The KABA MAS X-09™ High Security Safe Lock.

A Hands-On Presentation at LockCon 2008.

Sneek, The Netherlands, 10 Oct 2008, Michael U. Huebler.

TOOOL
The Open Organisation Of Lockpickers

LockCon 2008

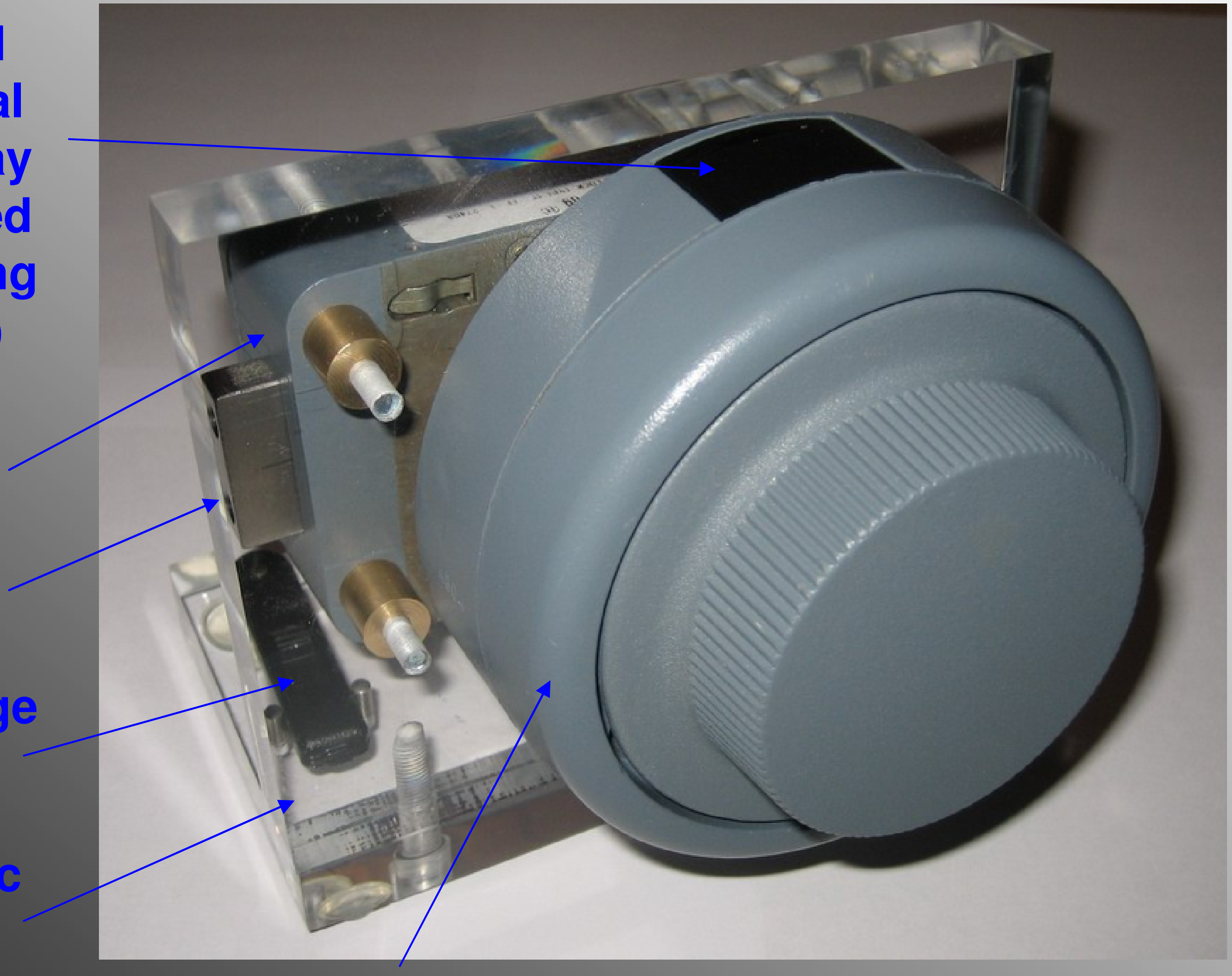
Presentation outline.

- Overview and features.
- Looking inside – why it's secure against bumping and vibration.
  - The motor.
  - The gears / slide / bolt mechanism.
  - A brief look into the other components.
- Why it's secure against a lot of other attacks.
- Links to patents etc.
- Questions.

The KABA MAS X-09™. Overview and features.

- An electronic combination lock for military top-secret containers.
- Self-powered: No batteries required. Turning the dial powers the lock.
- Easy to use: A display shows the combination you are dialing (3 x 2 = 6 digits) and symbols.
- Audit trail: The lock counts the number of openings as well as unsuccessful attempts.
- Dual-responsibility and supervisor-subordinate modes can be configured (two 6-digit combinations required).
- A “lock on back cover” (LOBC) pin tries to keep the lock itself locked up.
- 3rd generation, improved over the original X-07™ and X-08™.

The demo lock.
The main parts and how to use it.



Liquid Crystal Display (limited viewing angle)

Lock case

Bolt

Change key

Acrylic demo stand

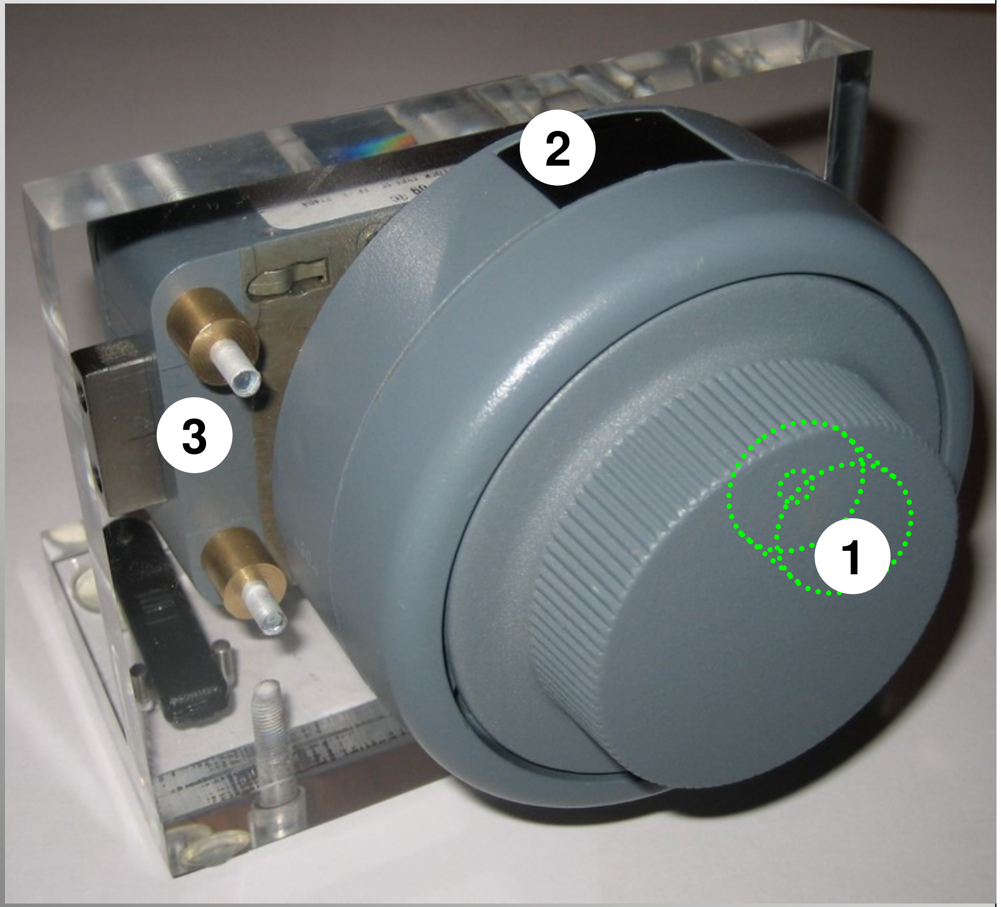
Dial ring

To dial 123456:

- Turn left (power the lock) until you see a (random) value on the display.
- Continue to turn until 12 is shown.
- Turn right to 34.
- Turn left to 56.
- Turn right. “OP” will be displayed and the lock will open.

The general concept.
Basic operation principle.

1. A generator in the dial ring provides electrical energy as well as direction and step signals to a microcontroller in the lock case.
2. The LCD shows the dialed combination.
3. A motor in the lock case couples the bolt mechanism to the dial, and the bolt can be retracted.



Presentation outline.

- Overview and features.

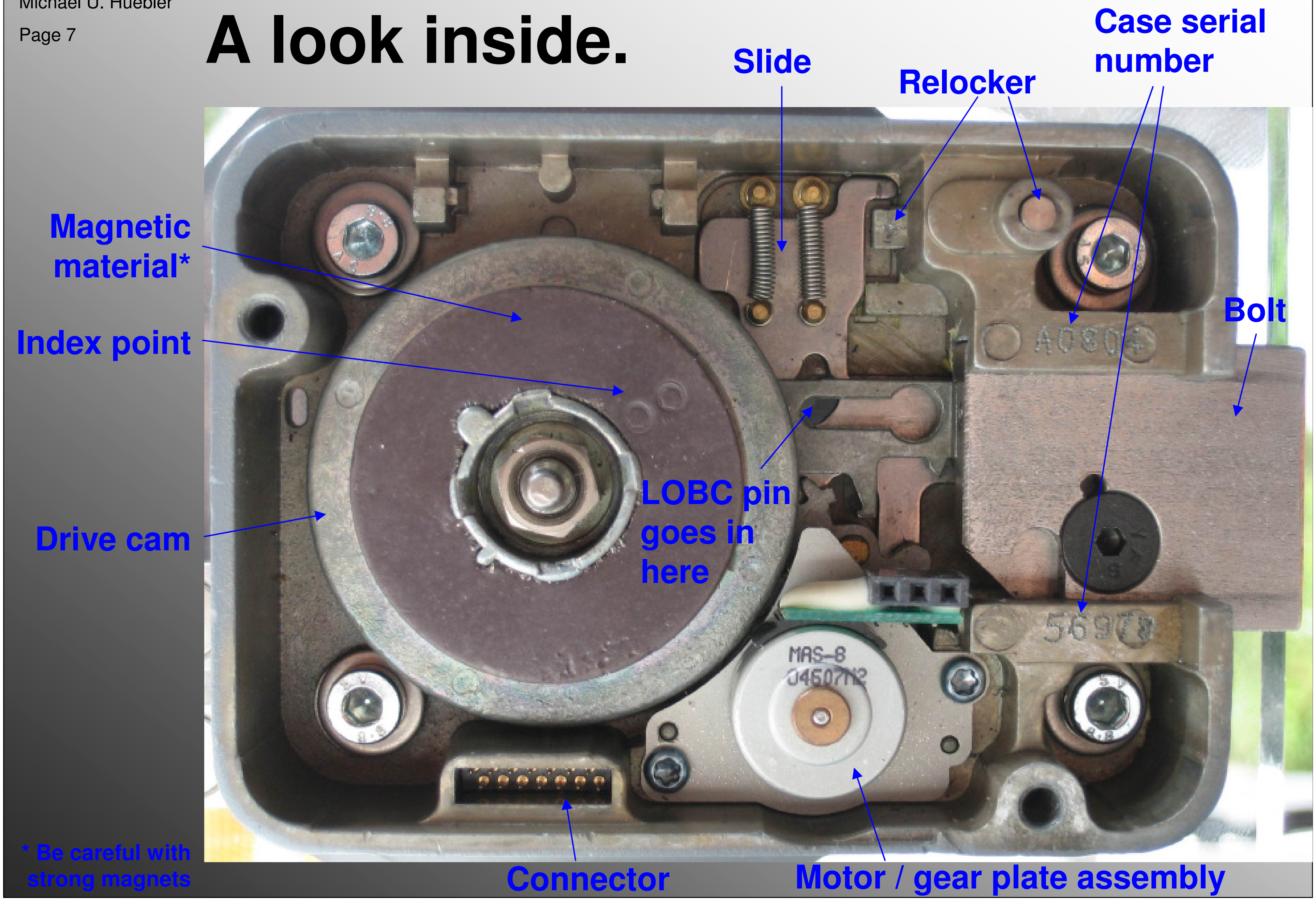
- Looking inside – why it’s secure against bumping and vibration.
  - The motor.
  - The gears / slide / bolt mechanism.
  - A brief look into the other components.

- Why it’s secure against a lot of other attacks.

- Links to patents etc.

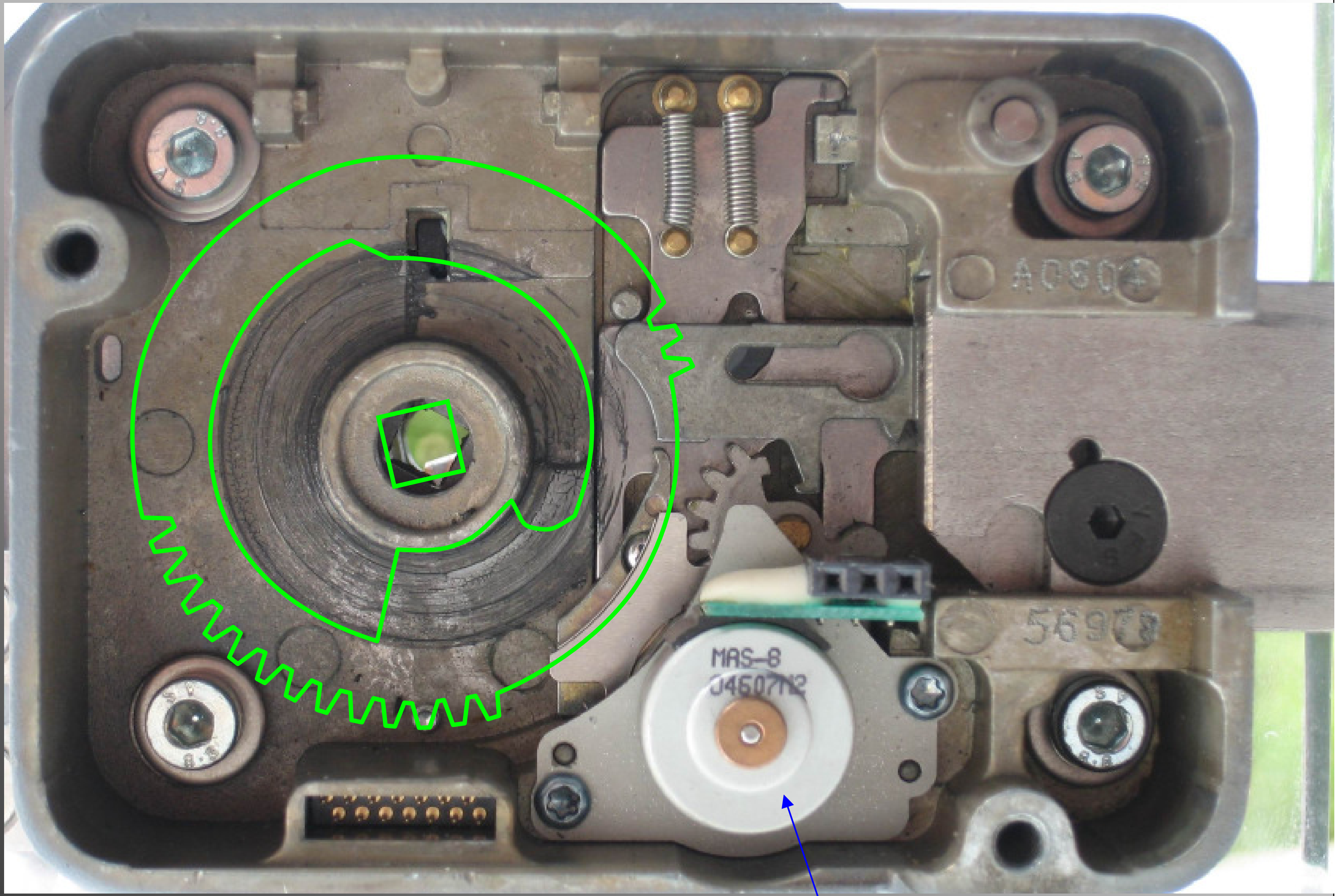
- Questions.

The lock case.
A look inside.



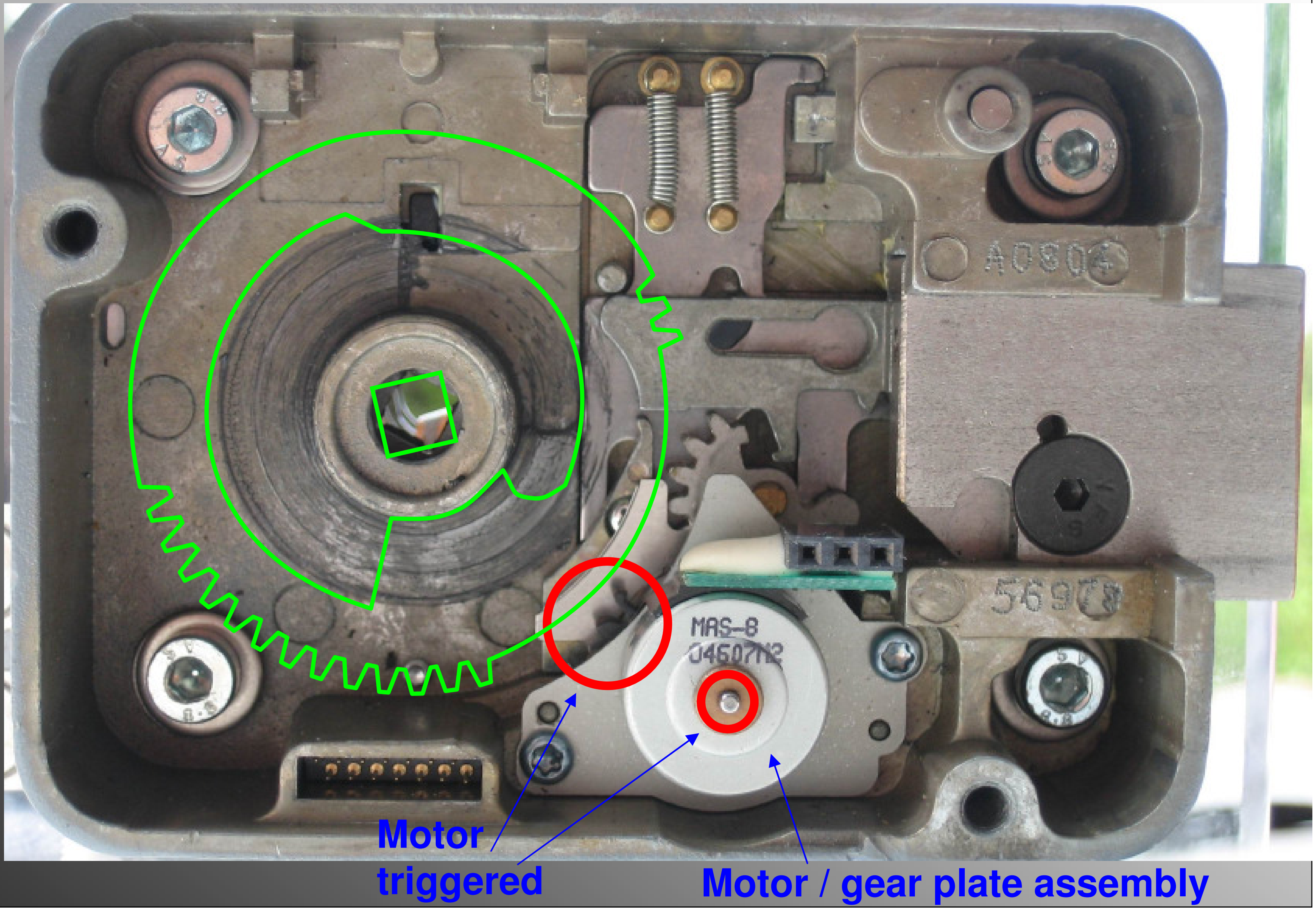
* Be careful with strong magnets

Drive cam removed.

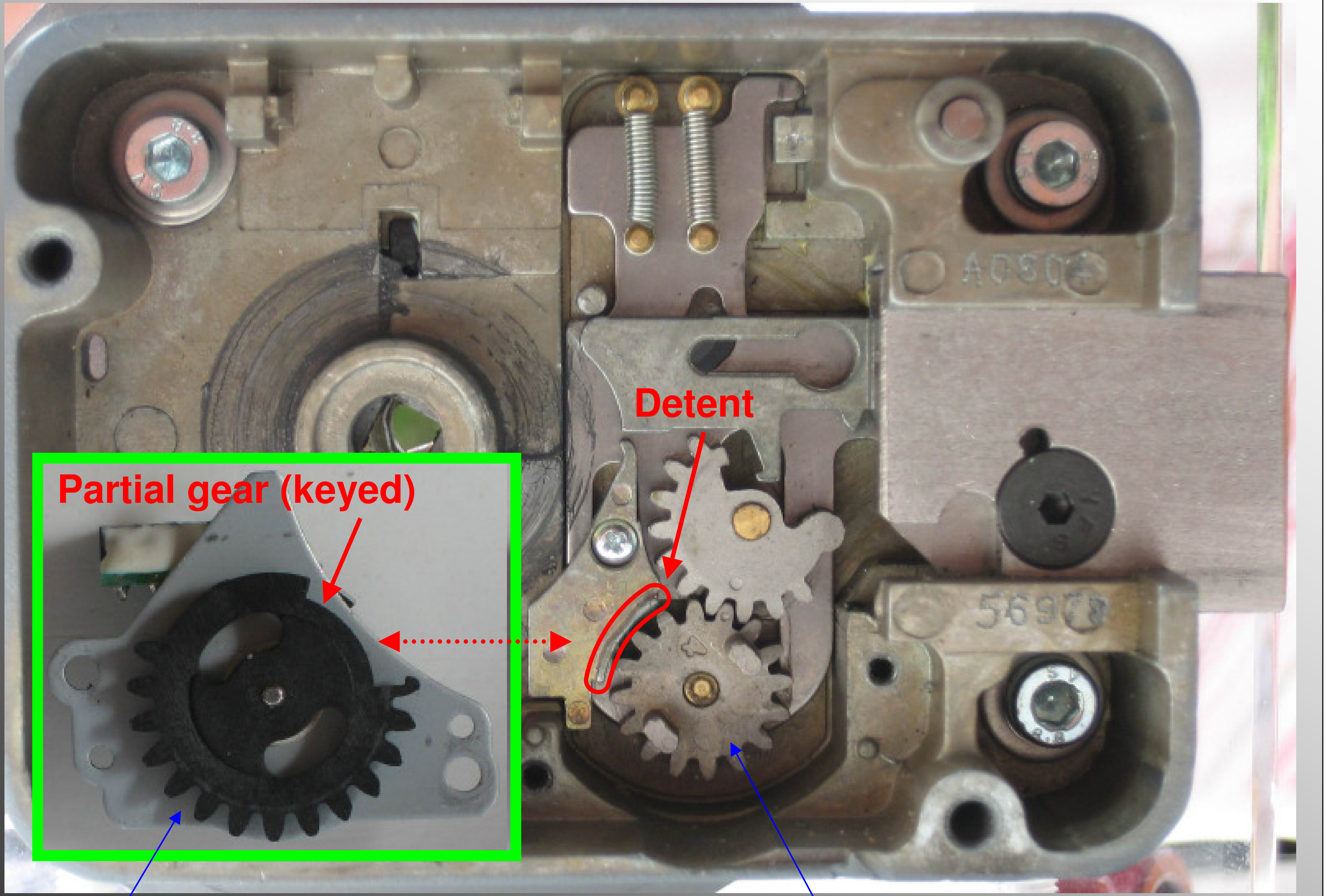


Motor / gear plate assembly

Motor triggered.

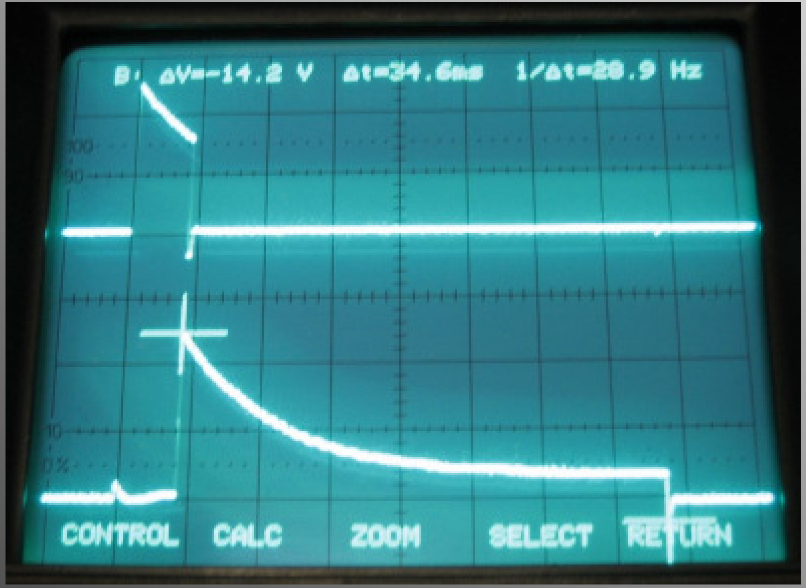


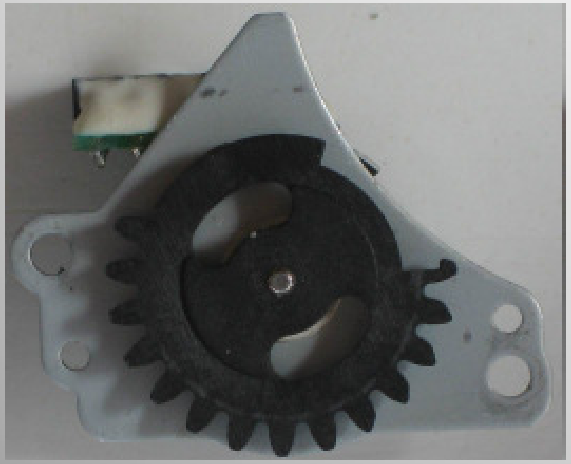
The motor. Secure against bumping and vibration.



The motor. Electrical parameters.

- Patent No. US6731025
- Needs to pull AND turn the gear wheel.
- The motor has 2 electromagnetic coils, the lock generates 2 current pulses to activate them sequentially:



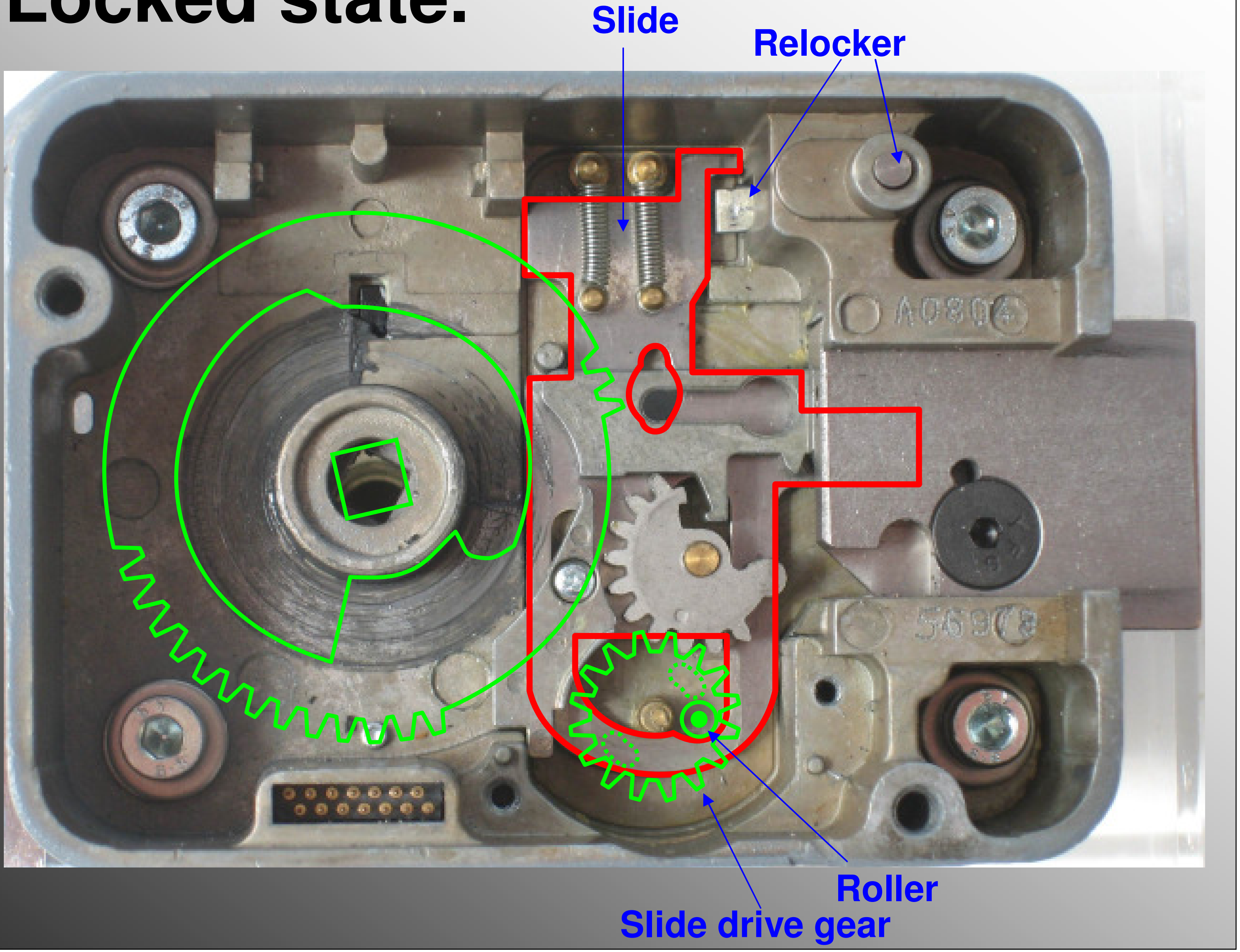


- Powering both coils at the same time also works fine.
→ Motor demonstrator: 9V battery, capacitor, switch that connects the capacitor to either battery (‘charge’) or coils (‘trigger’).

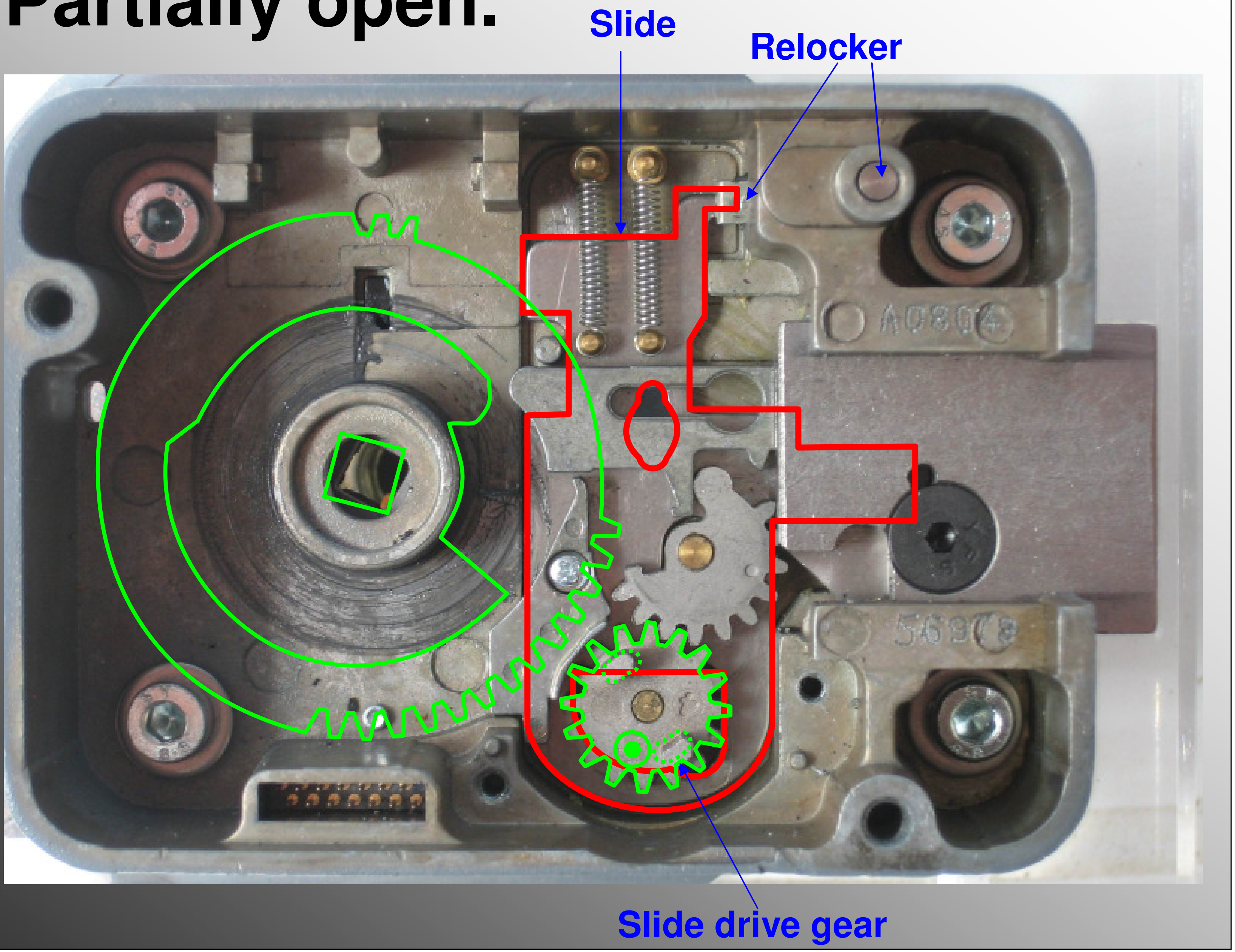
Presentation outline.

- Overview and features.
- Looking inside – why it's secure against bumping and vibration.
  - The motor.
  - The gears / slide / bolt mechanism.
  - A brief look into the other components.
- Why it's secure against a lot of other attacks.
- Links to patents etc.
- Questions.

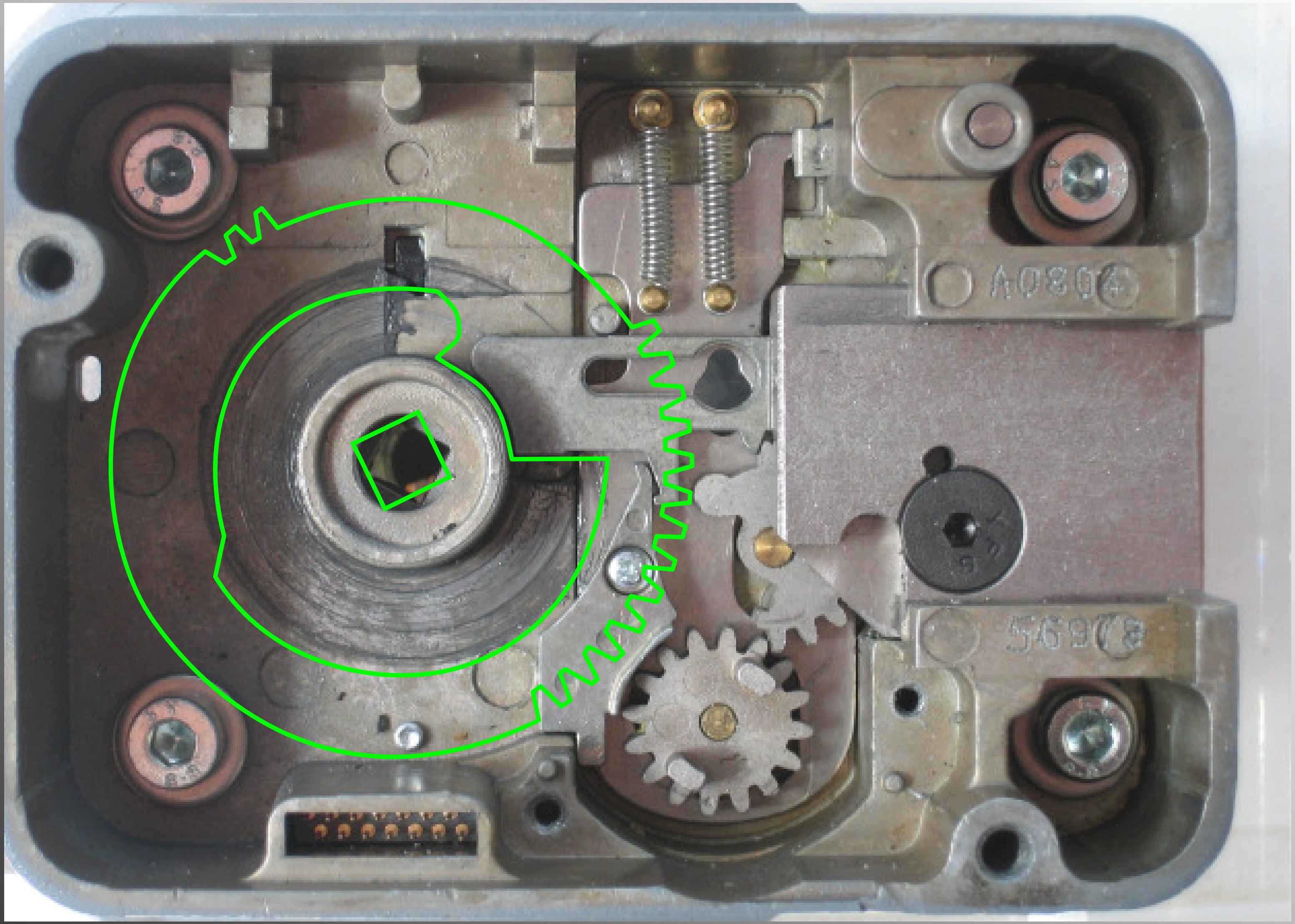
Slide operation.
Locked state.



Slide operation.
Partially open.



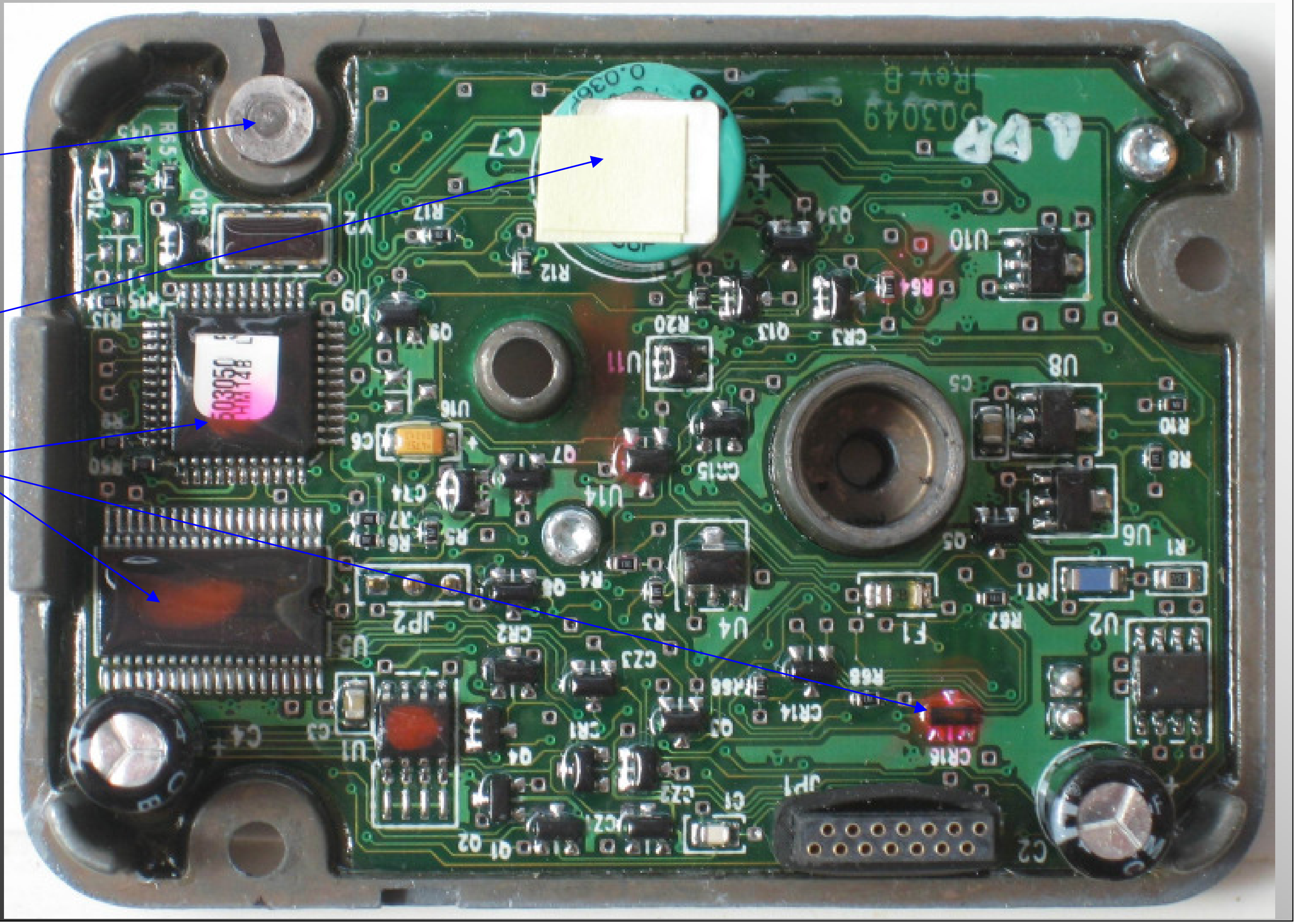
Bolt fully retracted.



Presentation outline.

- Overview and features.
- Looking inside – why it's secure against bumping and vibration.
  - The motor.
  - The gears / slide / bolt mechanism.
  - A brief look into the other components.
- Why it's secure against a lot of other attacks.
- Links to patents etc.
- Questions.

The electronic card (back cover assembly).

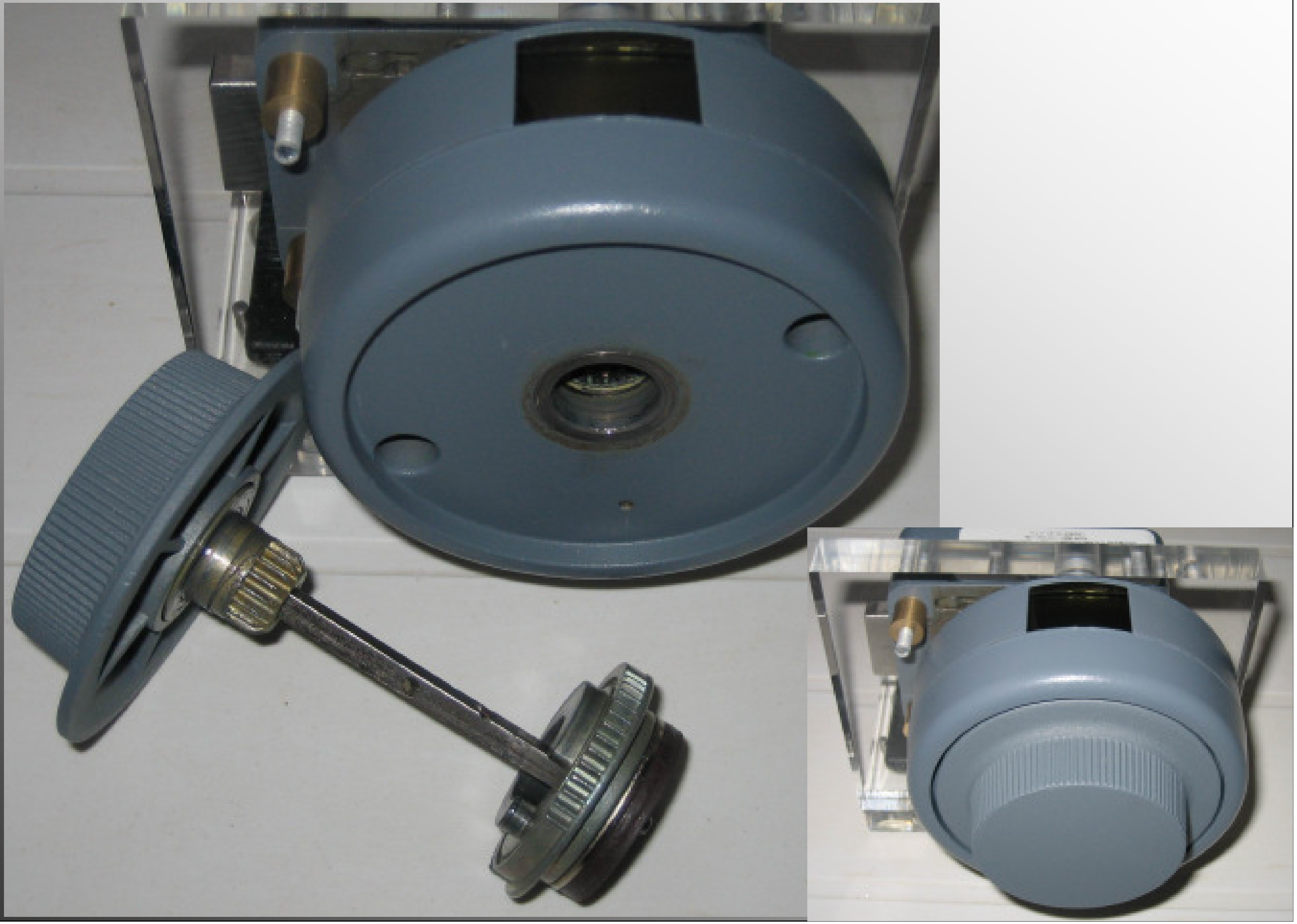


Thermal relocker activator

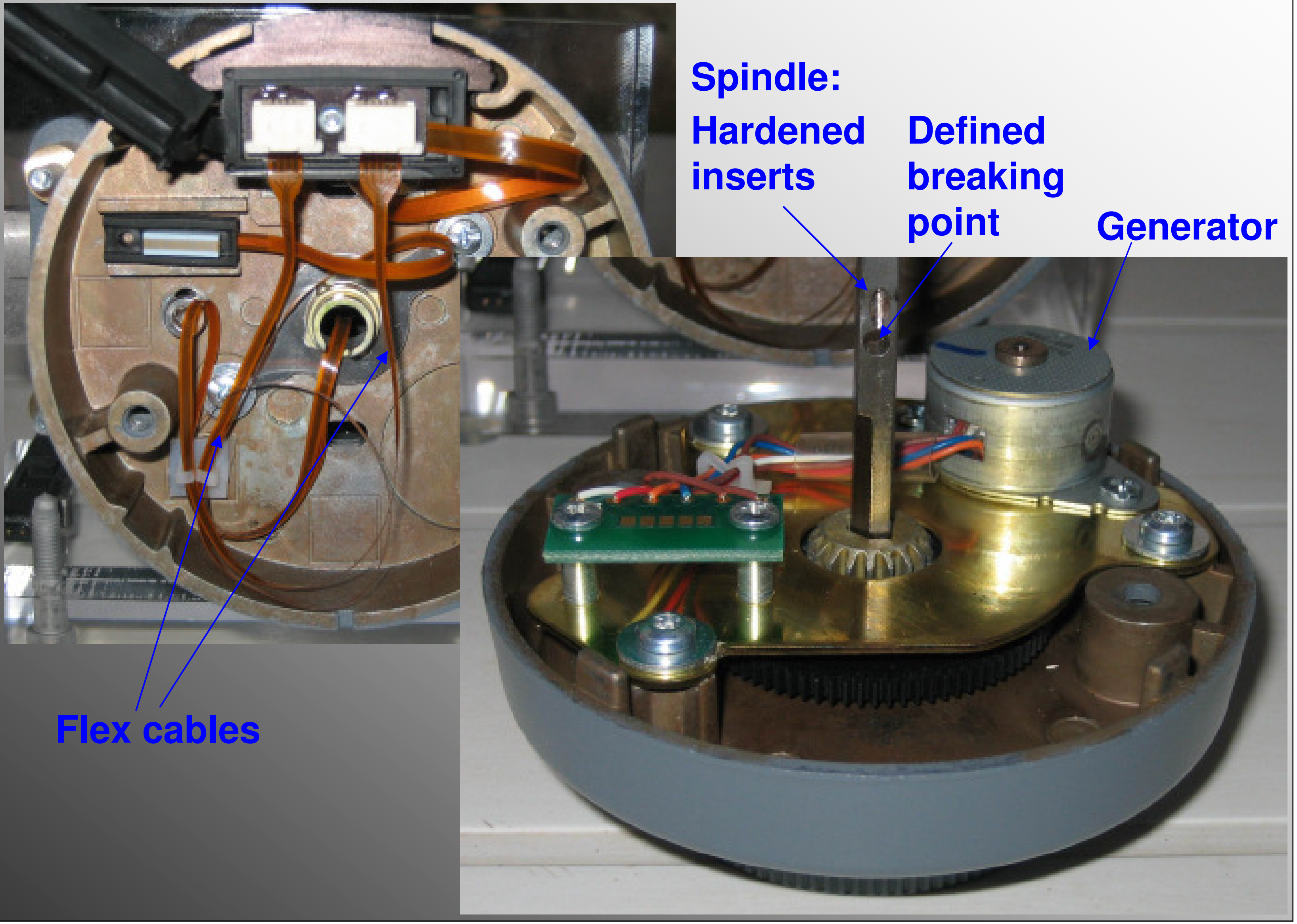
Serial number sticker

UV-active paint

The dial ring.



The dial ring.
A look inside.



Spindle:

Hardened inserts

Defined breaking point

Generator

Flex cables

Presentation outline.

- Overview and features.
- Looking inside – why it's secure against bumping and vibration.
  - The motor.
  - The gears / slide / bolt mechanism.
  - A brief look into the other components.
- Why it's secure against a lot of other attacks.
- Links to patents etc.
- Questions.

Special security features for top secret documents.

Special features have been included to prevent surreptitious opening of the lock, including attempts to extract the combination and replace the lock after a destructive attack, for example:

- The software design tries to prevent reverse engineering / extracting the combinations (e.g. encrypted internal counters and random generator seeds, changing memory locations).
- Maximum dialing speed limit to slow down auto-dialers.
- The electronics board is randomly marked with UV-active paint.
- The connection between the lock body and the dial / LCD assembly seems to be somewhat obfuscated.

Source: LSS+ 5.0 by Marc Weber Tobias, KABA MAS product brochure, FF-L-2740A.

Special security features for top secret documents (continued).

- Meets U.S. Federal Specification FF-L-2740A, e.g.
  Fail secure against high-voltage, vibration, and R/F.

- Audit: Counts all openings (cannot be reset). Counts unsuccessful opening attempts after 3 incorrect combinations.

- Wrong Try Penalty: 10-14 errors results in a 3 minute time out.
  15 errors or greater results in a 4 minute time out.

- Lock on back cover (LOBC) pin prevents removing the back cover without the combination*.

  *Don’t rely on this feature, though.

Source: LSS+ 5.0 by Marc Weber Tobias, KABA MAS product brochure, FF-L-2740A, own investigations.

Further reading.

- Manufacturer’s Website:
  http://www.kaba-mas.com/a.php?page=x-09_main

- U.S. Naval Facilities Engineering Command – DoD Lock Program:
  https://portal.navfac.navy.mil/go/locks (see X-09 “Ordering Info”).
  Has some details on the use of the lock, as well as FF-L-2740A.

- Patents:
  US6741160 (General concept of the X-0x locks)
  US6731025 (Motor)
  US6038897 (Lock on back cover)

Thank you! More questions?

The author can be reached at mh@tosl.org.

Disclaimer
The opinions expressed here are those of the author only; the author is not affiliated with the lock manufacturer in any way; the lock manufacturer or the author's employers have nothing to do with this document. All trademarks are the property of their owners. Some of the concepts and techniques mentioned in here might be protected by intellectual property rights such as patents. The information was derived only from the analysis of a single lock and / or other sources where mentioned and might be incomplete and / or contain errors. The author gives no warranty and accepts no liability whatsoever concerning this document.