code discs when key turned 90deg
- Phase3: At 90deg 2 (or 1) rear discs tries to turn the lock cylinder. If side bar entered the gates, lock cylinder with the key able to turn up to 180deg and lock opens.
- Phase4: Key turned 180deg counter clockwise. At 90deg side bar rises back. At 0 deg key can be removed, all discs at default state



https://toool.nl/images/5/58/Abloy.pdf



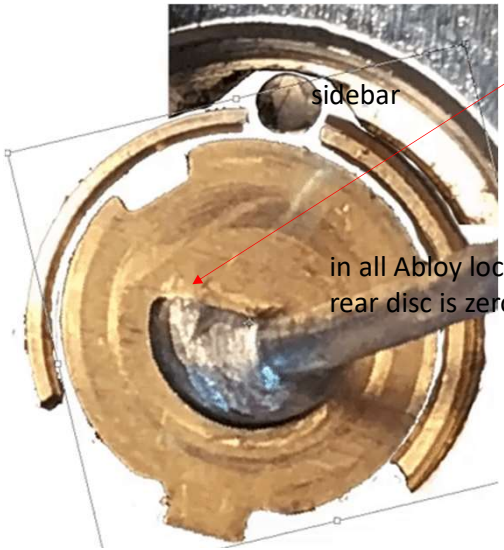
Used steps to develop Abloy picks

- Classic pick
  - This 100years+ old lock design wiped all of my own pick designs. Solo mode vs a boss mob
  - Became painfully familiar with the concept of Abloy lock picking
  - “Picking Abloy Classic-Theory and Practise” (by Matt ‘The Lock’ Smith, nick: HuxleyPig)
    - https://www.dropbox.com/s/y7ytddmmts13wii/AbloyBreakdown1.2FINAL.pdf
- Exec pick (for tight Finnish Exec type)
  - Build 0.1 offcentric aligned 1 keyway side using
  - Build 0.4 center aligned 1 keyway side using, tensioner based on a key
- Sento pick
  - Build 0.1 center aligned 1 keyway side using
  - Build 0.2 center aligned 1 keyway side using, tensioner based on a key
- Easy pick
  - Build 0.1 center aligned 1 keyway side using, tensioner based on a key
    - 2 rear discs controlled by tensioner
  - Build 0.3 center aligned 1 keyway side using, tensioner based on a key
    - 1 rear disc controlled by tensioner

Picking method of Abloy locks (for them all types)

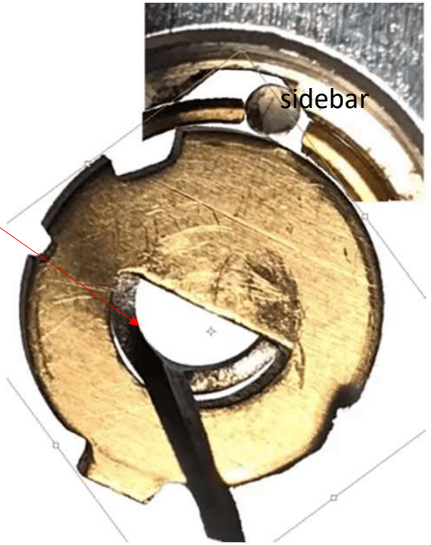
Abloy Classic lock type used as example (simpliest). Other Abloy lock types require differently shaped tensioner and picking tip (+added challenges).

Rear tensioner

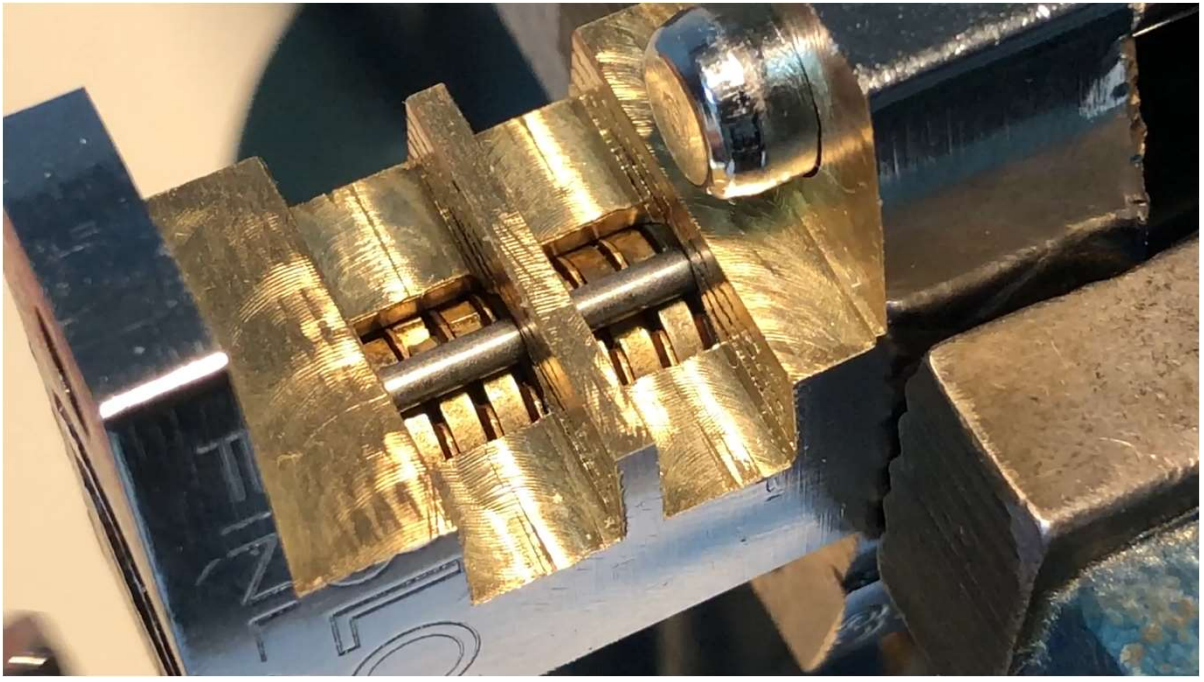


Classic 2in1 pick

Lock centric rotating picking tip



Test run with a cutaway PL330 Abloy classic

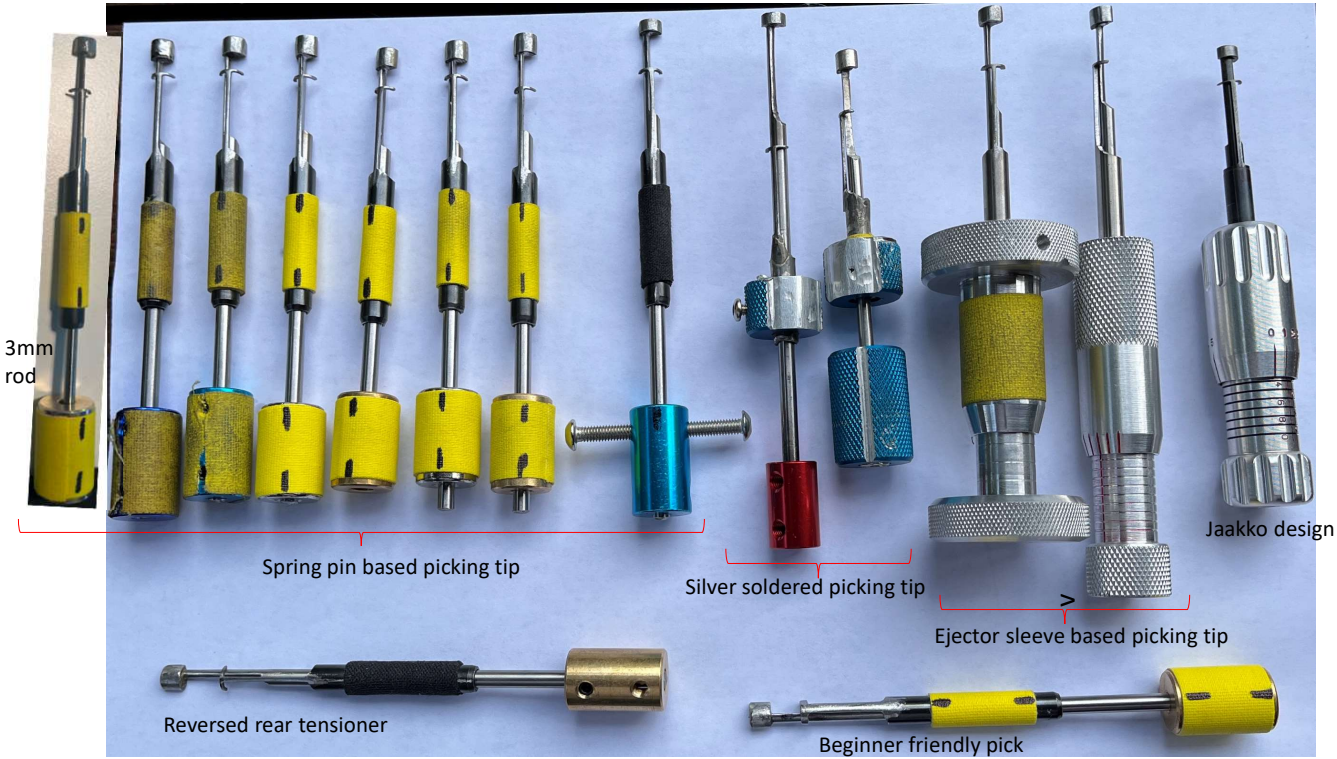


Steps:

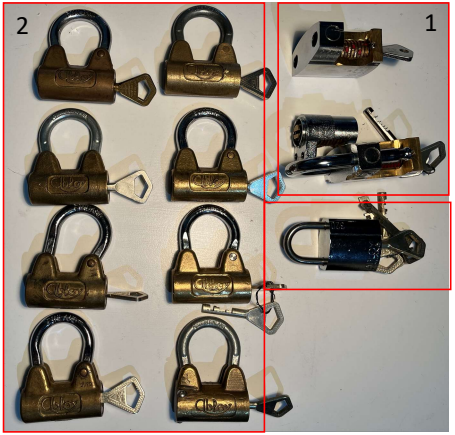
1. All discs 90deg clockwise dir
2. Lock tensioned using 1or2 rear discs
3. Turn each disc individually
4. If a disc wobbles, it's correctly set (for now) and need to re-check after moving other discs. Note: false gates

5. Lock opens

Different Abloy Classic picks that I have



Lockcon-23 nightshift Workshop: Abloy Classic picking



Tiers:

1. Cutaway locks (optional)
    - beginner friendly cutaway lock
    - 2 pcs of cutaway locks, one with strange cuttings
2. Guided lock picking, option to look at the key
    - A set of padlocks
    - 1 pcs of strange padlock
3. Pwn2own (after completed tier 2)
    - A set of padlocks, no key, no guiding
    - If lock is picked: lock,key,pick 2own

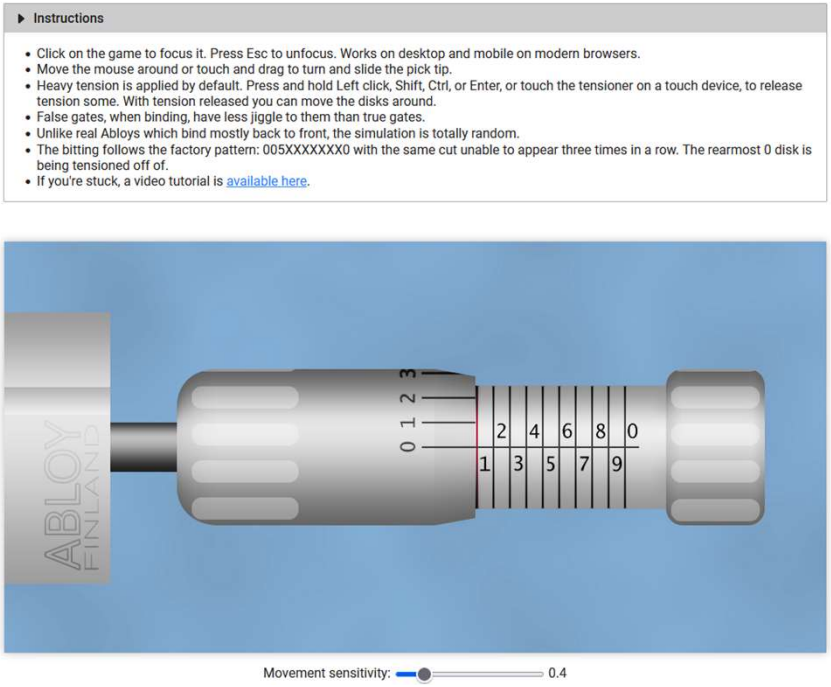
Participants should have:

- Vice / similar to hold the lock while picking

Ways to lower the barrier for the beginners to familizarize with Abloy lock picking

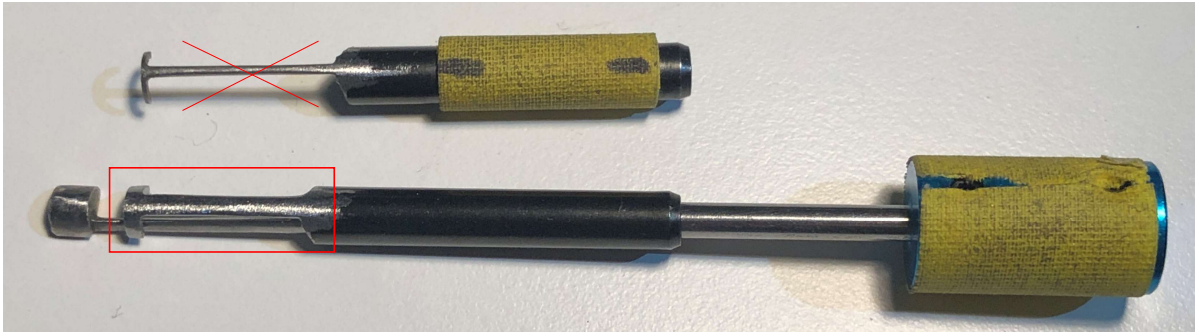
https://assamow.com/abloysim/

Abloy Classic picking simulator



Ways to lower the barrier for the beginners to familizarize with Abloy lock picking

beginner friendly pick and customized lock for it



Tiny picking tip replaced by

Robust picking tip

Customized lock, all zero cut discs replaced with something else

Every other code disc replaced by wide open fixed fat spacer

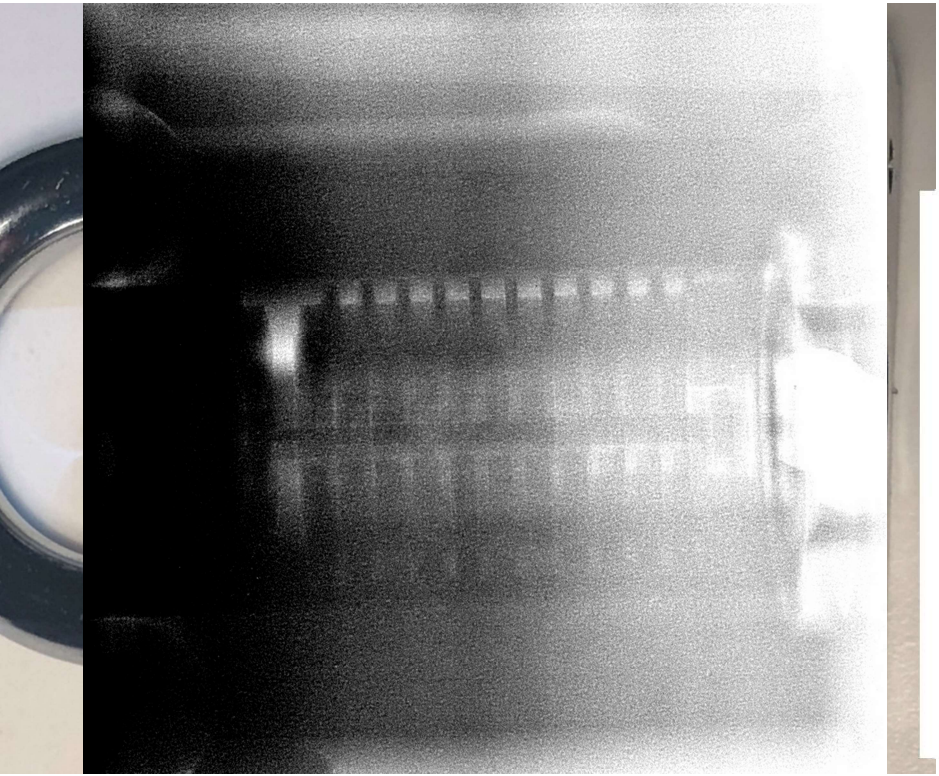
Ways to lower the barrier for the beginners to familizarize with Abloy lock picking

Cutaway lock

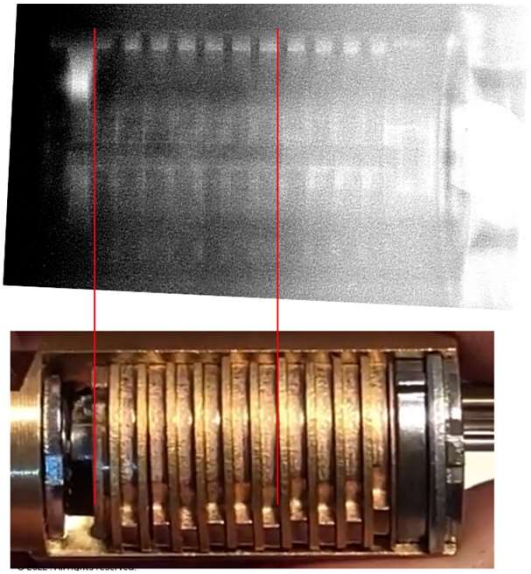
Paint added into each disc for better visualization of picking status

Paint added into each true gate for better visualization of picking status

Tested ideas to improve picking process

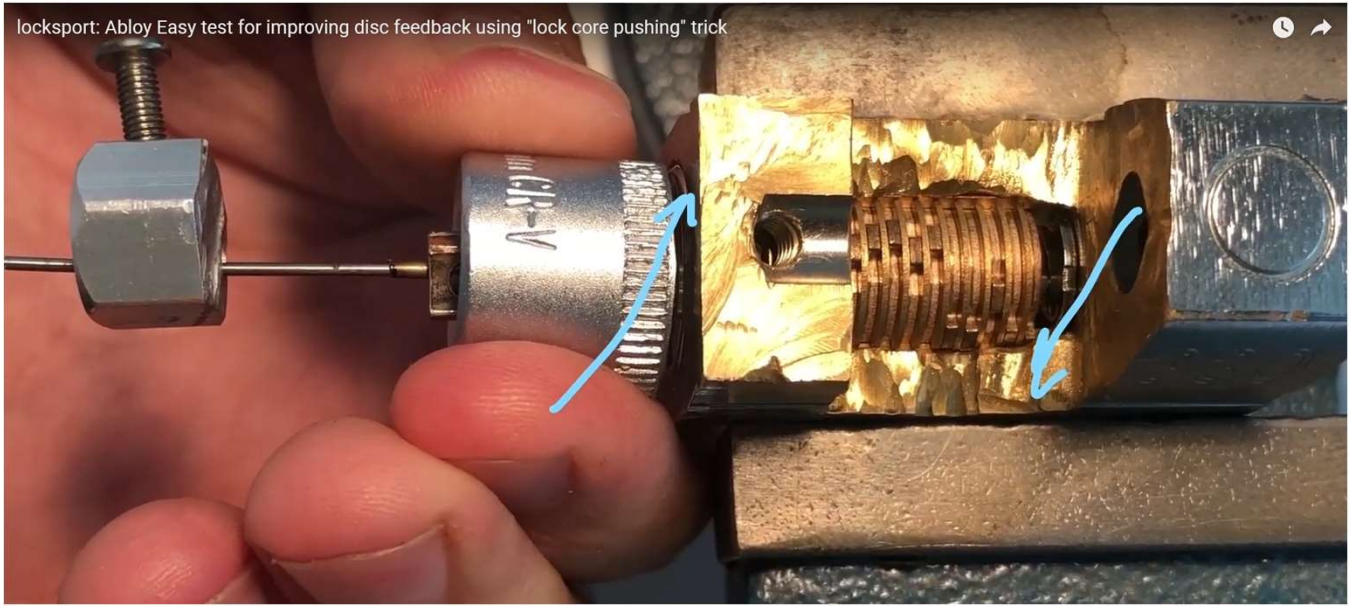


X-ray the lock to see where the true gates are
Abloy Easy PL330 (this function for those pin tumbler locks)



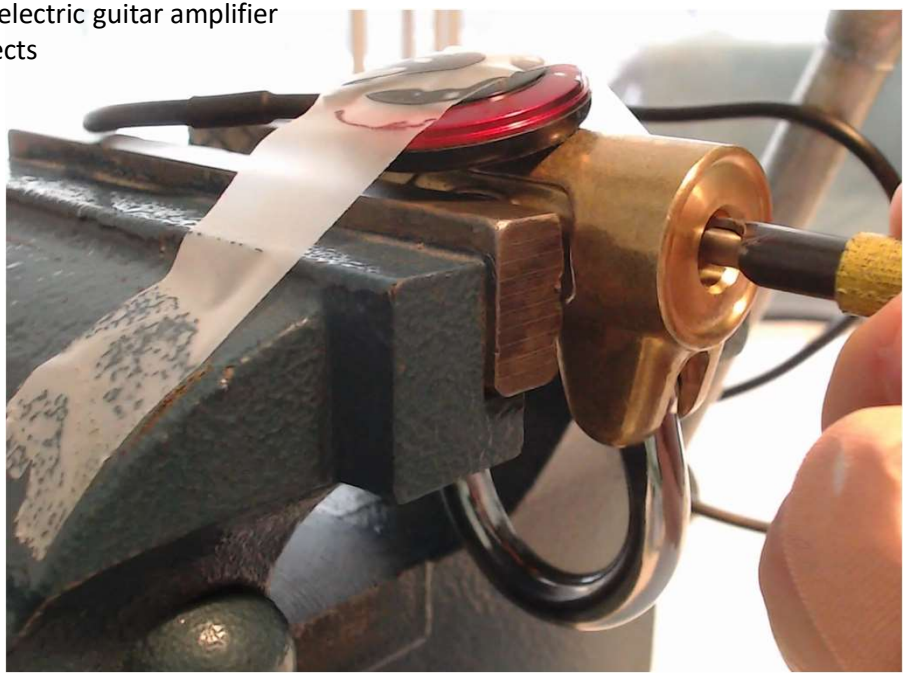
Tested ideas to improve picking process

Improve side bar contact with discs by pushing the lock core towards the side bar



Tested ideas to improve picking process

Contact mic with electric guitar amplifier
- Great sound effects



Tested ideas to improve pick making process

Issue: How to make sure that the rod of picking tip is center aligned to tip and the rod is straight?

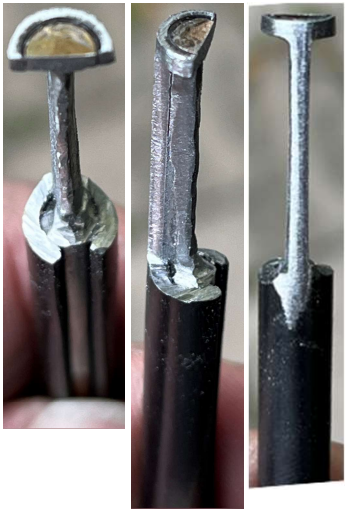
Solution: template based classic pick tip making

picking tip used as reference for template

template to be glued to spring pin

after some shaping

ready for finalization, remove template by heating

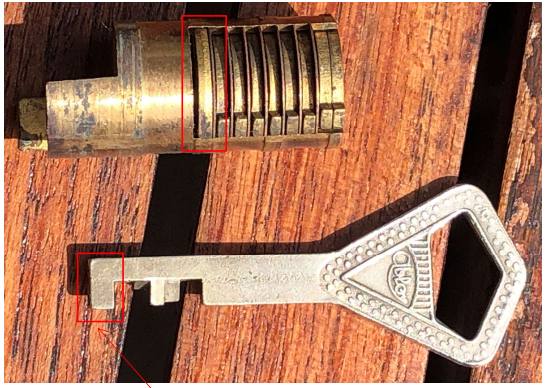


set of picks ready for locksport action

Why master keying helps in lock picking

Non-standard Abloy Classic locks

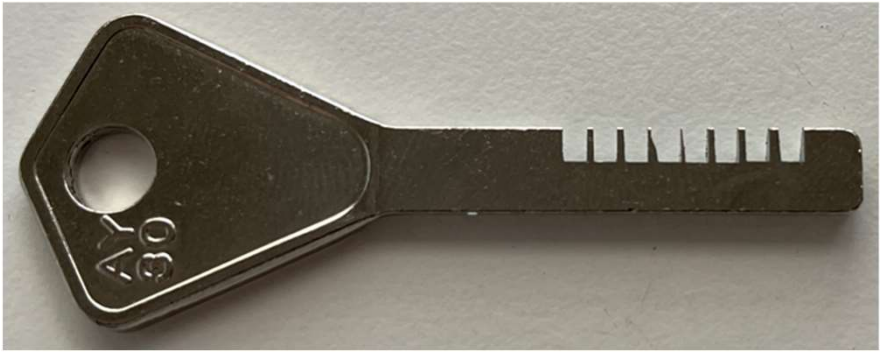
2 pcs of special locks so far: reverse tensioner required, tensioning from fixed fat spacer



Free turning, no disc for this

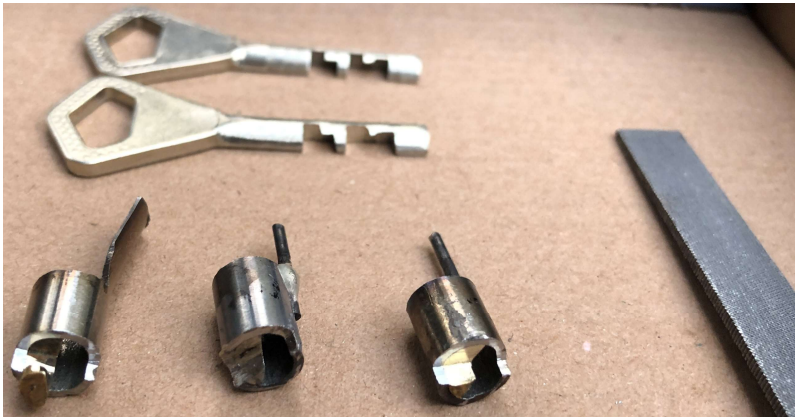
Impressioning attempt

- Key blank cutted with a Silca key cutter
- Need to practise more impressioning

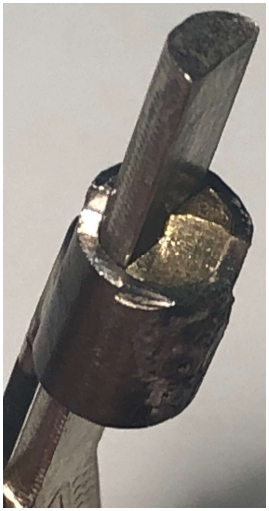


- This filed key is able to open the lock but did it based on known cuts

Key cutting: filing



1. Make filing template for each cut depth 1-5



2. Insert template to correct position in key blank

3. File following template profile
4. Repeat steps 2-3 for all cuts

- Functions okish but boring

Key cutting: Silca key cutting machine

- Bought old Silca key cutting machine: blade and driver belts were oldish
- Ordered new blade from Aliexpress, new belts from local belt manufacturer (best ever service)
- With new blade and belts the machine functions fine, can cut also Exec keys

Old blade able to obfuscate cuts

Tailored key tip

Just for fun

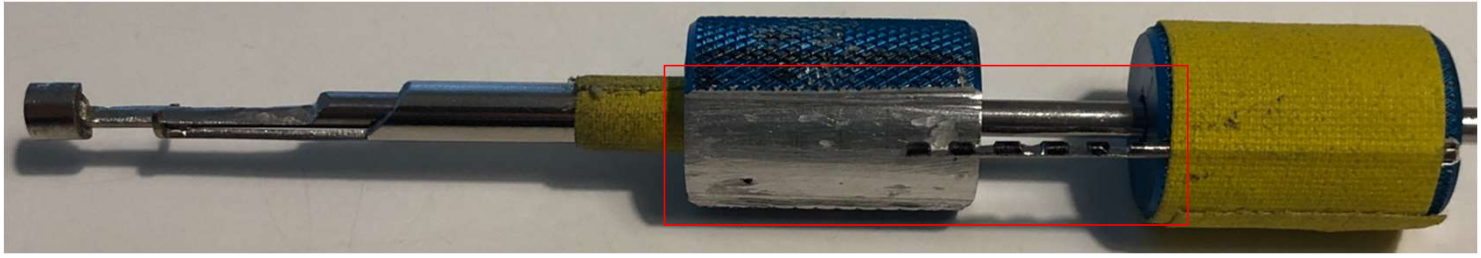
- Handbag padlock retrofit with Exec core

- Handbag padlock retrofit with Easy core
  - Nice present for some fellow locksporter?

Just for fun

- tested to make handles based on extension part of a flash light. Result was more a joke.
  - These handles are not completely preventing the picking but will make it a lot harder

- tested to mark turning angle area and disc number info into handle. This functions okish, but added value not big



- Learning: Don’t over complicate things. “If have hands, no need for handles”

Abloy Profile picks

Ejector sleeve based picking tip

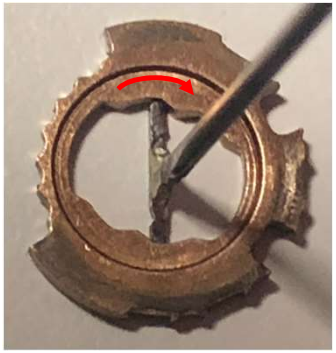
Silver soldered picking tip

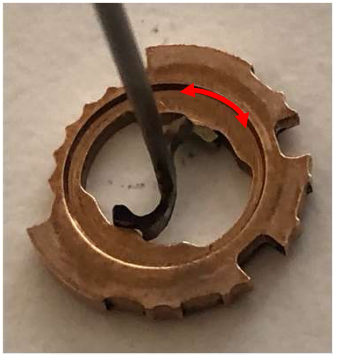
Classic picking tip (adaptation needed to counter antipick discs)

- So far I have got only few lock samples
  - Not too common in Finnish second hand markets
  - Not much experience on this lock type
- Seems to be challenging to make one universal pick

Used approach in pick development for a new lock model

- Use Google / Youtube / Discord to study what others have done already. Some a bit shy to share all the details.
  - Don’t invent a pick (or a wheel) again
- gut the lock, study how it operates
- Decide how to tension the lock: front or rear tensioning (or random tensioning)
- picking tip design
  - pick should be able to operate each disc individually without disturbing other discs
  - full turning angle to both directions, not just pushing
  - movement front-rear disc in both directions
- make a cutaway lock
  - In Abloy case one cutaway cover suitable for many lock core types
- improve pick builds as needed in order to be able to operate cutaway lock with it well enough
- a known lock picking
- An unknown lock picking

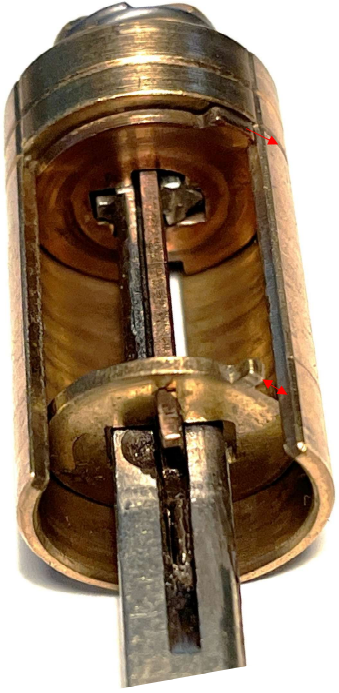




PL330 cutaway cover suitable for several Abloy lock core types

Abloy Exec pick design by Idanhurja

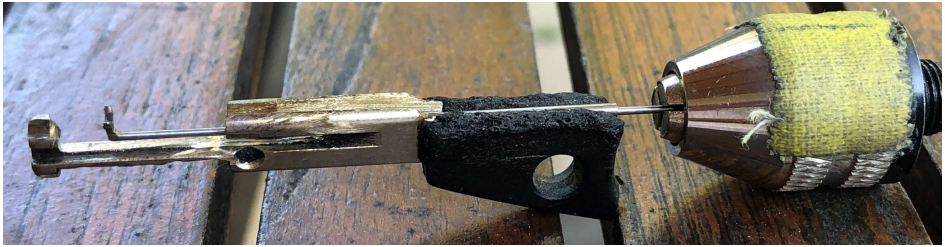
Remember slide 7: Picking method of Abloy locks (for them all types)



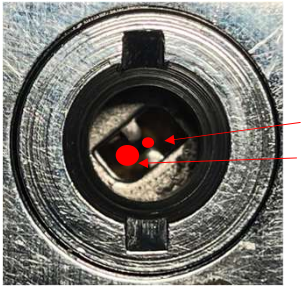
Rear tensioner

Center aligned 1 key way side using picking tip

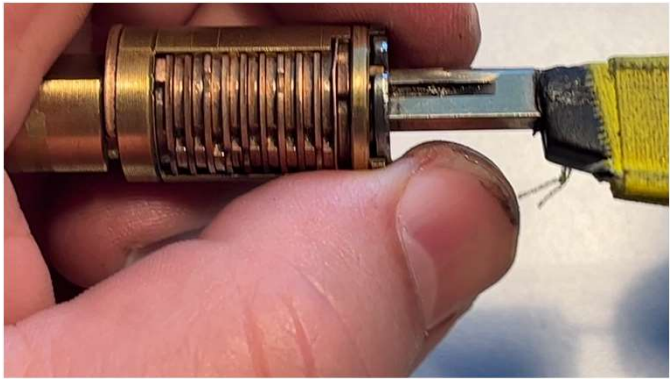
Build 0.4



Tensioner based on a key

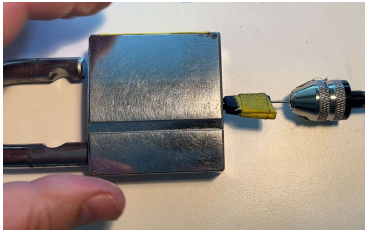


Rod profiles:
Picking tip
Tensioner

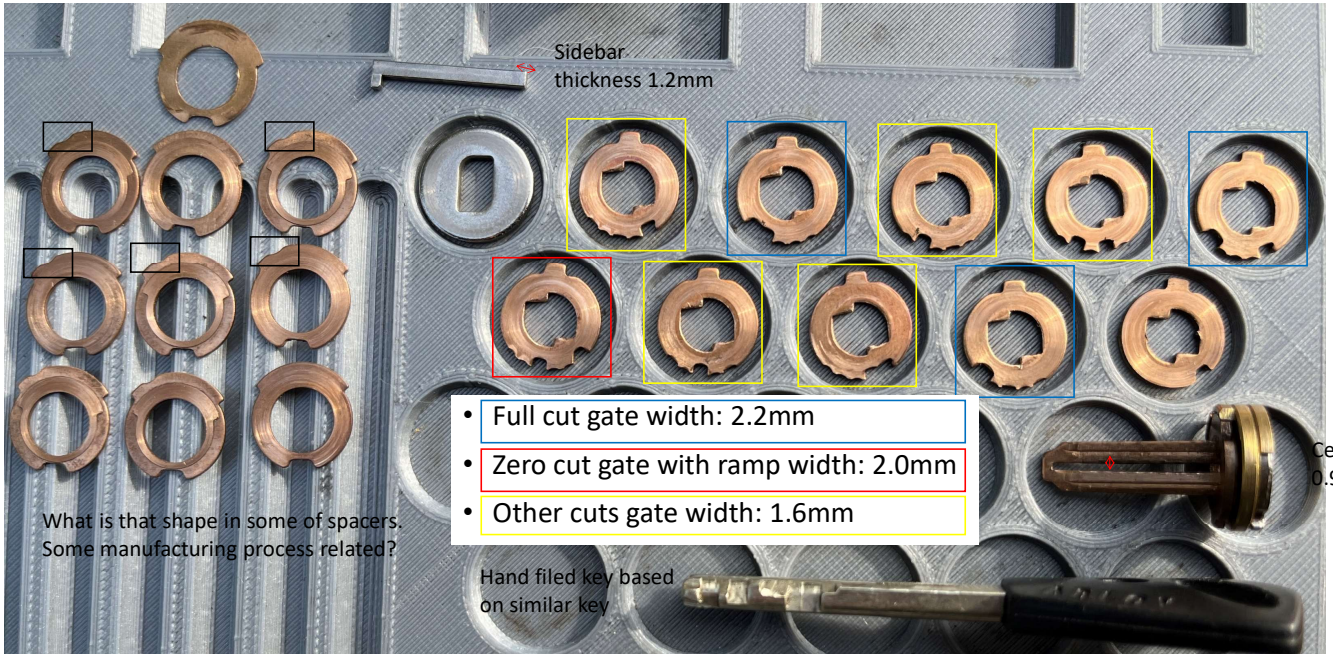


Test run to demostrate full turn for the last and for the first disc

Proven to be able to blind pick some padlocks

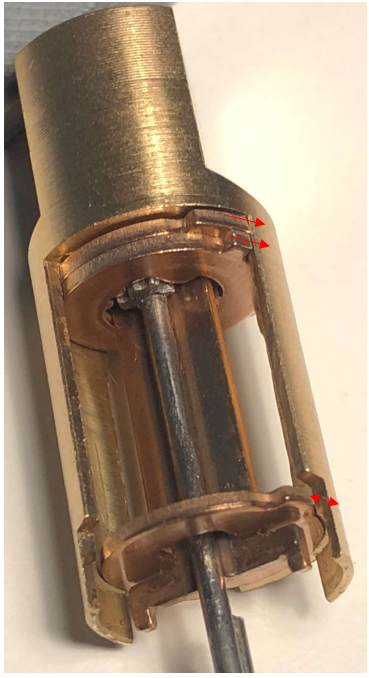


Discs of PL340 lock sample



Abloy Sento pick design by Idanhurja

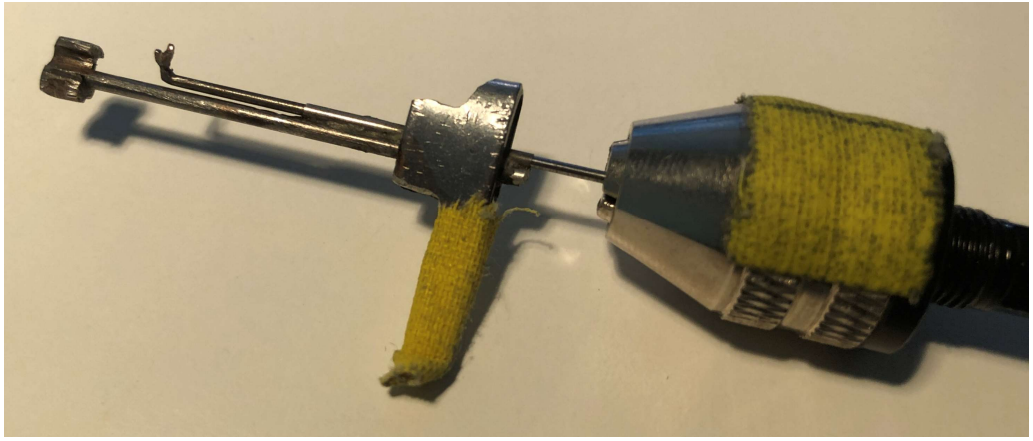
Remember slide 7: Picking method of Abloy locks (for them all types)

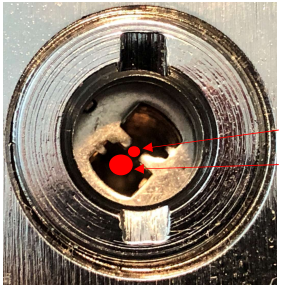


Rear tensioner

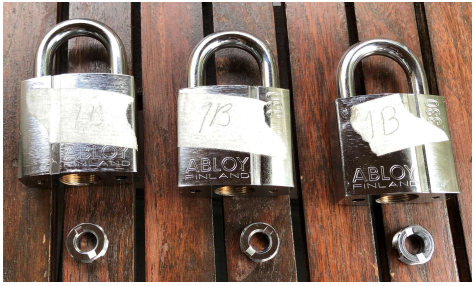
Center aligned 1 key way side using picking tip

Build 0.1





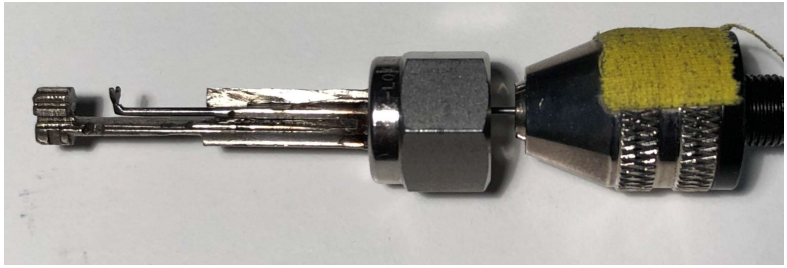
Rod profiles:
Picking tip
Tensioner



Proven to be able to blind pick a set of padlocks with key profiles: 2B, R2C and 1B

Build 0.2: Tensioner based on a key

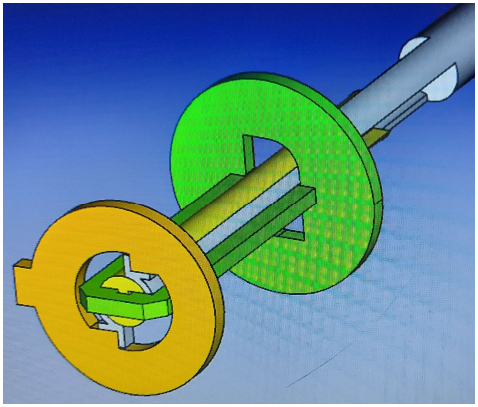
Limited usability for different Sento key profiles

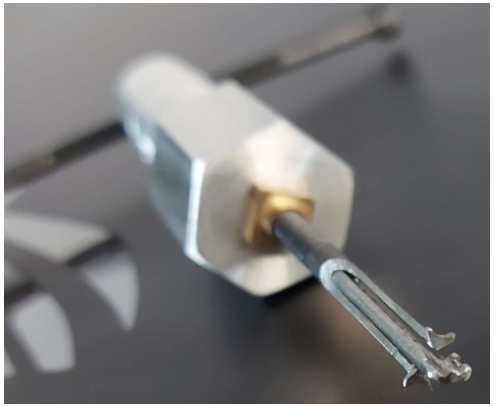


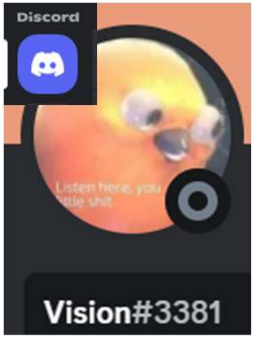
Rod profiles:
Picking tip
Tensioner

Abloy Exec/Sento pick design by Vision

Way cooler than my own Sento pick design! – but maybe with some limitations





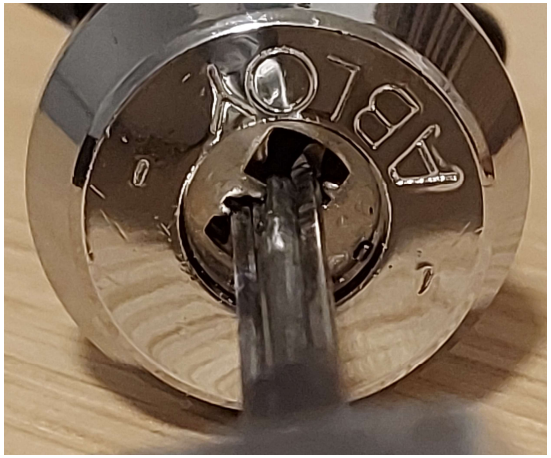


Rod profiles:

Picking tip

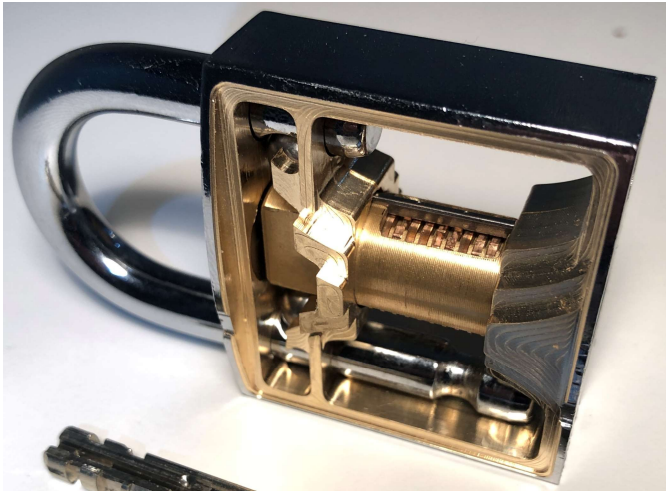
Tensioner

Picking tip



Abloy Easy

- Abloy Easy was announced publicly on April 16, 2021, superceding Abloy Sento.
- Abloy has patented Easy lock core technology (patent expires in 2040).
- One can expect that Easy will become one of the most common lock type used in Finland for protecting targets that require higher protection class that the traditional Abloy Classic can offer.



Abloy Easy Patent study

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)
(19) World Intellectual Property Organization
International Bureau
(43) International Publication Date
10 September 2020 (10.09.2020)
WIPO | PCT
(10) International Publication Number
WO 2020/178478 A1

It is an objective of the invention to improve the qualities of a disc tumbler cylinder lock against manipulation. The objective is attained as presented in the independent claim. Various embodiments of the invention are presented in the dependent claims.

The disc tumbler cylinder lock 100 and key 1 combination according to the invention comprises key rotation limiting means 101 and a guiding element 25, 48, 50 in the disc tumbler cylinder lock 100. The key 1 comprises grooves 5 for the guiding element. The guiding element comprises two rails 25, 48, 50, which make up a portion of the rotation limiting means 101 and each of the rails comprises at least one limiter protrusion 26. The limiter protrusions are arranged to extend inward in the disc tumbler cylinder lock, and the key 1 comprises at least one recess 6 for the limiter protrusions.

The rotation limiting means further comprise a front guide 22, 57, the front guide having the rails 35, 48, 50 in association therewith. The front guide and the rails are arranged to allow turning of the key 1, presently in its basic position in a disc tumbler cylinder lock, for releasing the locking of the disc tumbler cylinder lock, such that the limiter protrusions 26 of both rails move, upon turning the key, into the at least one recess 6 of the key. In other words, the rails 25, 48, 50 and the limiter protrusions thereof reduce the space of a key channel while moving inwards in the disc tumbler cylinder lock. This, in turn, makes manipulation through the key channel considerably more difficult.

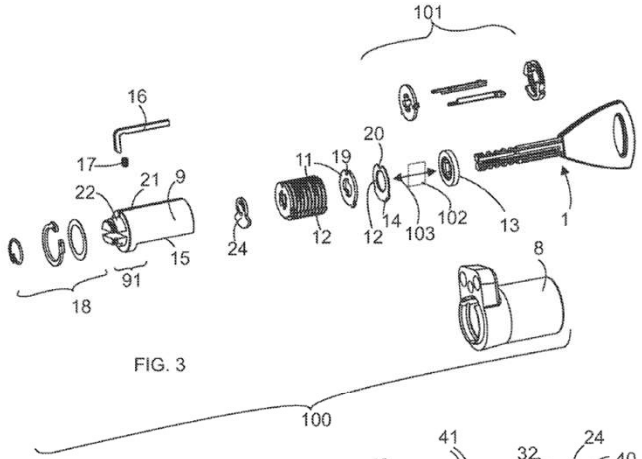


FIG. 3

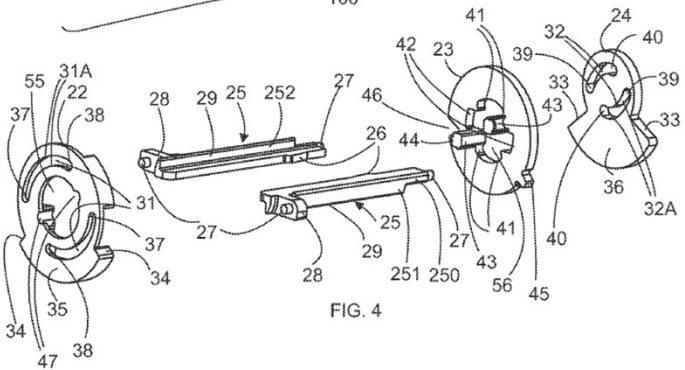
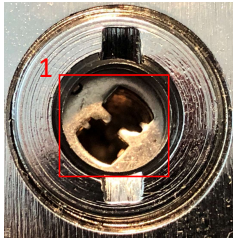
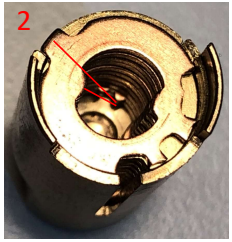


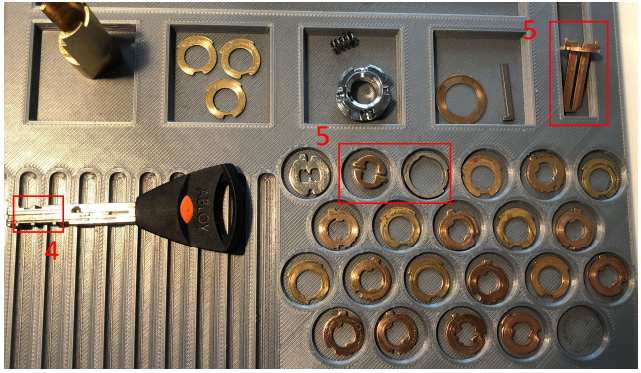
FIG. 4

Abloy Sento vs Abloy Easy PL330

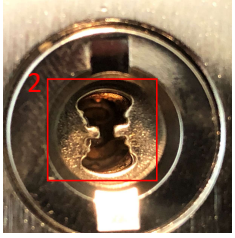
Sento

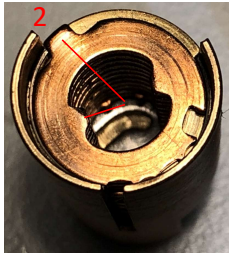






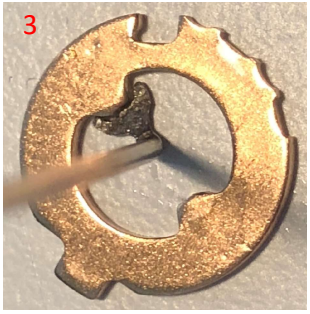
Easy





1. Key profile is different
2. Code discs has different angle offset

3. Identical picking tip head profile able to turn discs in both lock types



4. Added opening in the key

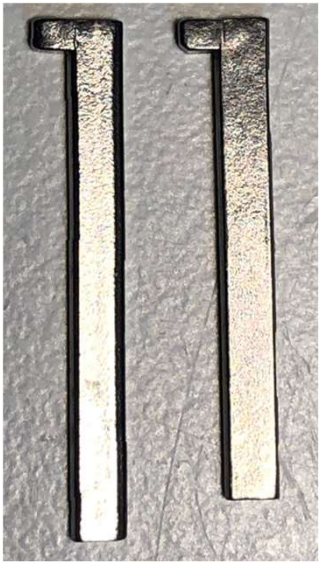
5. Key guiding element different

1. Both functions in the same PL330 frame

2. Rear zero cut disc(s) used for opening the lock / tensioning

3. Code discs:
Easy 10 pcs
Sento 9 pcs

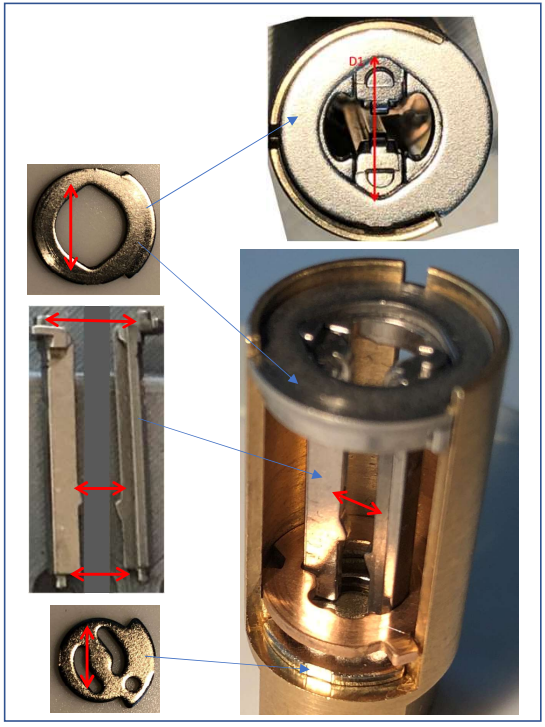
4. “overturning” disc



Abloy Easy improvements compared to Sento 1/3

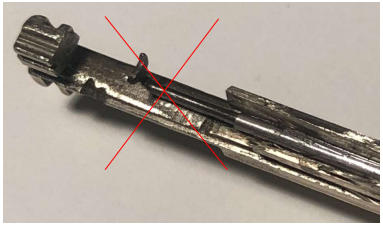
Keyguiding element is tapering while key is turned

"key can be entered" state



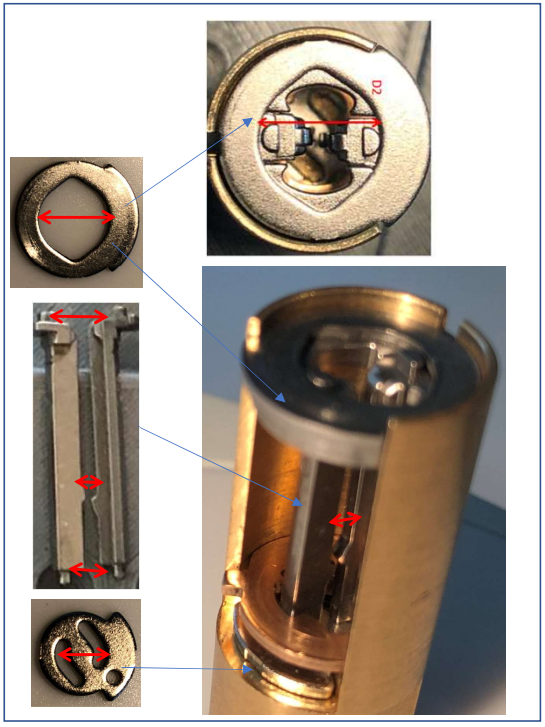
Turn the key

Front lemon disc forcing keyguiding elements to taper



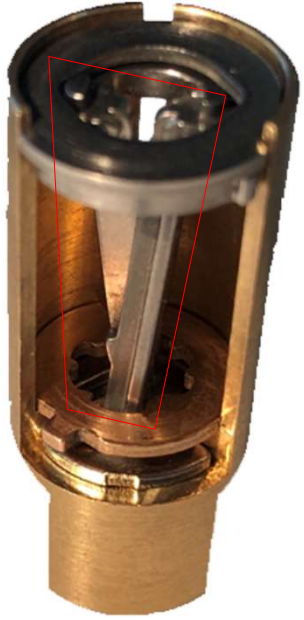
Rear support disc (69) forcing keyguiding elements to taper

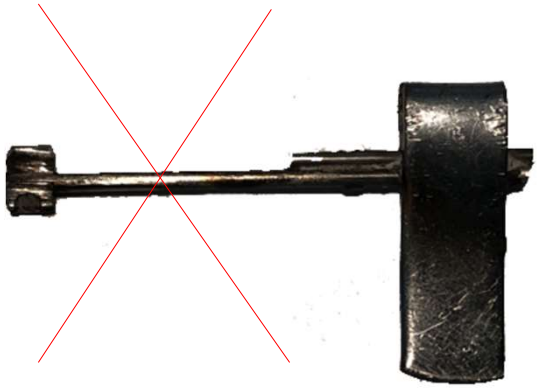
"key fully turned" state



Abloy Easy improvements compared to Sento 2/3

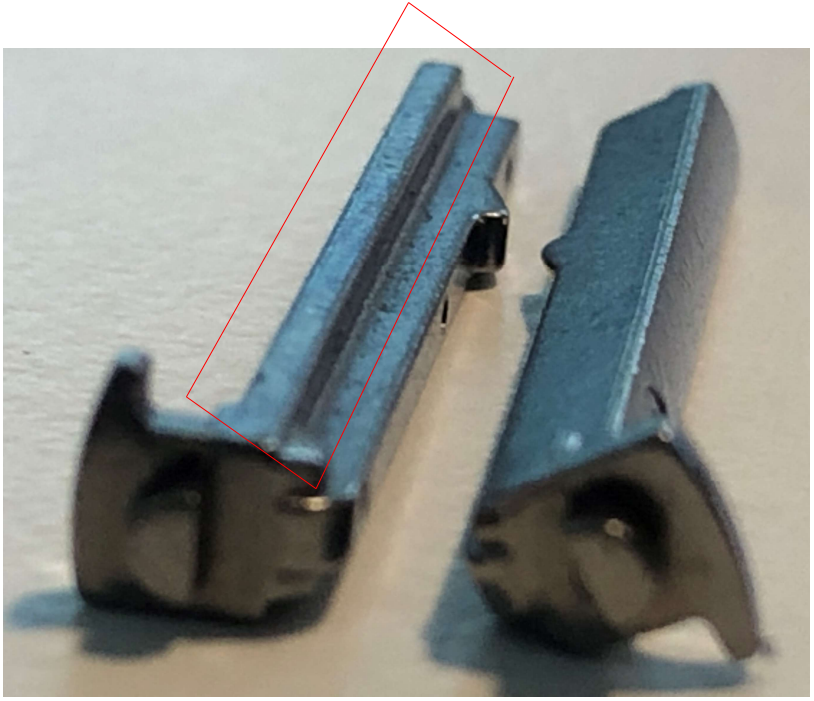
Keyguiding element is not a stiff structure, will twist easily if tensioned only from one end

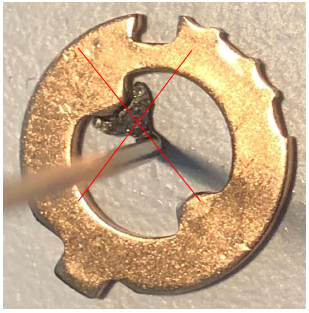




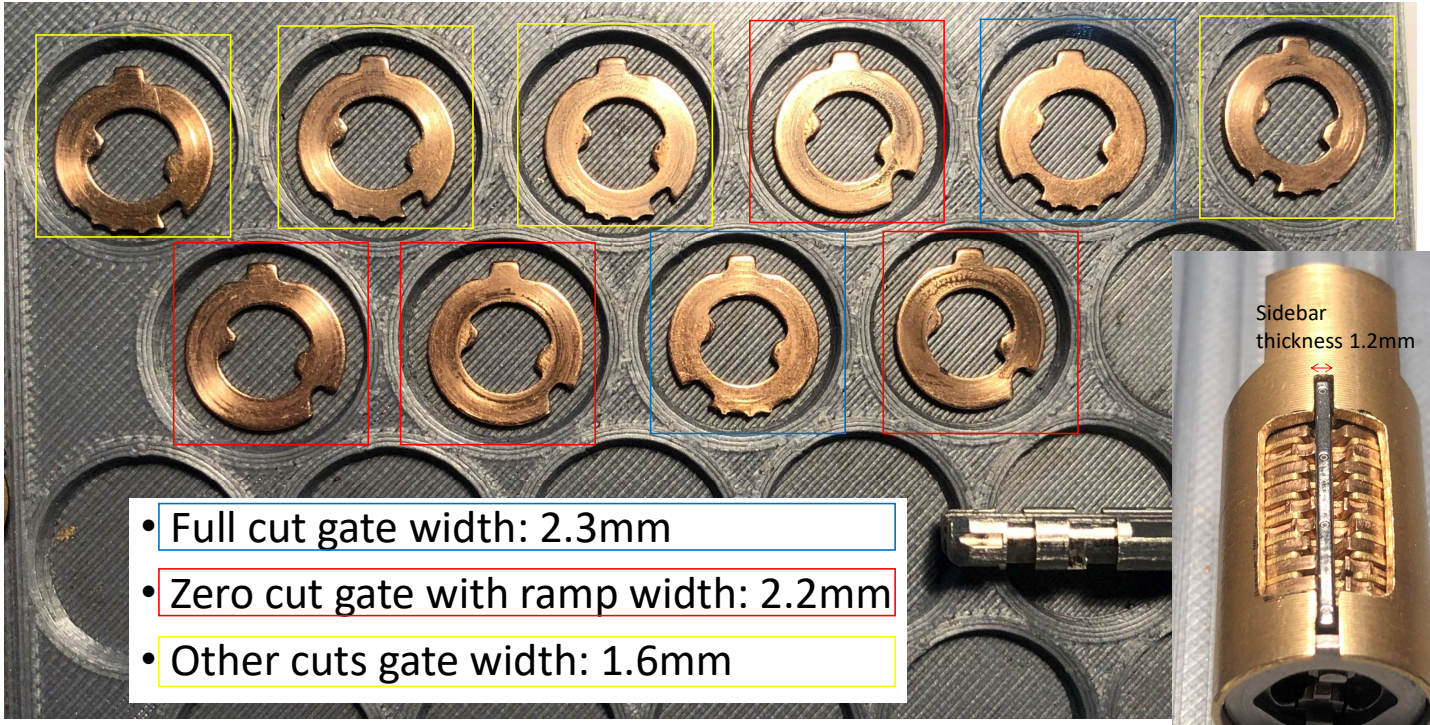
Abloy Easy improvements compared to Sento 3/3

Additional step in keyguiding element



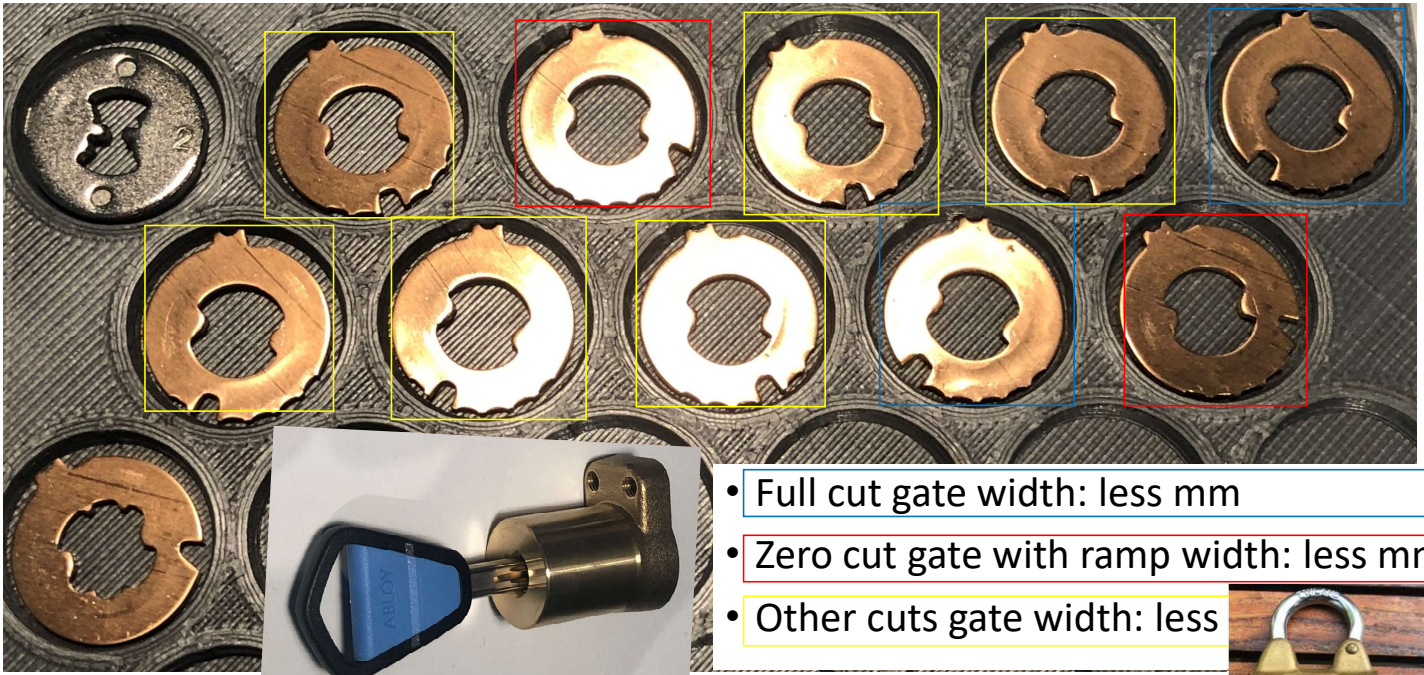


Discs of PL 330 and PL340 lock samples



In zero cut discs no false gates! (in these EUT)

Discs of door lock sample



- Full cut gate width: less mm
- Zero cut gate with ramp width: less mm
- Other cuts gate width: less

In zero cut discs there are false gates

Easy padlock vs Easy doorlock: differences

Door lock 12% harder to pick:

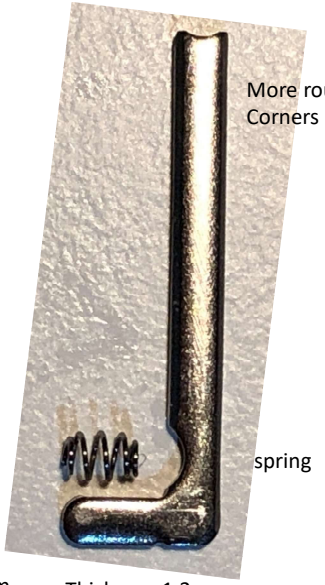
- Door lock discs has narrower gates
- Door lock discs has wider diameter: they jiggle less when at gate

Doorlock maybe less robust vs environmental conditions/dirty & harsh usage

Easy PL330 padlock sidebar

Thickness 1.2mm

Easy door lock sidebar



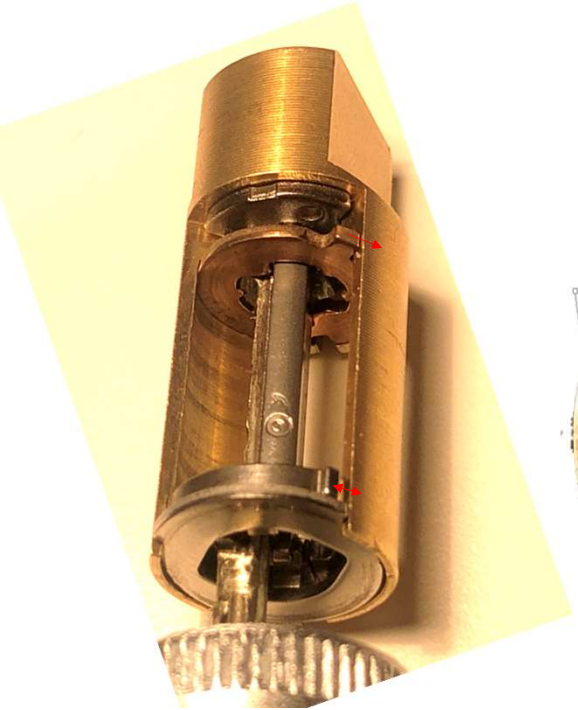
More rounded Corners

spring

Thickness 1.2mm

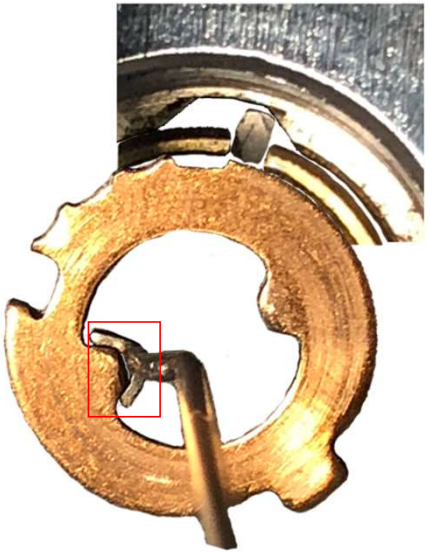
Abloy Easy pick design by Idanhurja

Remember slide 7: Picking method of Abloy locks (for them all types)

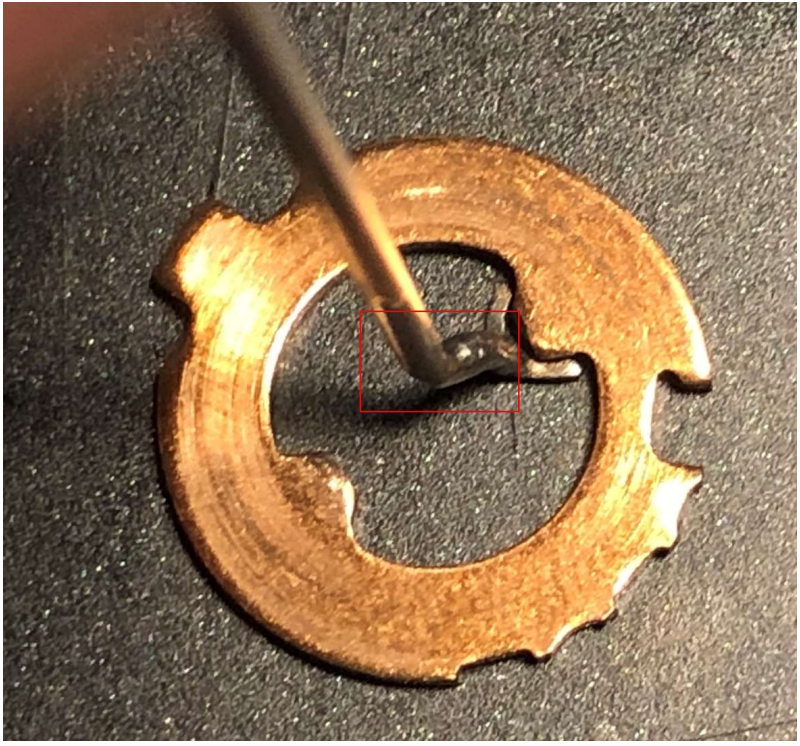


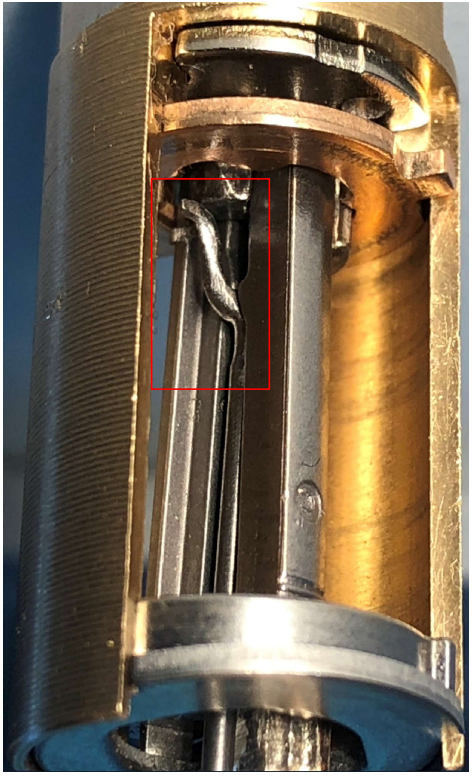
Rear tensioner

Center aligned 1 key way side using “shifted” picking tip

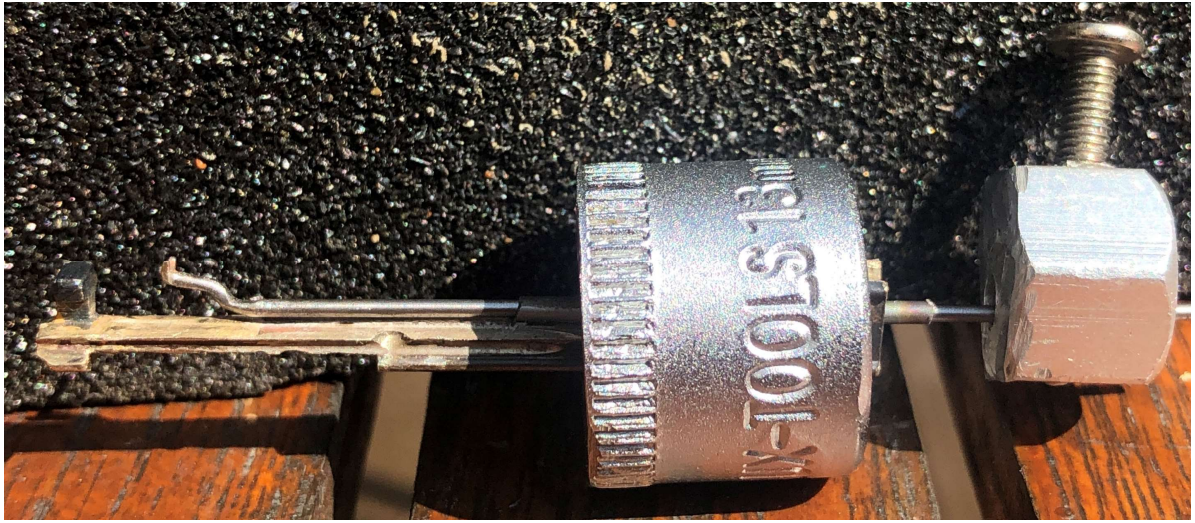


Abloy Easy “shifted” picking tip

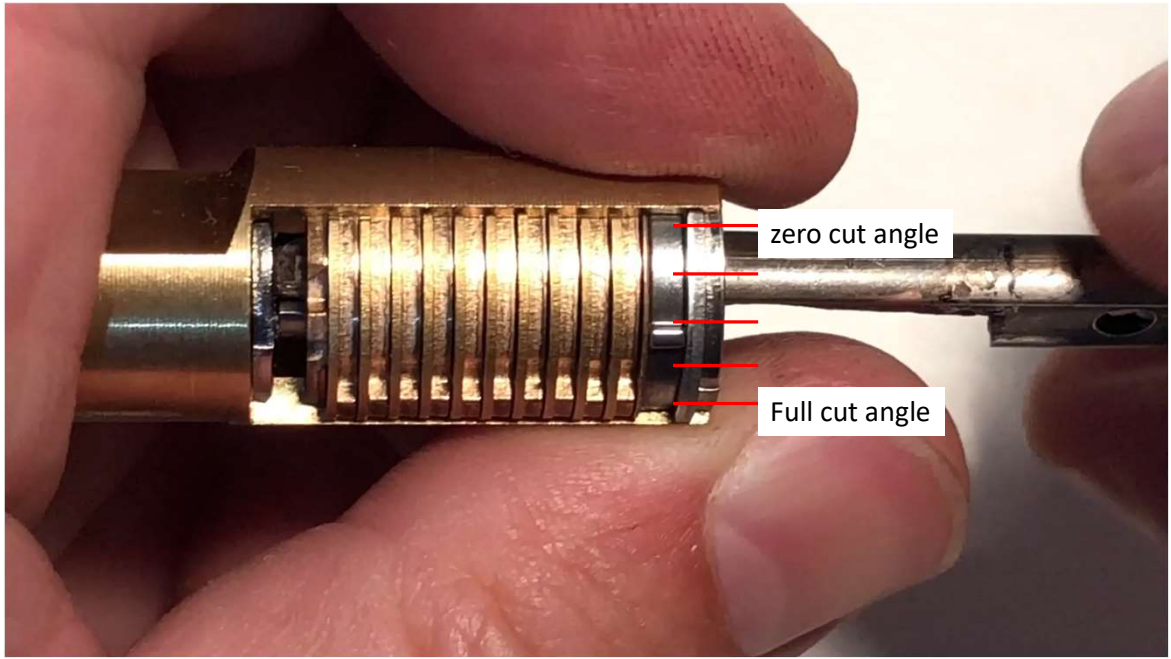


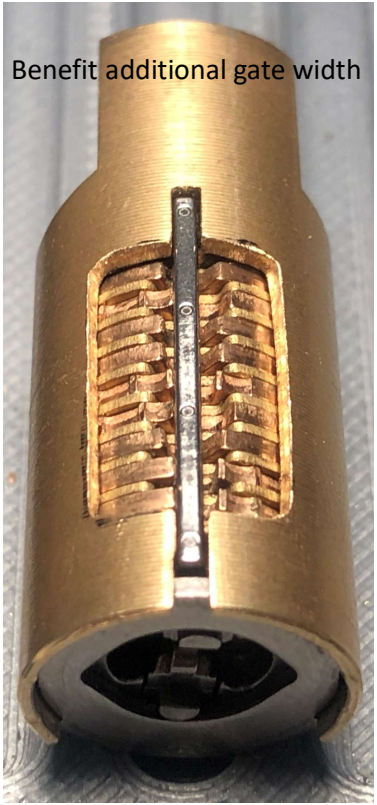


Build 0.3



Step1: Disc turning testing





Step2: Playing with a cutaway lock

Benefit:

- In zero cut discs there are no false gates
- In full cut disc, gate is wider
- Rest by jiggle/wobble testing: move a disc if its binding, if not continue with next disc
- And well, this is a known lock picking case

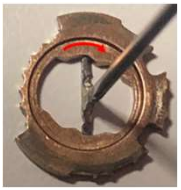
Step3: Abloy Easy picking: PL330 and a door lock

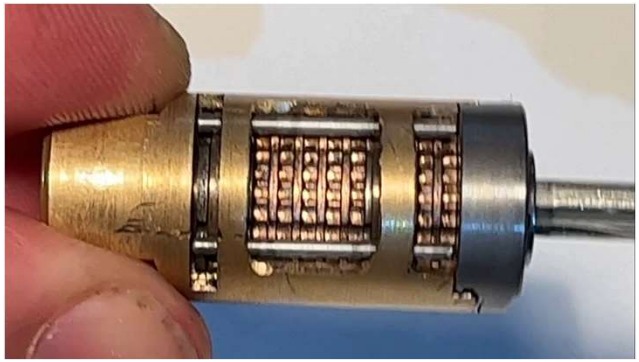
locksport: Abloy Easy picked & gutted with pick build 0.3 (part 3/3)

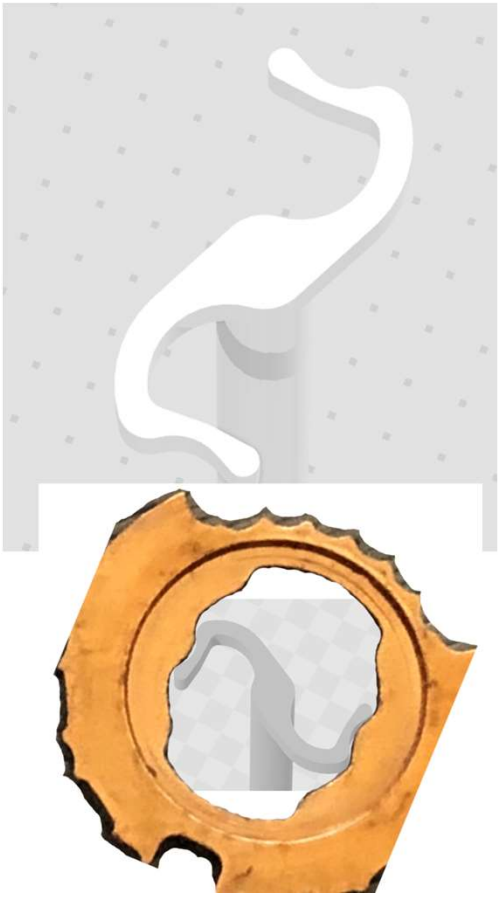
locksport: Abloy Easy cylinder lock picked & gutted

Abloy Protec2

- Atm too complicated for me, picking requires too much luck
  - Disc blocking system, I don’t know any convenient way to counter it
  - Turning angle limitation for my picking tip design.
  - I-shape pick not convenient when turning disc to counter clock wise dir







Thank you Lockcon!