mh: Electronic Locks—Bumping and Other Mischief

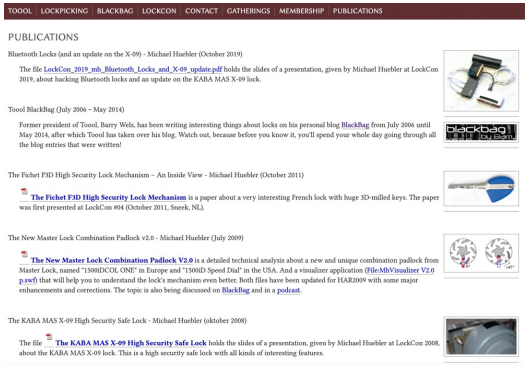
Recorded Talk:

https://youtu.be/h9JXXgYUqjU?t=1422

About mh (he/him)

- Lock enthusiast
  - Longtime passion for locks
  - Lock sport
  - Papers about locks
  - Conference Talks

https://toool.nl/Publications



Conference Talks on YouTube:
https://www.youtube.com/playlist?list=PLa9wckl5om107xq_yTQ8mooDxtLzqGy4Q

- COVID-19 SW project: Warn-App-Companion

https://github.com/mh-/corona-warn-companion-android

https://play.google.com/store/apps/details?id=org.tosl.warnappcompanion

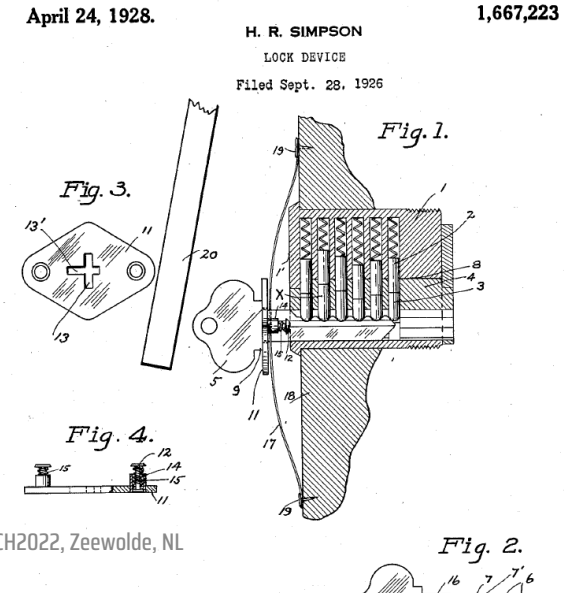
Attacks on Electronic Locks

	Mechanics	Electronics / Software
Lock-Specific	Turn-Before-Lockout Shimming High Pressure Air Magnets	Replay Bad Crypto Spiking Copy Lock-Specific Key Side Channels Liquids Brute-Force Extract Master Secrets Avoid Time Penalty Fault Injection
Generic	“Bumping”: Shock, Vibration High Speed Rotation / Acceleration, High Torque	Copy RFID Key High Voltage

“Bumping Locks”

- Well-known technique for **mechanical pin tumbler** locks:

H. R. Simpson, 1926:


April 24, 1928. 1,667,223

H. R. SIMPSON

LOCK DEVICE

Filed Sept. 28, 1926

Fig. 1.

Fig. 3.

Fig. 4.

Fig. 2.

Barry & Rop (Toool NL), 2005:

Bumping locks

How to open Mul-T-Lock (pin-in-pin, interactive, 7x7), Assa (6000 Twin), DOM (ix, dimple with ball), LIPS (Octro dimple), Evva TSC, ISEO (dimple & standard), Corbin, Pfaffenhain and a variety of other expensive mechanical locks without substantial damage, usually in under 30 seconds, with little training and using only inexpensive tools.

Barry Wels & Rop Gonggrijp
Toool - The Open Organization Of Lockpickers
barry@toool.nl, rop@toool.nl

Last revision: January 26, 2005

http://www.toool.nl/bumping.pdf

Abstract

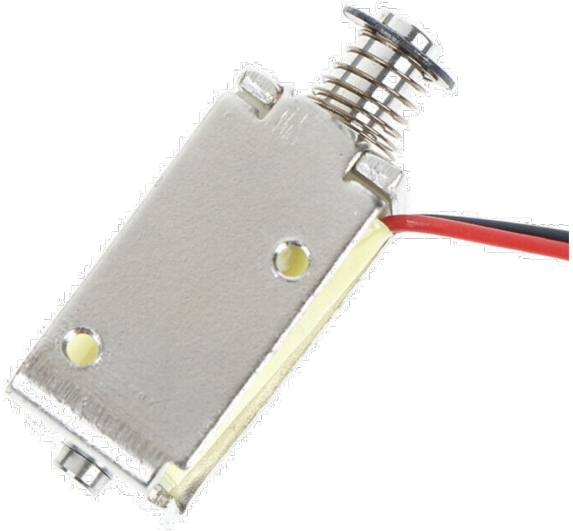
In this paper we describe an underestimated lock-opening technique by which a large variety of mechanical locks can be opened quickly and without damage by a relatively untrained attacker. Among other things we examine how this works, why

“Bumping Electronic Locks”

- It’s also a well-known technique for **cheap electronic safes:**

Video: Ray, muCCC

Well, solenoids…



- Solenoids are susceptible to mechanical shock and magnetic fields

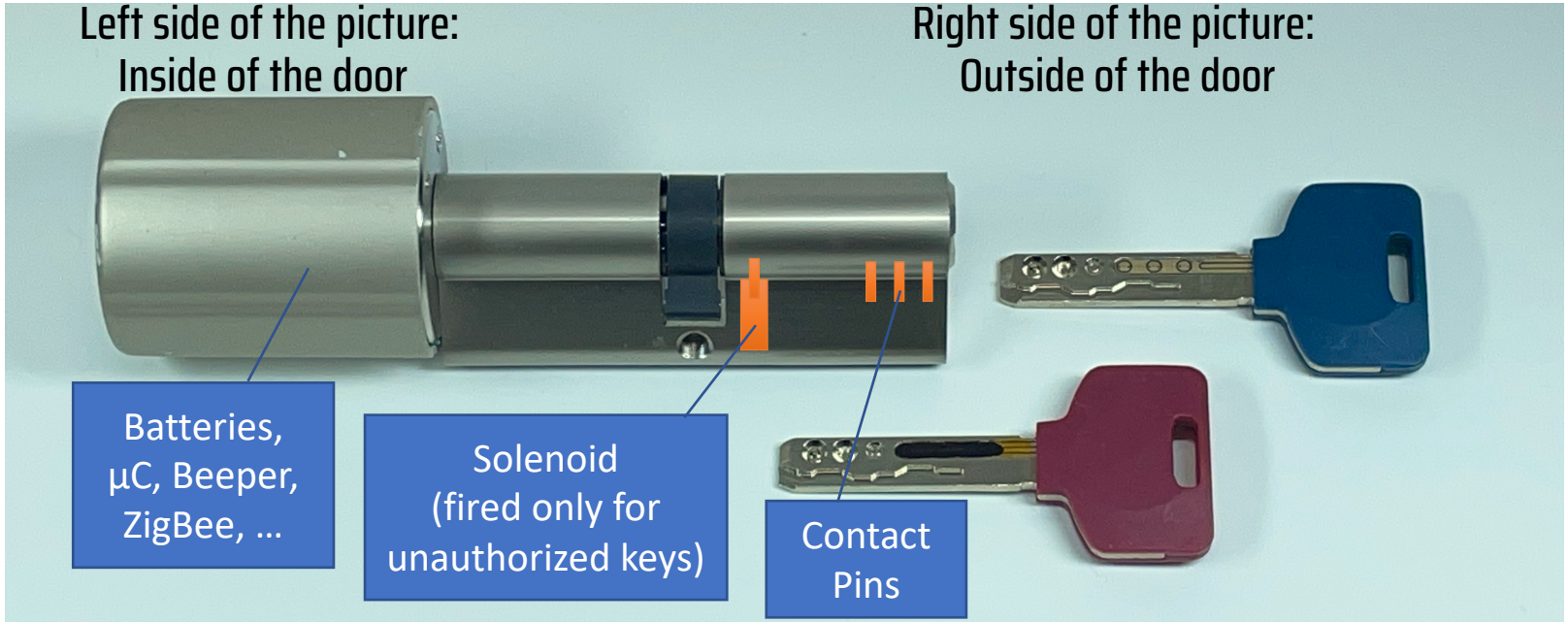
→ it's widely accepted that motors, e.g. with a lead screw, offer higher security

Image source:
https://www.ebay.de/itm/353568861746 (seller "exyfpo-89")

Specific Mechanical Attack

	Mechanics	Electronics / Software
Lock-Specific	Turn-Before-Lockout	
Generic		

A modern lock with a solenoid



Generic Mechanical Attack

	Mechanics	Electronics / Software
Lock-Specific		
Generic	Bumping	

But – it has a motor!

- This key box has a motor, which can pull down a spring-loaded latch.

(This apparently was the first version; more recent versions lock the latch in place when the box is closed.)

https://youtu.be/FLCHqalm2Y8?t=104

The problem is the spring…

To **move the mass** in a spring-mass system "**from the outside**", you have two main options:

- Collision (Conservation of Momentum)
- Inertia – move the outside system (with multiple hits == vibration, you may trigger a resonance)

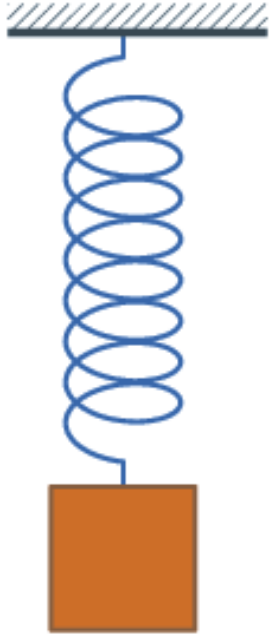


Image: By Oleg Alexandrov - self-made with Matlab. Converted to gif animation with the ImageMagick convert tool (see the specific command later in the code), Public Domain, https://commons.wikimedia.org/w/index.php?curid=2292351

Let’s test the theory

(1st Live Demo)

The demo lock cylinder

Battery, µC, Beeper, keypad, RFID, BLE, magnetic override lock - all in the outside knob

Demo Lock #1

Motor, with *axially spring-loaded clutch element*

Some FAQ

Q: Why test this in a door replica?

A: It's only a real attack vector, if enough torque can be transmitted to retract the bolt (at least in most locks...) – mounting it in a door lock proves that.

Q: If there's a motor drive, why does the electronic lock use springs?

A: Users will turn the knob to angles where the clutch cannot engage, or users might apply so much torque that the motor cannot disengage the clutch.

Q: Why are the springs so weak?

A: To reduce battery consumption of the lock.

Is this a real problem?

But this attack is not silent, and may leave some traces, e.g. dents, brass chips…

→ Depends on your use case.
In a lobby next to 24/7 security guards – probably ok.
On my house / garage / storage, and especially with VdS or SKG*** rating (supposed to resist drilling for a few minutes) – not ok.

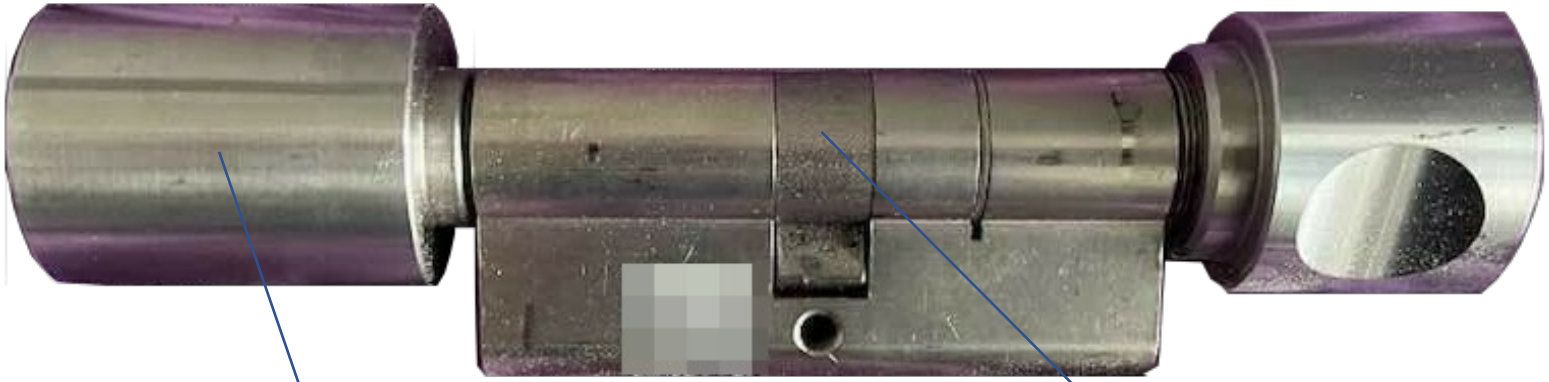
But the lock will fail (possibly secure) after a number of these attacks

→ Yes, that's annoying for me as a pen tester, but doesn't concern a real attacker who just wants to open *once*.

Thou shalt not use **axially** spring-loaded clutch elements in thy lock designs!

Where it all started...

Demo Lock #2

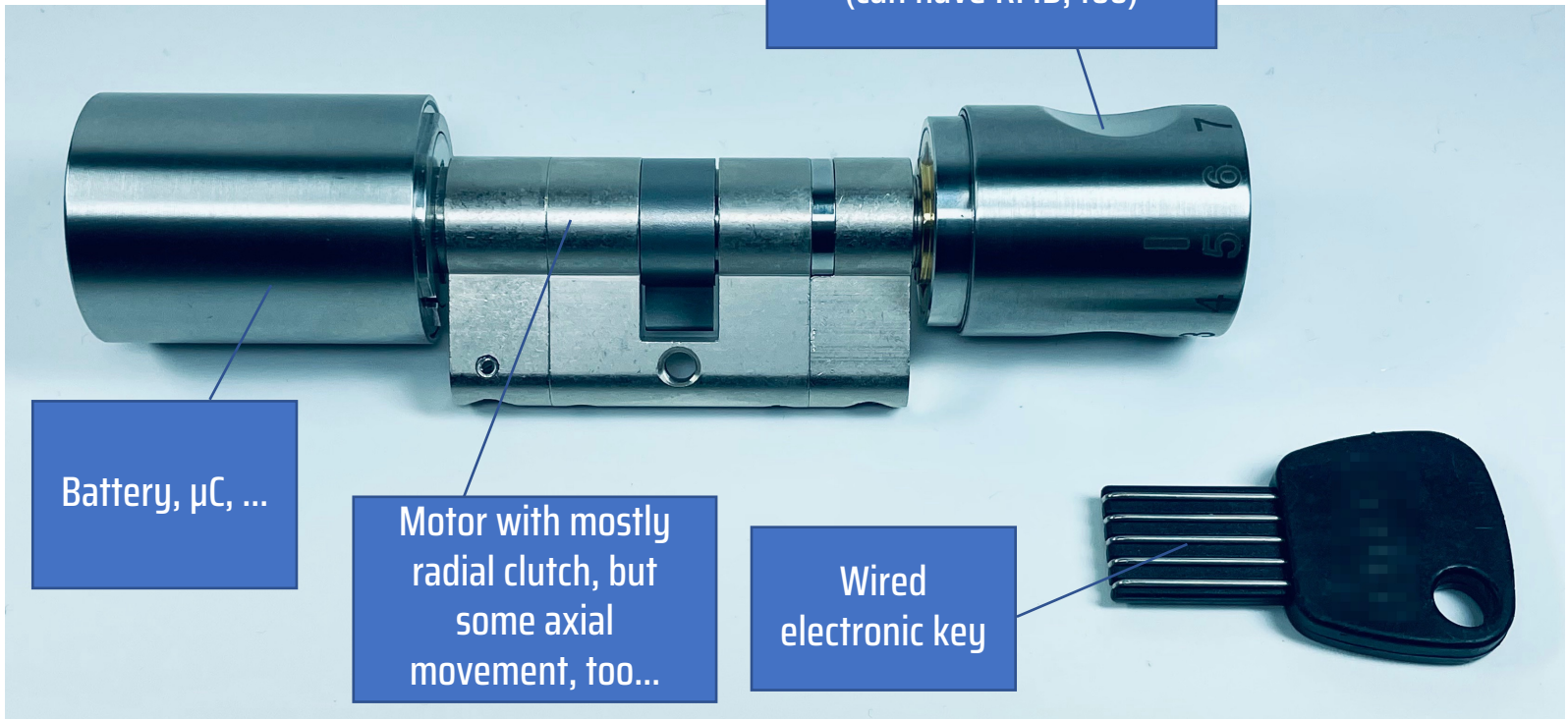


Battery, µC, ...

Solenoid-based clutch

Wired Electronic Key

Demo Lock #3



Specific Electronic Attack

	Mechanics	Electronics / Software
Lock-Specific		Bad Crypto Avoid Time Penalty
Generic		

Cryptologically encrypt it like it's 1999!

- "Read and copy protected through cryptologically encrypted dialogue procedure"
- BUT: Key only has a little PIC controller, what would you expect?
- Standard Reverse Engineering procedure
  - Use logic analyzer to record transactions → Understand physical layer
  - Write Logic2 low-level analyzer → Understand logical layer: 40 bits challenge-response
  - Make analyzer based on Teensy → Understand "encryption" (see next slide)
  - Make key simulator based on Teensy → Copy keys.
- (Optional: Try to enter code digits via the key interface, find time-penalty bug.)

The People Who Stare at Bits...

Challenge:						Response:					
1111111111	00010001	00010001	00010001	00010001	00010001	68d28a0c7e	01101000	11010010	10001010	00001100	01111110
1111111112	00010001	00010001	00010001	00010001	00010010	58b18d8c66	01011000	10110001	10001101	10001100	01100110
1111111113	00010001	00010001	00010001	00010001	00010011	48908f0c6e	01001000	10010000	10001111	00001100	01101110
1111111114	00010001	00010001	00010001	00010001	00010100	3877828c56	00111000	01110111	10000010	10001100	01010110
1111111115	00010001	00010001	00010001	00010001	00010101	2856800c5e	00101000	01010110	10000000	00001100	01011110
1111111116	00010001	00010001	00010001	00010001	00010110	1835878c46	00011000	00110101	10000111	10001100	01000110
1111111117	00010001	00010001	00010001	00010001	00010111	0814850c4e	00001000	00010100	10000101	00001100	01001110
1111111118	00010001	00010001	00010001	00010001	00011000	f9fb9c8c36	11111001	11111011	10011100	10001100	00110110
1111111119	00010001	00010001	00010001	00010001	00011001	e9da9e0c3e	11101001	11011010	10011110	00001100	00111110
111111111a	00010001	00010001	00010001	00010001	00011010	d9b9998c26	11011001	10111001	10011001	10001100	00100110
111111111b	00010001	00010001	00010001	00010001	00011011	c9989b0c2e	11001001	10011000	10011011	00001100	00101110
111111111c	00010001	00010001	00010001	00010001	00011100	b97f968c16	10111001	01111111	10010110	10001100	00010110
111111111d	00010001	00010001	00010001	00010001	00011101	a95e940c1e	10101001	01011110	10010100	00001100	00011110
111111111e	00010001	00010001	00010001	00010001	00011110	993d938c06	10011001	00111101	10010011	10001100	00000110

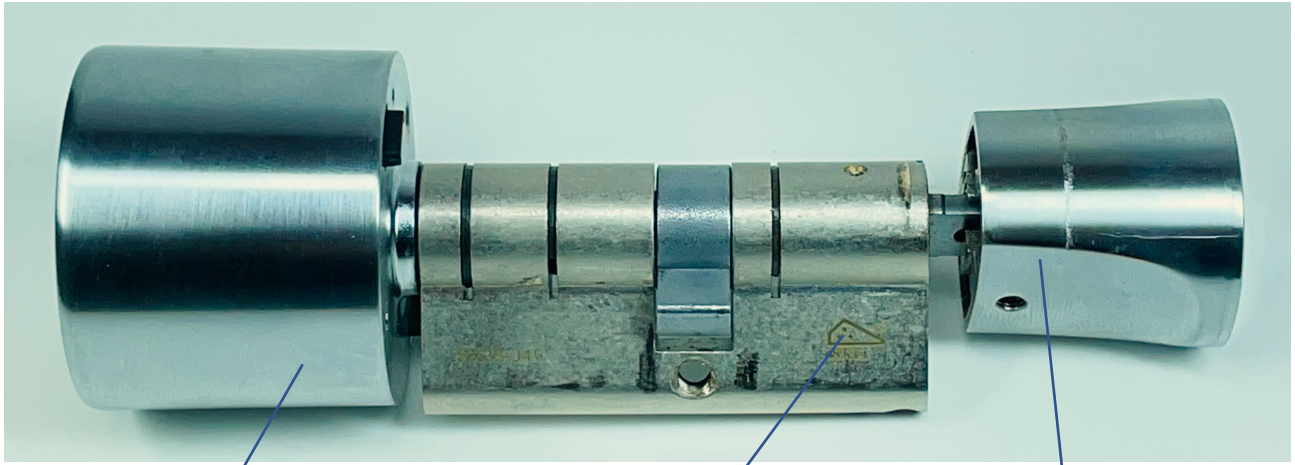
- Not a lot of diffusion...
  (Claude Shannon, 1945: a single bit change in the plaintext should cause about half of the bits in the ciphertext to change)
- The whole procedure can be implemented by two Linear Feedback Shift Registers.
- Thank you: Ray, mkie, Sec, Robert, Avanti, and all the others from muCCC and SSDeV!

Generic Mechanical Attack

	Mechanics	Electronics / Software
Lock-Specific		
Generic	Bumping	

A very strong smart lock cylinder

Demo Lock #4

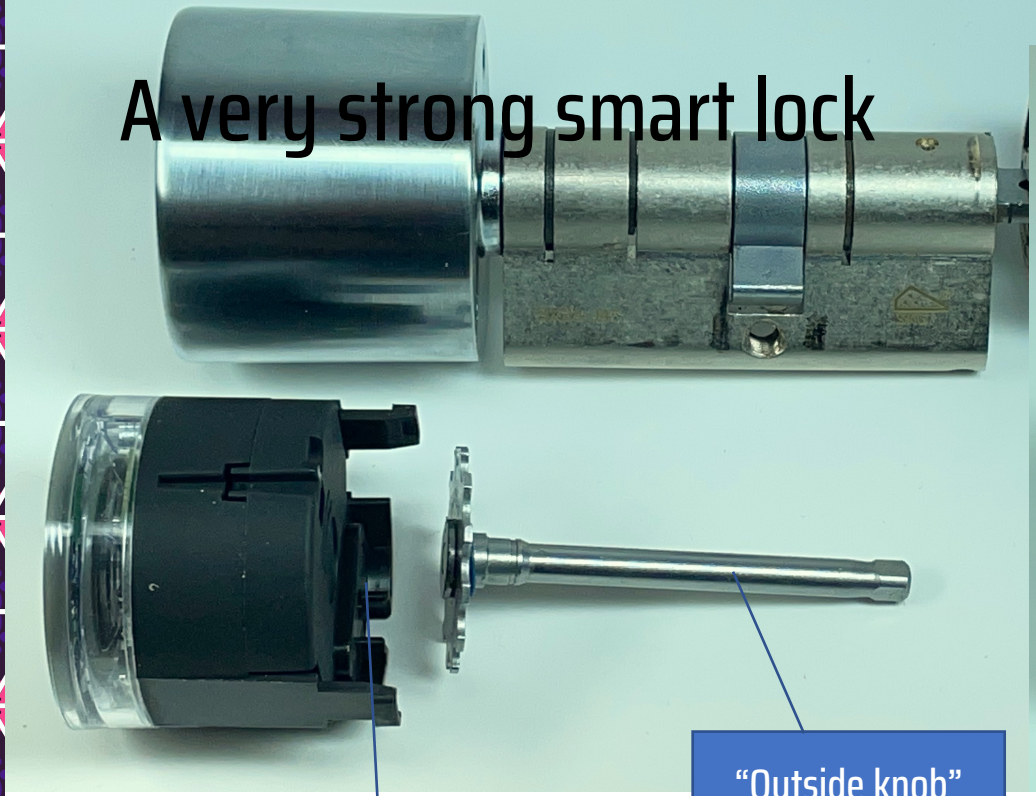


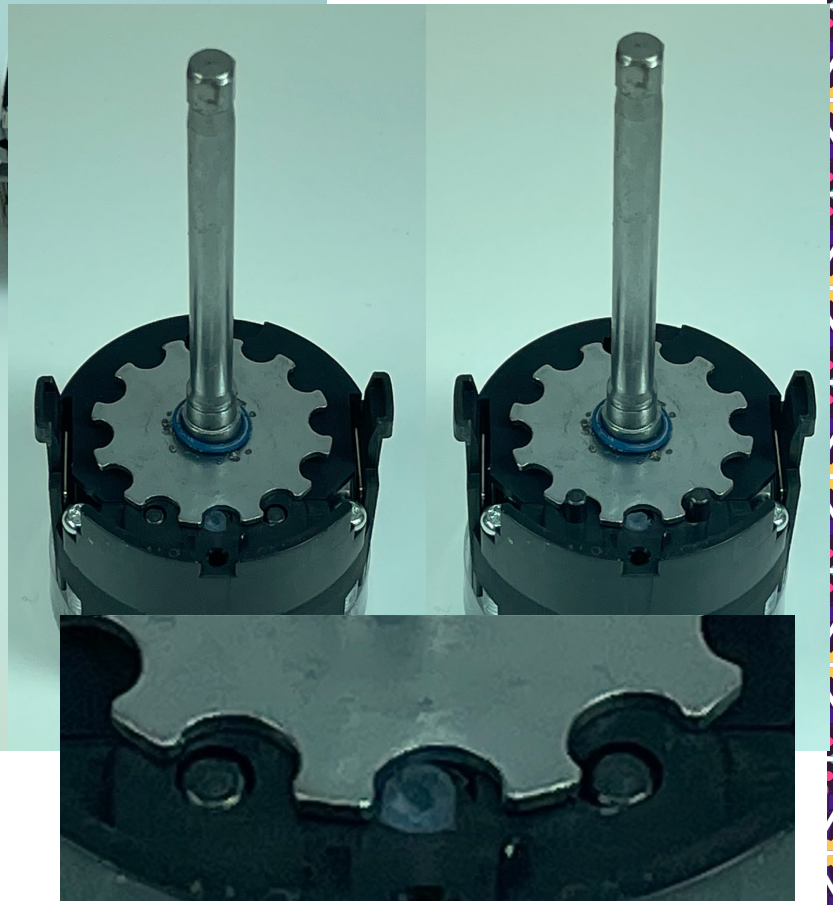
Battery, µC, Beeper, BLE, ...

Strong drill protection

Completely “passive” outside

A very strong smart lock



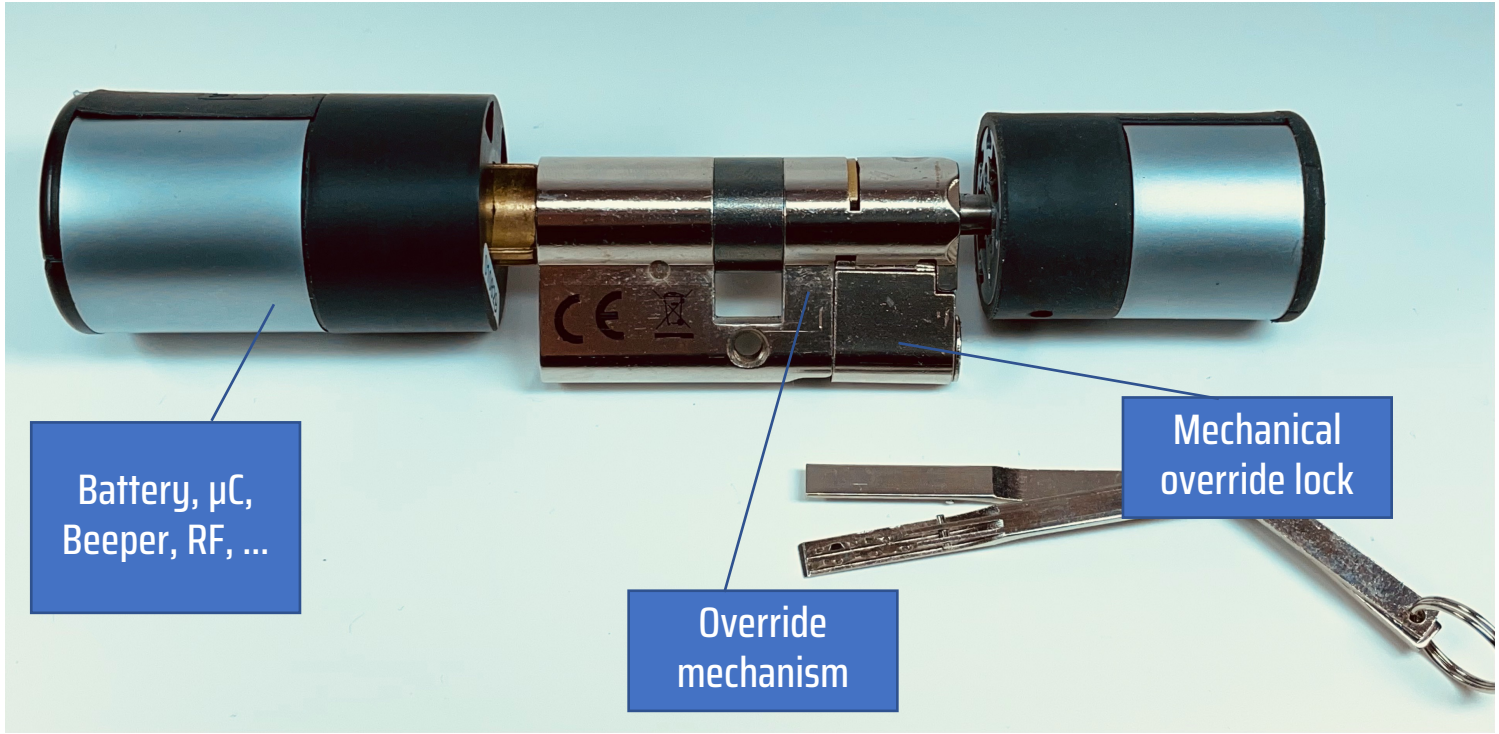


Electronics module with two *axially spring-loaded clutch pins*

“Outside knob” axis

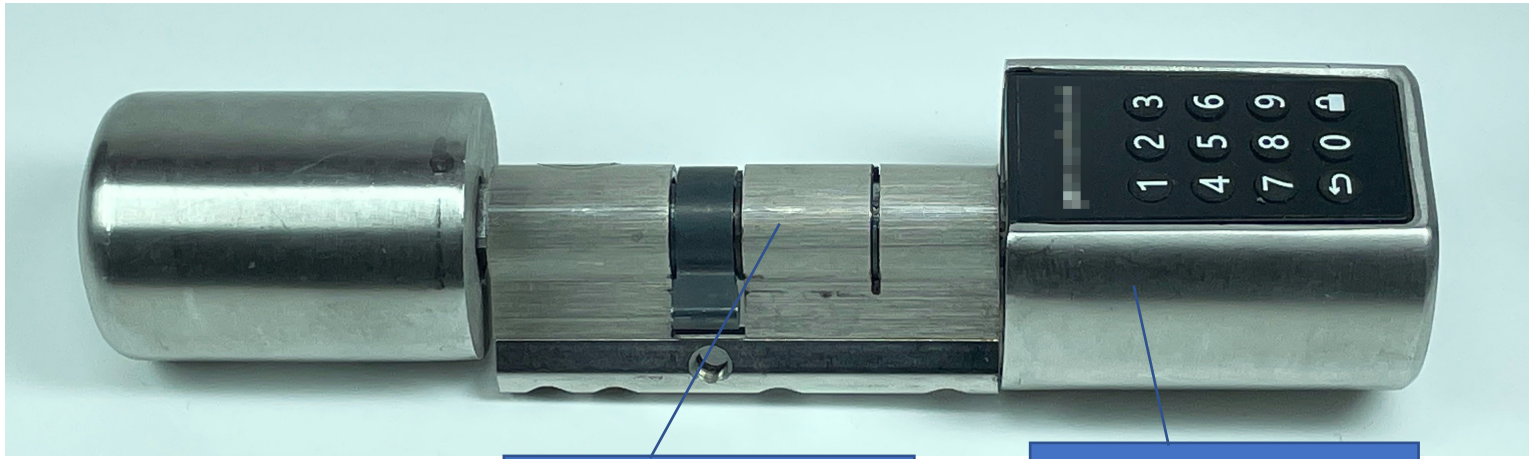
Radio Controlled, with Mechanical Override

Demo Lock #5



A very cheap electronic lock cylinder

Demo Lock
#6, #7

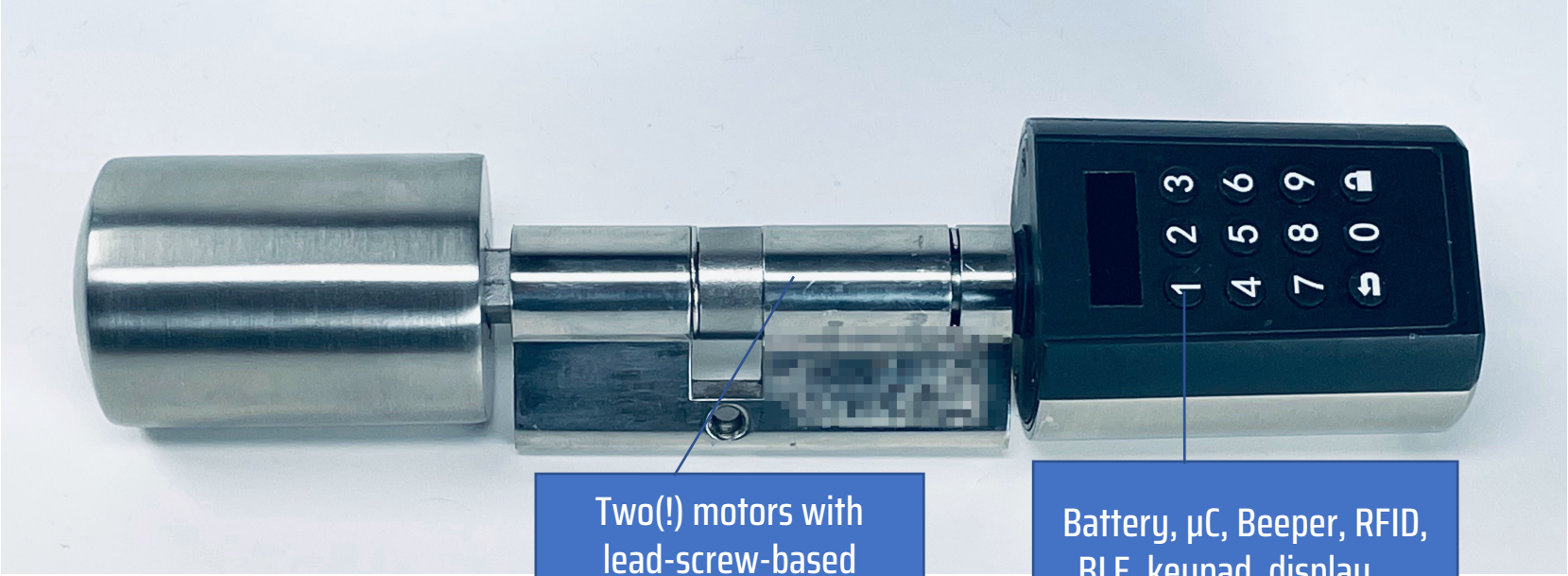


Motor with
lead-screw-based
spring-loaded clutch

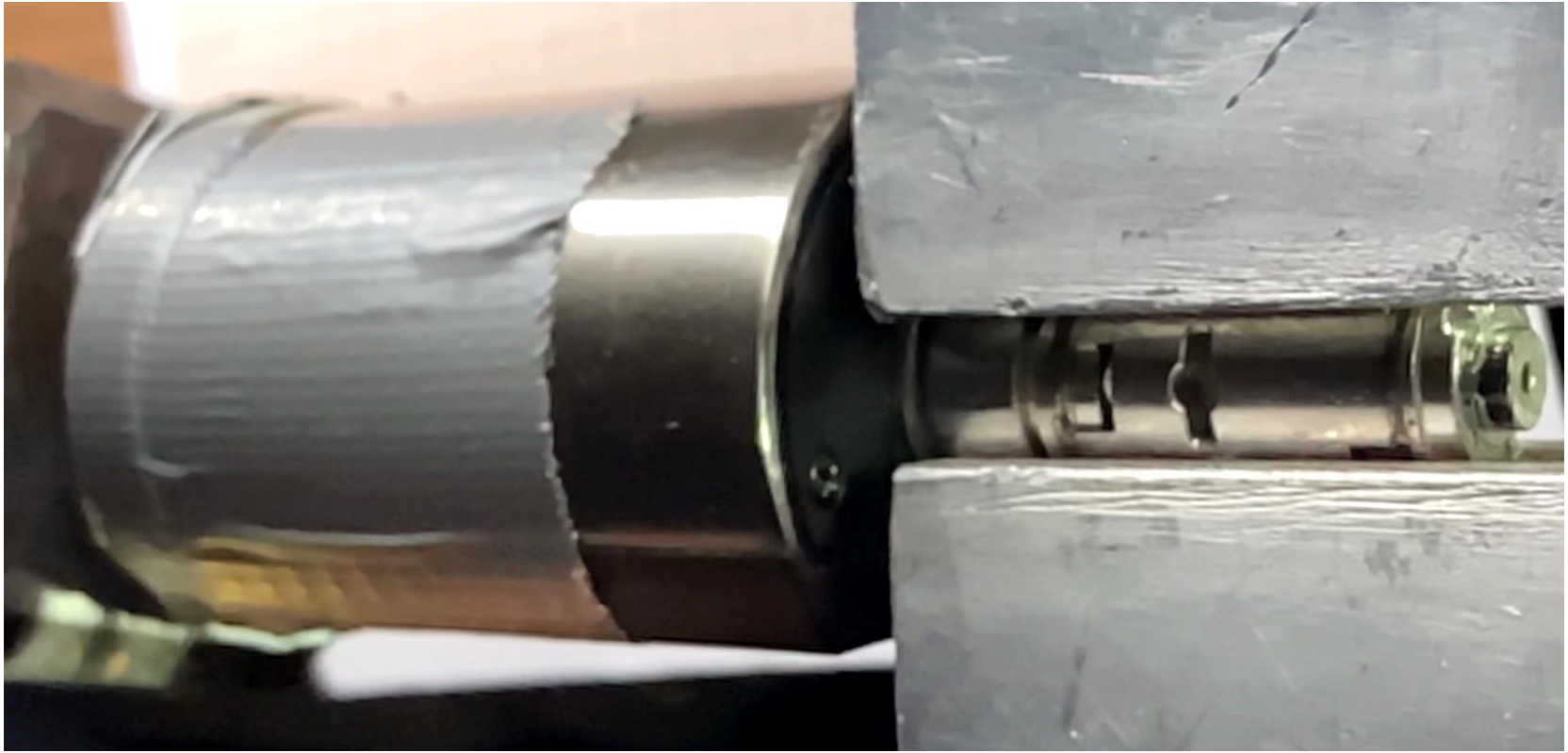
Battery, µC, Beeper,
keypad, ...
All in the outside knob

Next generation

Demo Lock #8



Slow motion sequence



Another live “bumping” test

(2nd Live Demo)

Tools

Rotary Hammer (electro-pneumatic)

No Name, **~1.5 J**, ~45 EUR incl. battery, charger

[CZ] FASGet 2.2J 10000bpm Electric Jack Hammer

- 19800mAh Battery Capacity
- 2.2J Strong Endurance
- Powerful Cylinder Impact

$43.99 ~~US$134.99~~

Email Only

Makita DHR243, **2.0 J**, ~200 EUR + battery

PABH 20-Li B2 or similar, **1.0 J**, ~30..40 EUR + battery

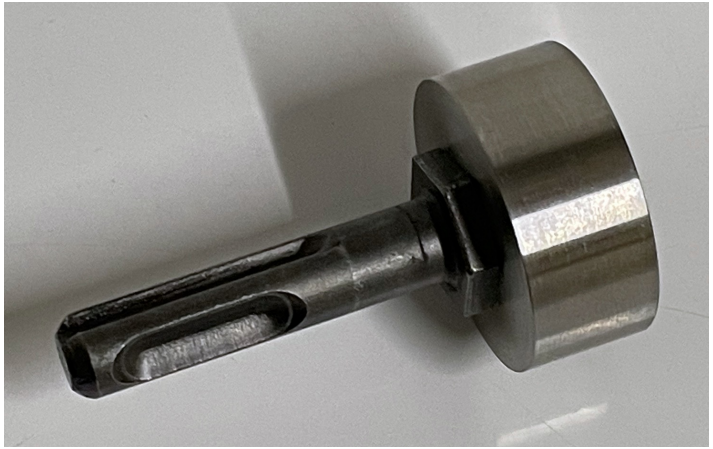
Images: Banggood, Makita, Lidl

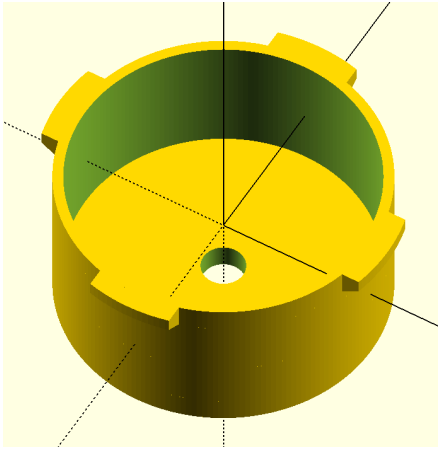
Tools

SDS Plus Adapter

+ TPU Cover

(3mm, 100% percent infill)

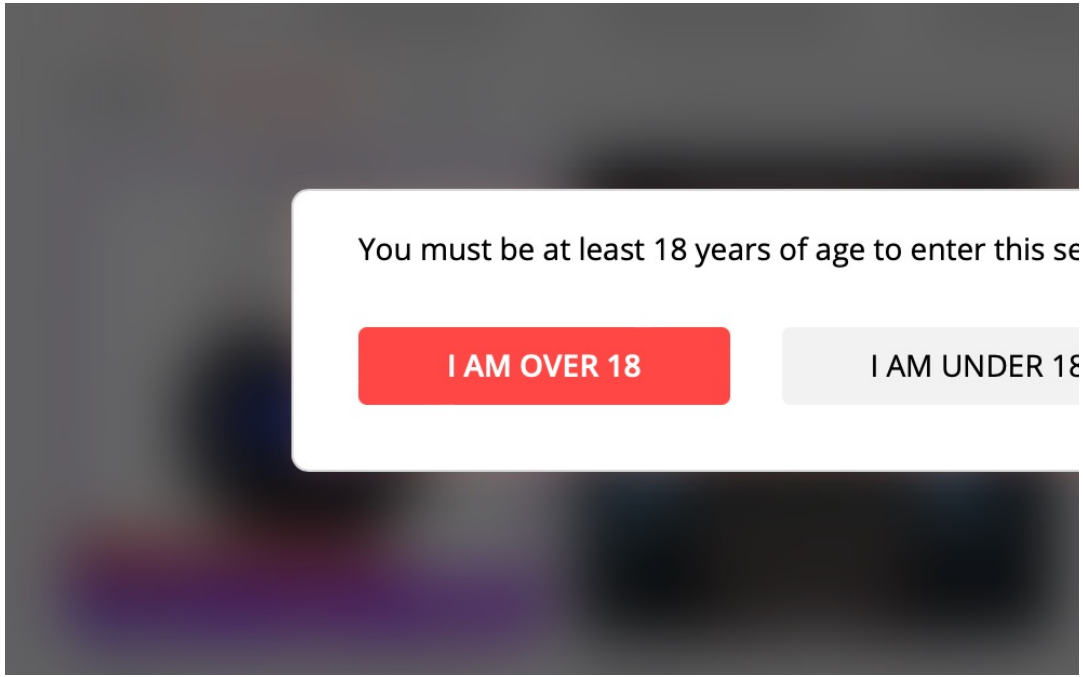


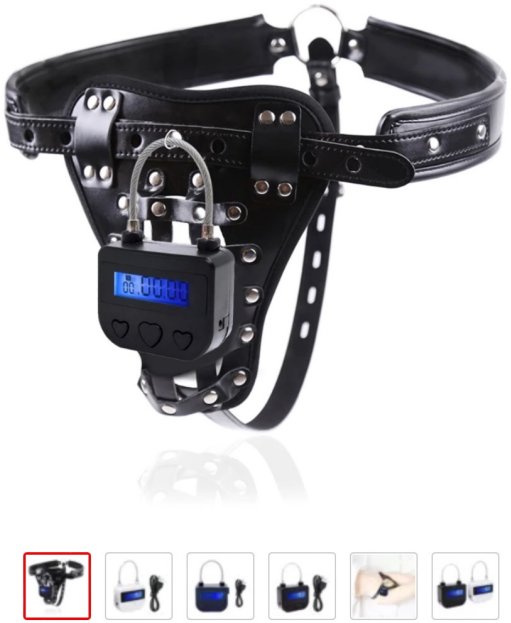


+ Duct tape, or

+ 3D Prints from TPU

Other Mischief...





Generic Electronic Attack Attempt

	Mechanics	Electronics / Software
Lock-Specific		
Generic		Fault Injection

Resetting locks

- Tesla Coil “EMP Generator”
- Advertised as a device that can make slot machines pay out money
- Can mainly disturb and/or reset, only the simplest electronic devices.
  Works on alarm clocks, calculators.

(There may be more vulnerable locks out there)


Little Black Box / Tesla Coil in action unlocking Singgate China Digital Lock!


No worry the tesla circuit provide you high security

Generic Mechanical Attack

	Mechanics	Electronics / Software
Lock-Specific	Rotating Magnet	
Generic		

Influence the motor from the outside

- Reverse the polarity of the motor magnet from the outside, then cause a “closing” action.
- “Pull” the iron core of a motor with a strong (rotating) magnet.
- Turn a plug with a motor very fast (→ centrifugal force), accelerate / decelerate very fast (→ inertia).

Thanks for your attention!

- Meet me at
  - MCH2022
    - **Village: Lockpicking (next to Stage Clairvoyance)**
    - DECT: 6464
  - LockCon – 25..28 Aug 2022, Baarlo, NL
  - SSDeV, muCCC (Munich, Germany)
  - mh@tosl.org