Why the Bellcore attack is not working against an ENIGMA machine. Parts 1 and 2

Rump session CRYPTO 08: August 20

Jean-Jacques Quisquater
UCL CRYPTO Group

Special Guest: *David Kahn*

ALERT: Paper introduces 4 new attacks

WARNING included

Bellcore attack (1996)
http://jya.com/belcor.txt

Put a *cryptographic device* into a *microwave oven* in order

- to induce fault(s) before or during computations and

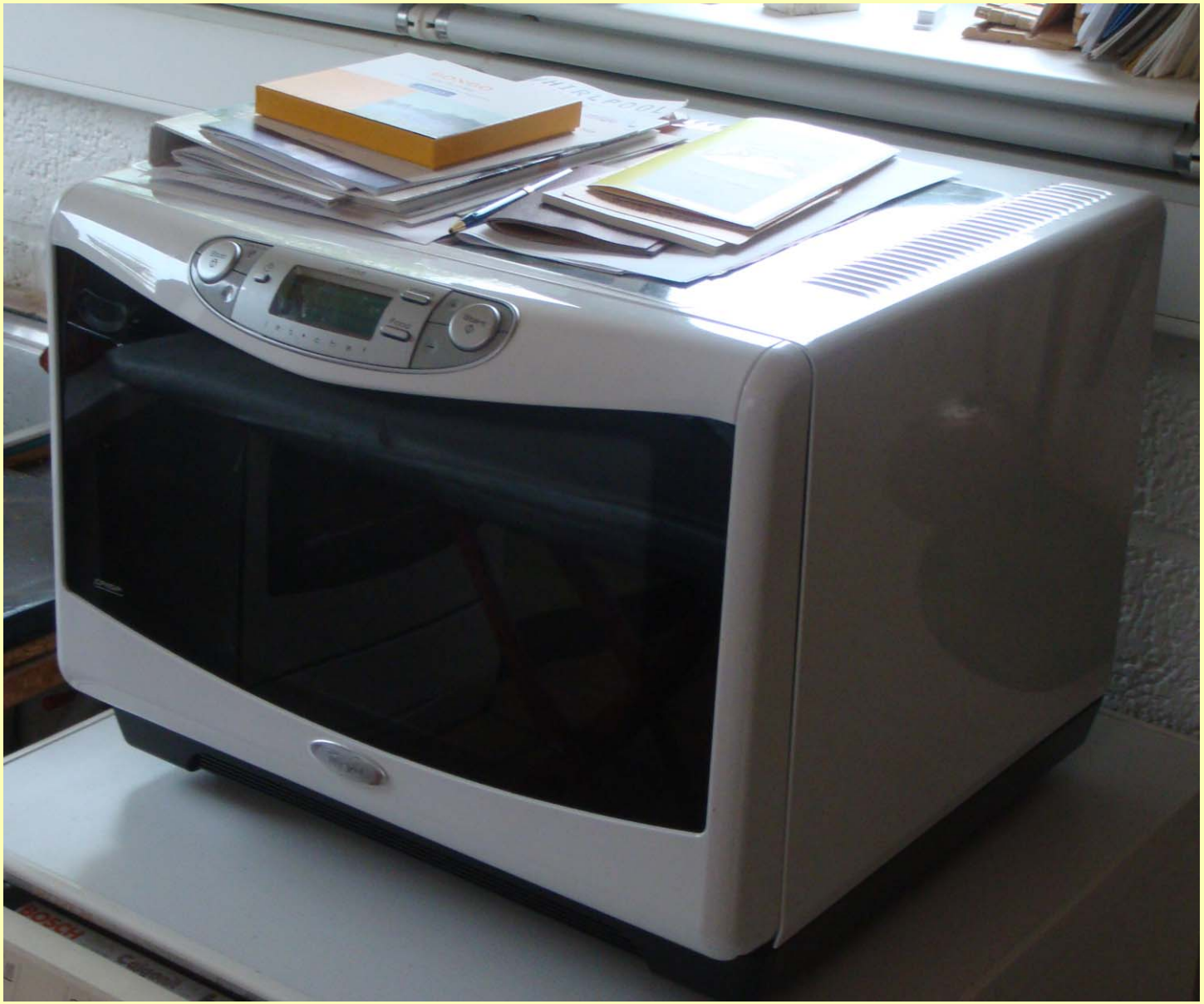
- to recover the secret key using simple computations …

- " *Our attack*," Dan Boneh explained, **"*is basically a creative use […] of faults …*"**

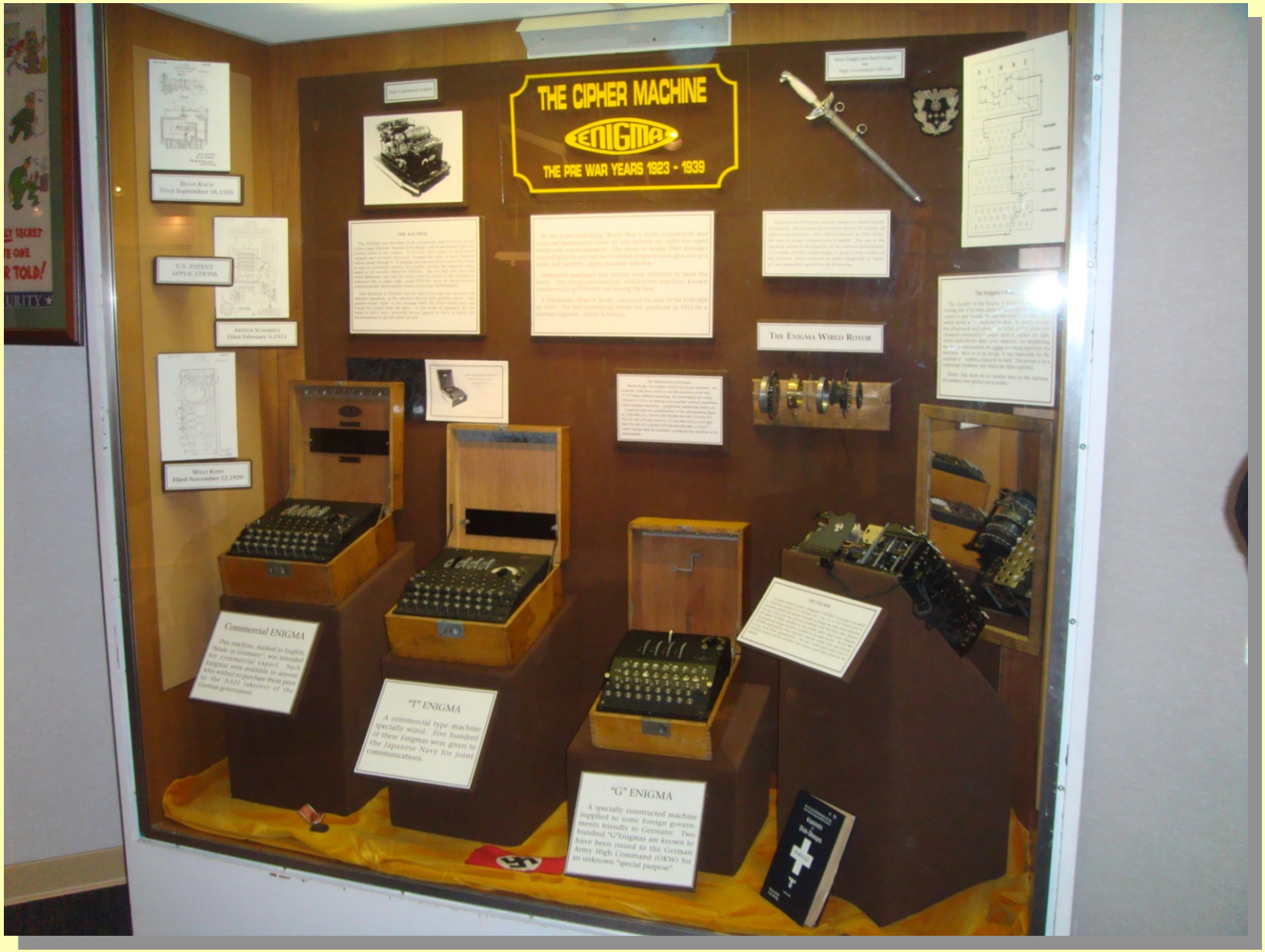
New idea

- Try that on *old electromechanical devices* like seen in the NSA museum during CHES 2008.
- Let first attack the **ENIGMA** machine …
- and let’s go to the kitchen …

Modern microwave oven

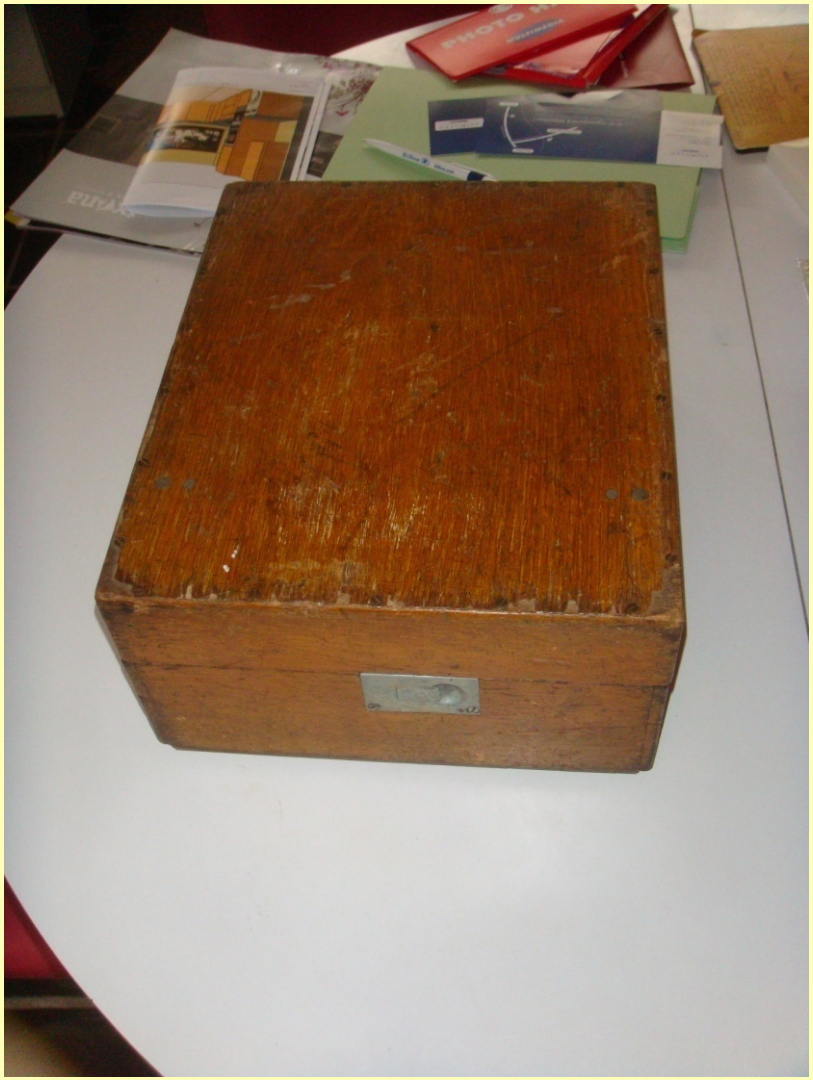


NSA museum ... No Such Attack

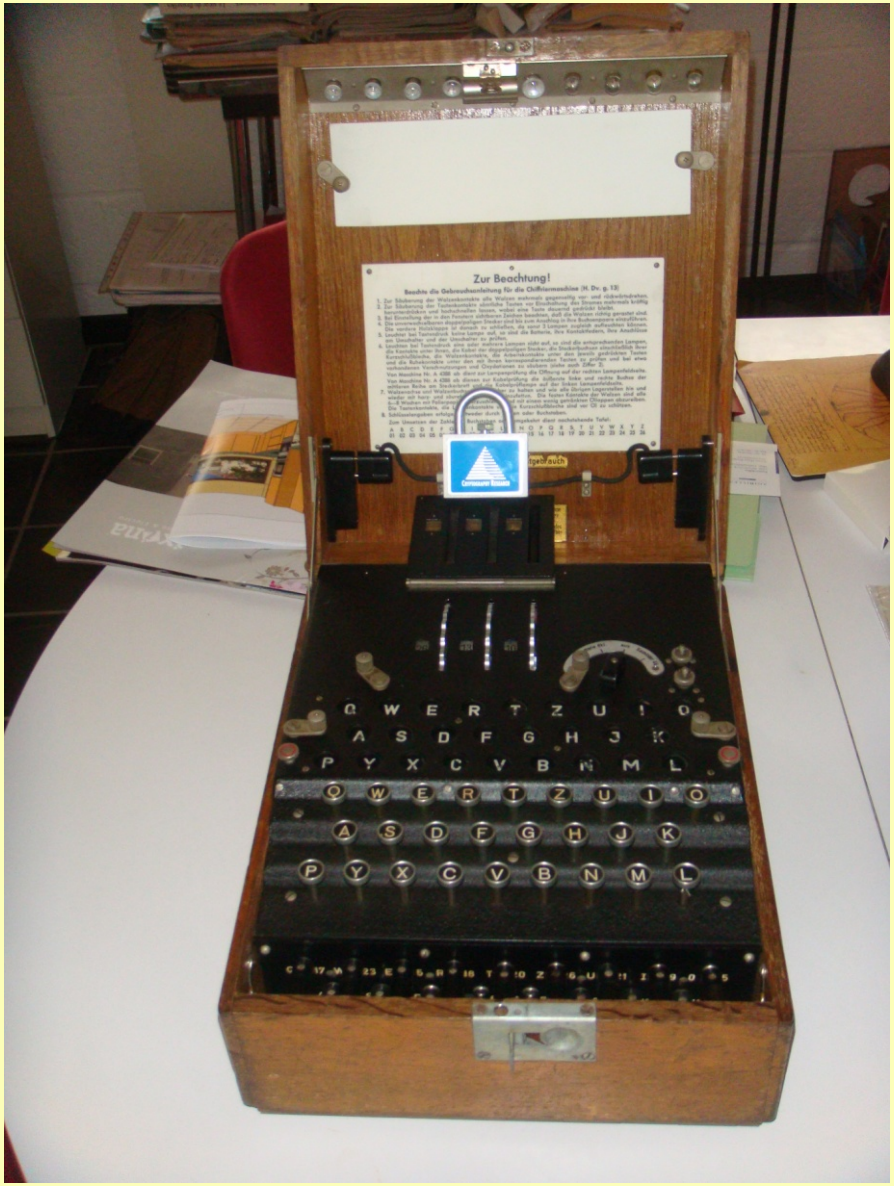


Ask to an expert

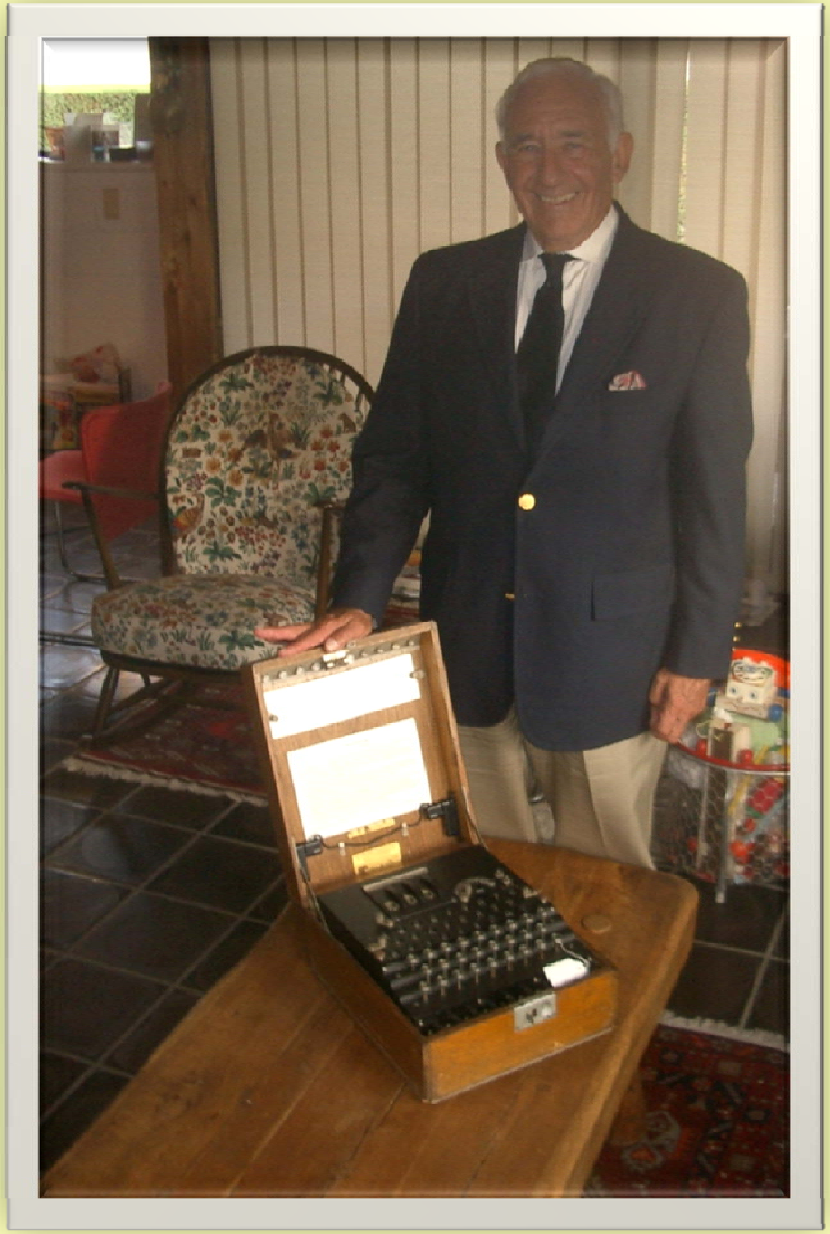
ENIGMA (3 rotors)



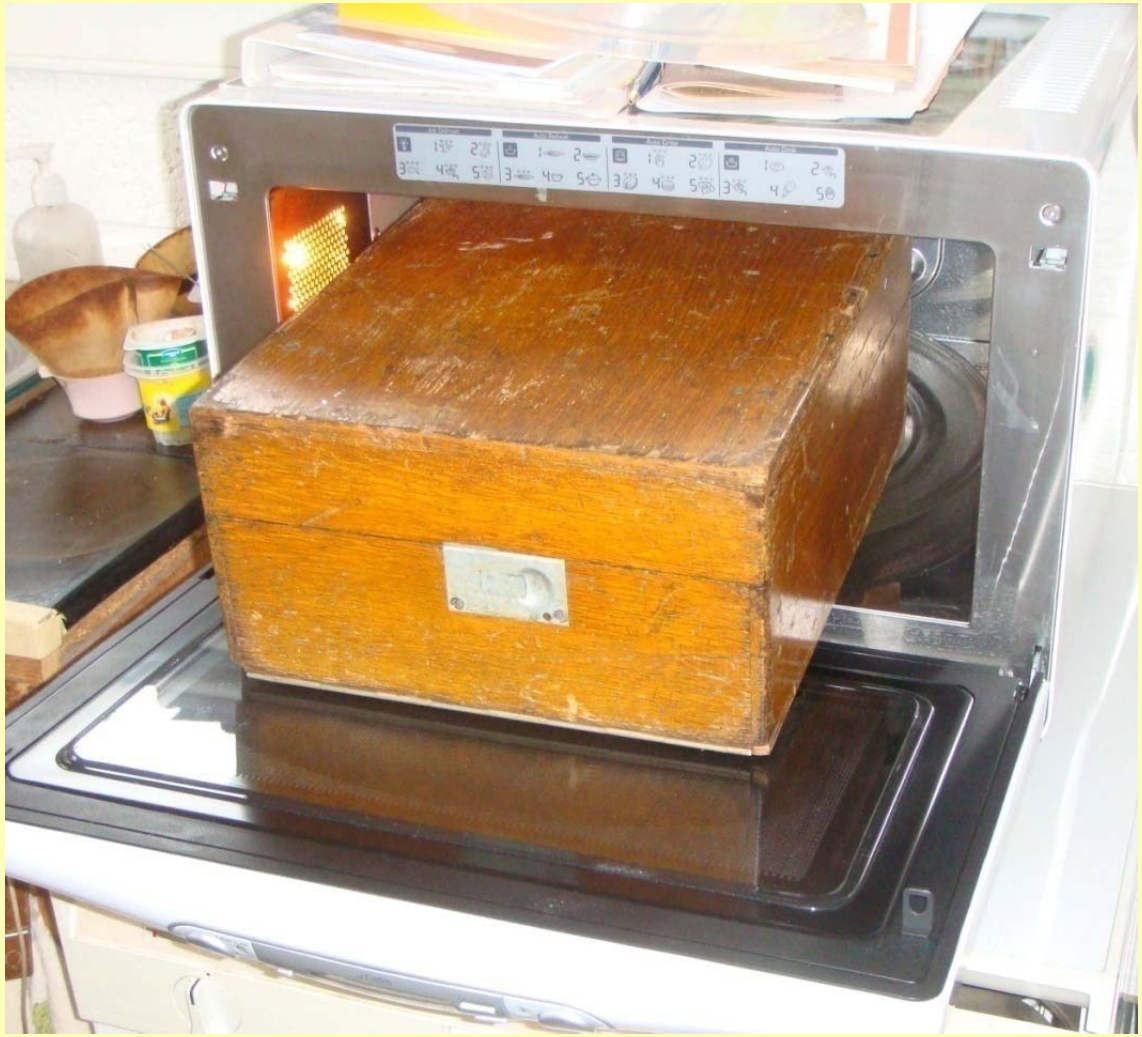
Surprise when open …



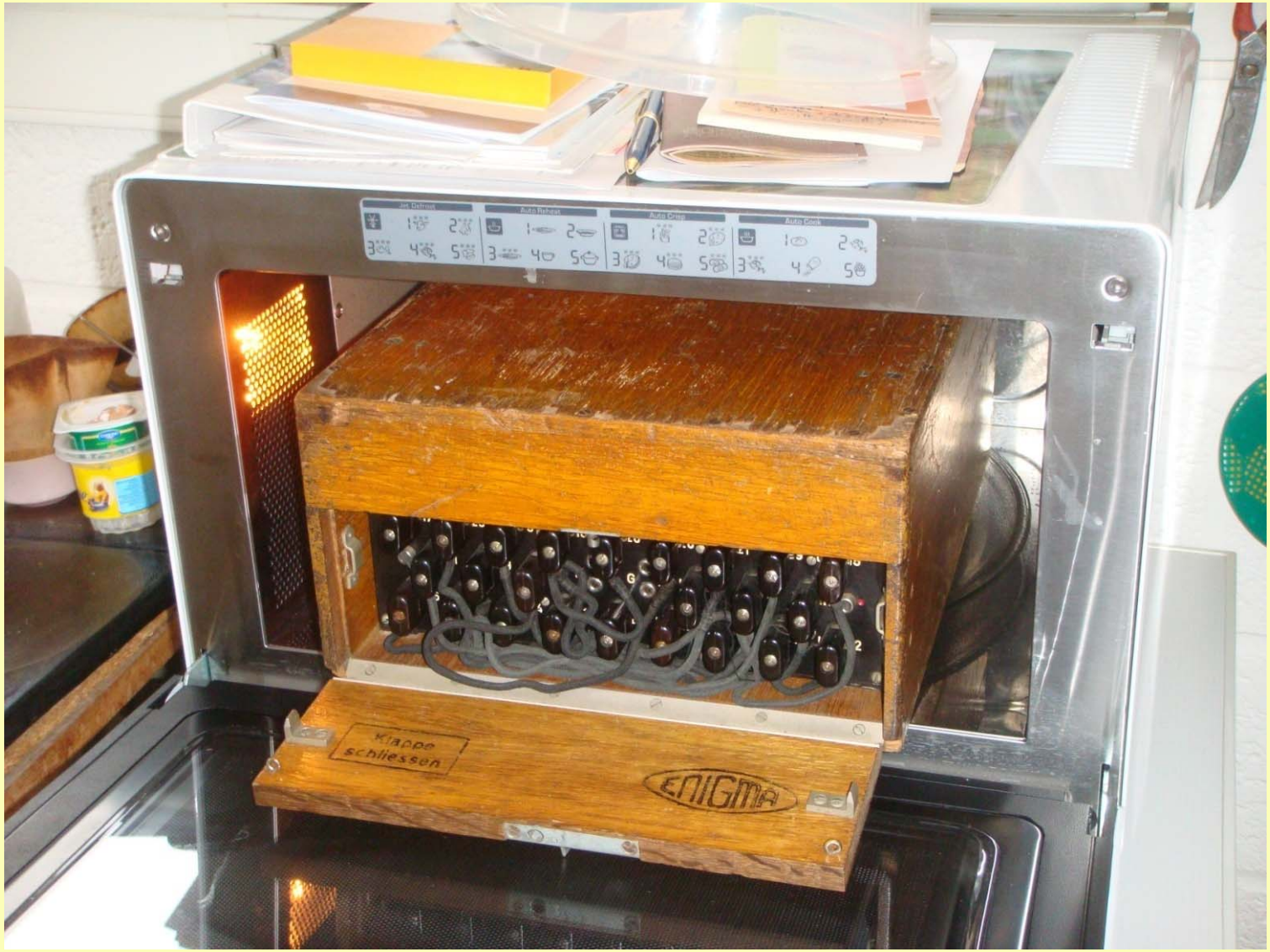
Official photo before the experiment



In the microwave oven ...Woodbox attack



Semi-open-woodbox attack



End part 1

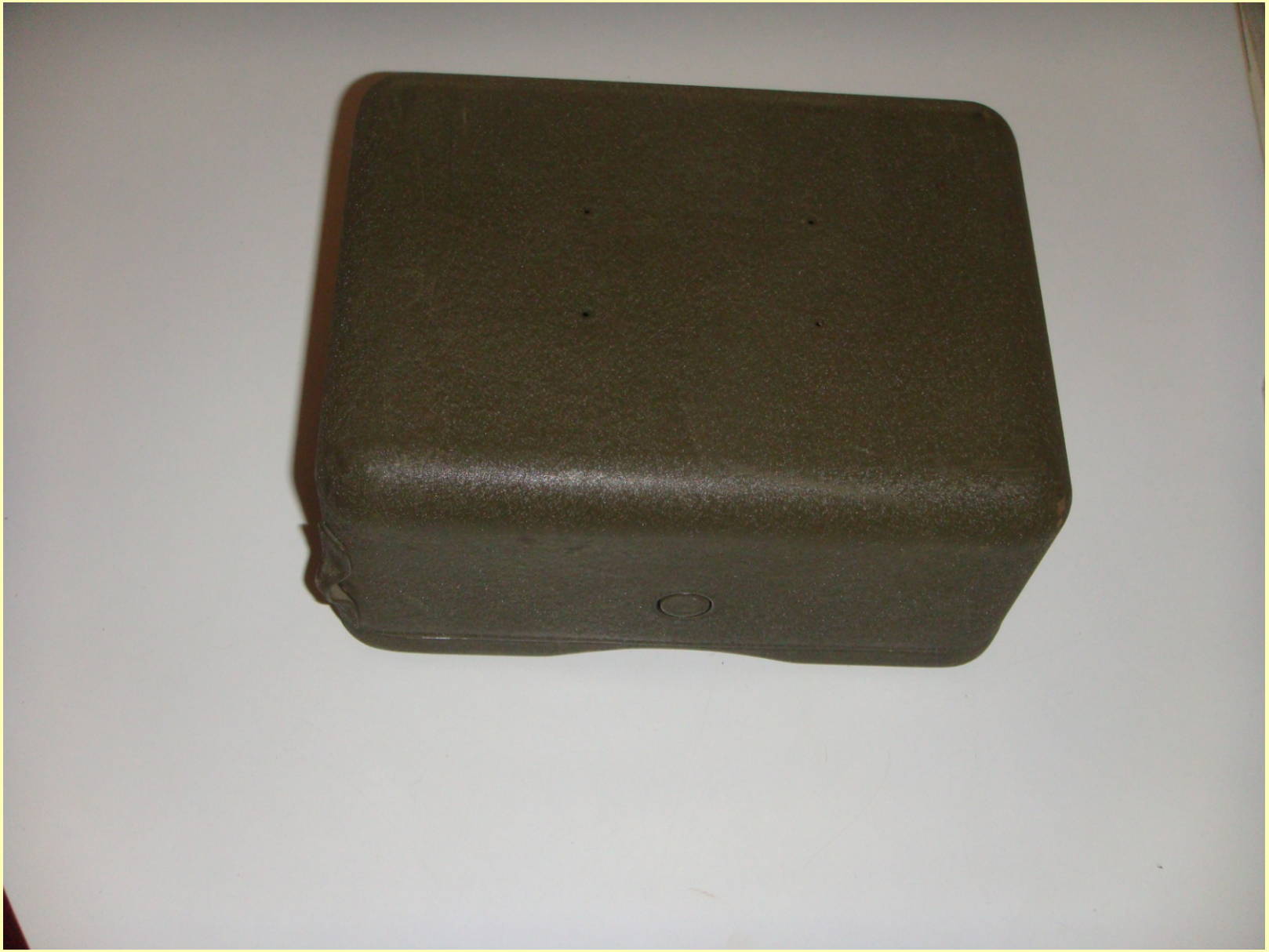
First conclusions

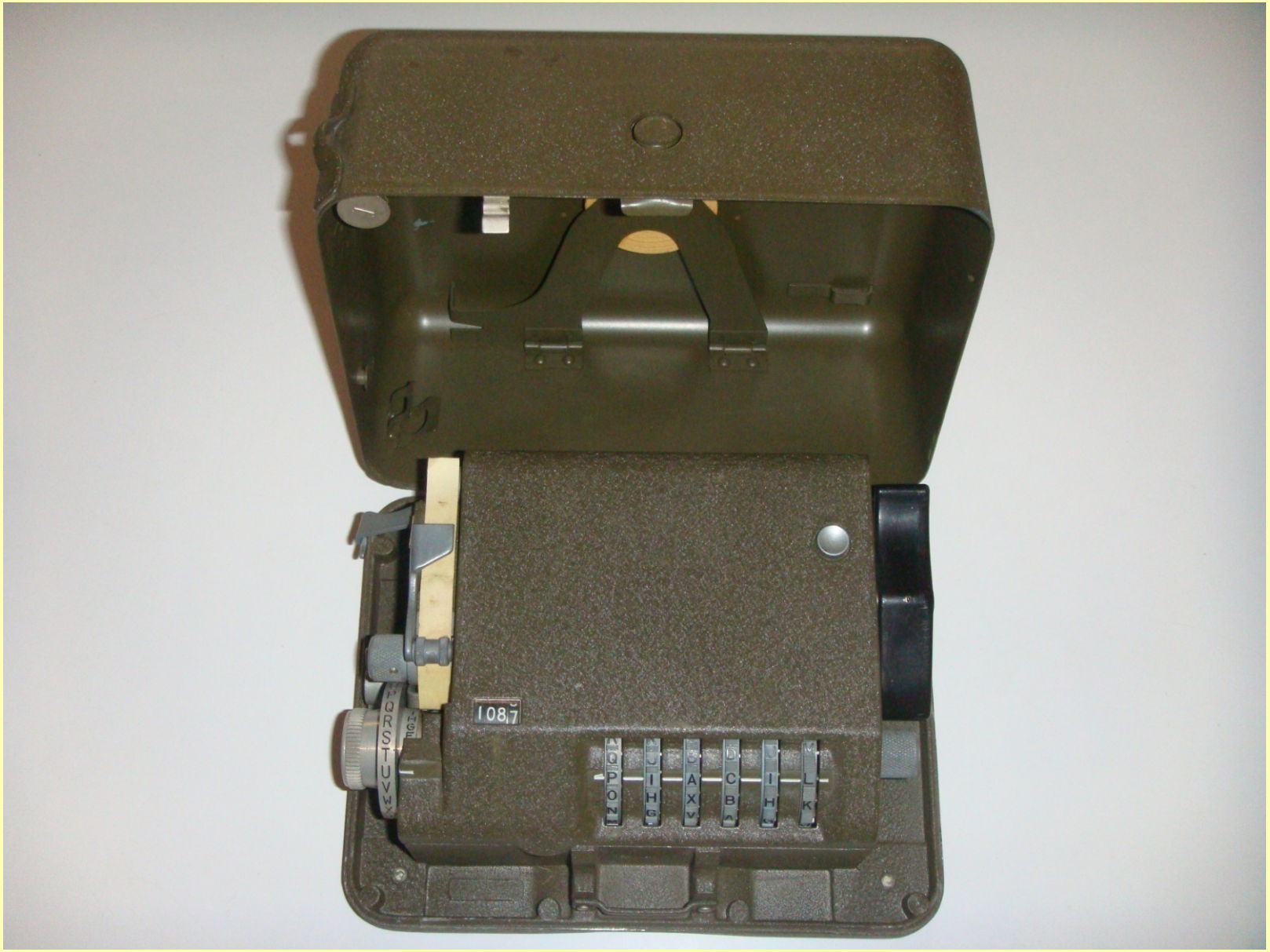
- Setup is not perfect

More work needed

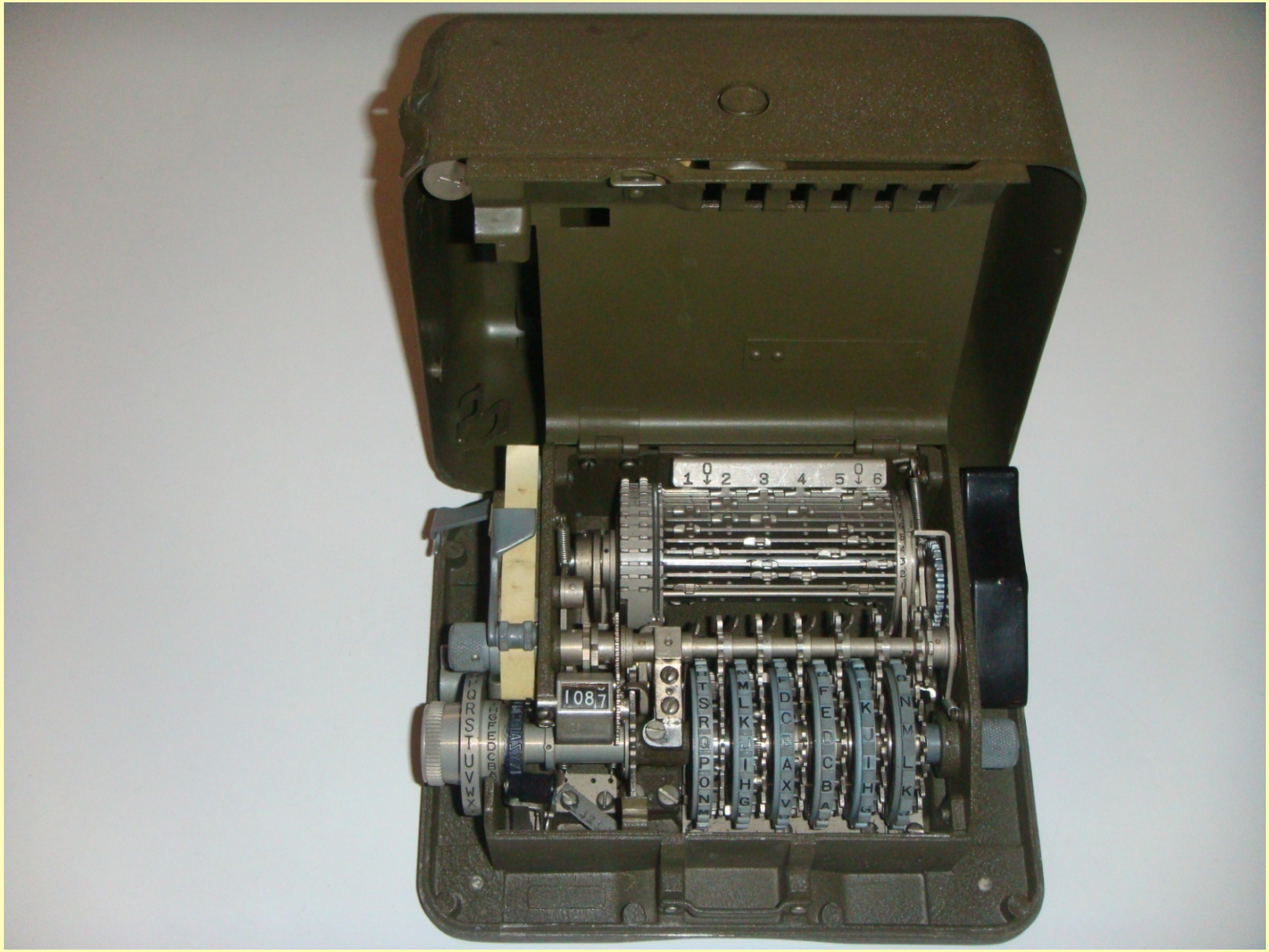
- **Other microwave oven**
- **Other devices (M-209)**

Part 2: M-209 (Hagelin)

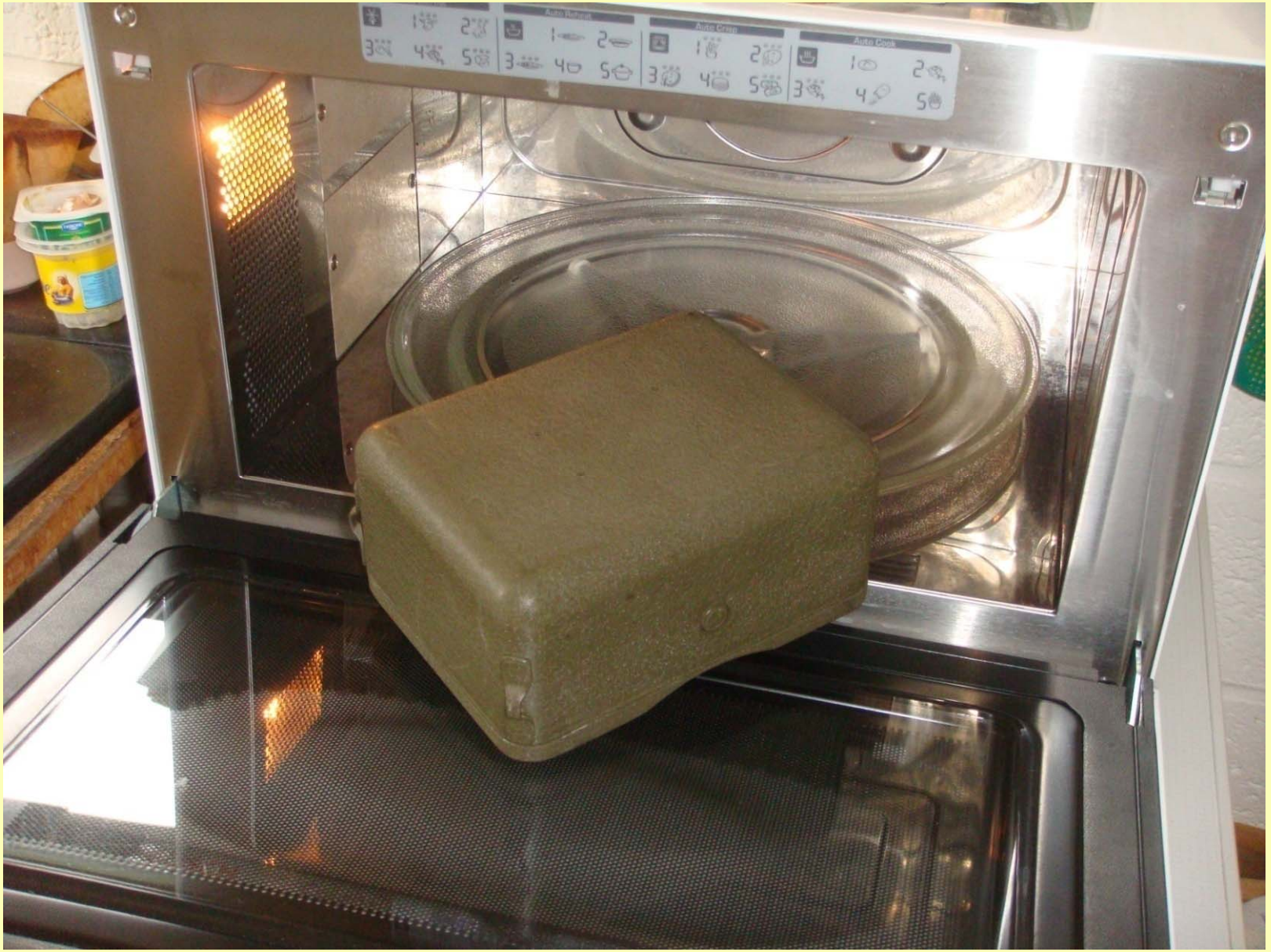



1087

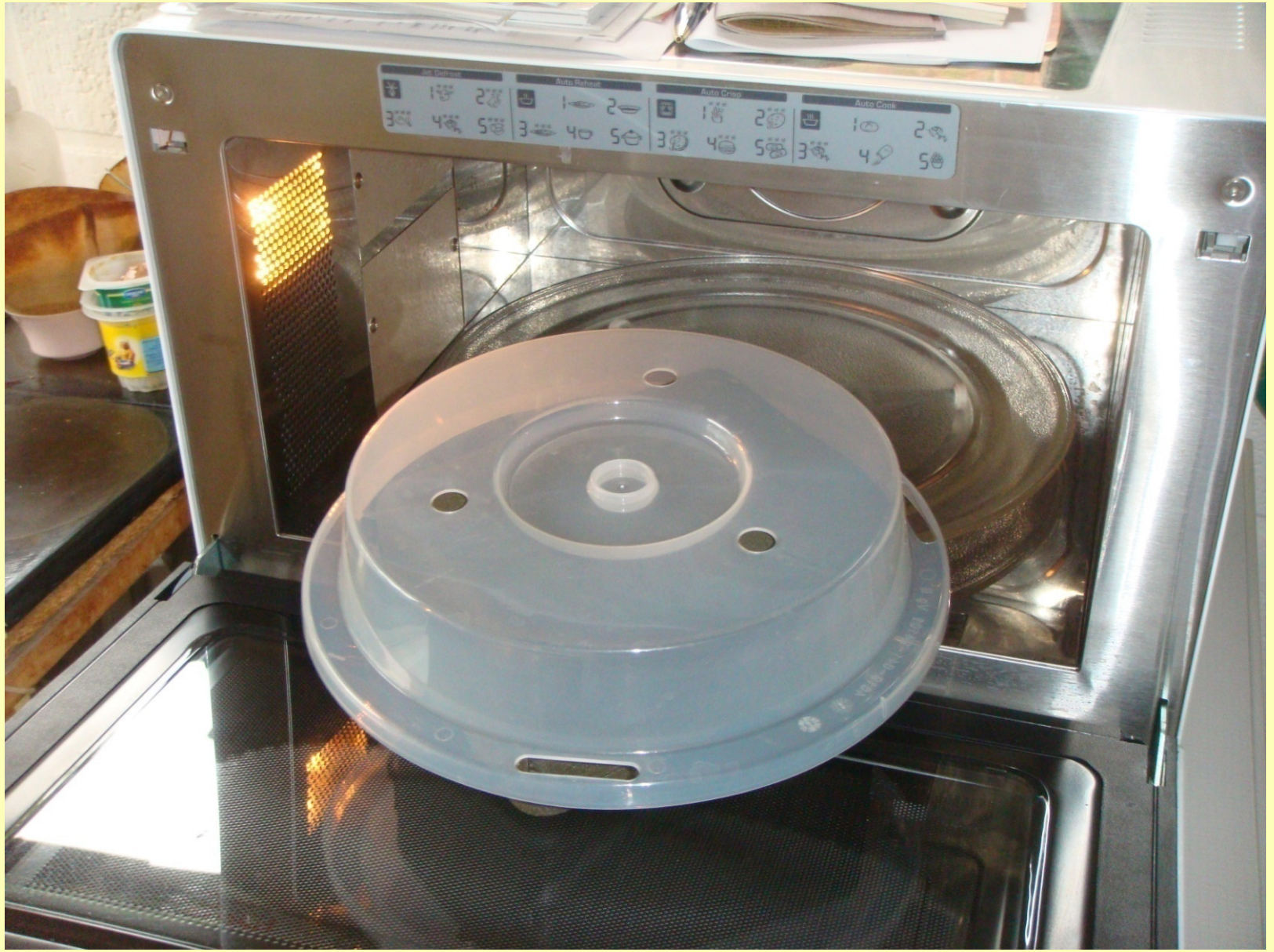
Not DPA protected



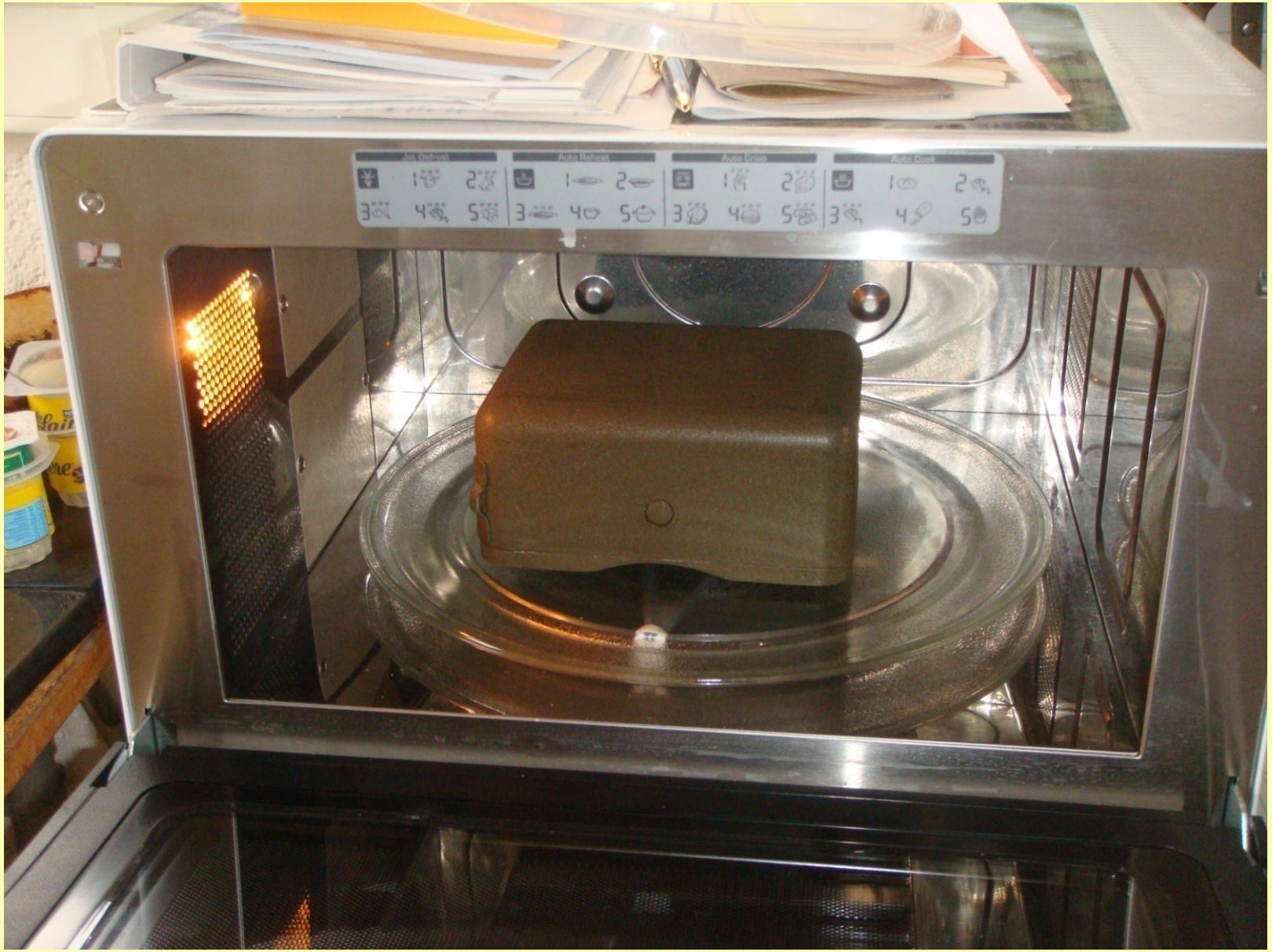
Setup is now OK! Metalbox attack



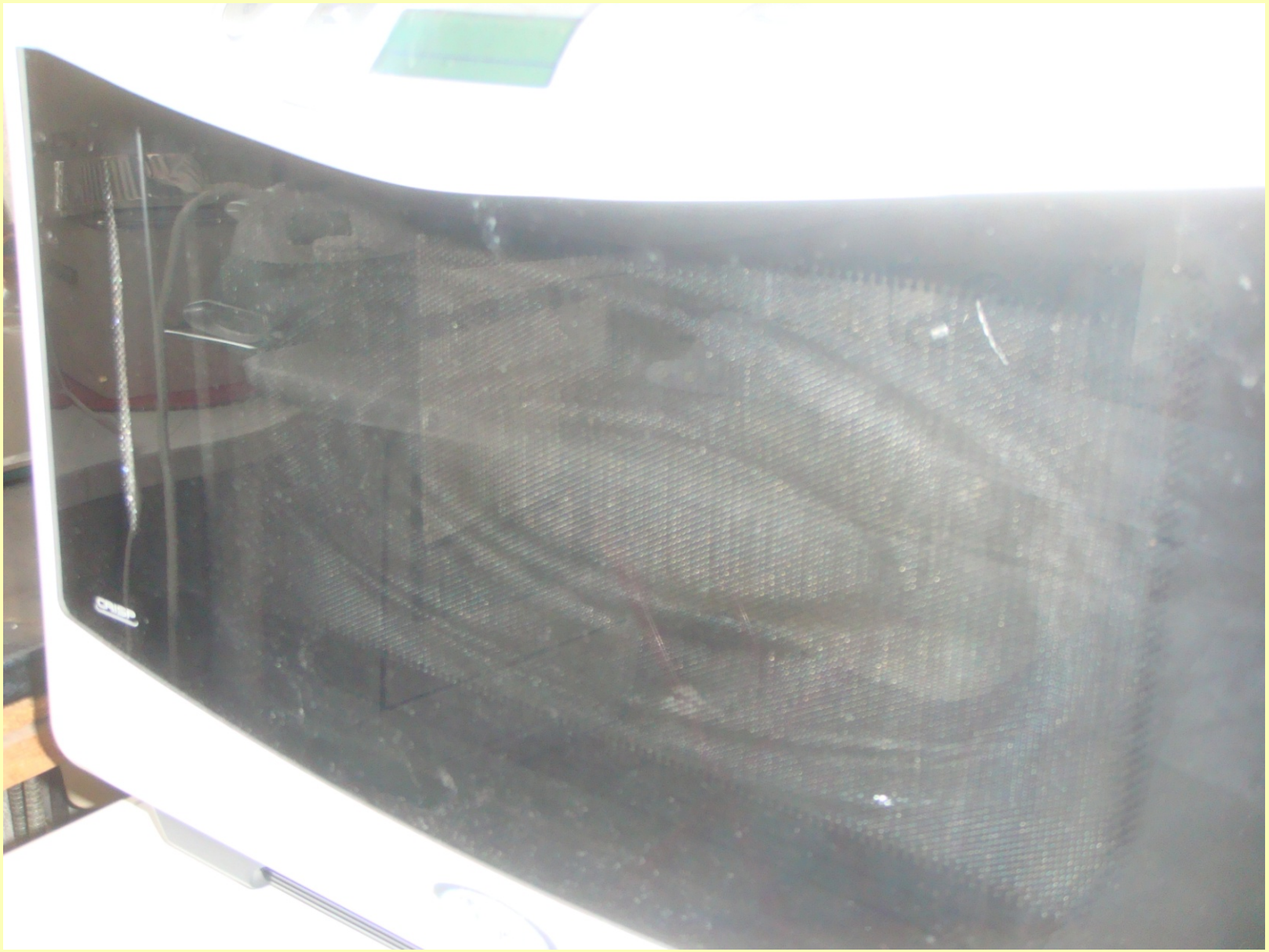
Cover or not?



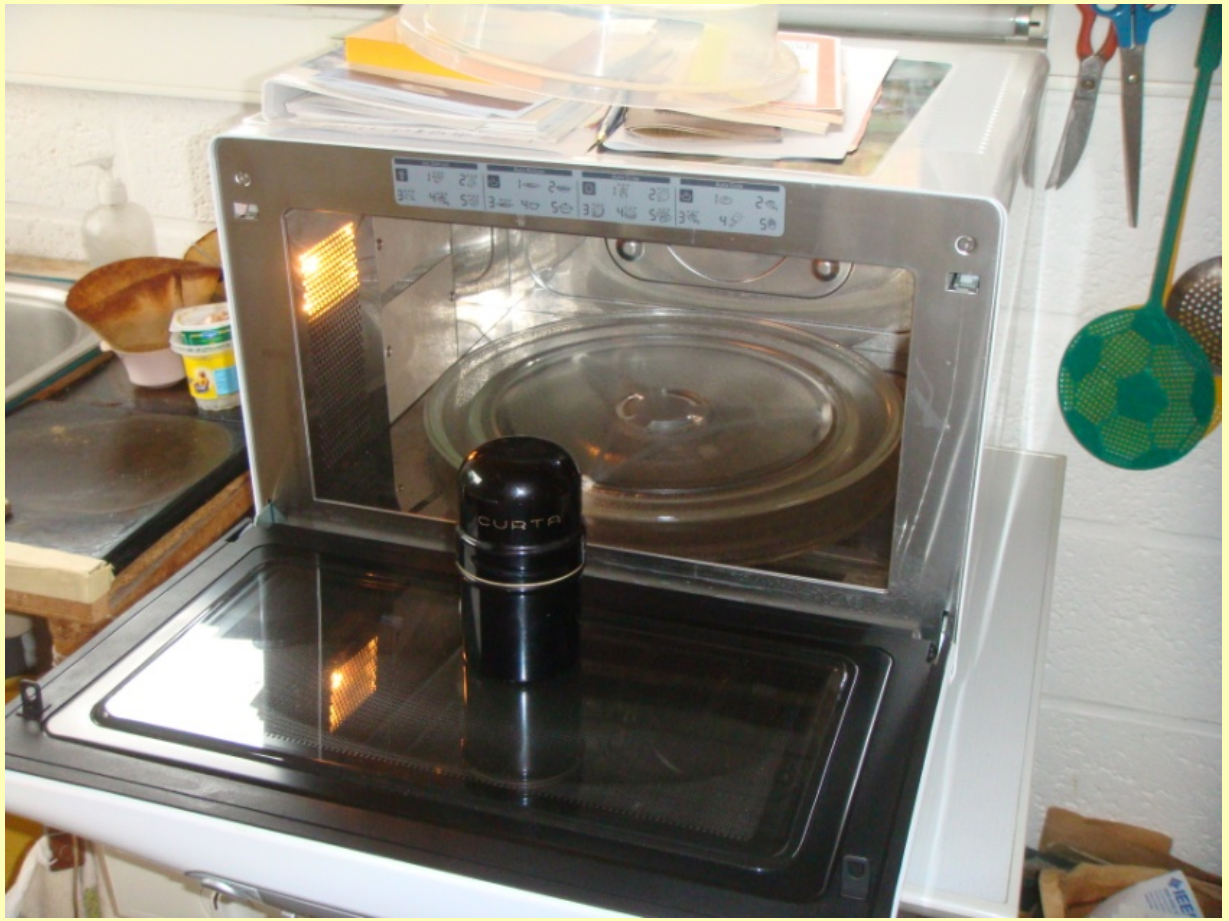
Ready?

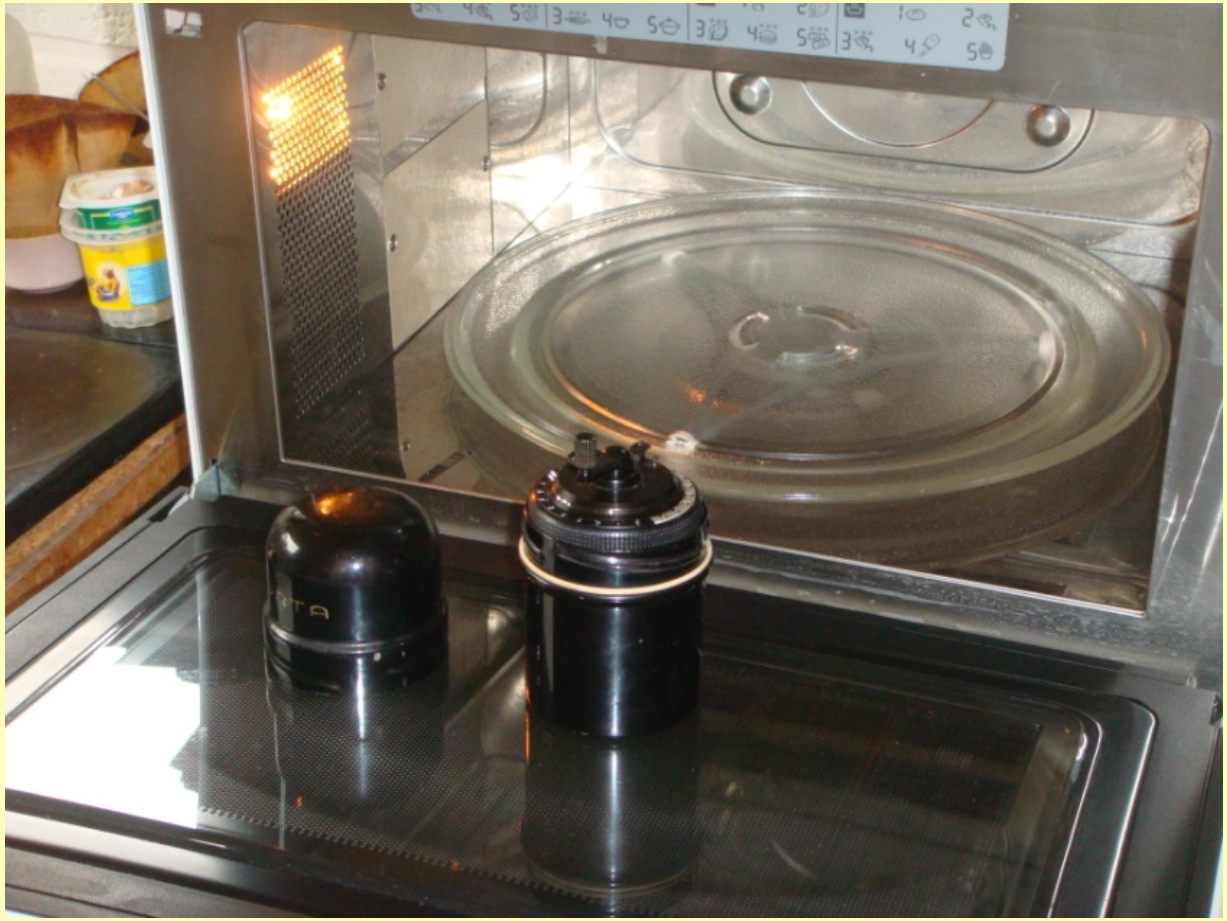


Running

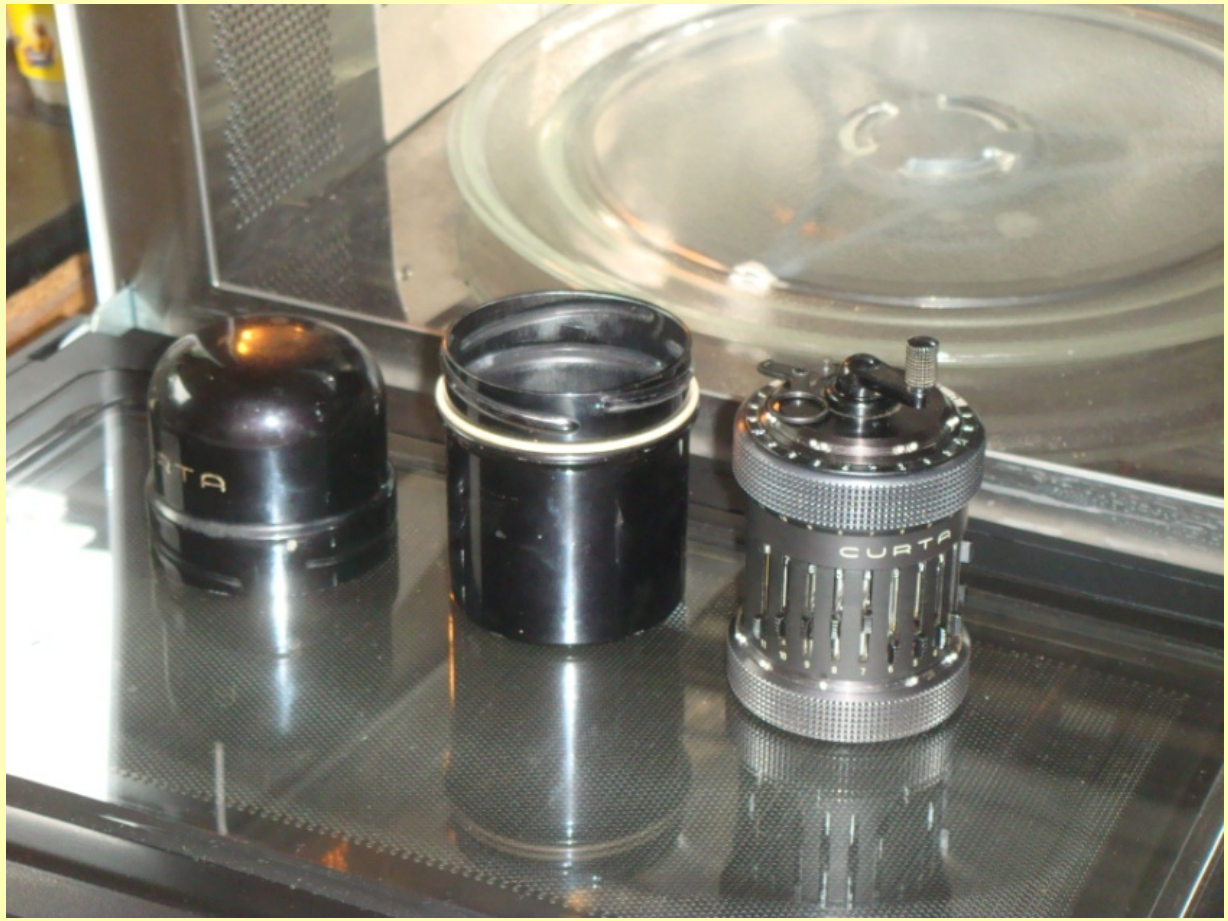


Opening …



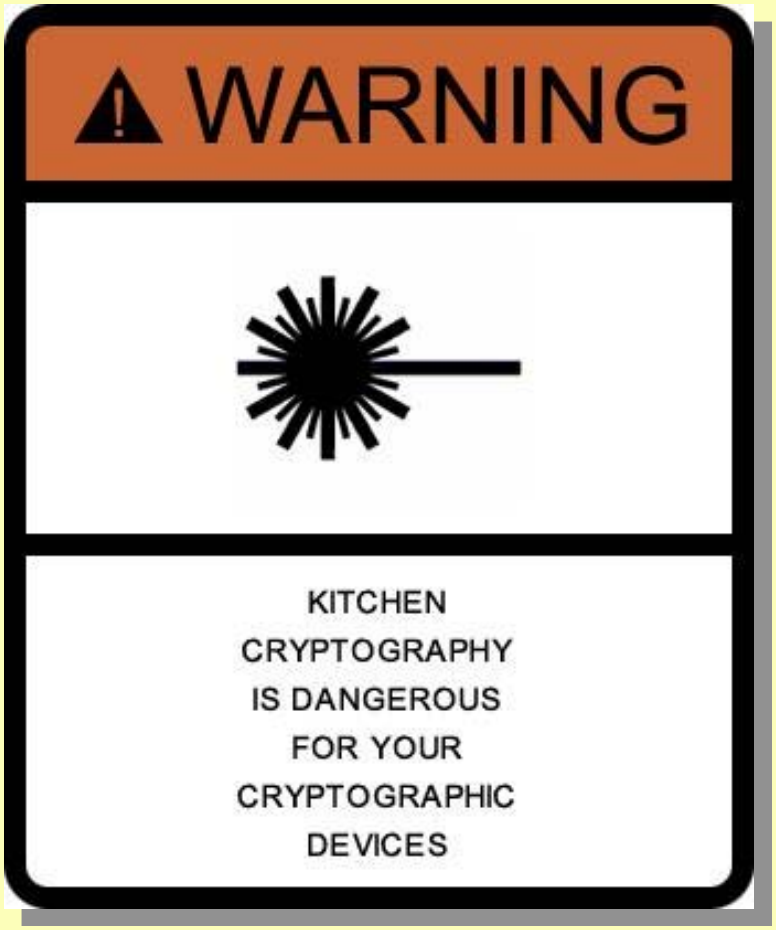


Cryptography disappears …



Conclusions

- Thanks to the microwave oven *no more bug*
- No more working cryptography
- Beware the new attacks



- Work in progress

Next time: Milk attack against Keelog products