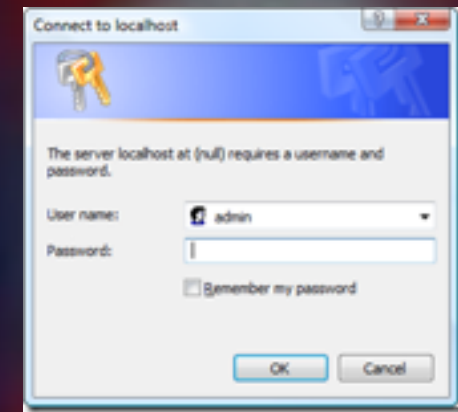


Zur Unsicherheit moderner Authentifizierungsverfahren



Passwort



Chip



Biometrie



STARBIG

god
sex
love
secret



CCC, DE

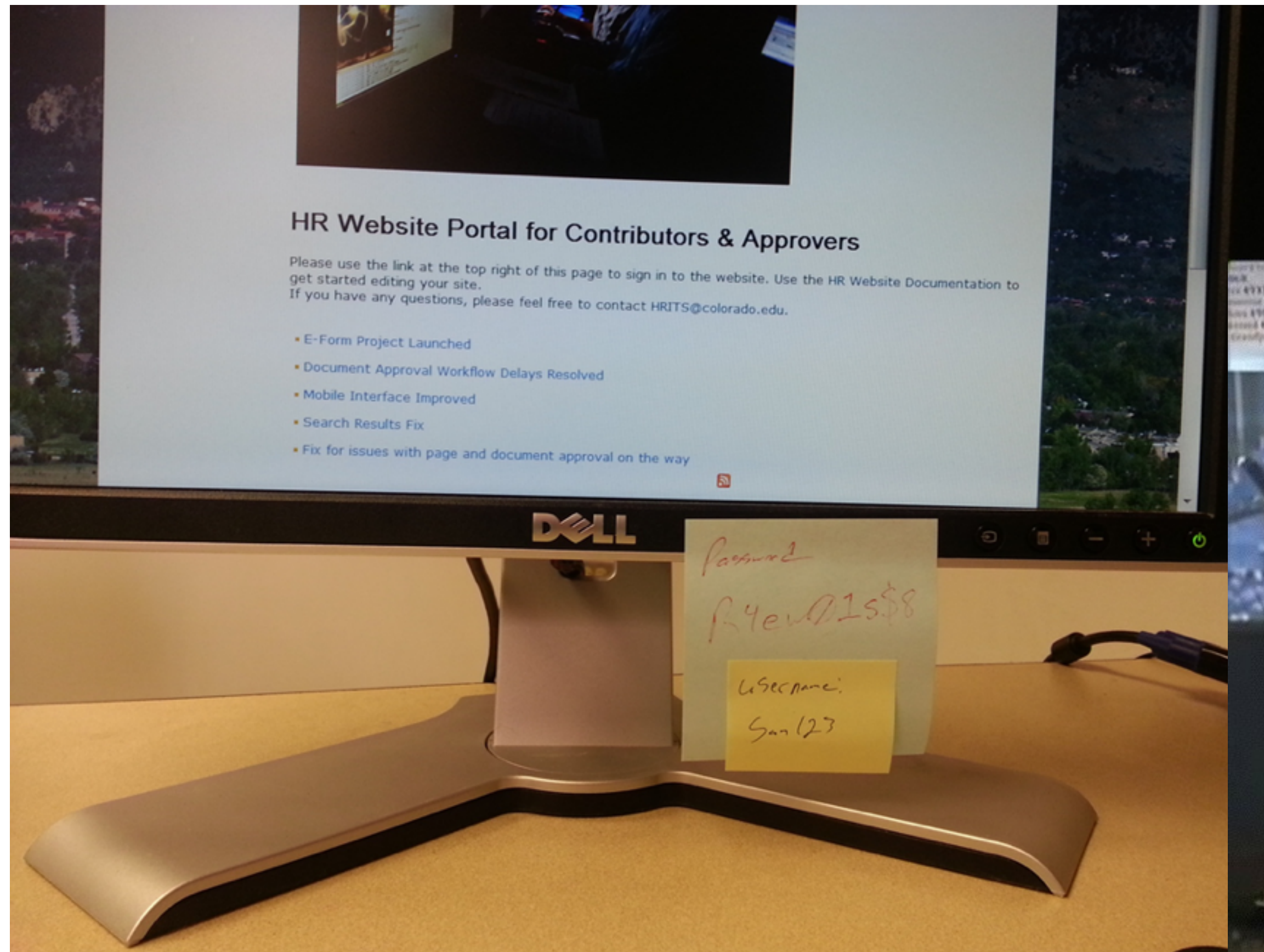
Passwort

Chip

Biometrie

Zur Unsicherheit moderner
Authentifizierungsverfahren

Post-it am Monitor



<http://microsoftmercenary.com/wp/wp-content/uploads/2015/02/image9.png>
<http://cdn1.spiegel.de/images/image-834158-galleryV9-gbup-834158.jpg>

schlechte Passworte

Poor Password Choices

4.7% of users have the password password;

8.5% have the passwords password or 123456;

9.8% have the passwords password, 123456 or 12345678;

14% have a password from the top 10 passwords

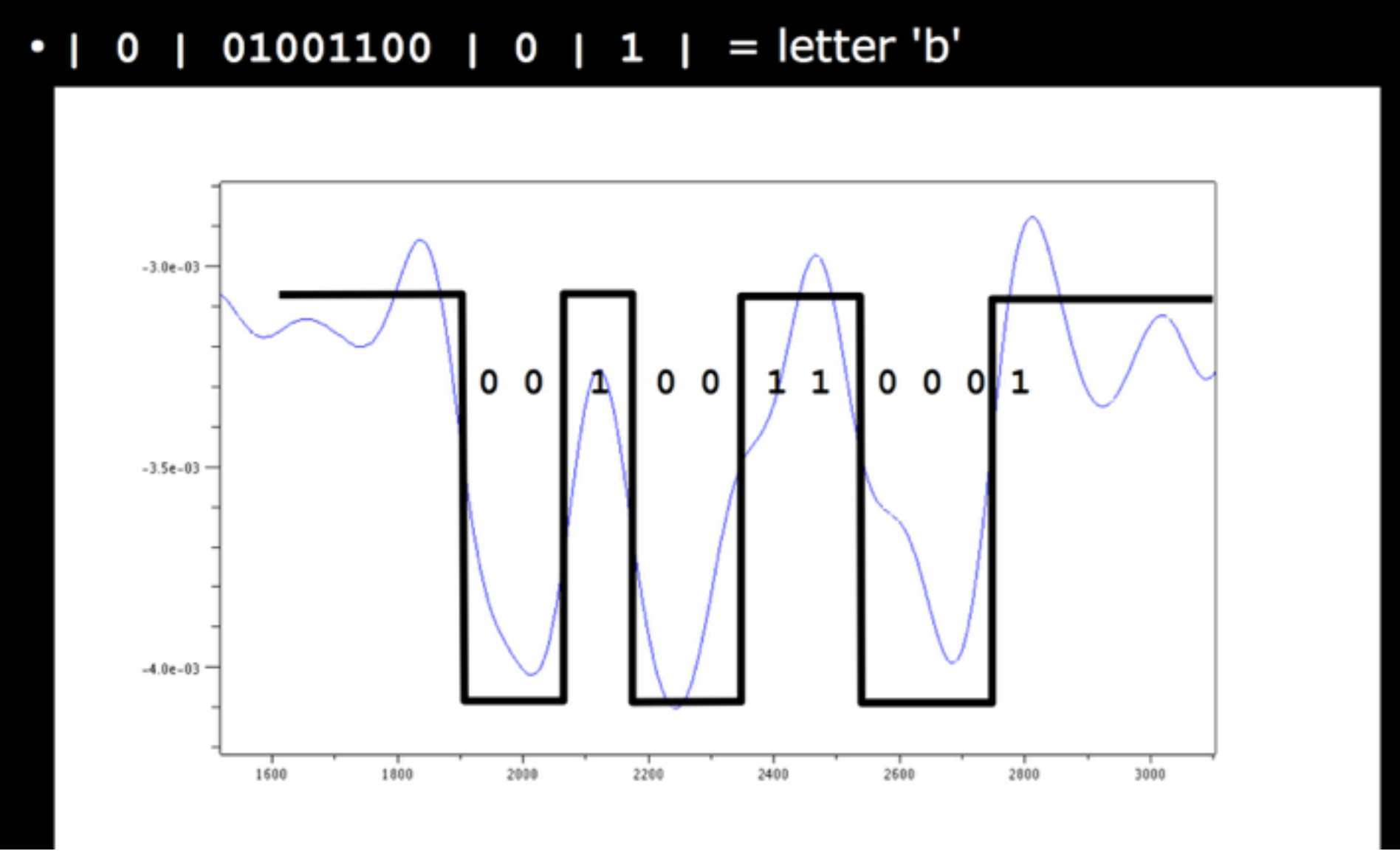
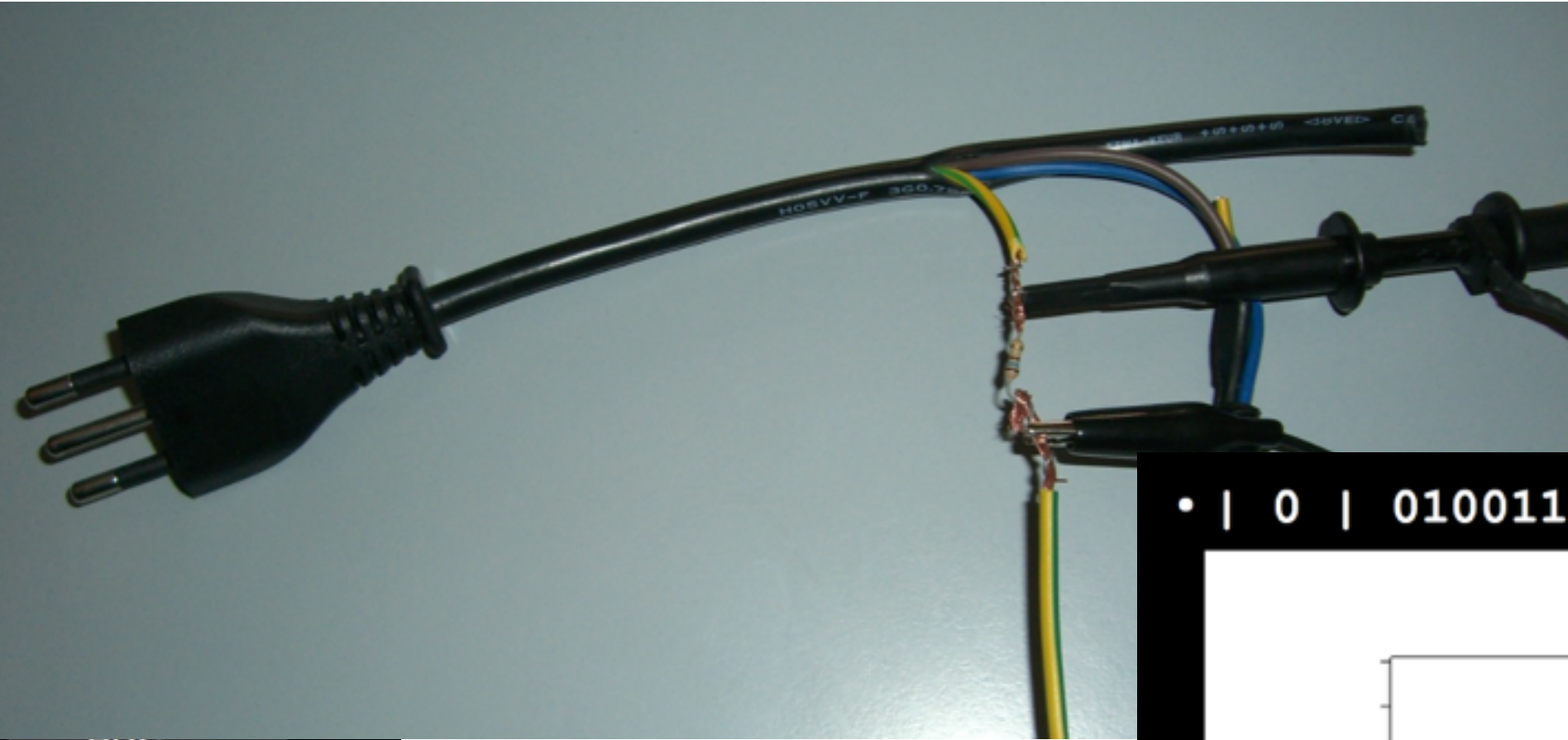
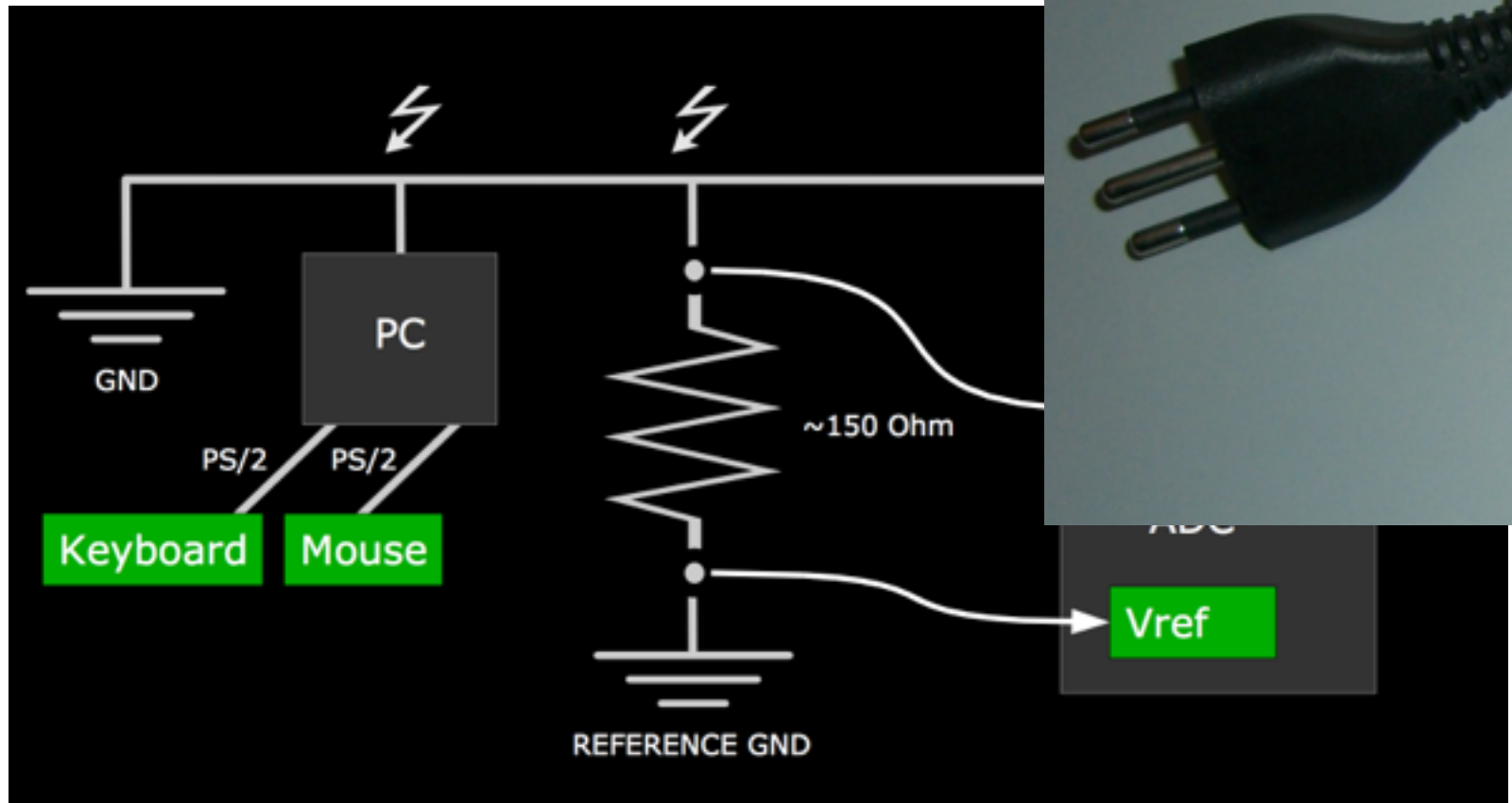
40% have a password from the top 100 passwords

79% have a password from the top 500 passwords

91% have a password from the top 1000 passwords

twitter: @jcleblanc | hashtag: #ConvergeSE

Seitenkanale



<https://inversepath.com>

Keylogger



Funkttastaturen

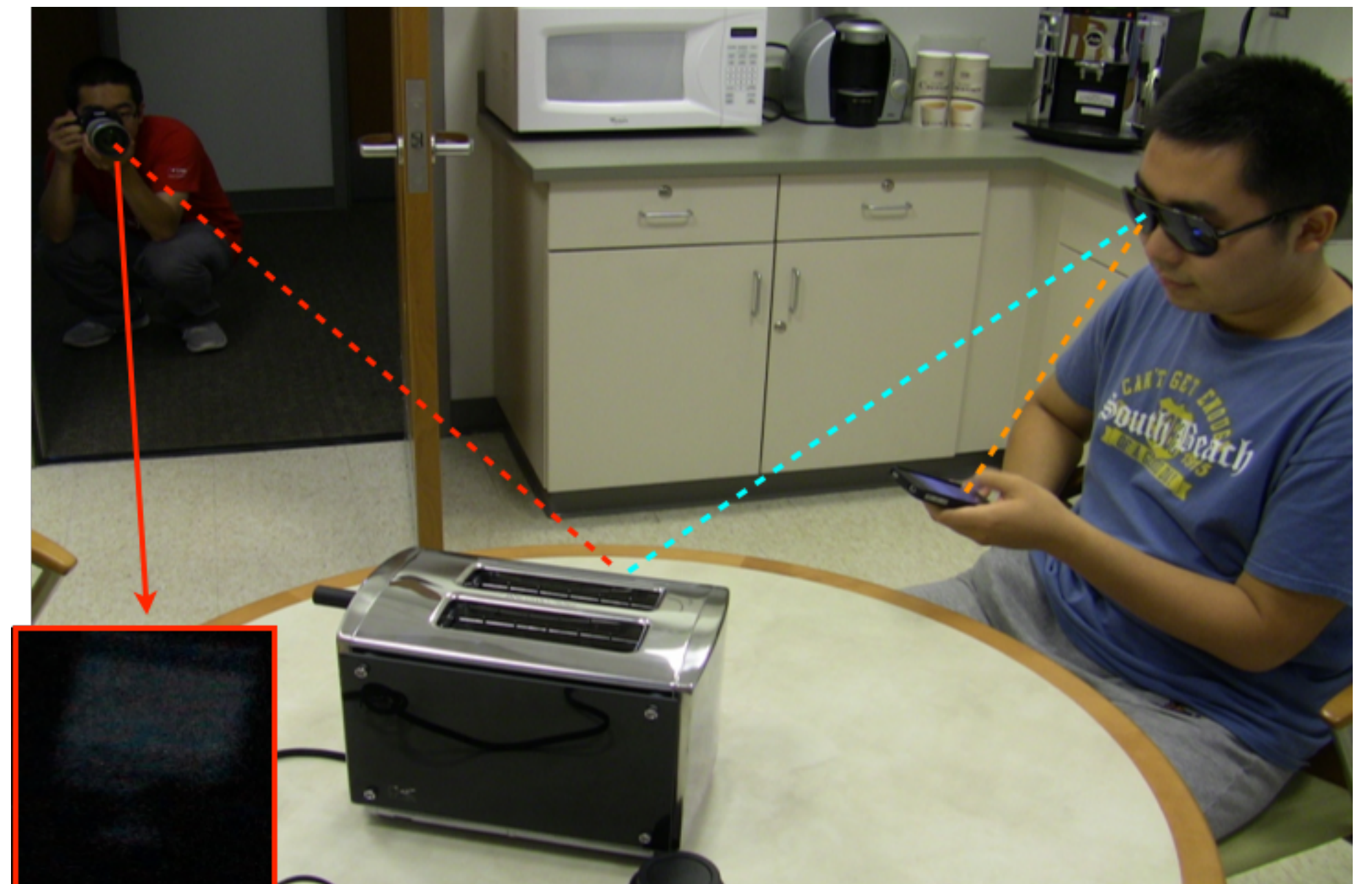


- KeyKeriki v1.0 – 27MHz
- KeyKeriki v2.0 – 2,4GHz
- KeySweeper

aus der Ferne



direkt oder ueber Eck



http://jacobsschool.ucsd.edu/news/news_releases/release.sfe?id=791
<http://cs.unc.edu/~yix/SeeingDouble/images/2.png>

Generation Selfie





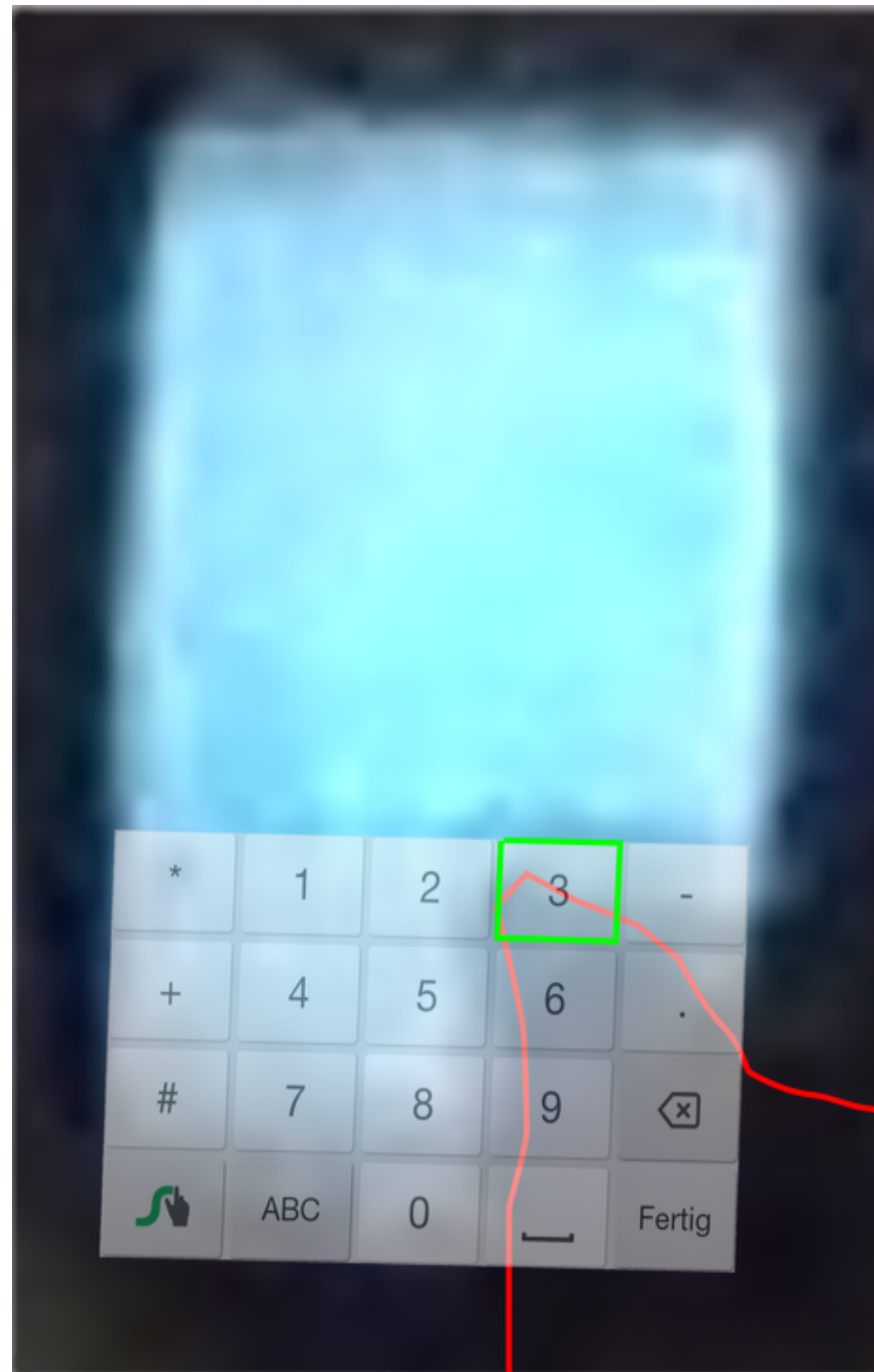




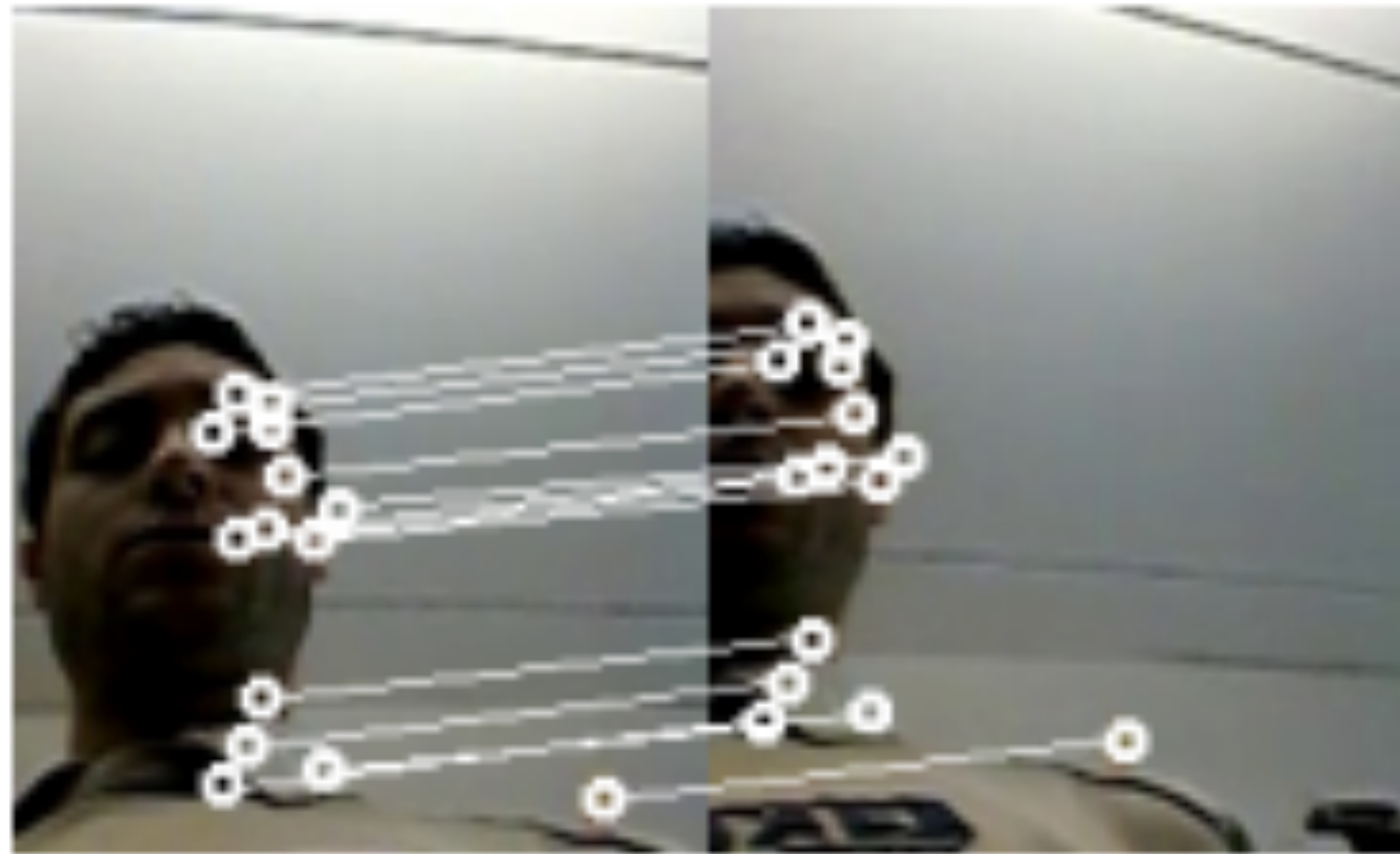




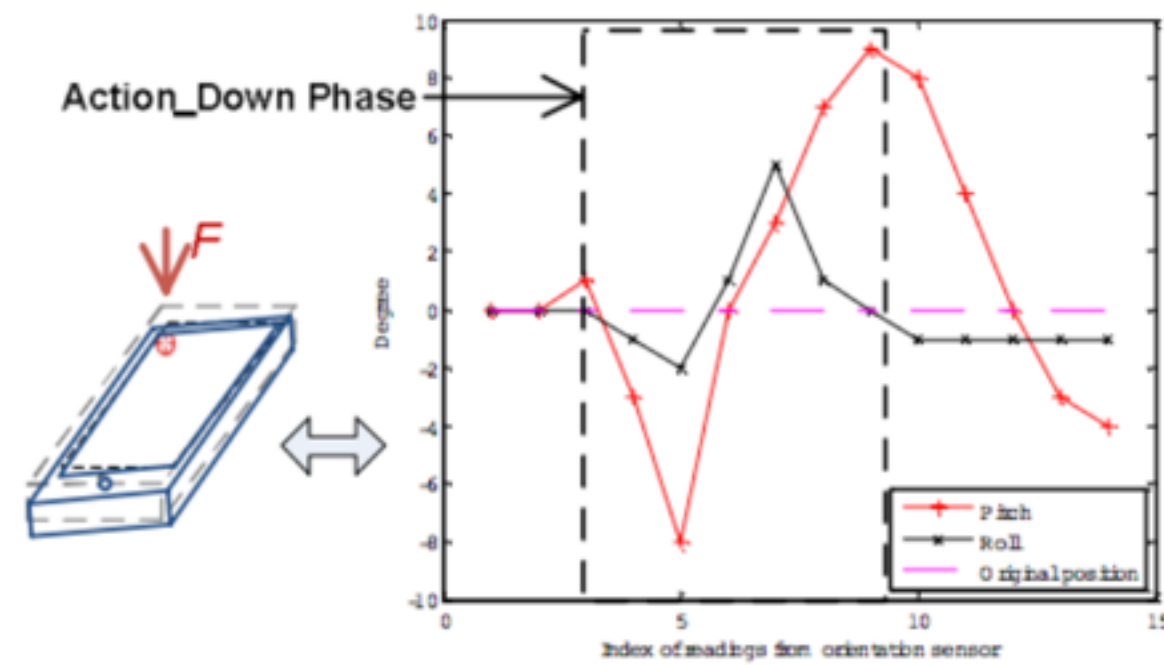
corneal key logger



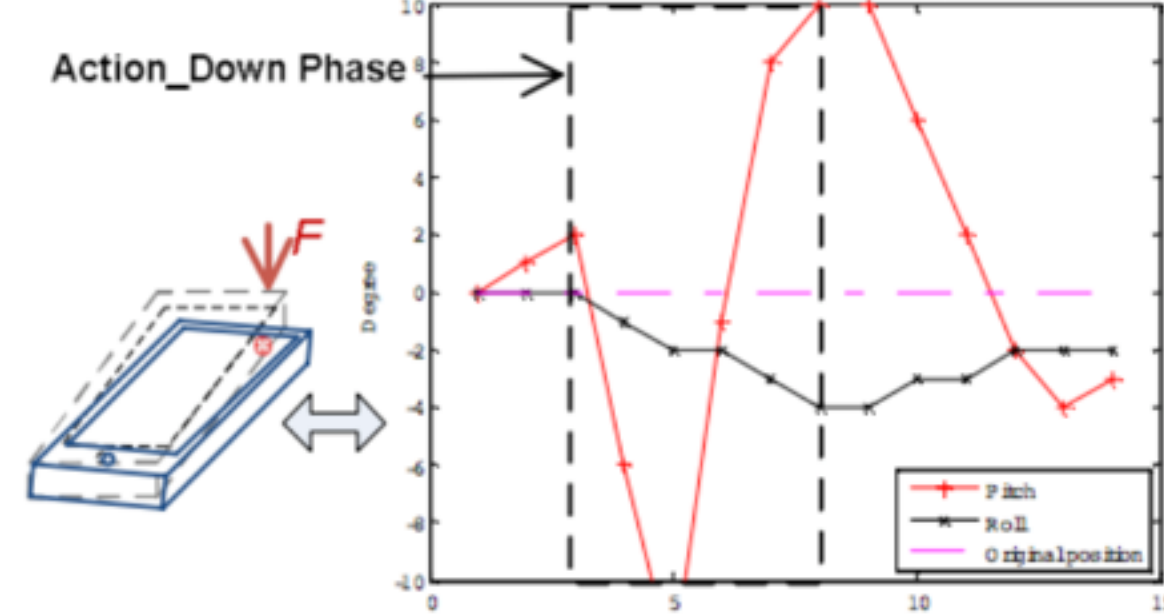
motion detection



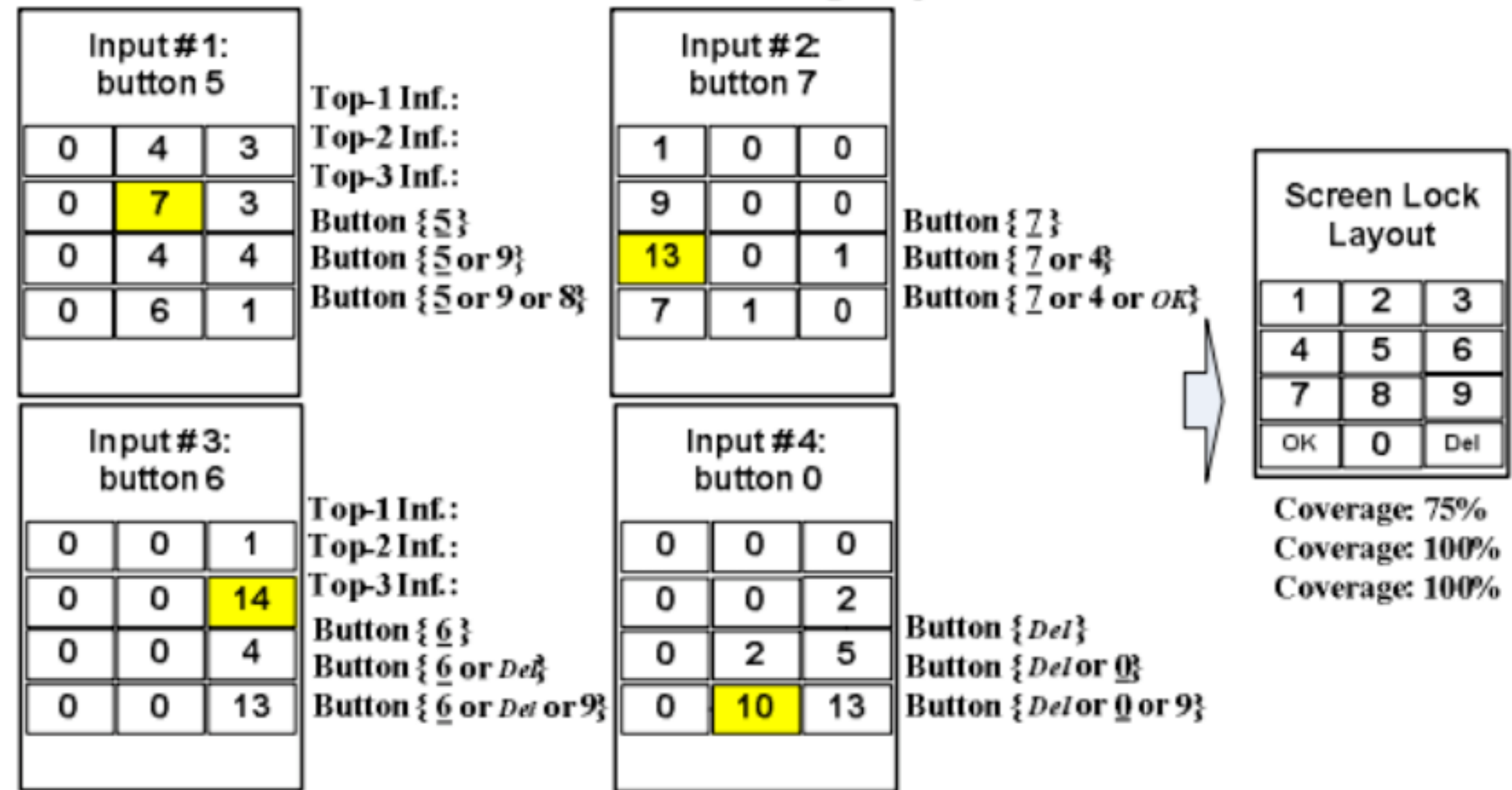
motion detection 2



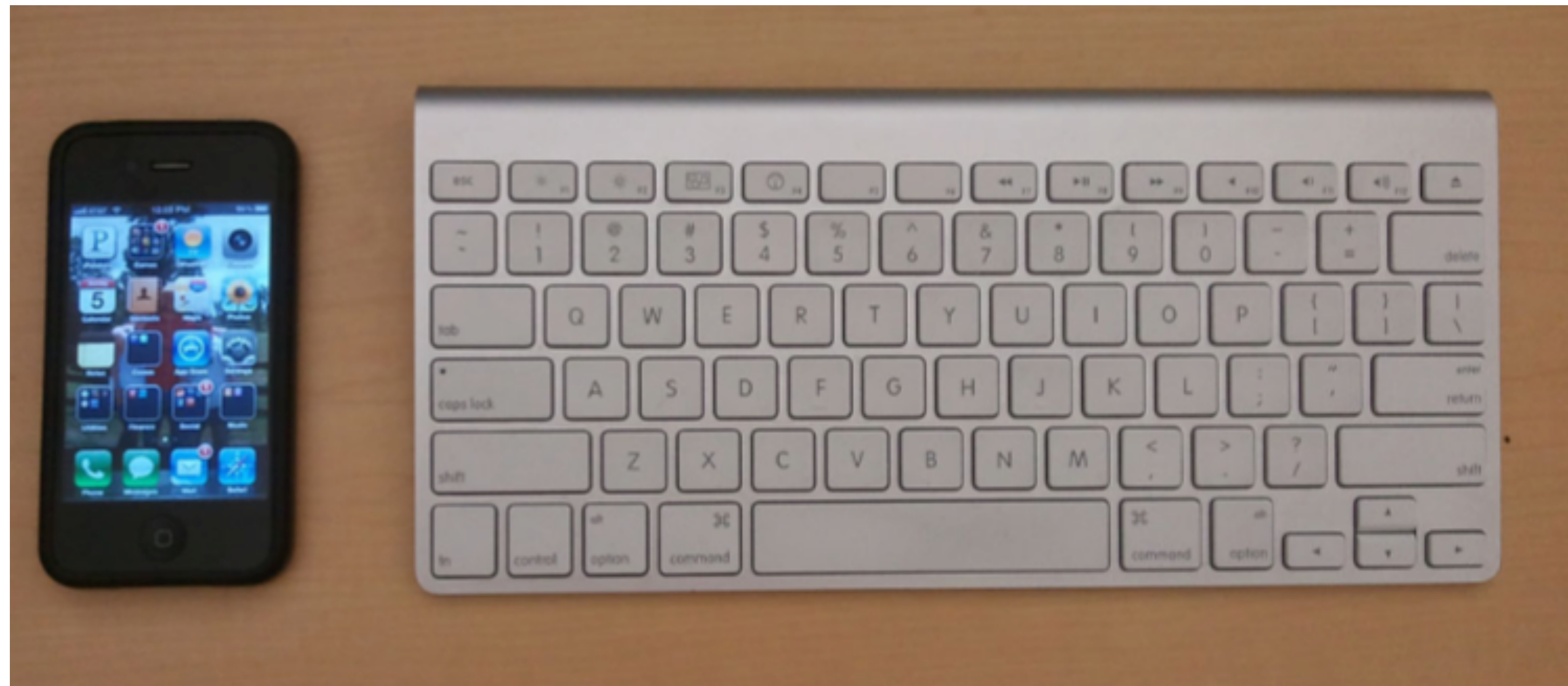
(1. a) when tapping the top left (1.b) corresponding orientation sensor readings during the tap event



Distribution of inferred labels after entering the passwords "5 7 6 0" for 32 rounds



motion detection 3

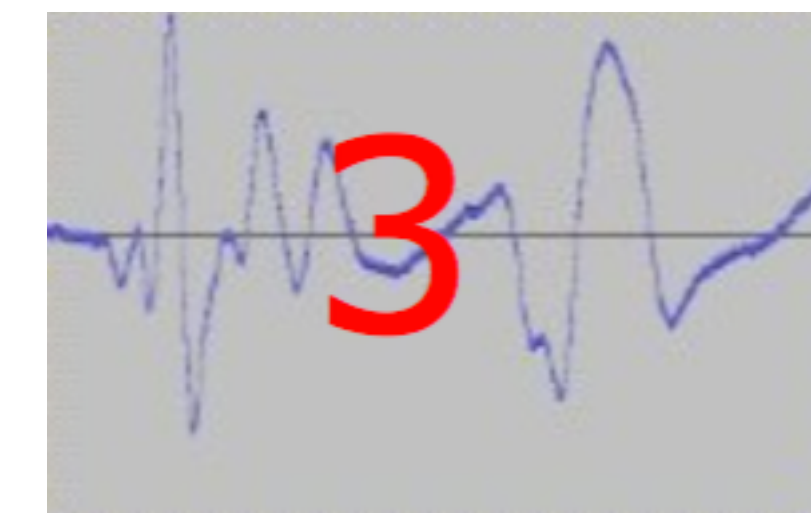
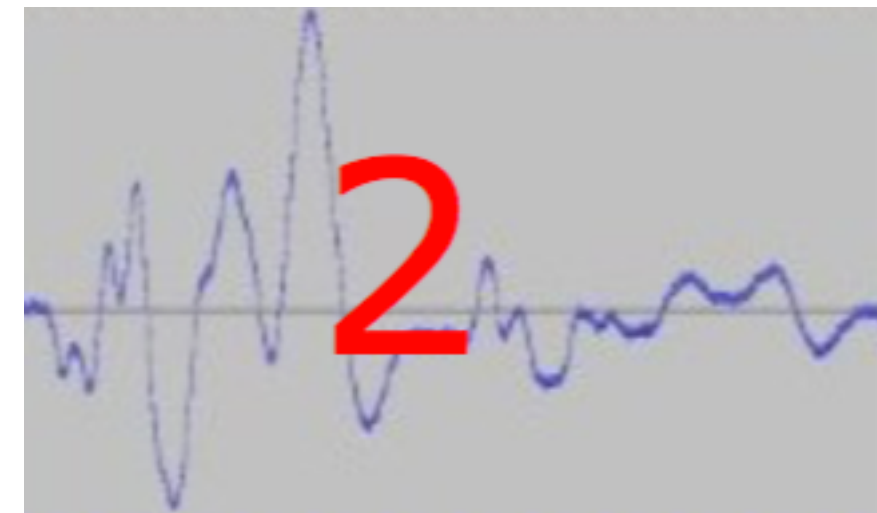
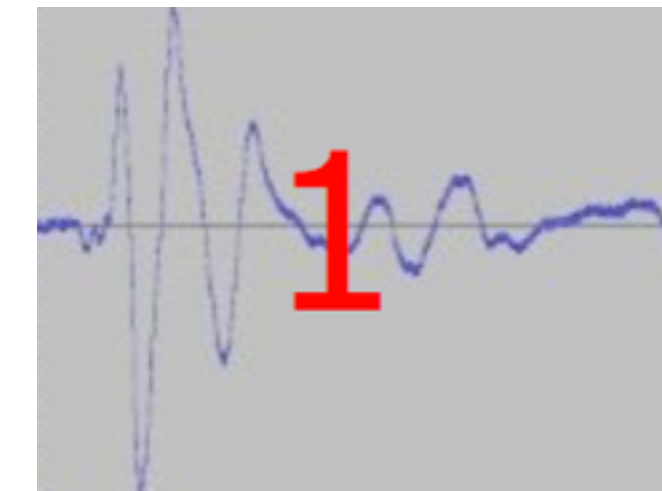
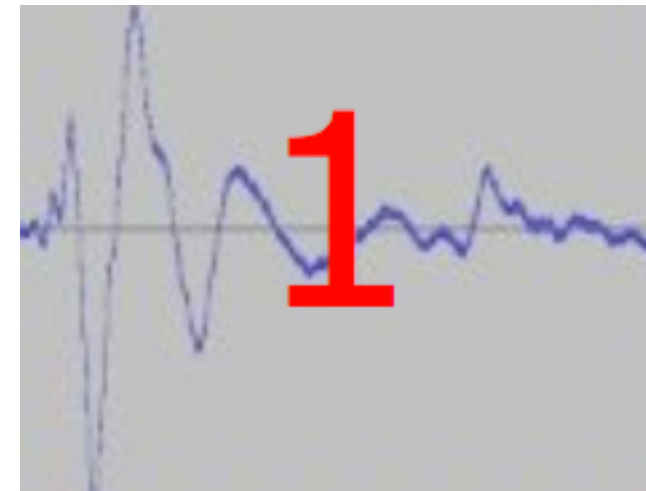
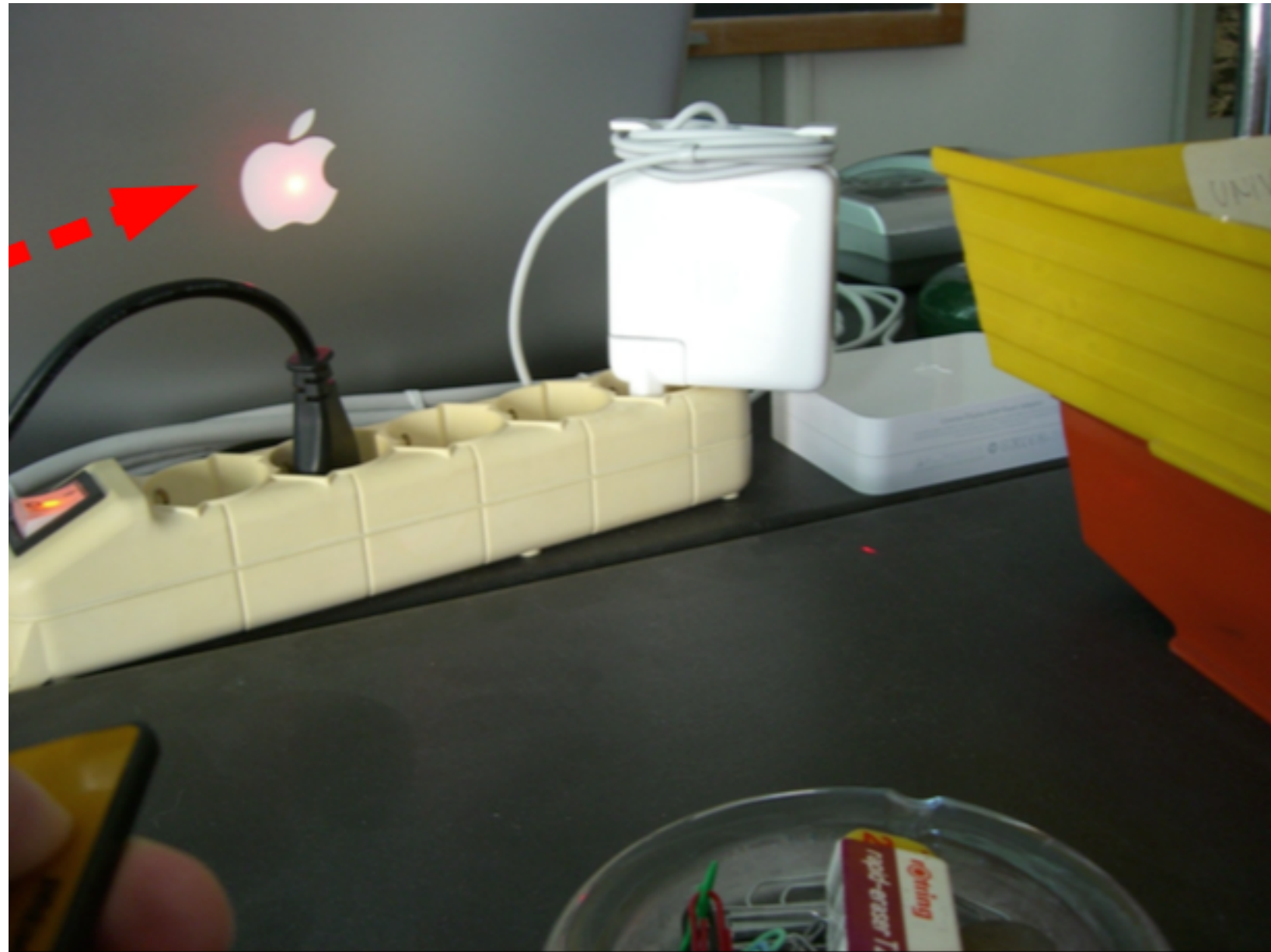


(sp)iPhone: Decoding Vibrations From Nearby Keyboards Using Mobile Phone Accelerometers

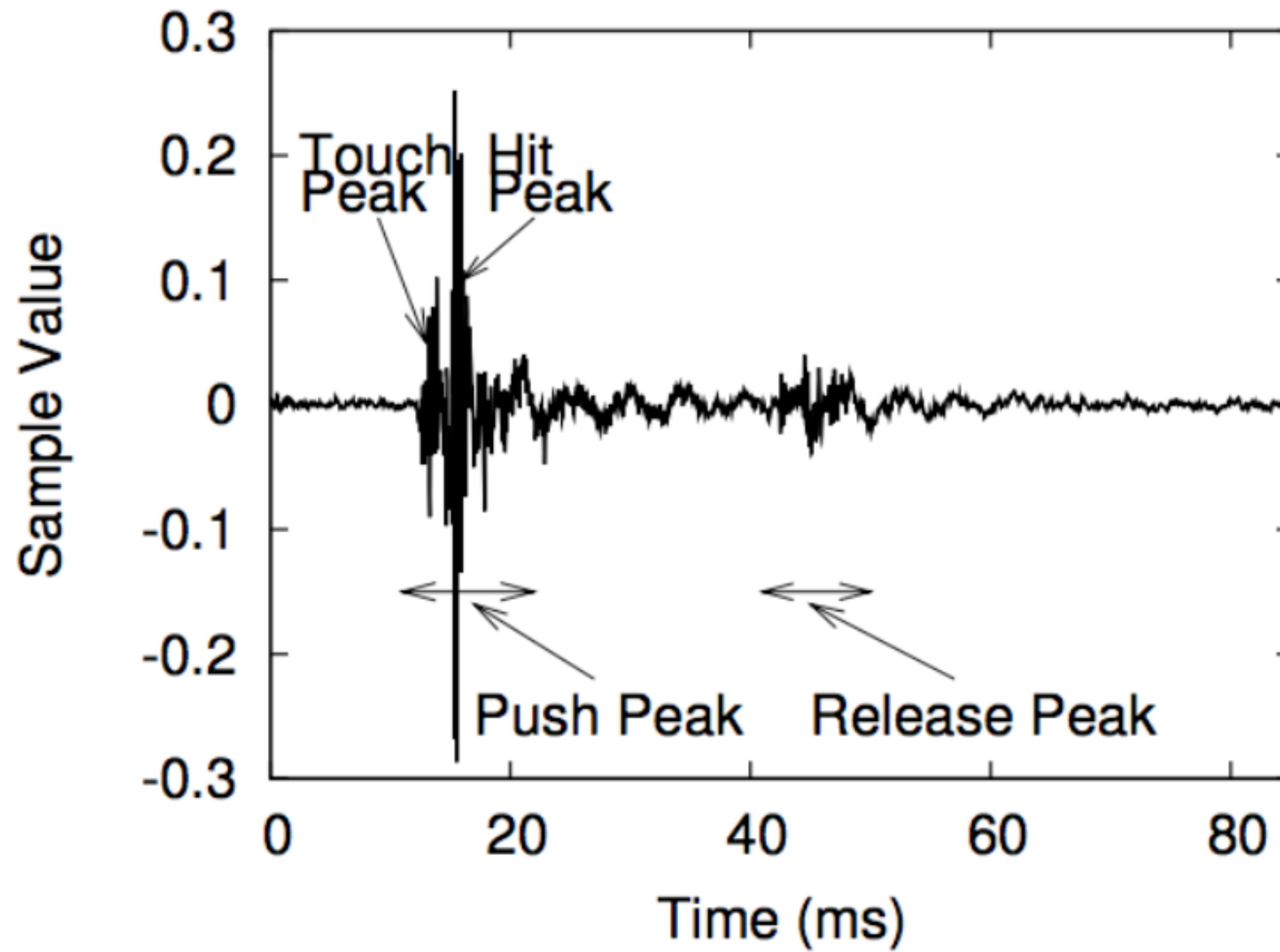
Smartwatch und Fitbit



motion detection 5



Tastaturgeräusche



visual microphone



High speed video
(actual video playing here)

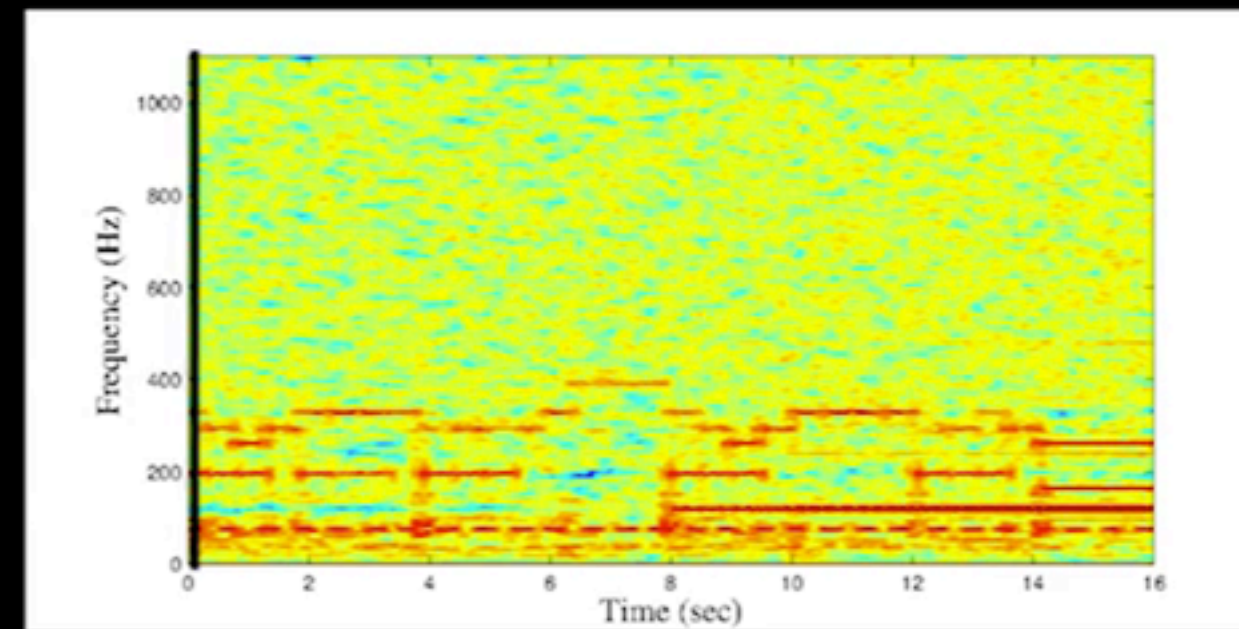


Object

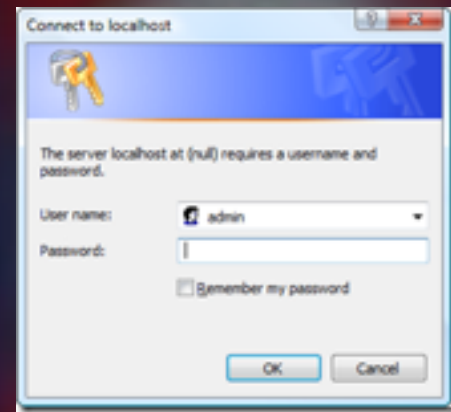
visual microphone



High speed video
(actual video playing here)



Sound Recovered
From Video



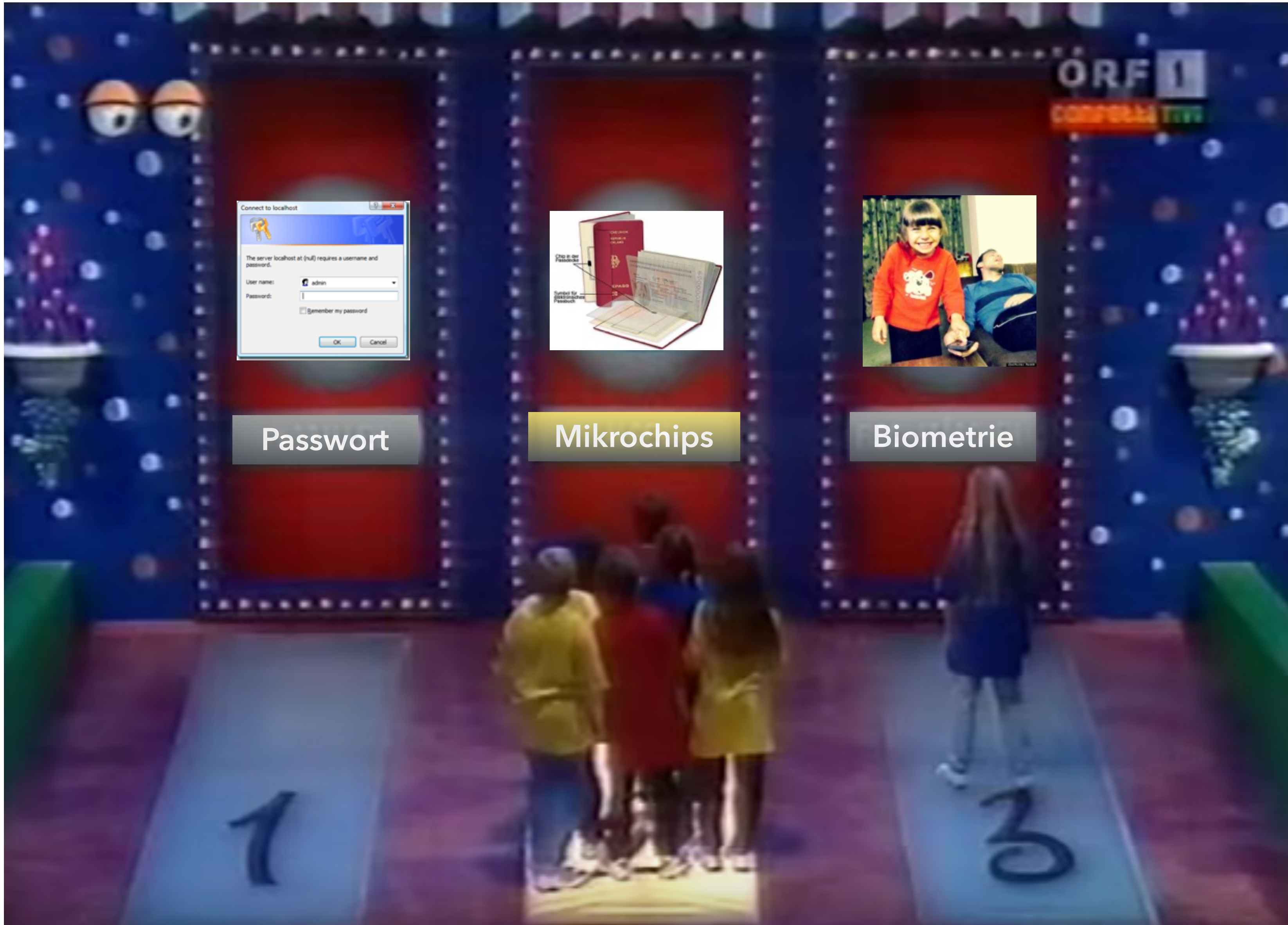
Passwort



Mikrochips



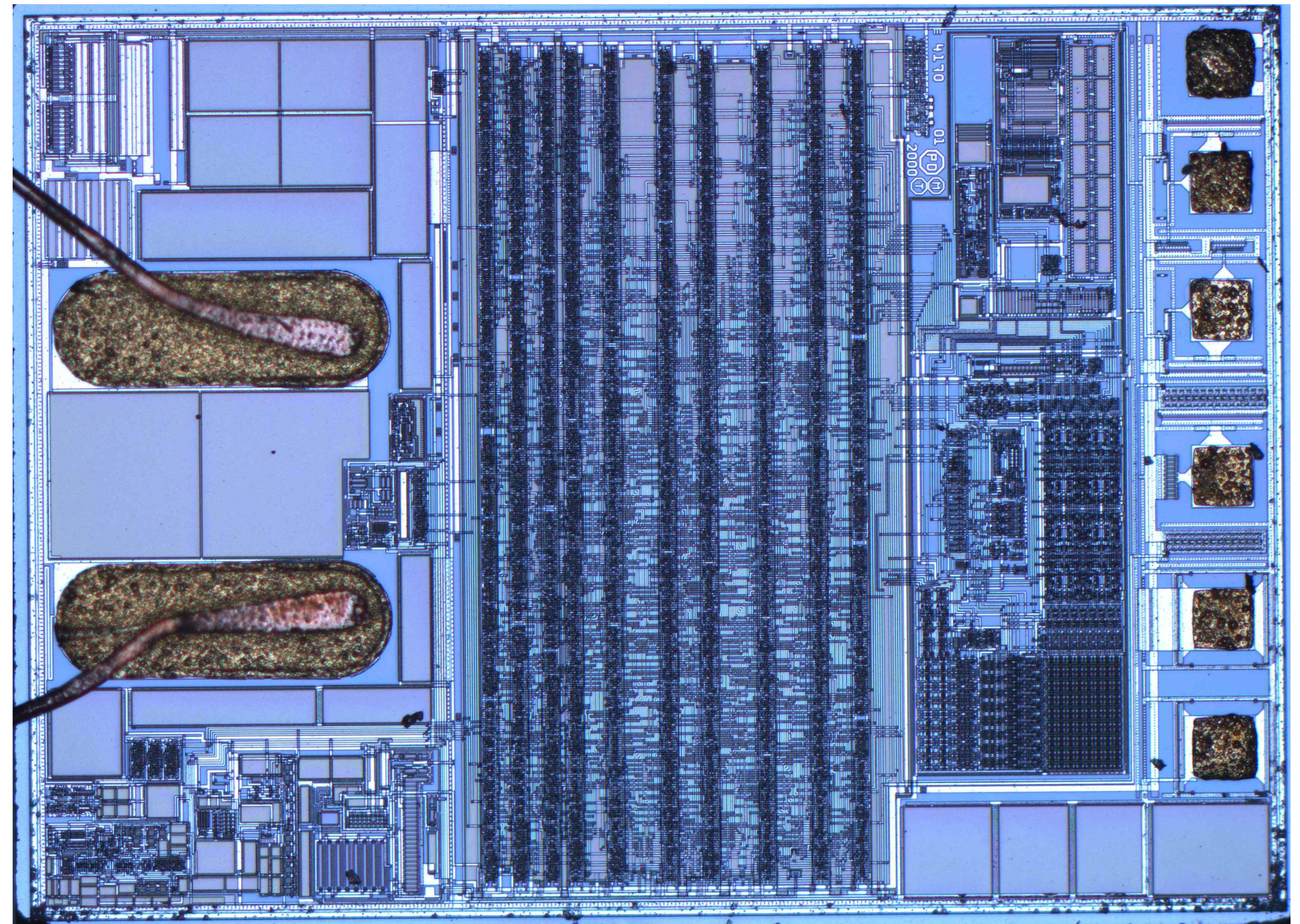
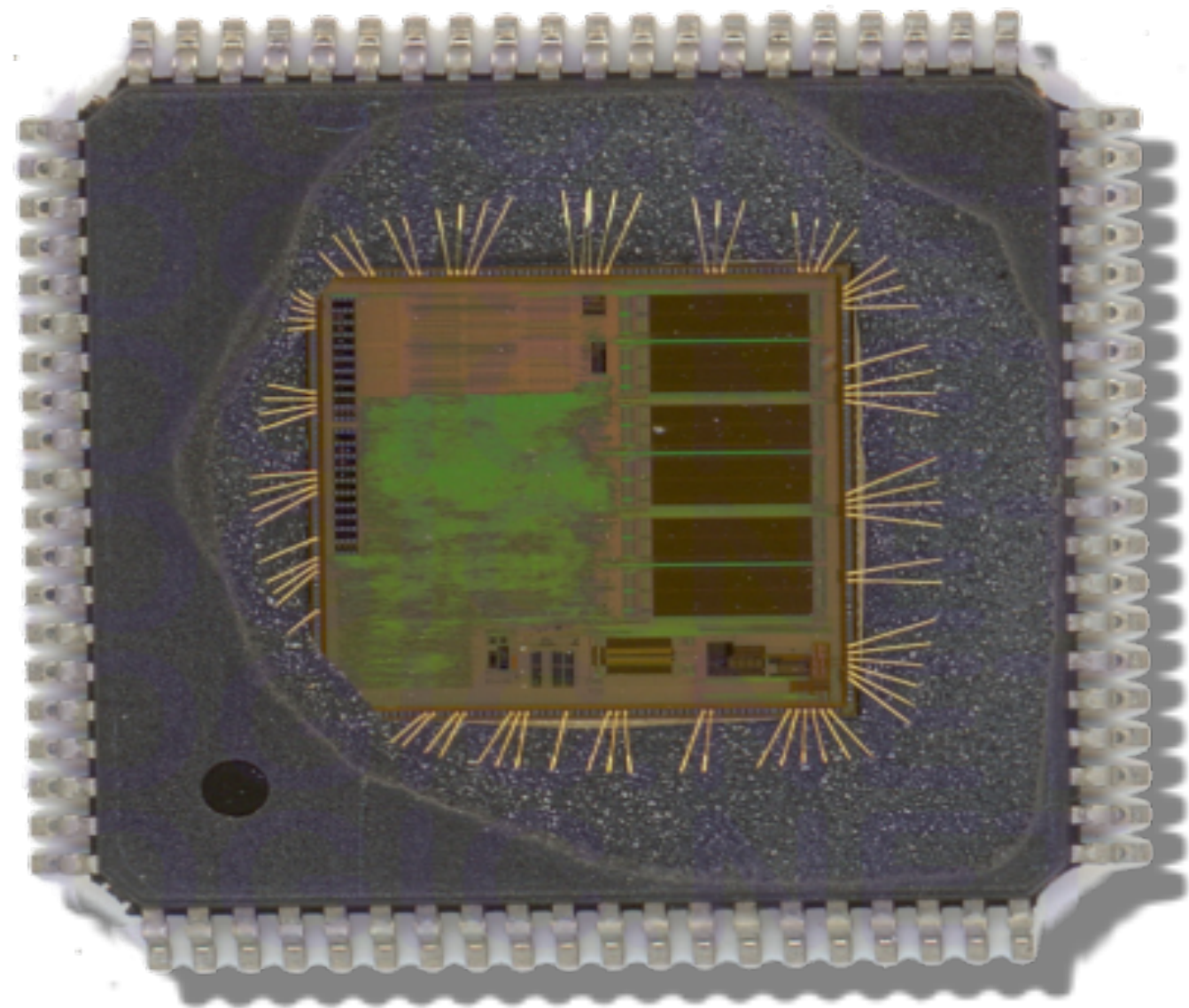
Biometrie



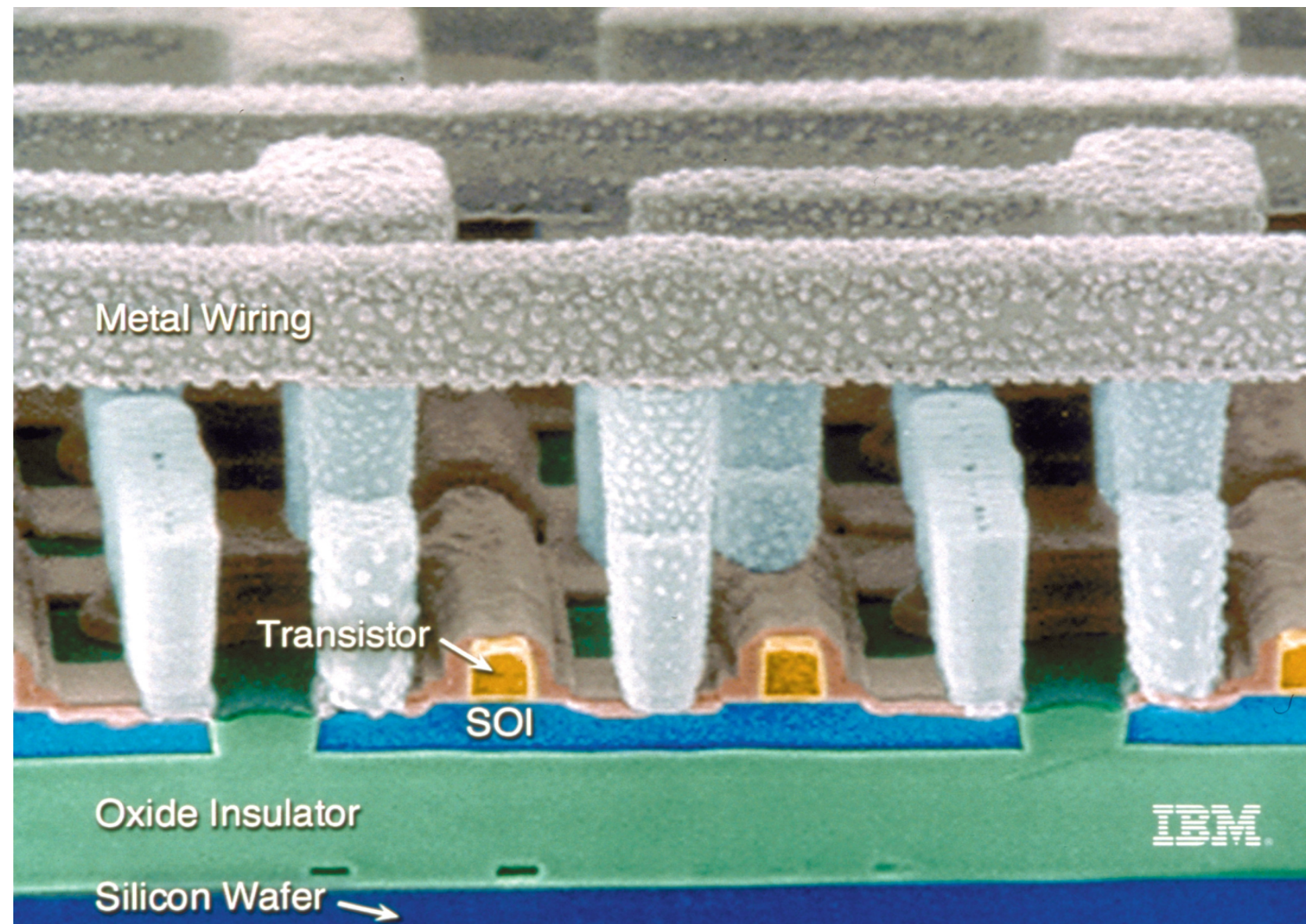
Chip extrahieren



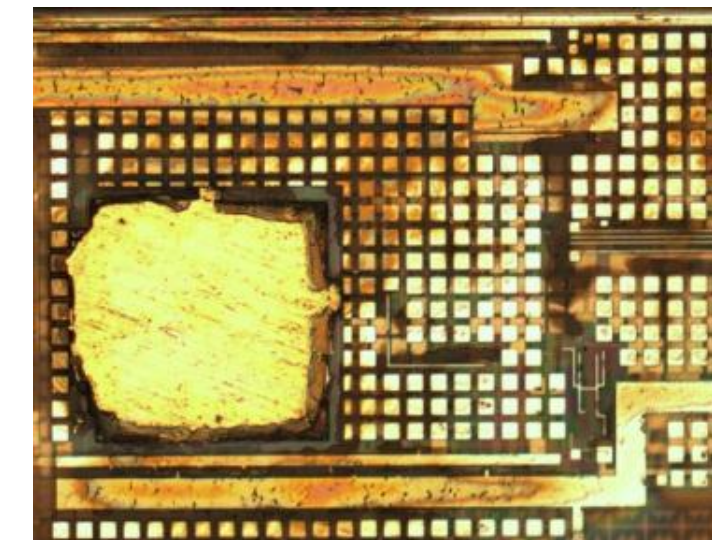
chip extrahieren



Aufbau eines Chips

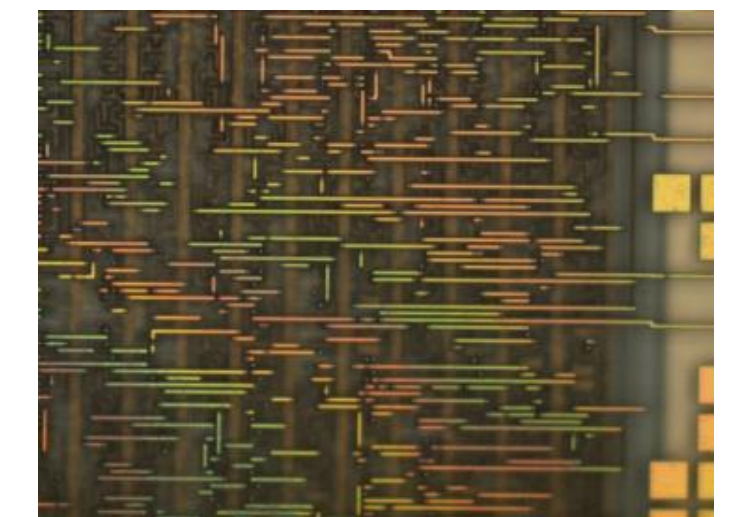
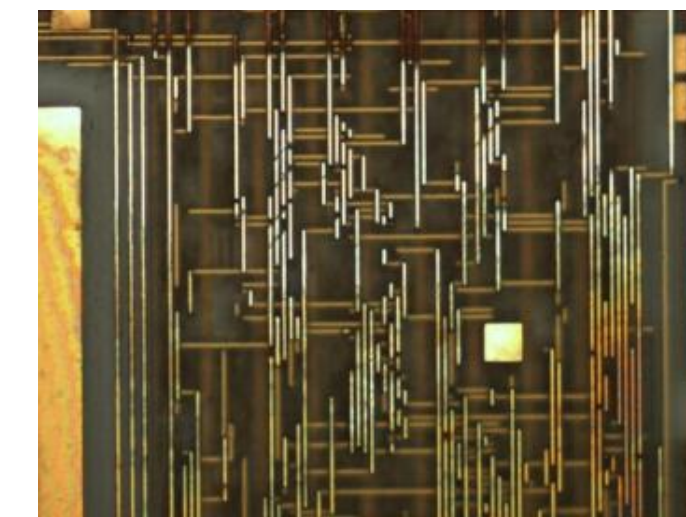
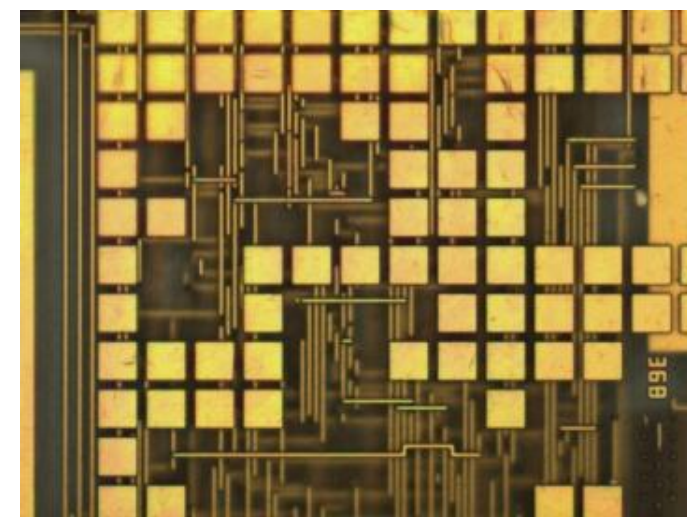


http://www.ece.utep.edu/courses/web5392/Notes_files/mos_fabrication.ppt.pdf



Cover layer

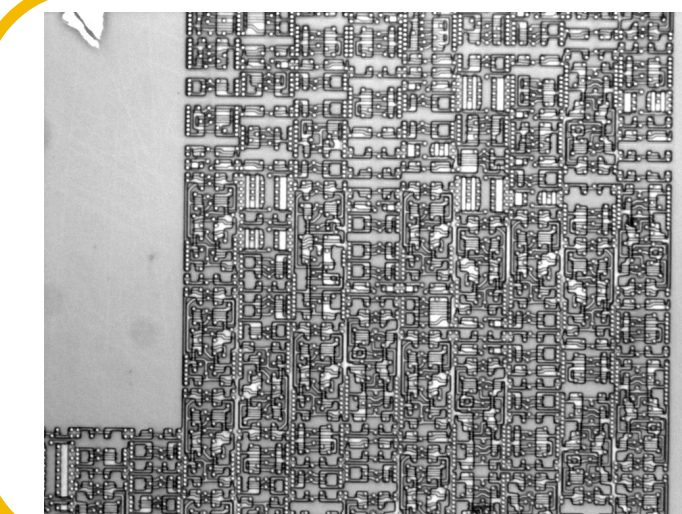
3 Interconnection layer



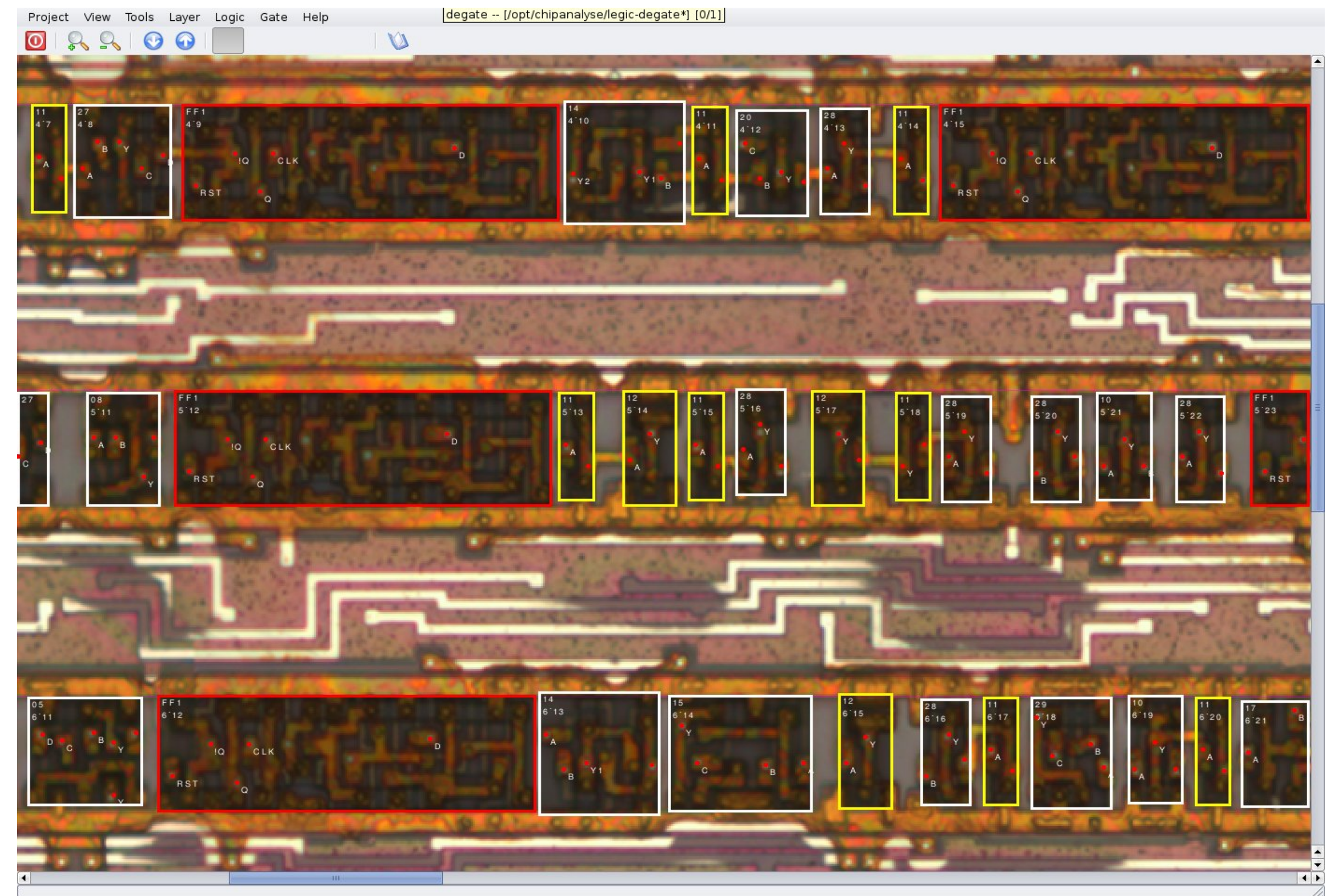
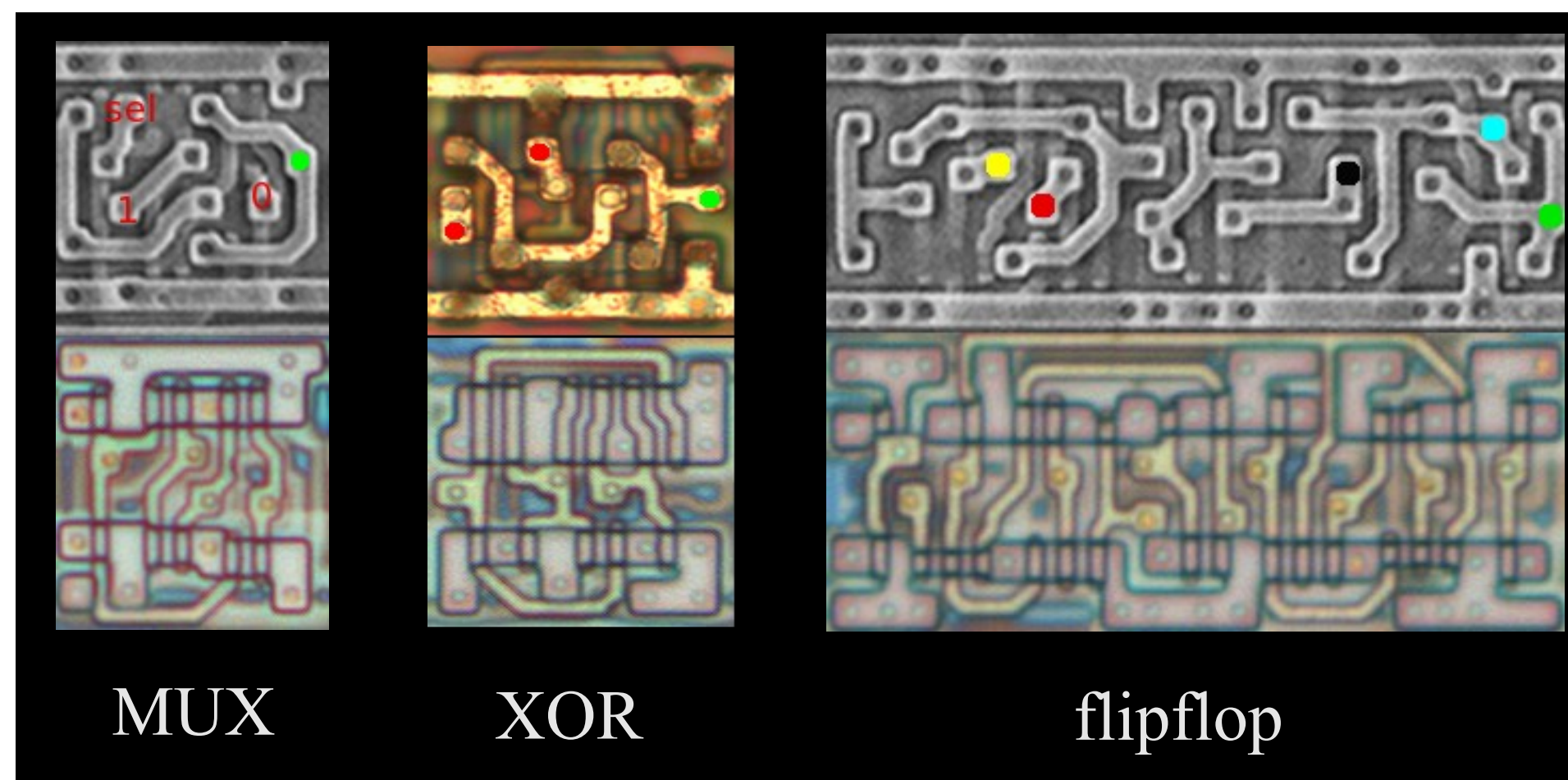
Logic layer



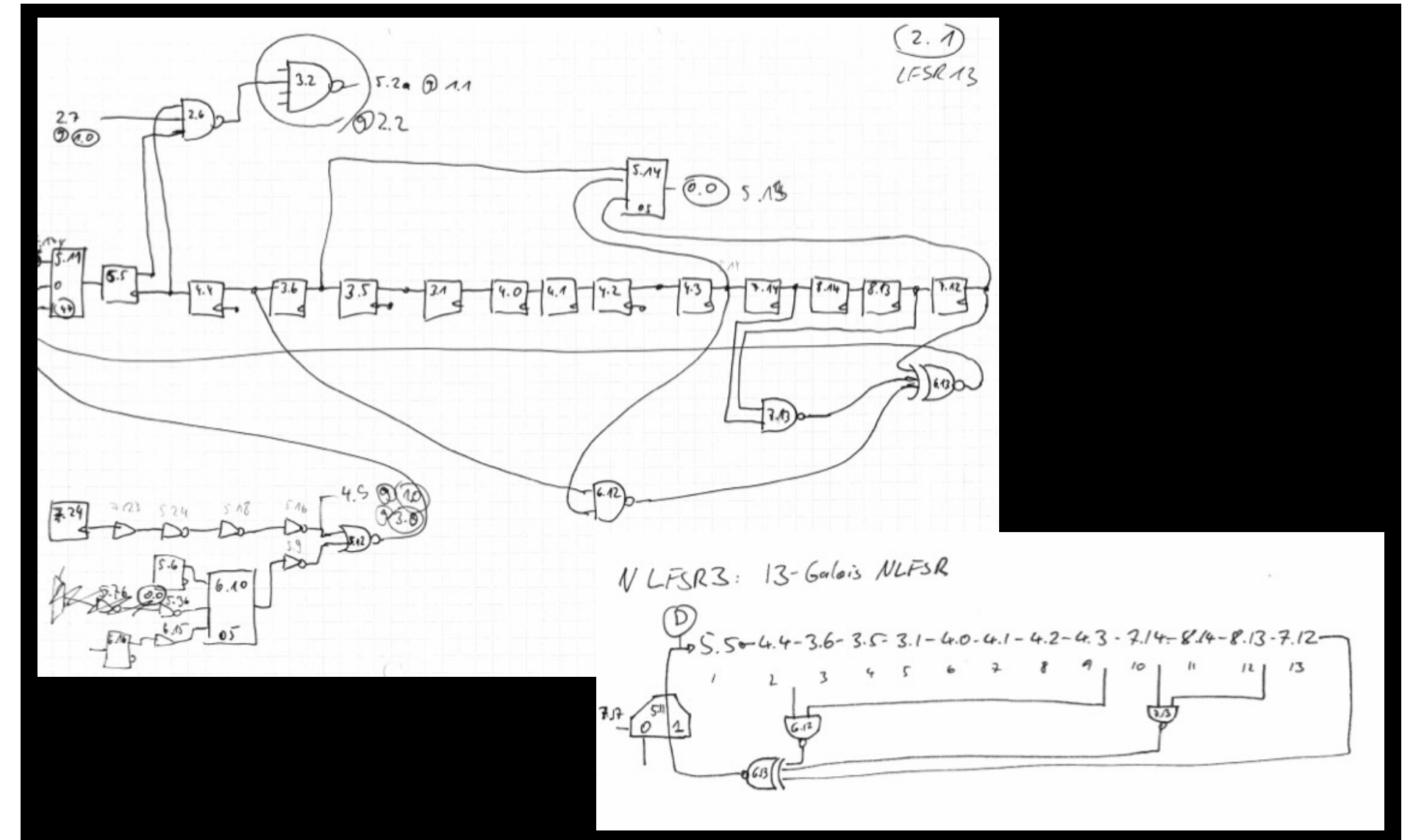
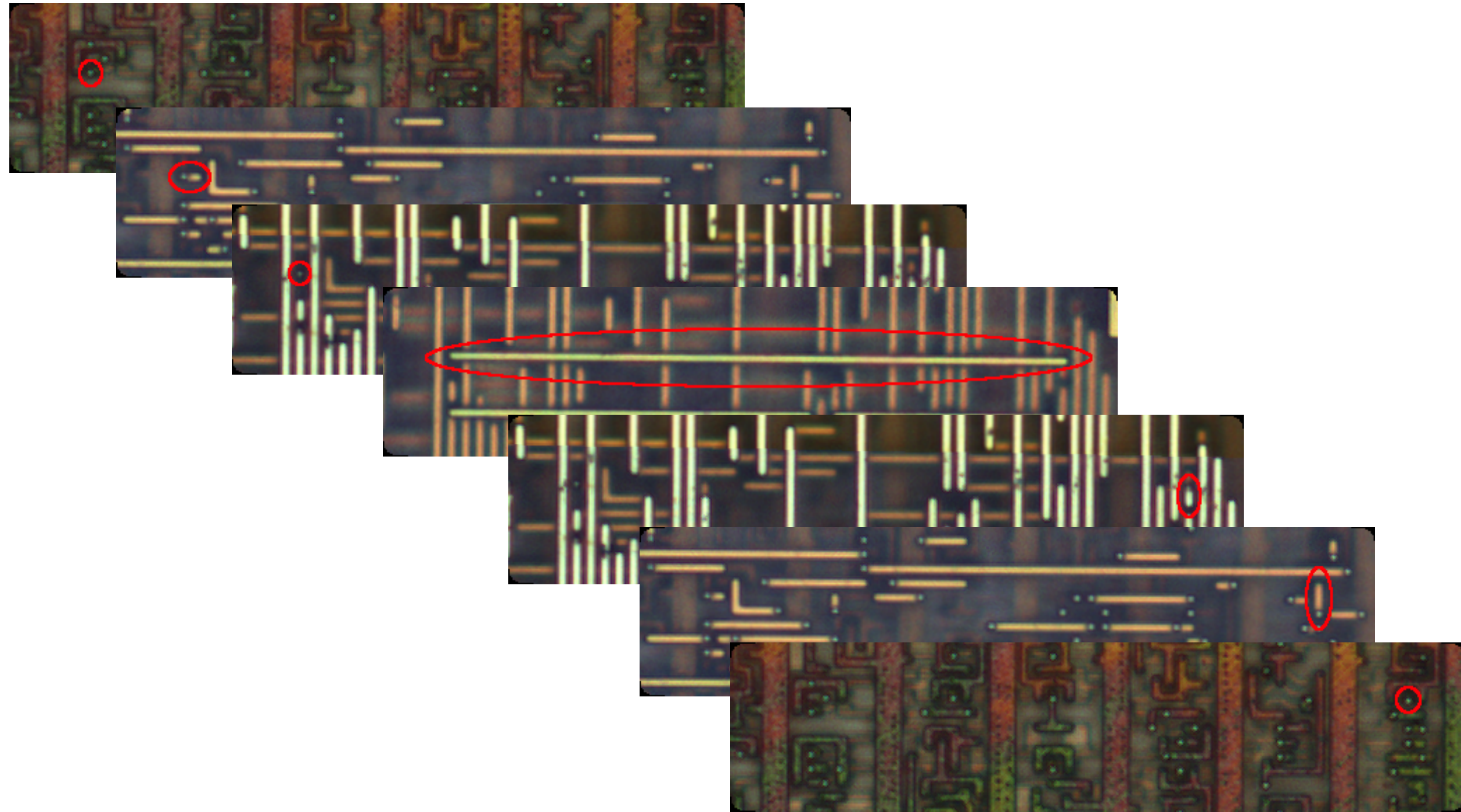
Transistor layer



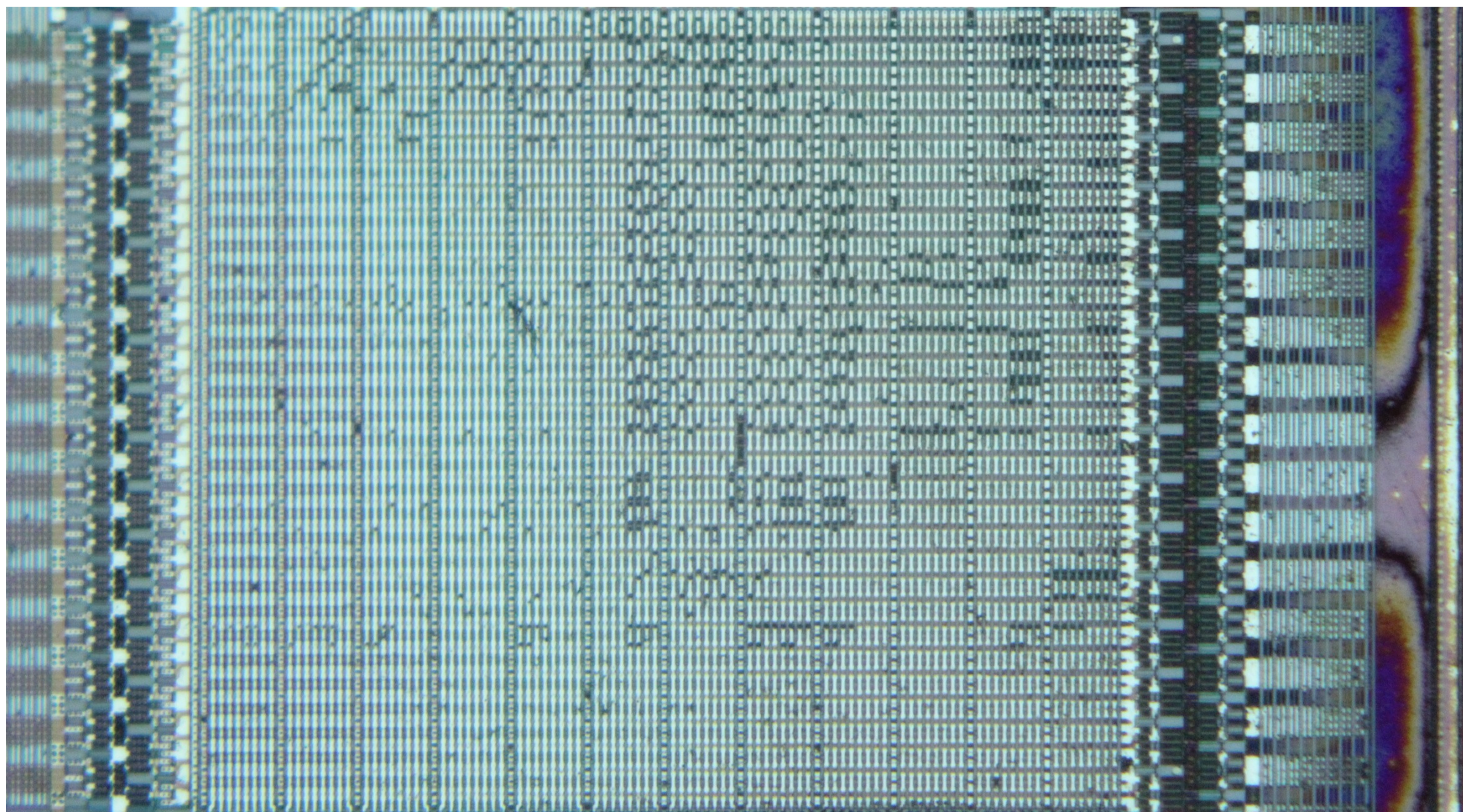
Gatter



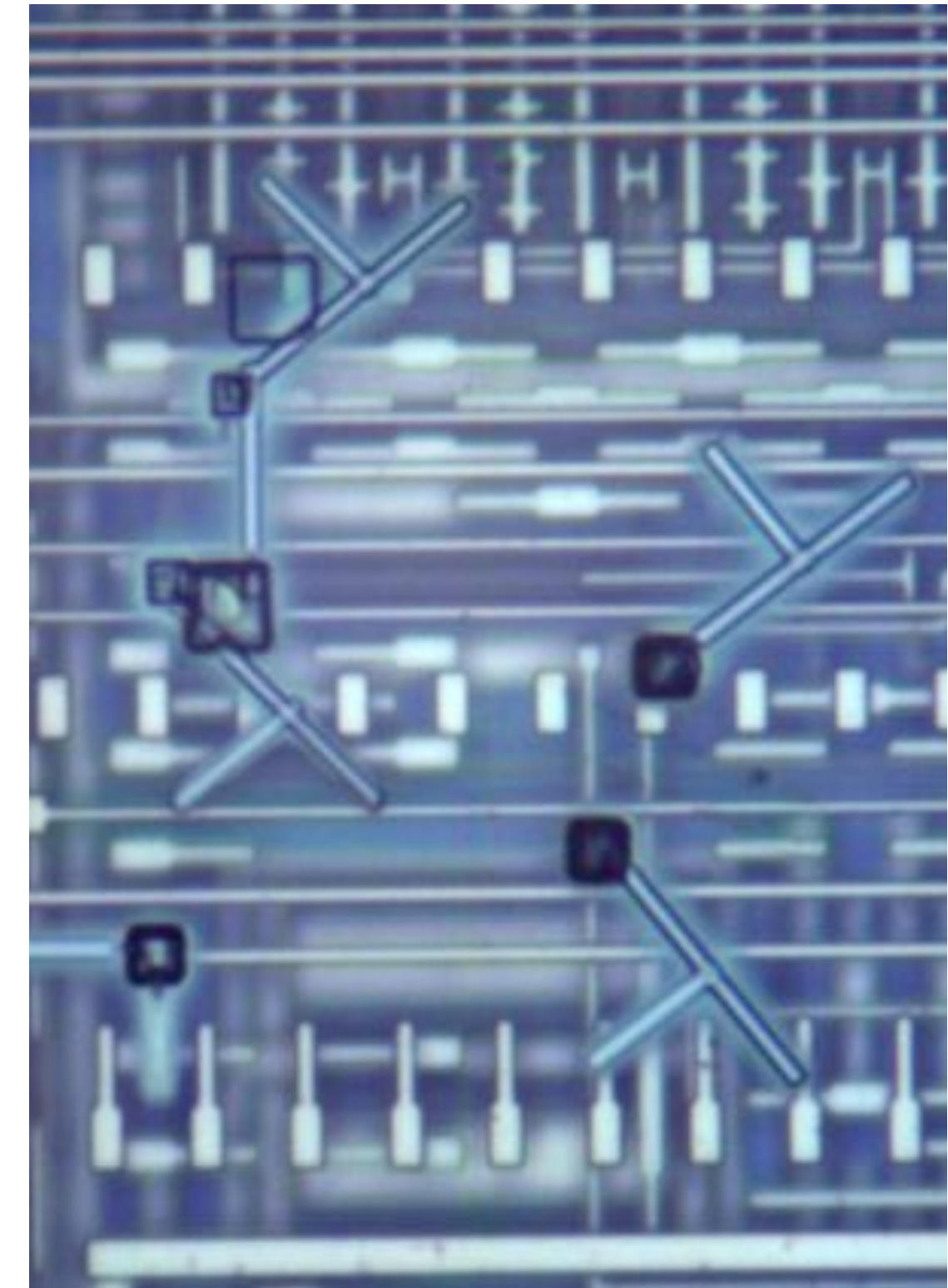
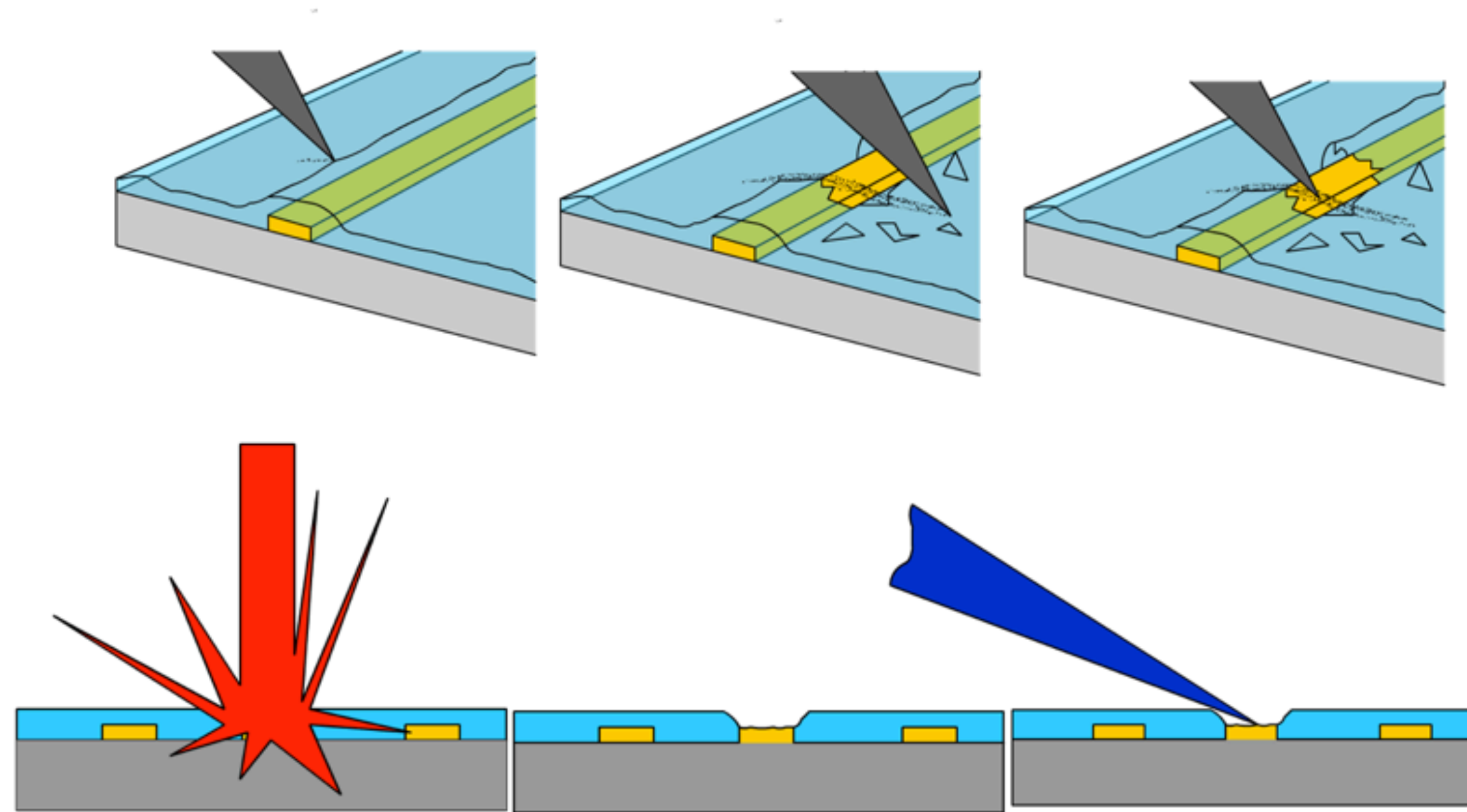
Tracing



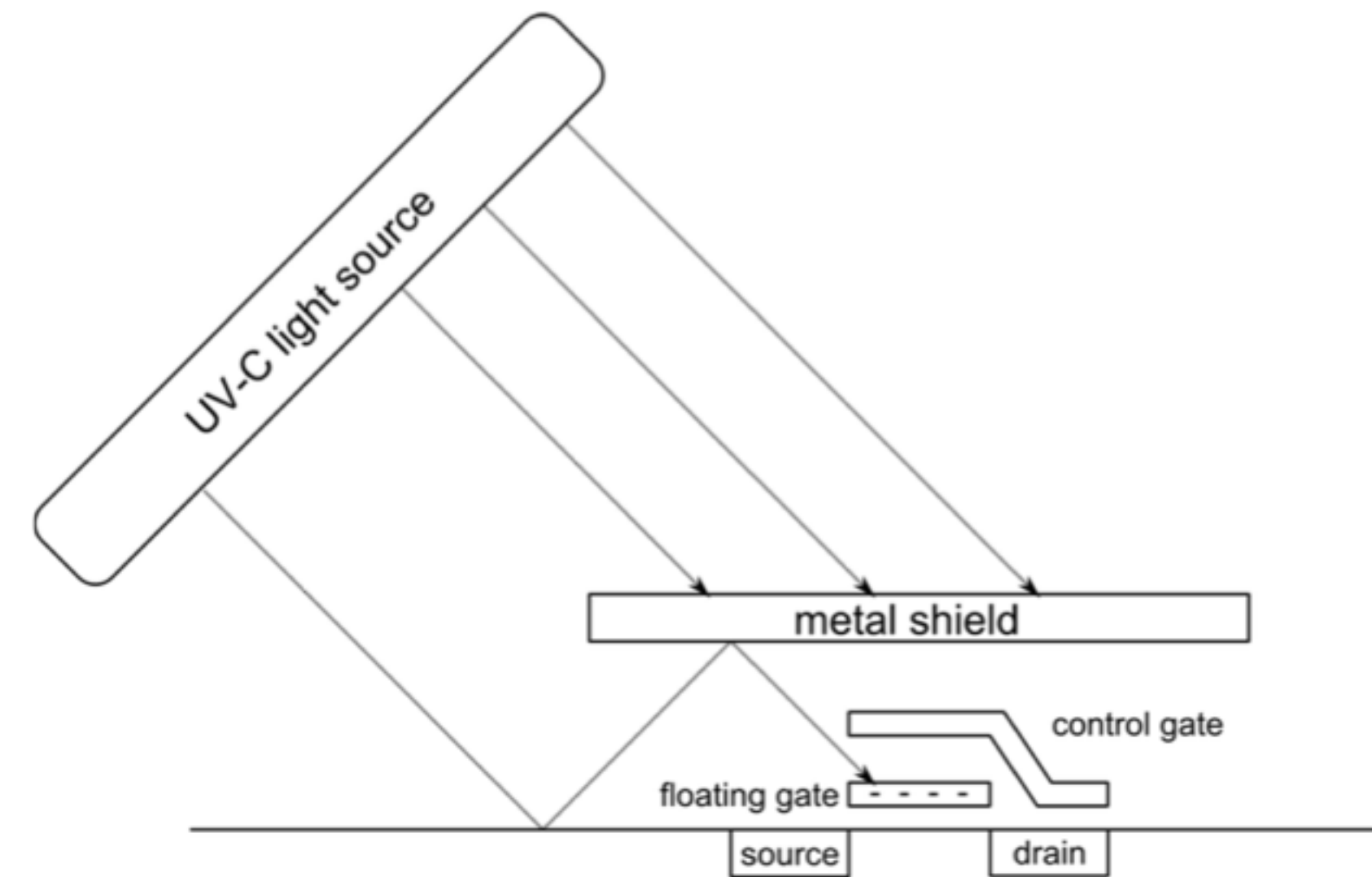
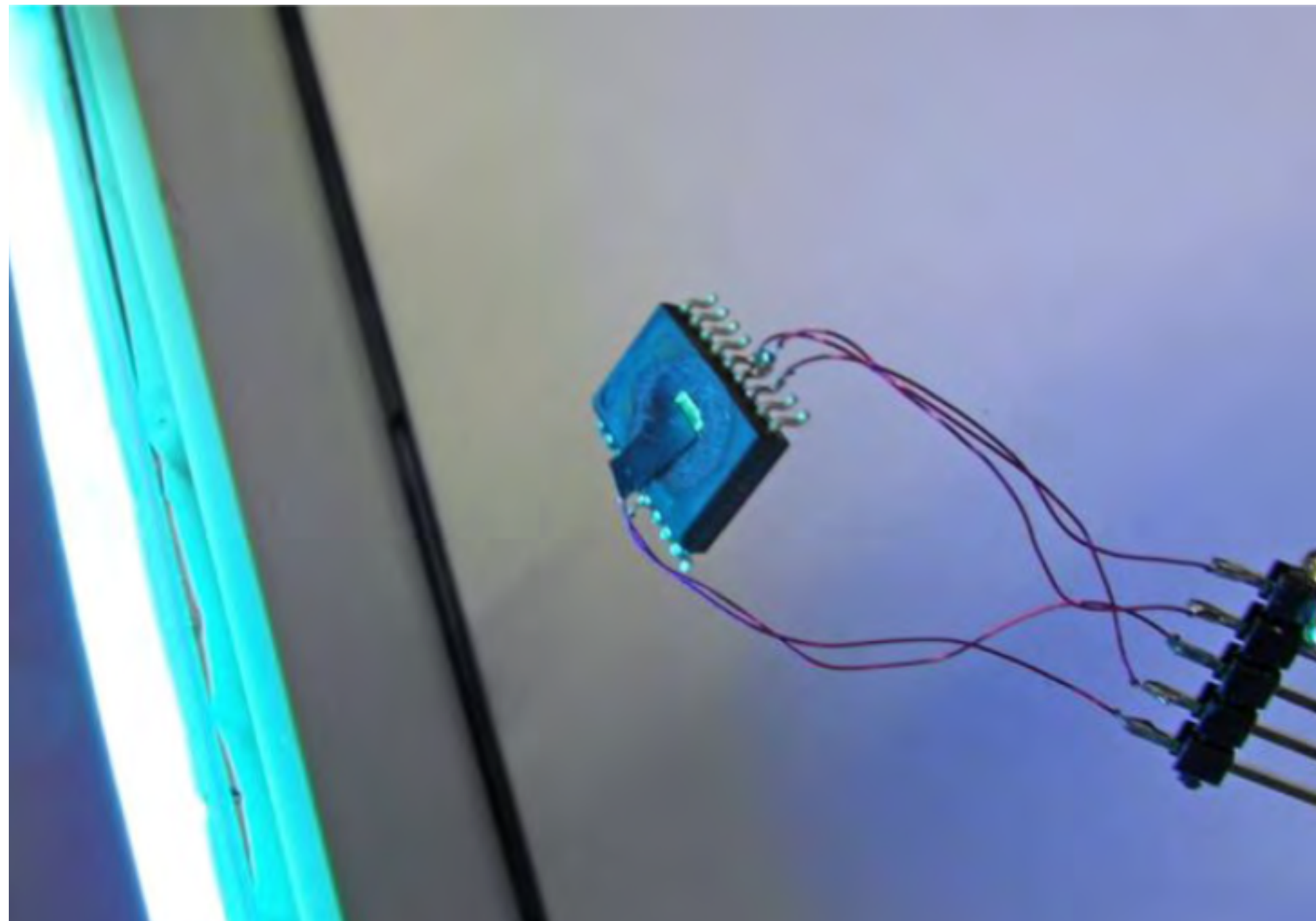
ROM readout



probing

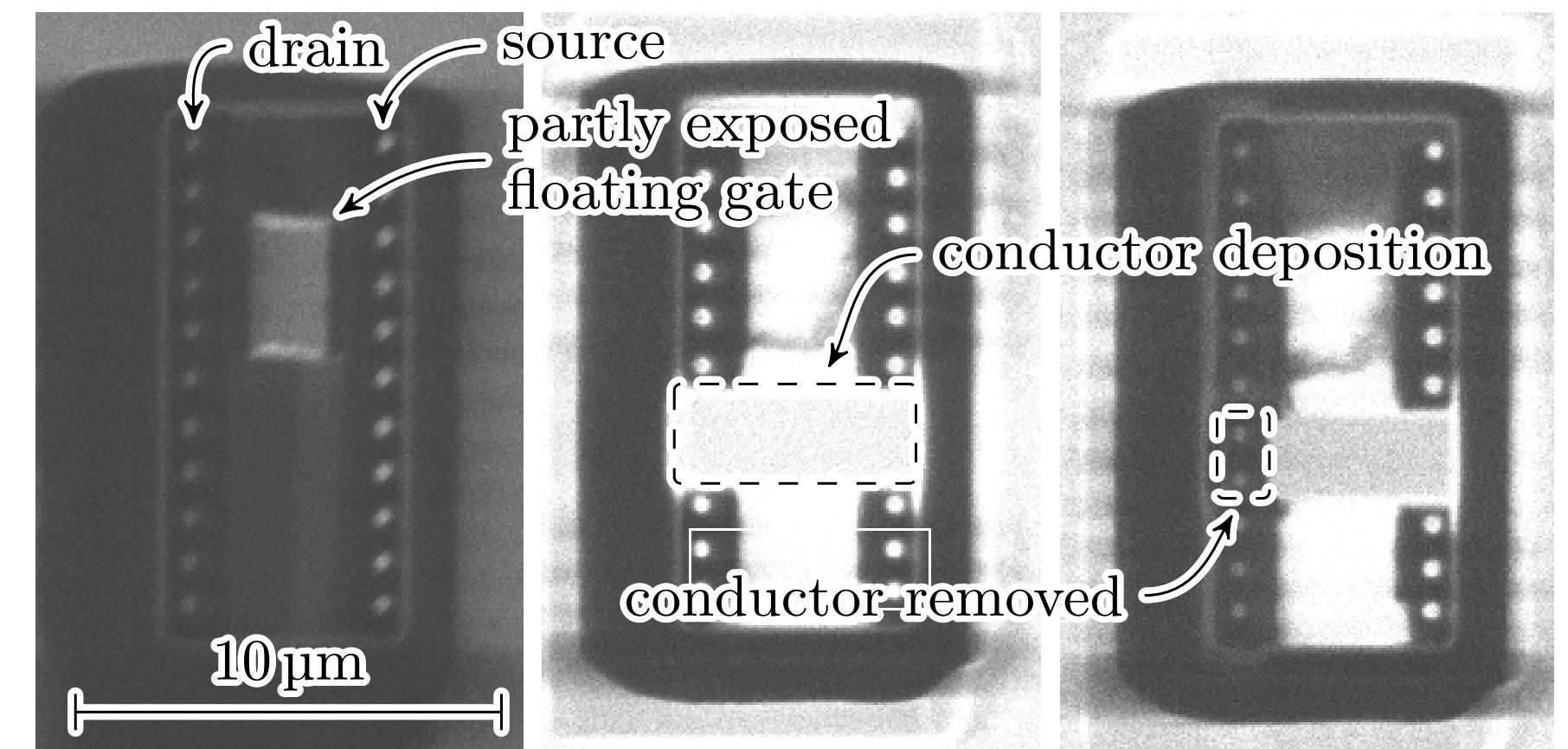
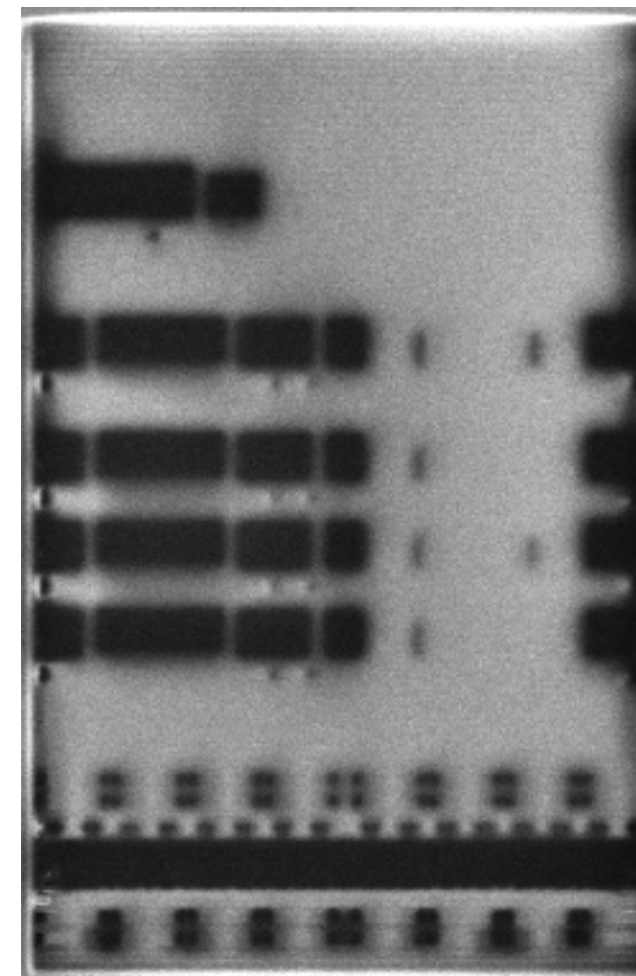
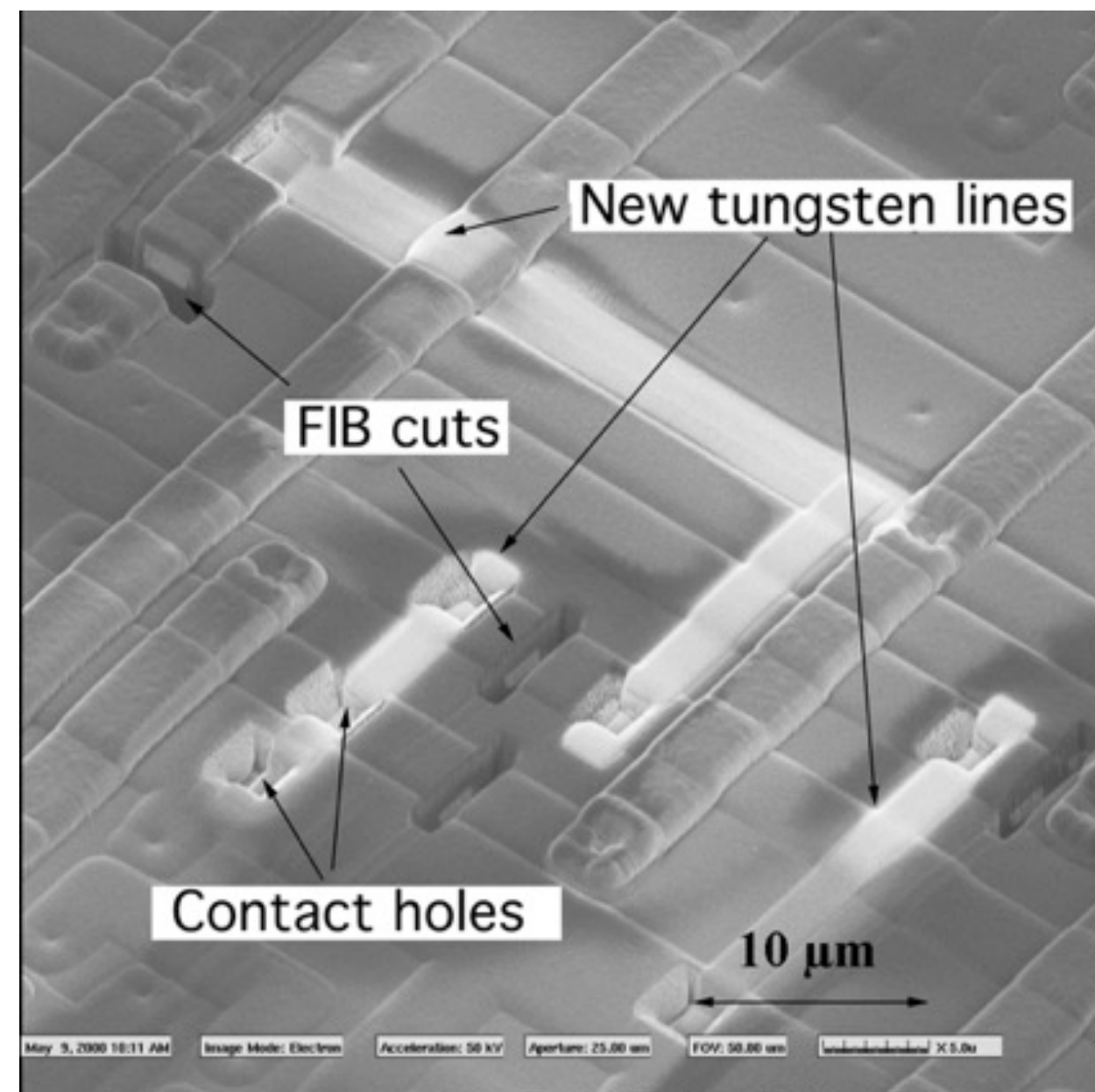


Fuses

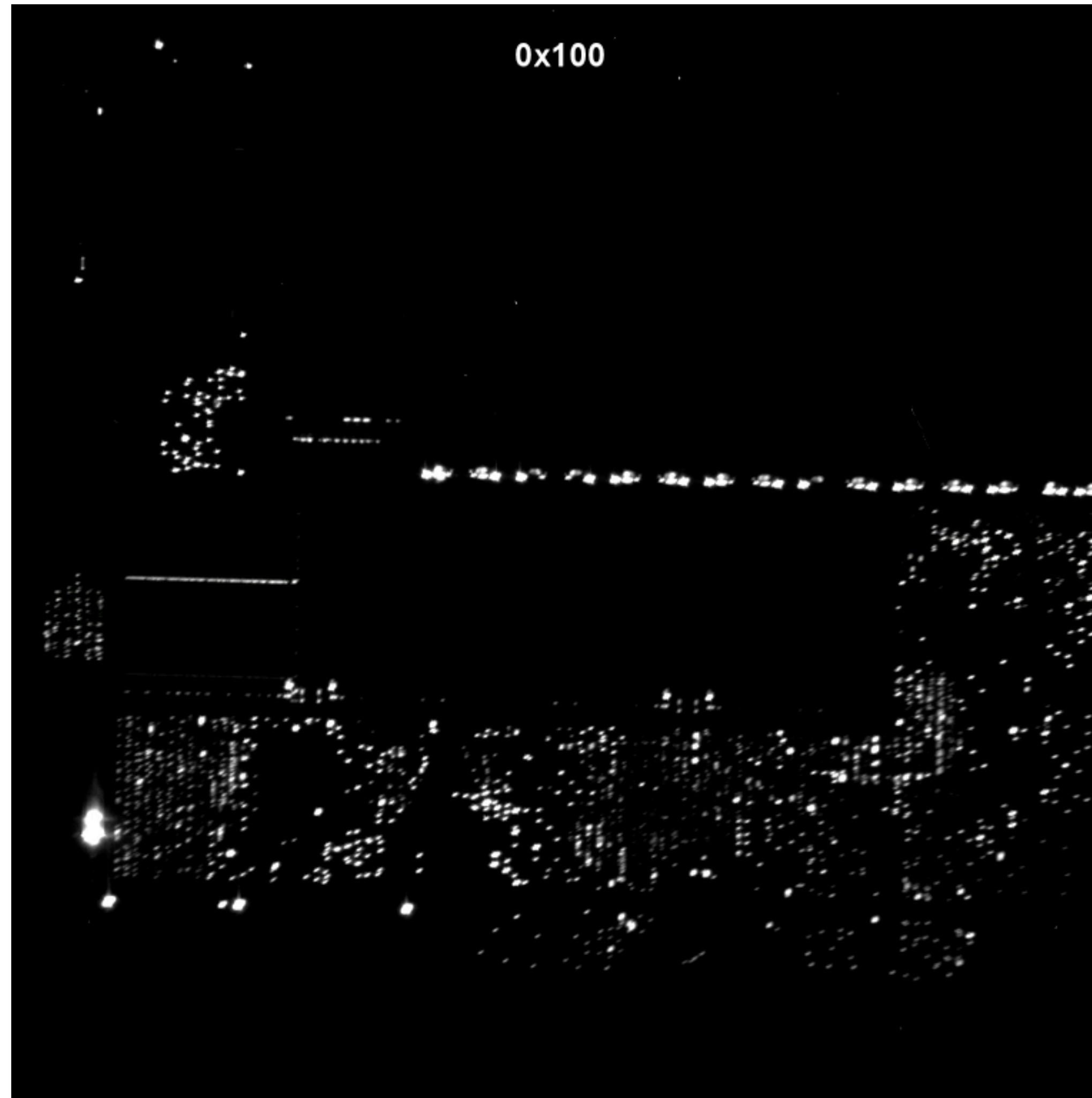


Quelle: Timo Kasper

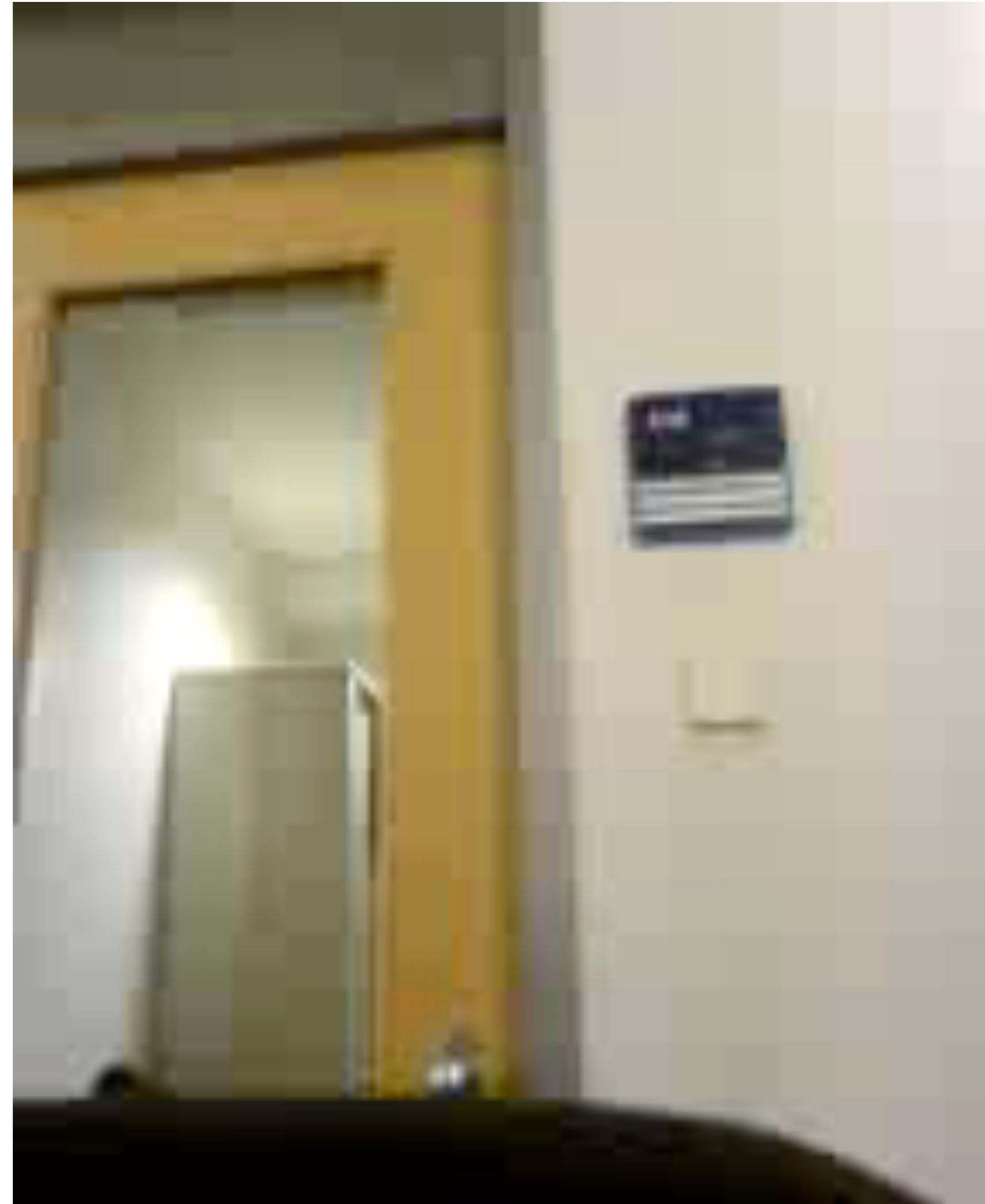
FIB: kein Chip ist sicher



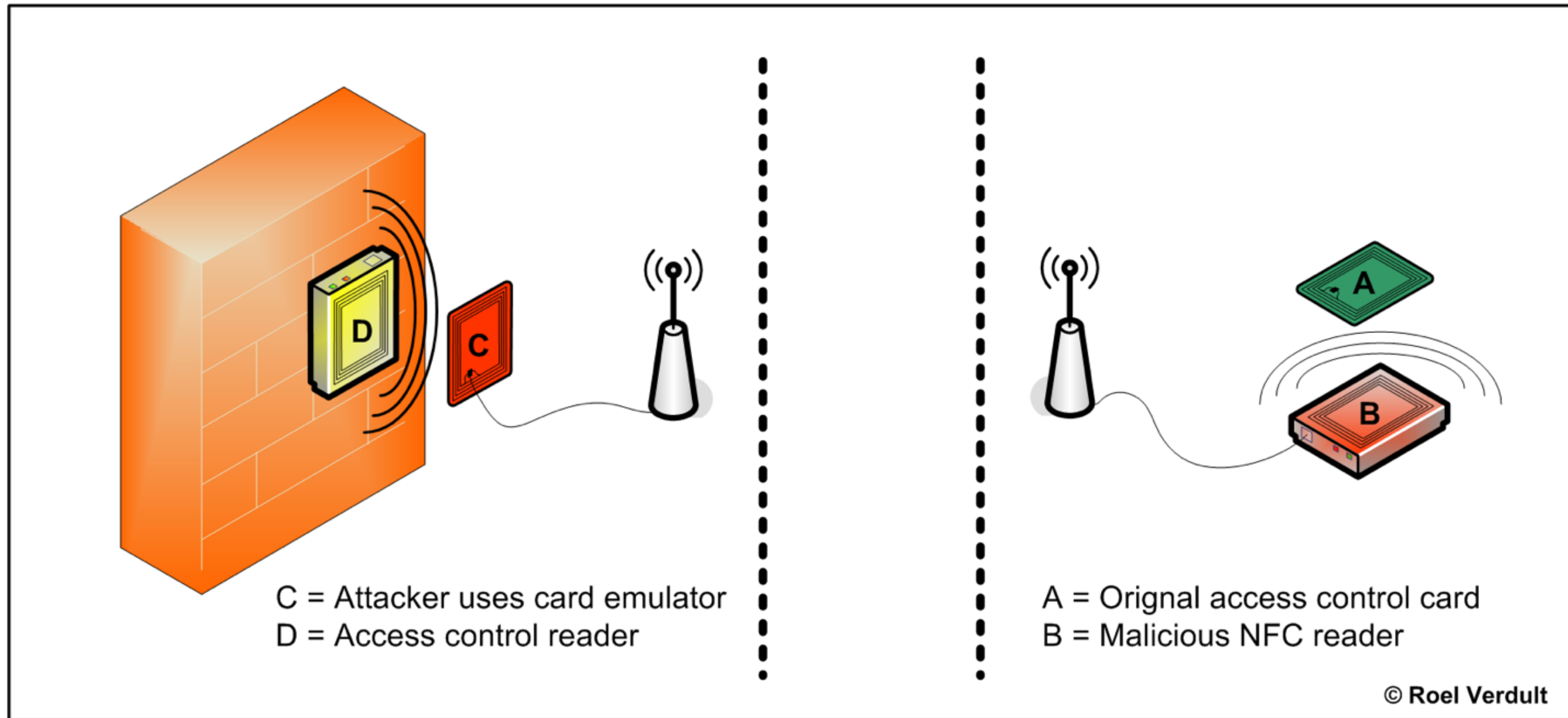
optical side channel

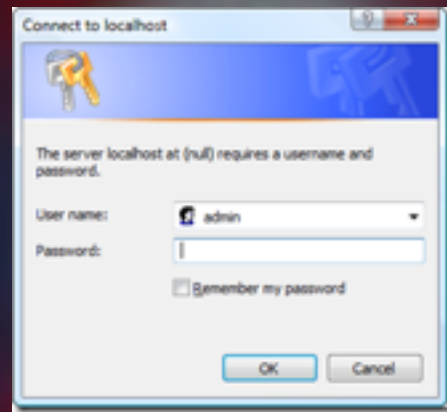


replay attack



relay attack





Passwort



Biometrie

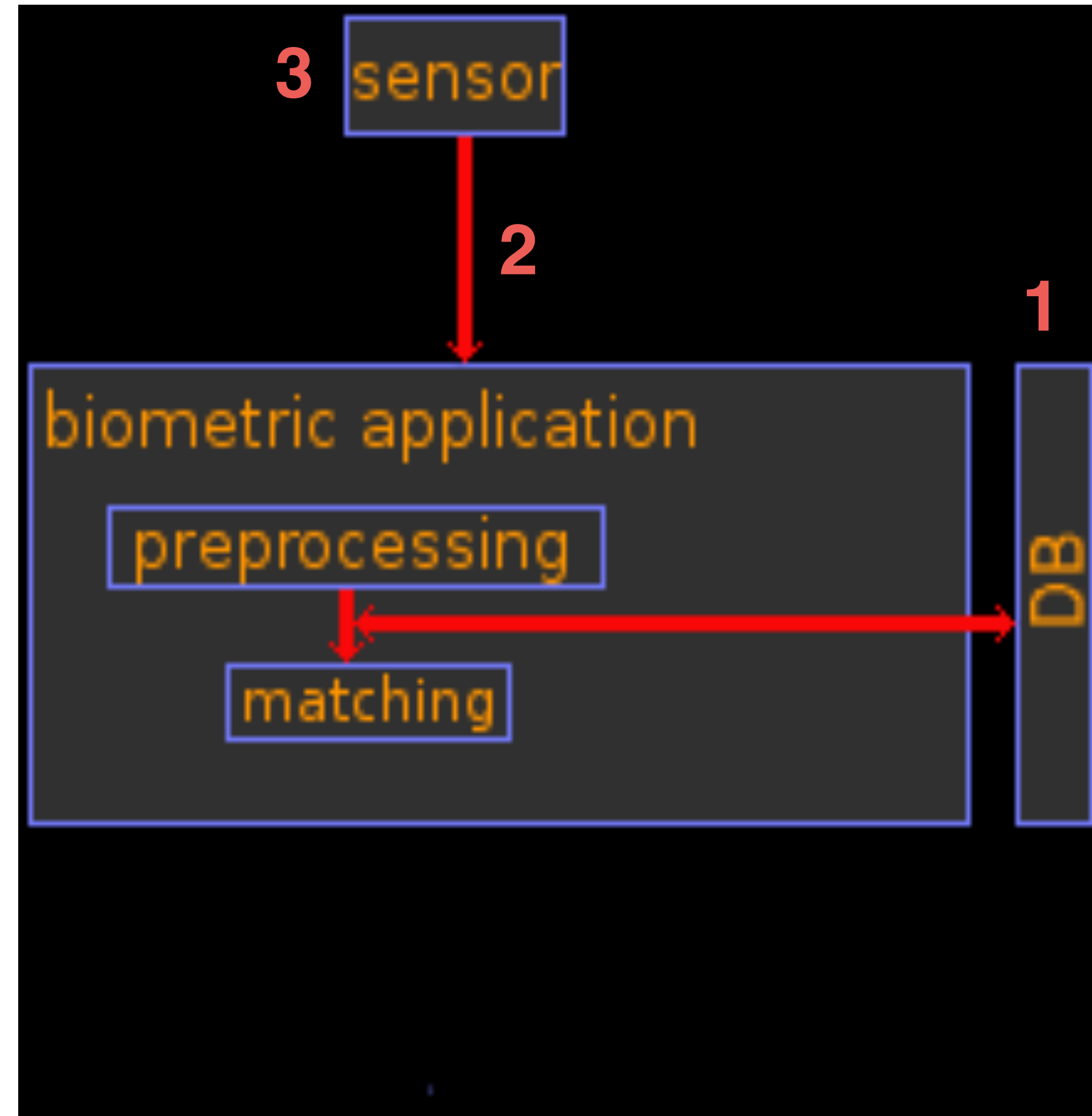


Mikrochips

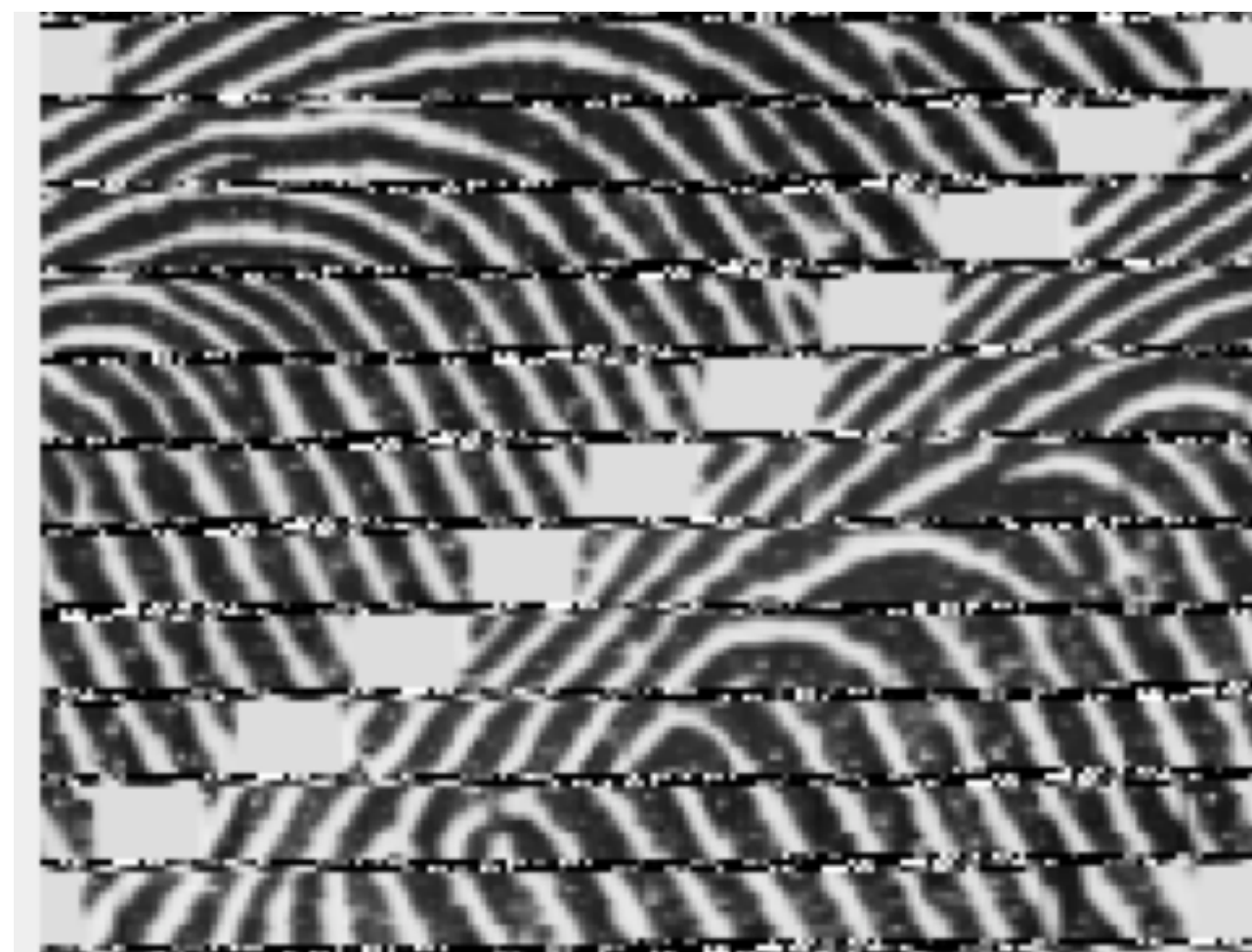


Biometrische Systeme

- Angriffspunkte
- Datenbank
- Kommunikation
- Sensor



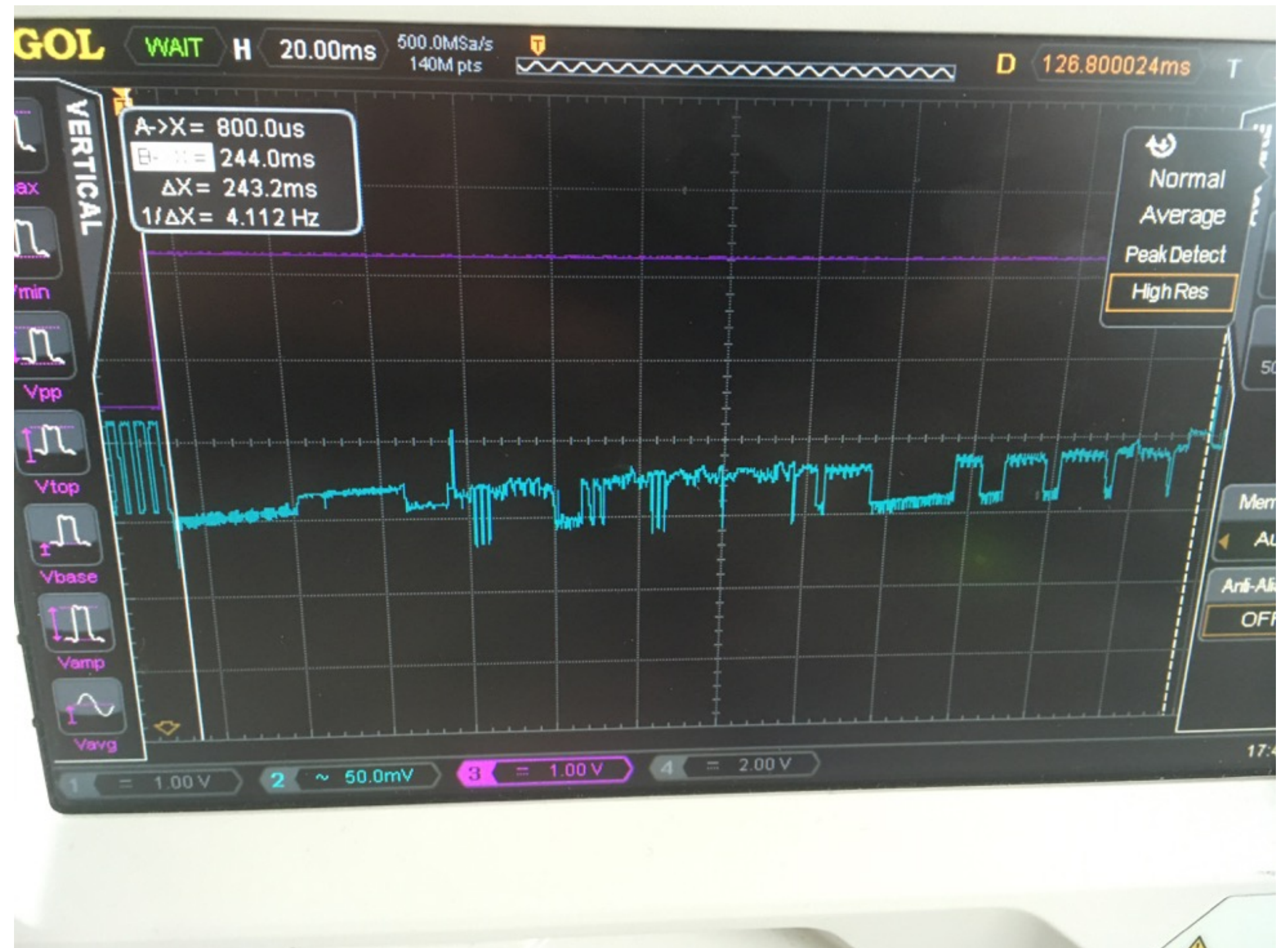
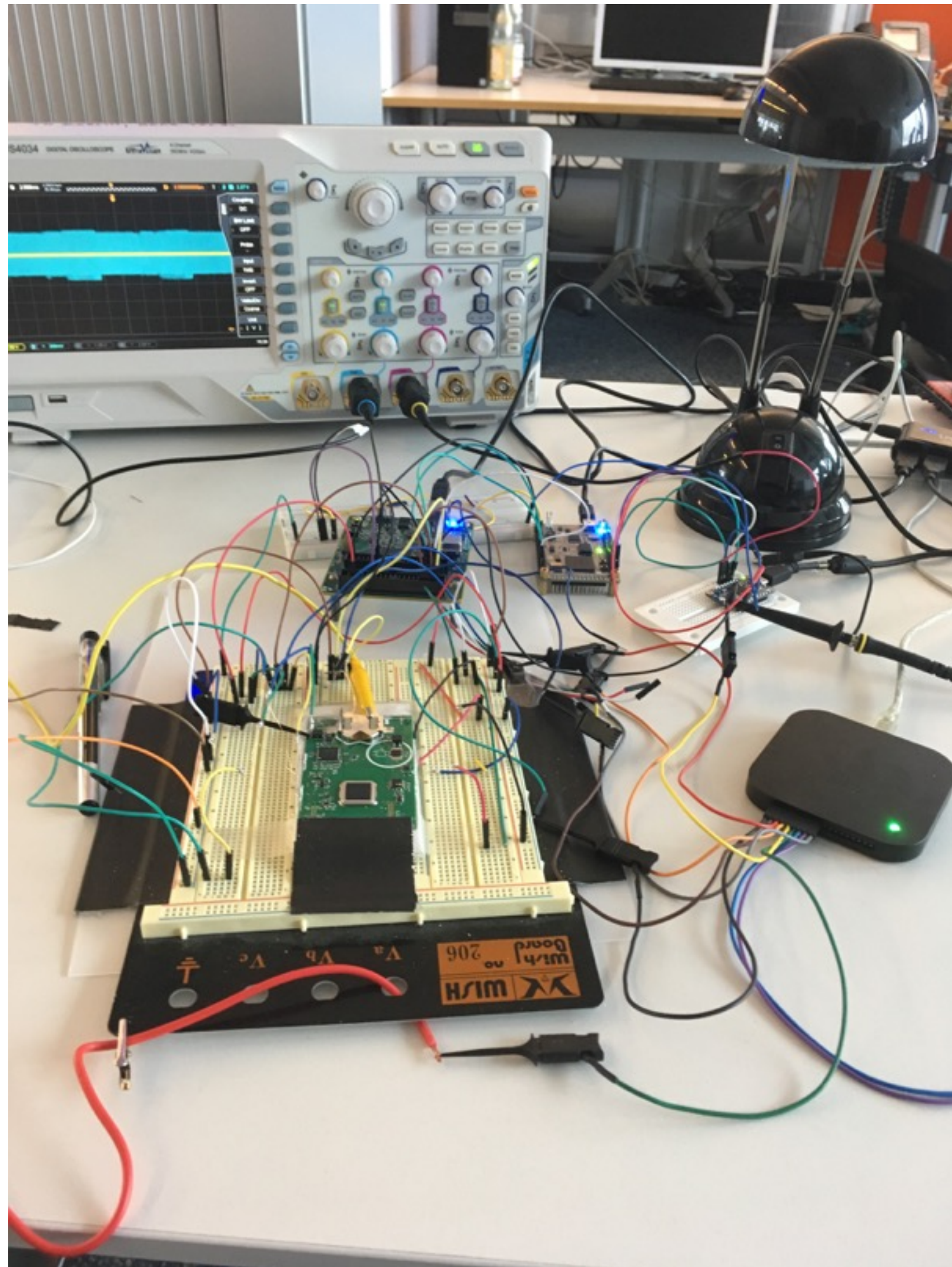
sniffing



replay attack



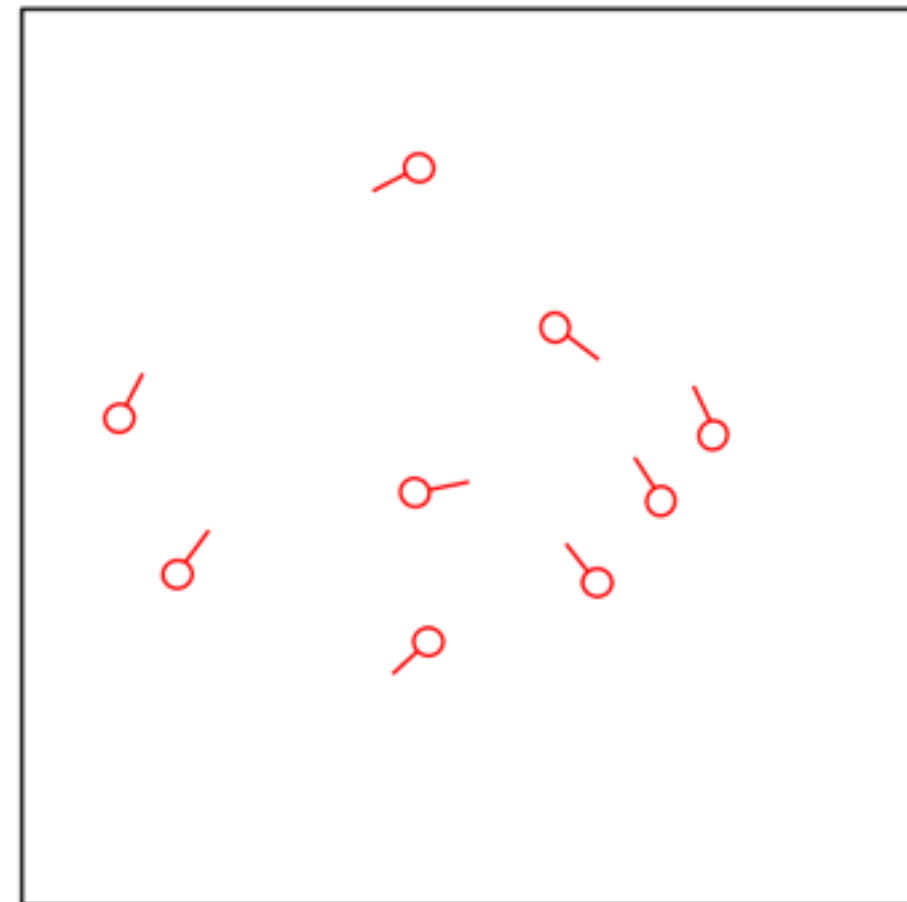
side channel



from template to image



```
0000000 46 4d 52 00 20 32 30 00 00 00 00 3c 00 00 00 c0  
0000010 00 c0 00 c5 00 c5 01 00 00 00 3c 05 80 8a 00 99  
0000020 c8 54 40 9e 00 99 ce 52 80 84 00 a5 a3 51 40 6f  
0000030 00 51 c0 49 80 88 00 b1 b8 3e 00 00
```



Hacker klauen Fingerabdruck



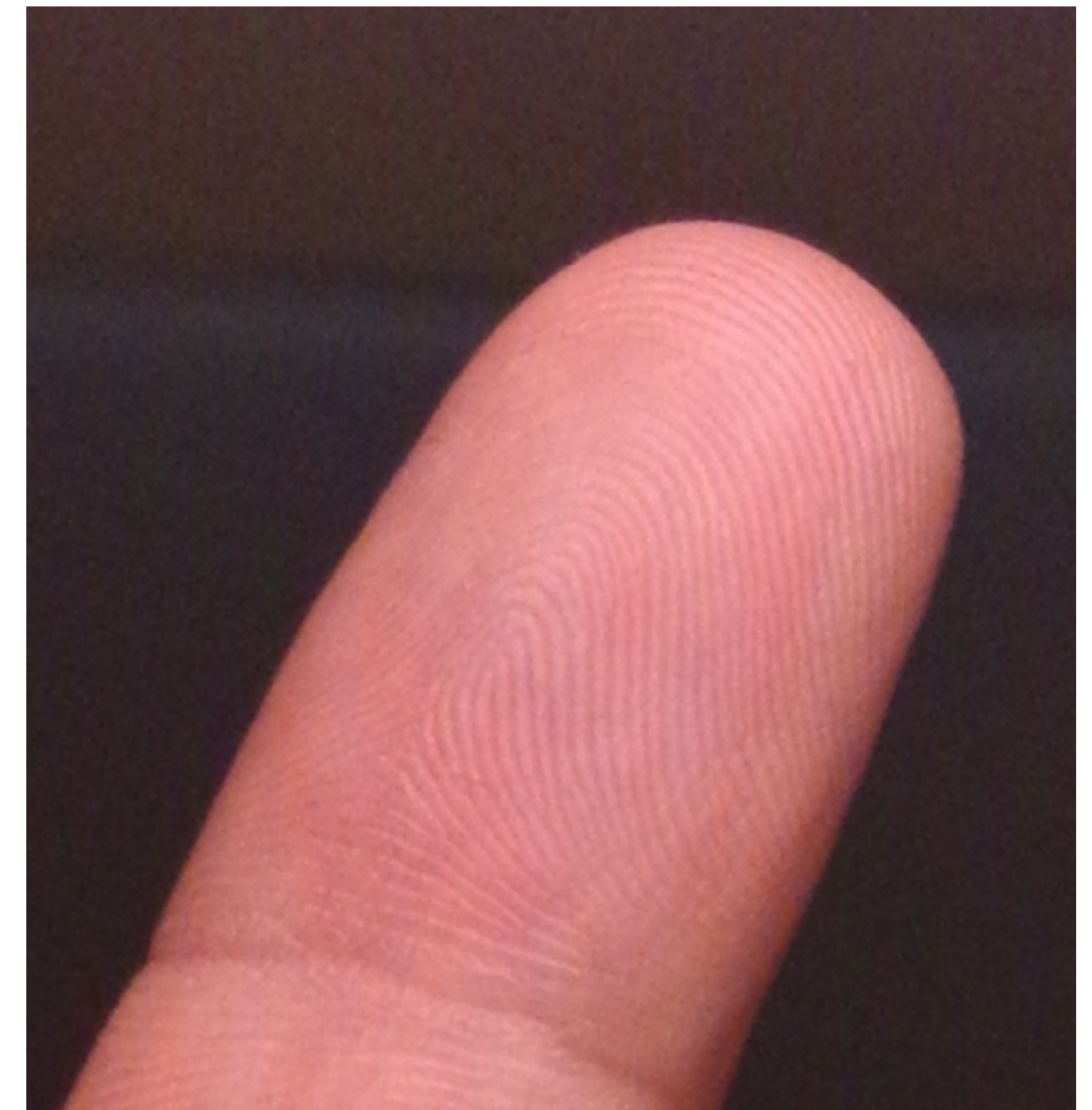
was die Polizei kann...



anonyme Erpresserbriefe



Fingerabdrücke fürs Fotoalbum



Zeig mir deine Hand ...



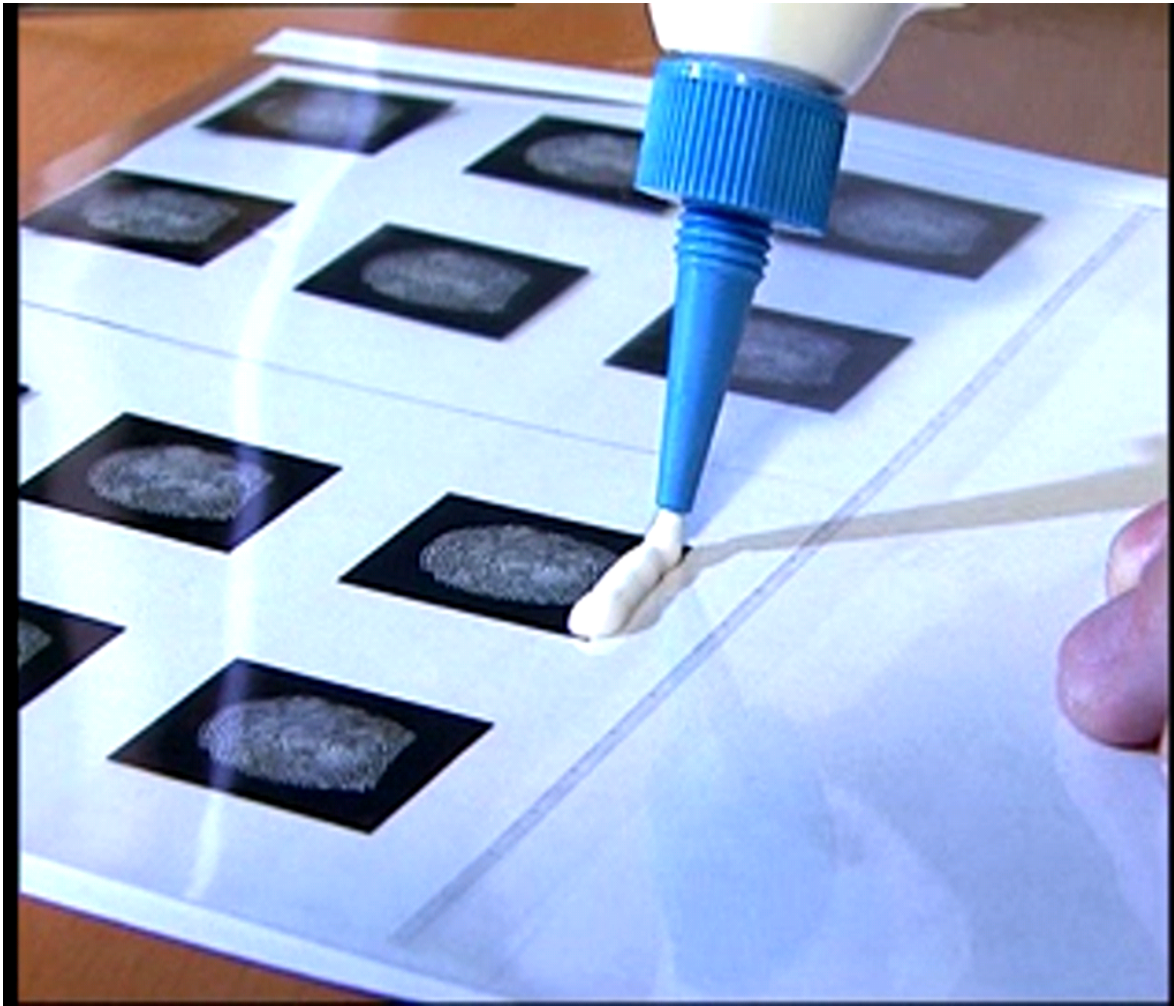


Dr. von der Leyen

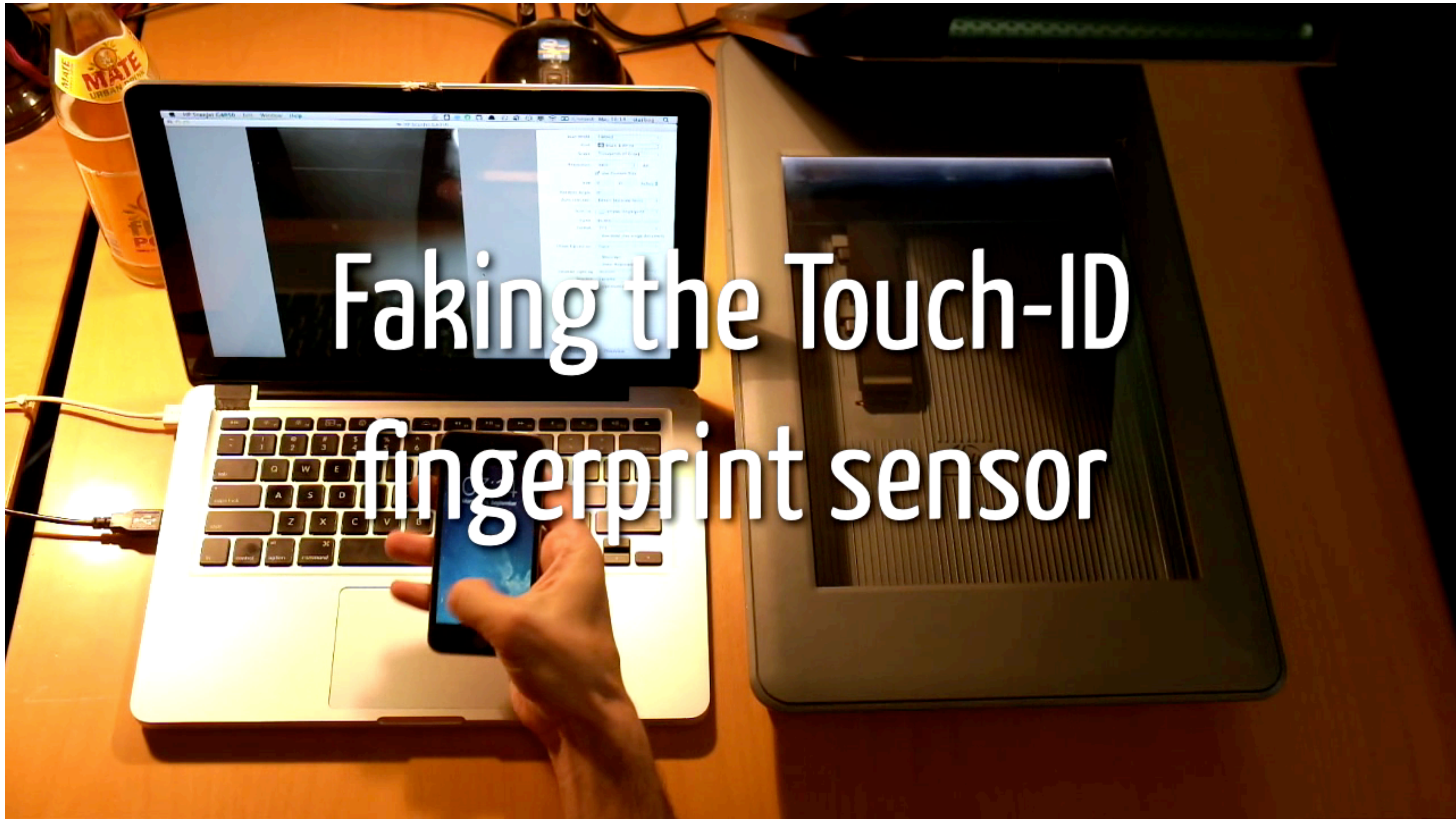
im Internet



Attrappenbau



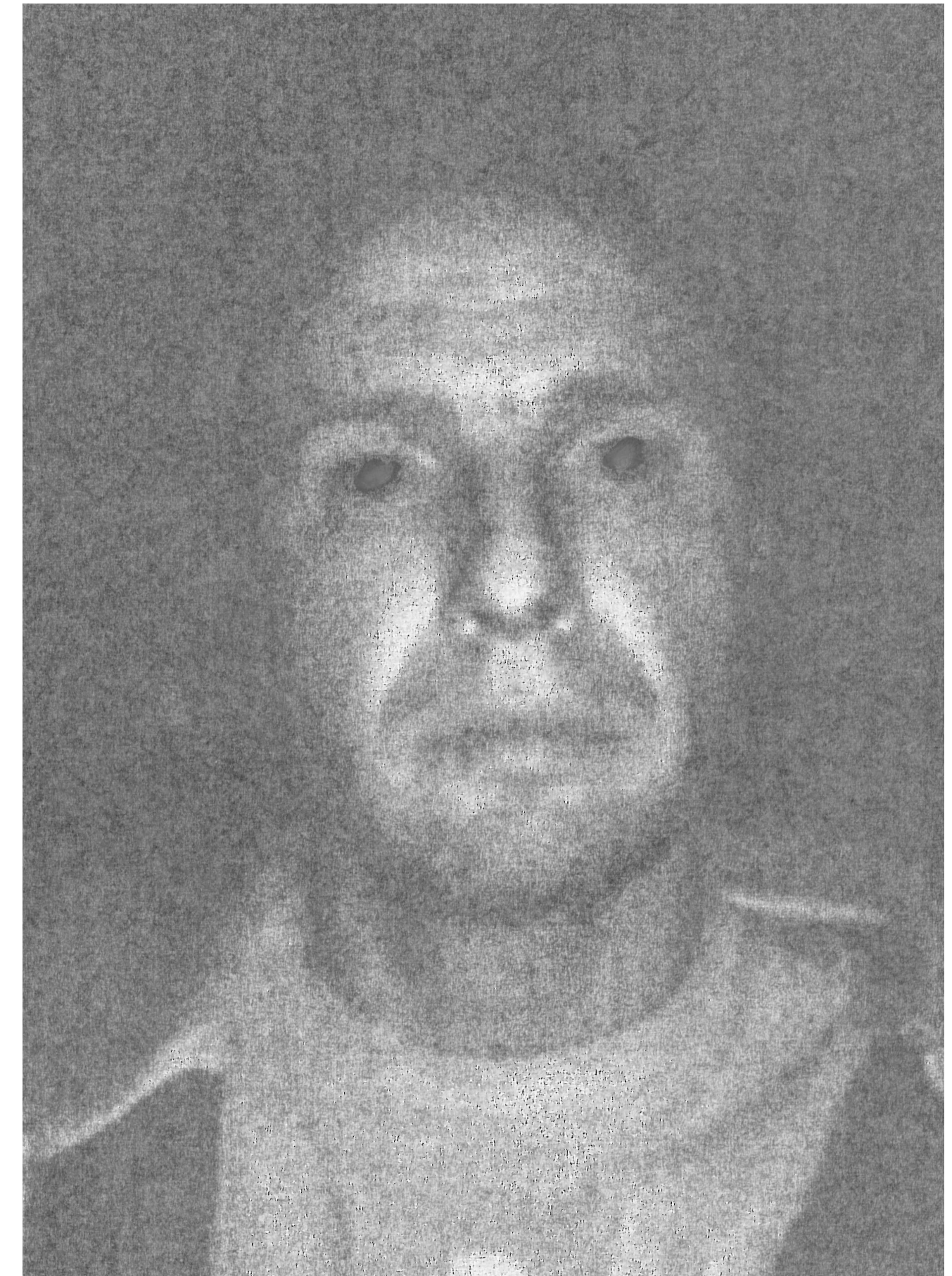
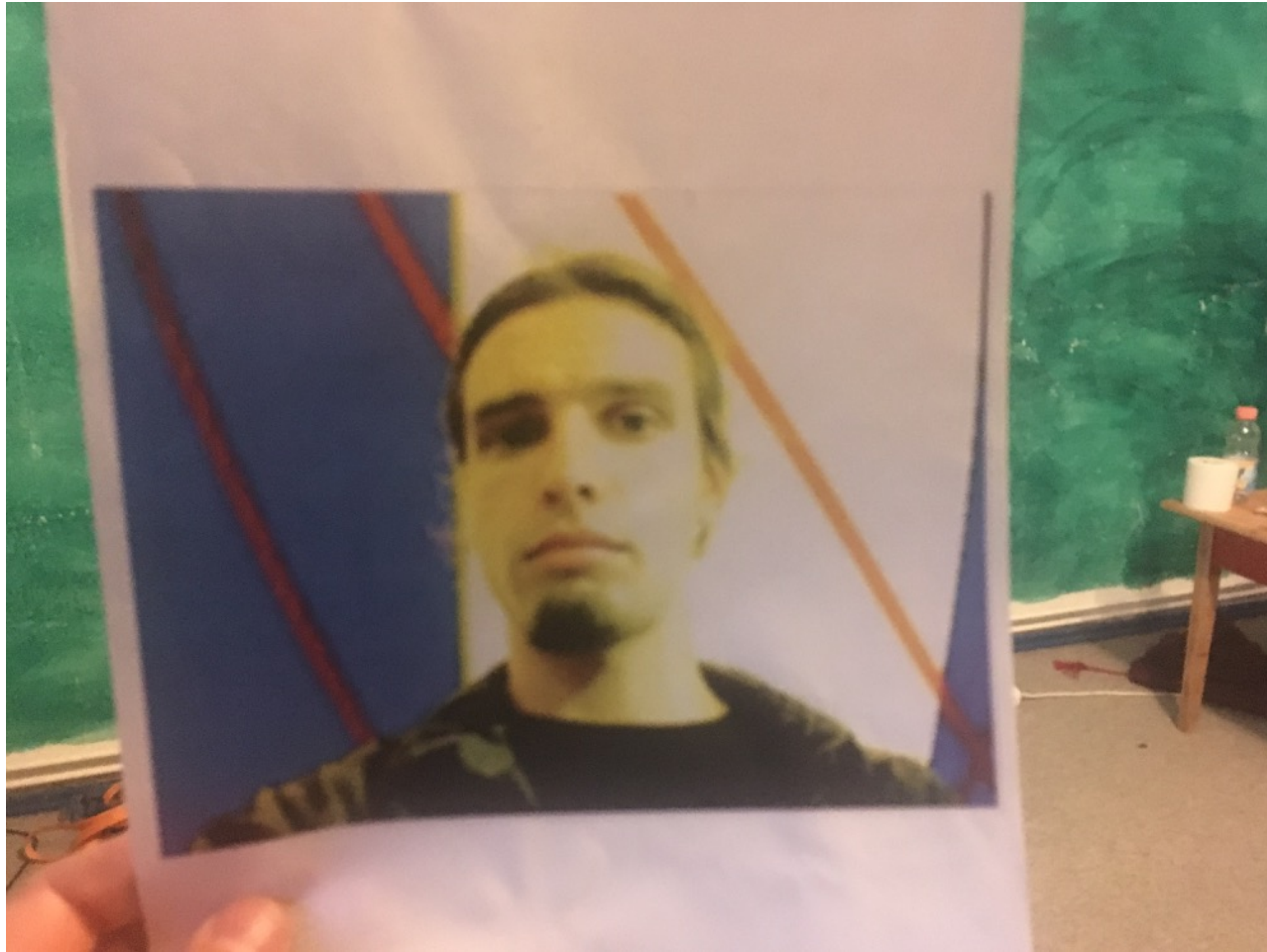
Faking the Touch-ID fingerprint sensor



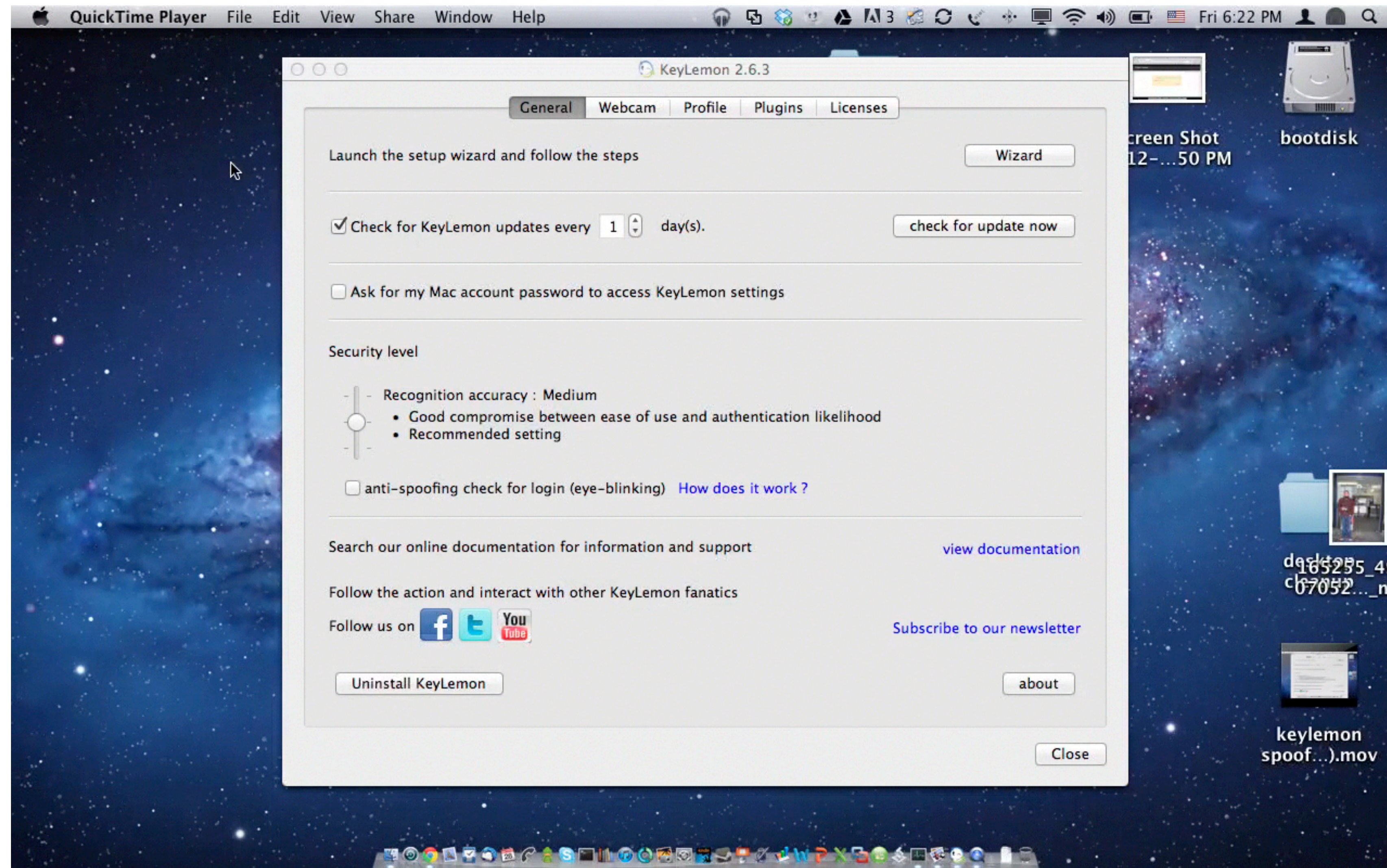
Finger aus dem Drucker



I see faces



Gesichtserkennung *gähn*



Bewegtbilder



mastercard



face manipulation

Comparison to Previous Work



Input Video



[Cao et al. 14]
(RGB only)



[Thies et al. 15]
(RGB-D)

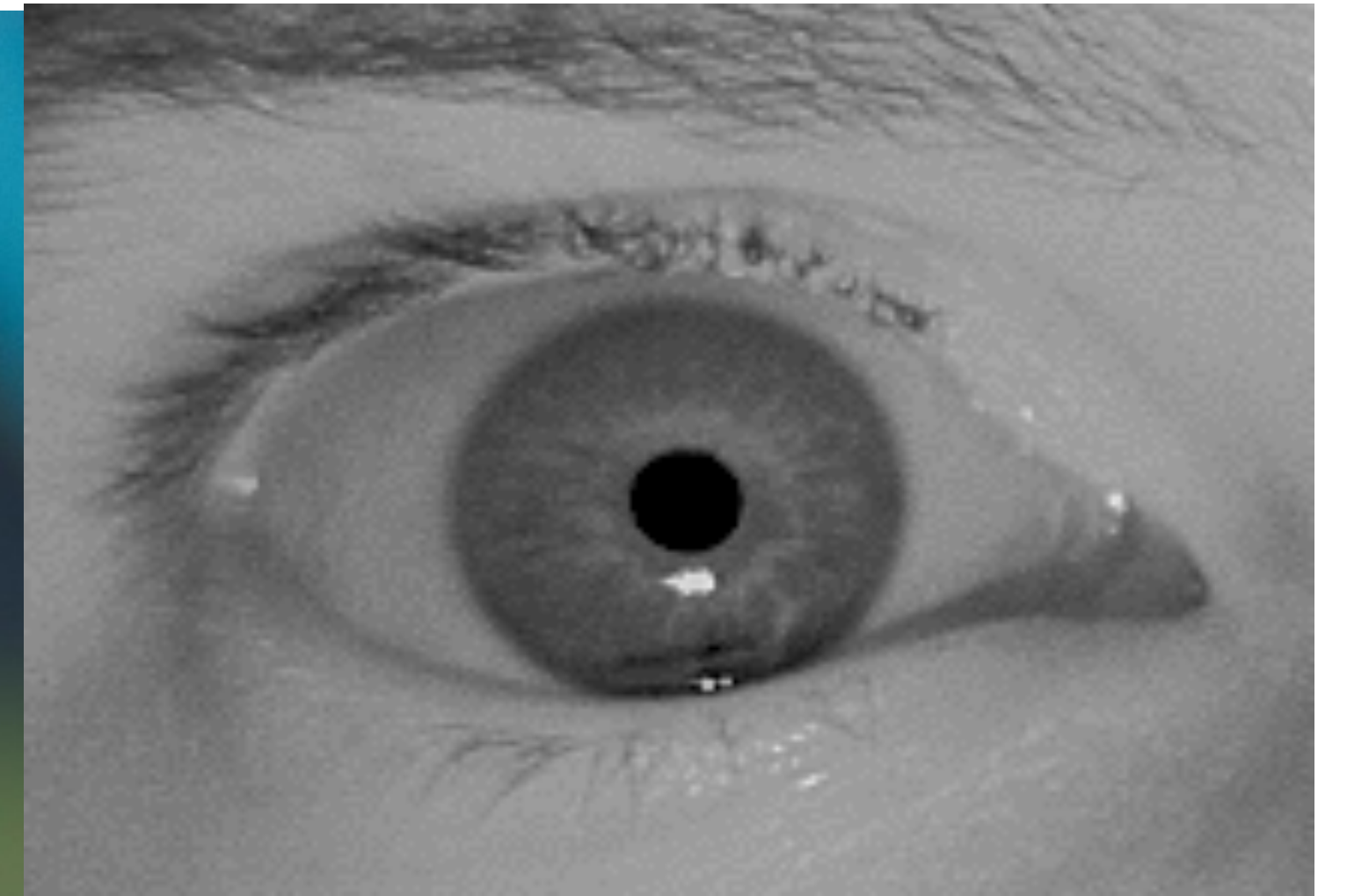


Ours
(RGB only)

die dritte Dimension



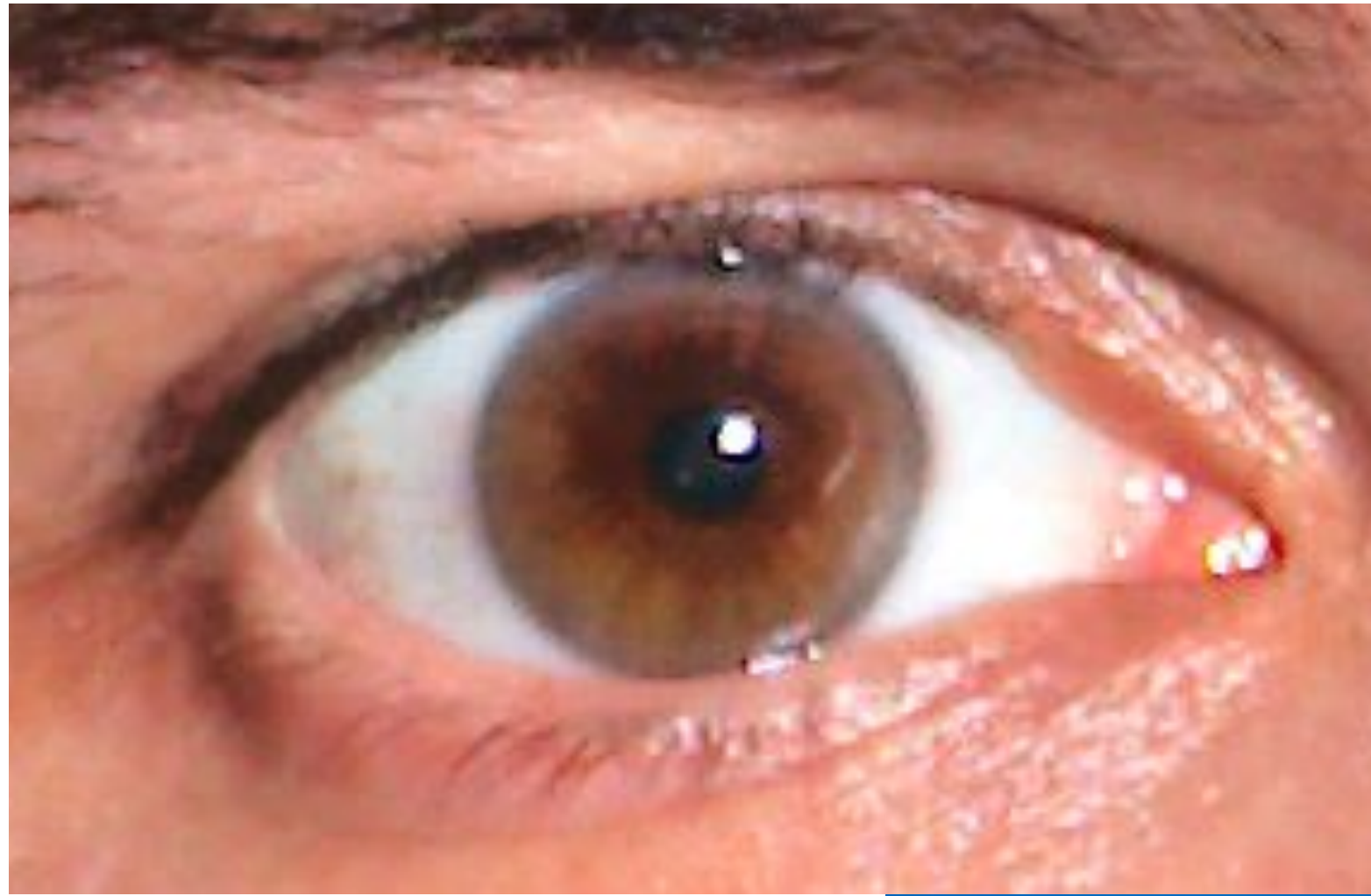
schau mir in die Augen



sooooo einfach



schau mir in die Augen



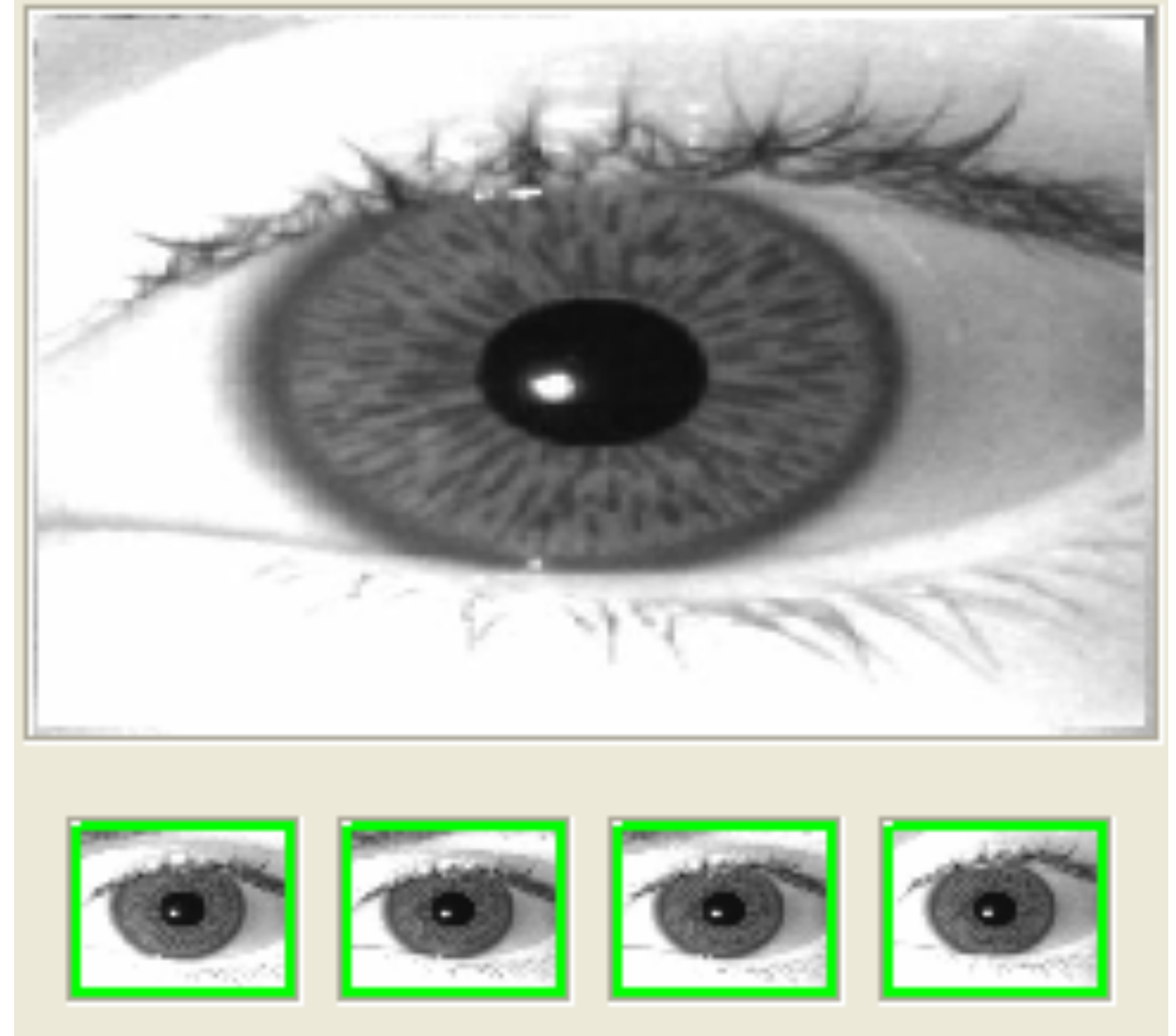
... und ich sage dir, wer du bist



distance [m]	diameter [pxl]
3	153
4	131
5	100
6	80
7	67



unsichtbare Identität

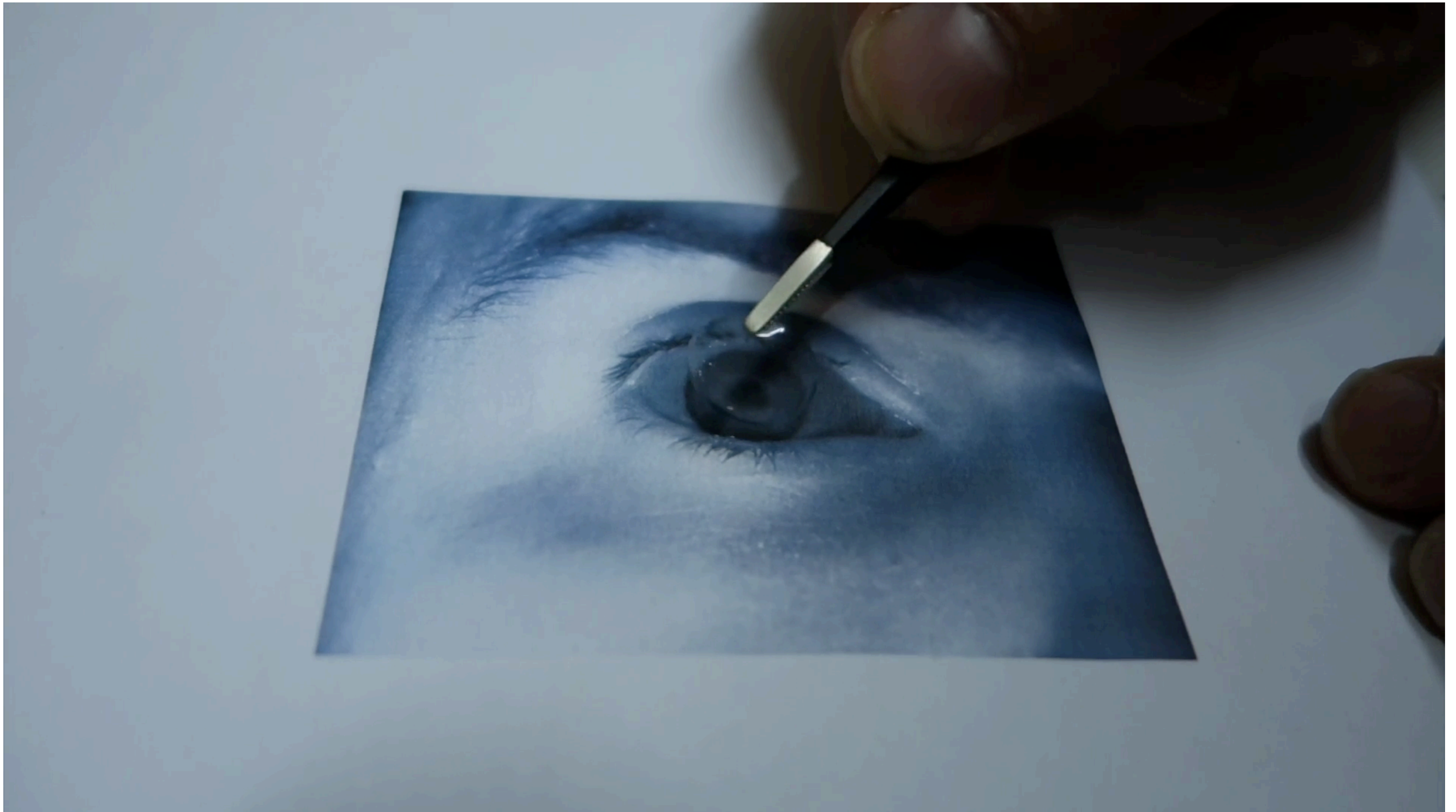


AI(b|p)träume?

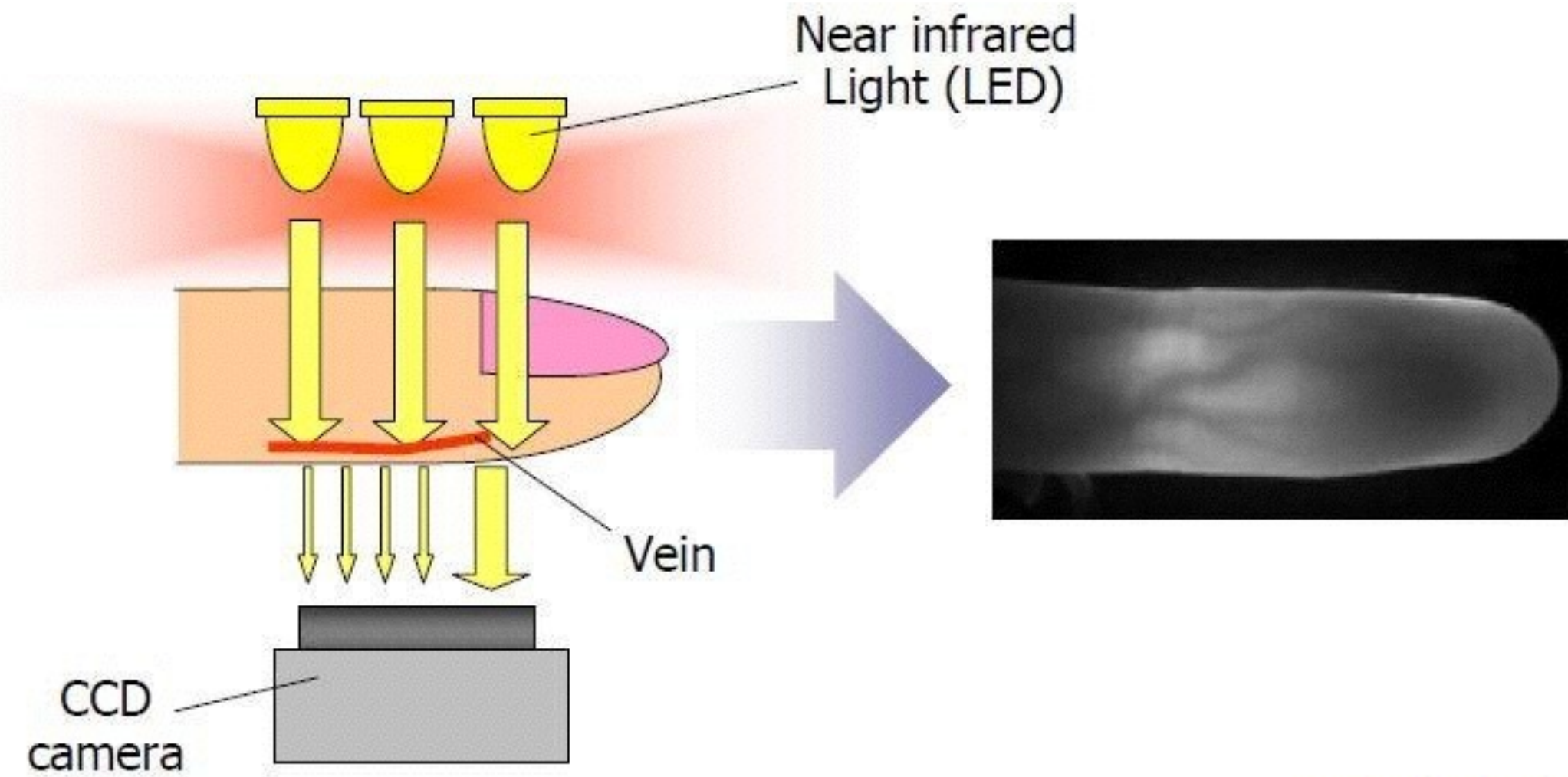


die Partei liefert

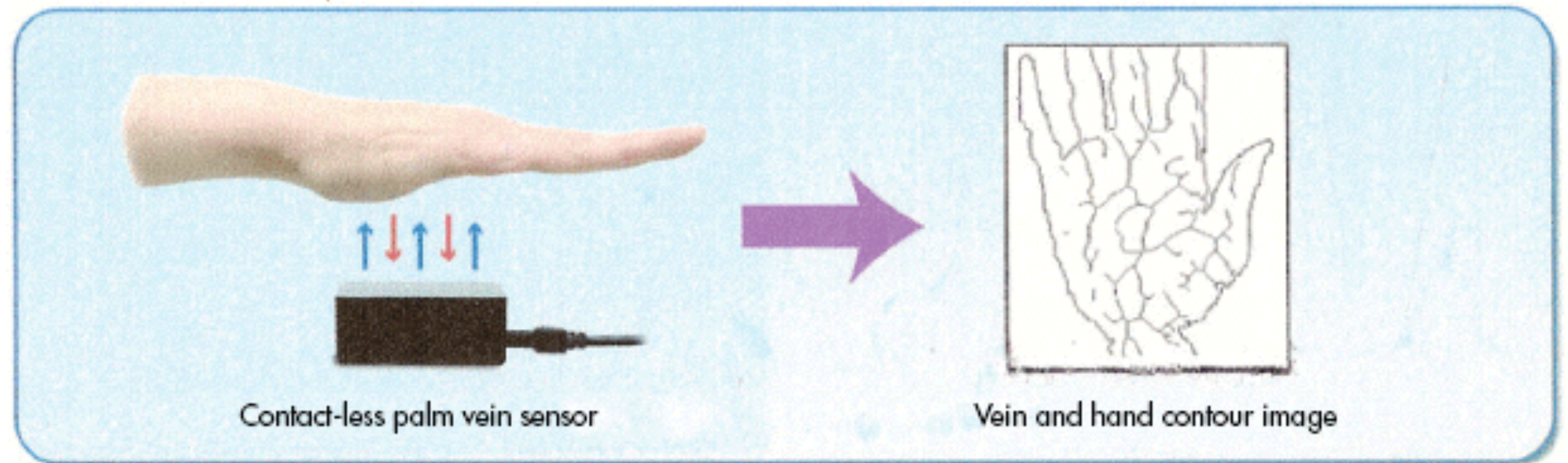




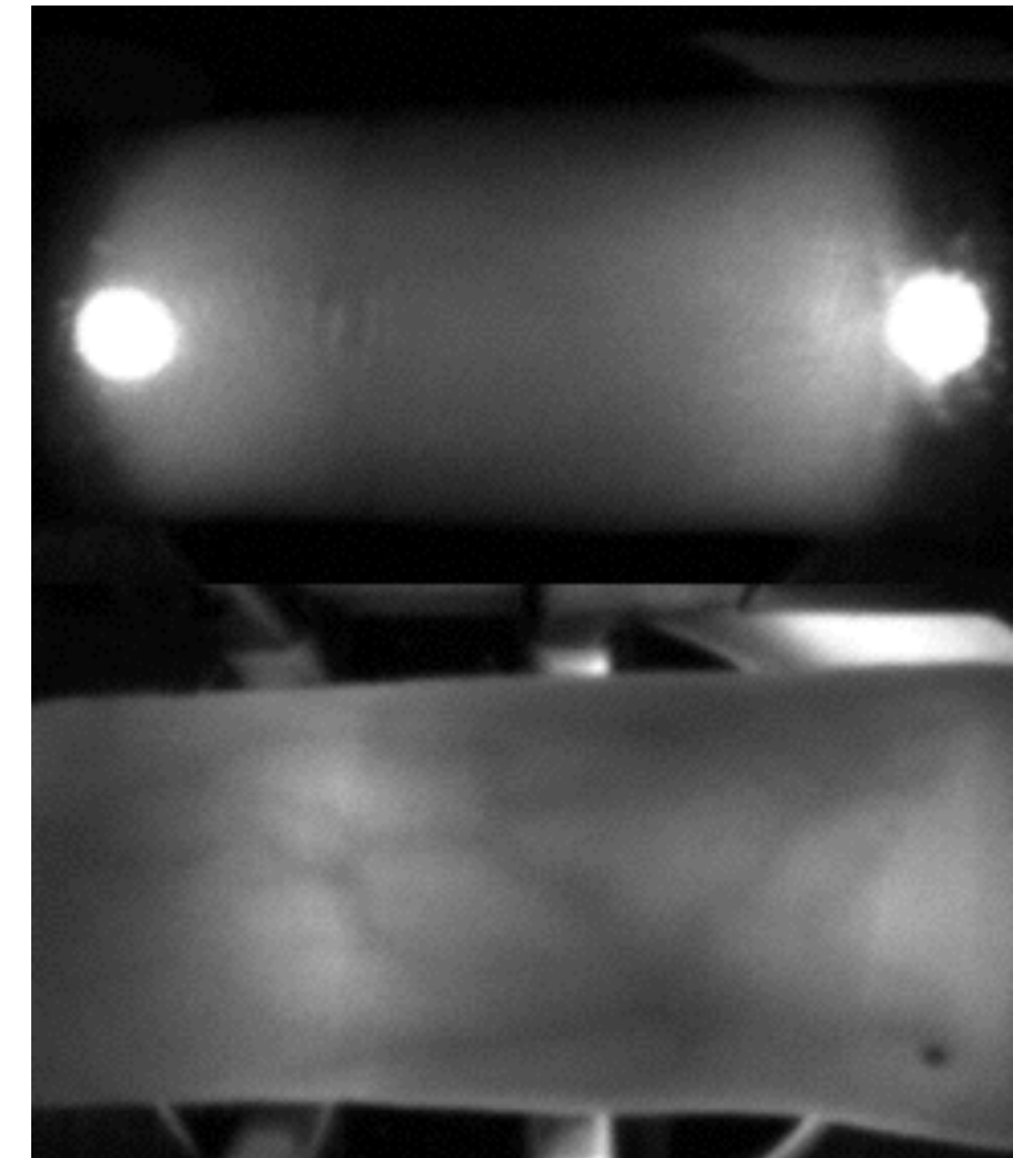
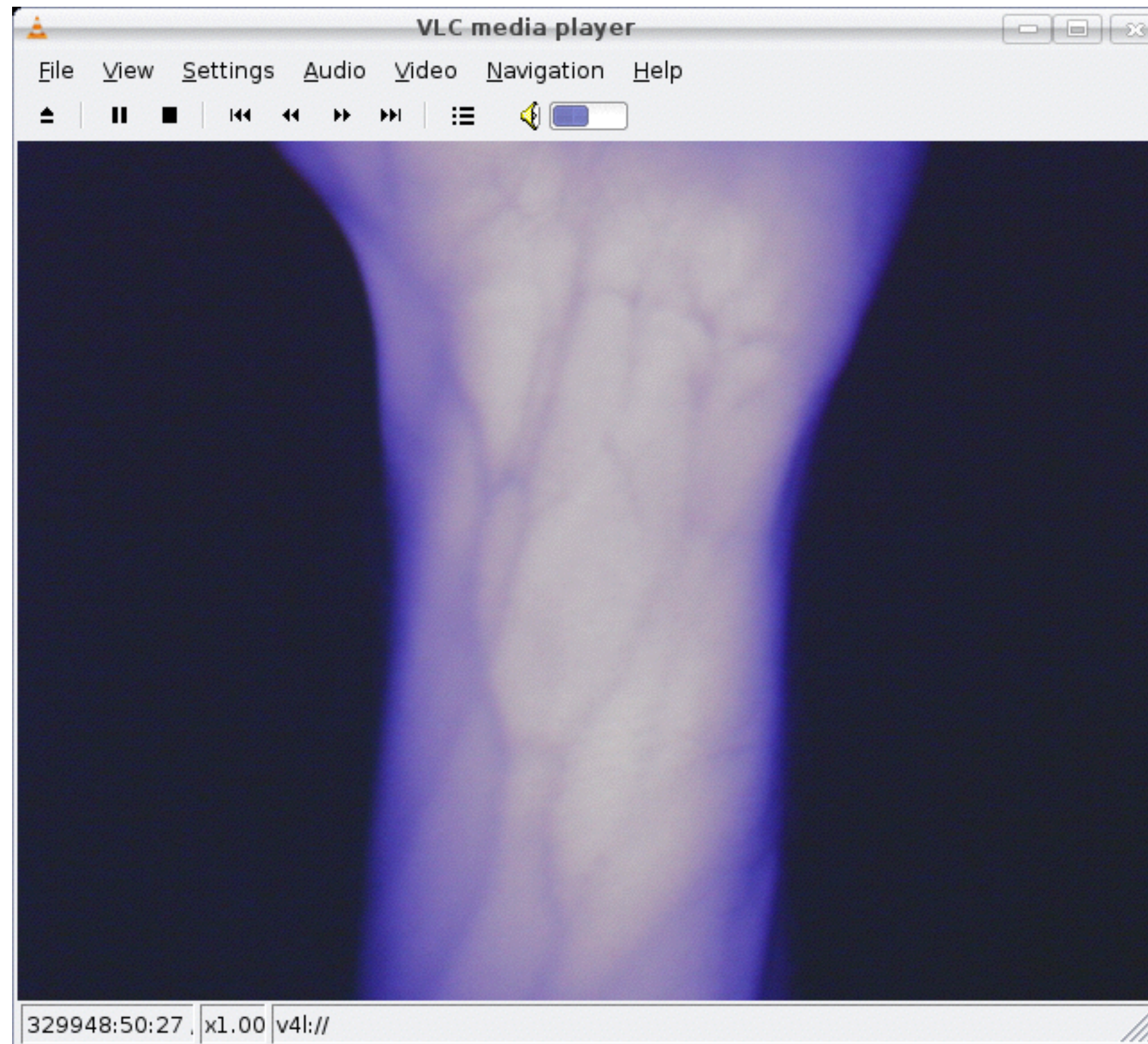
Venenerkennung



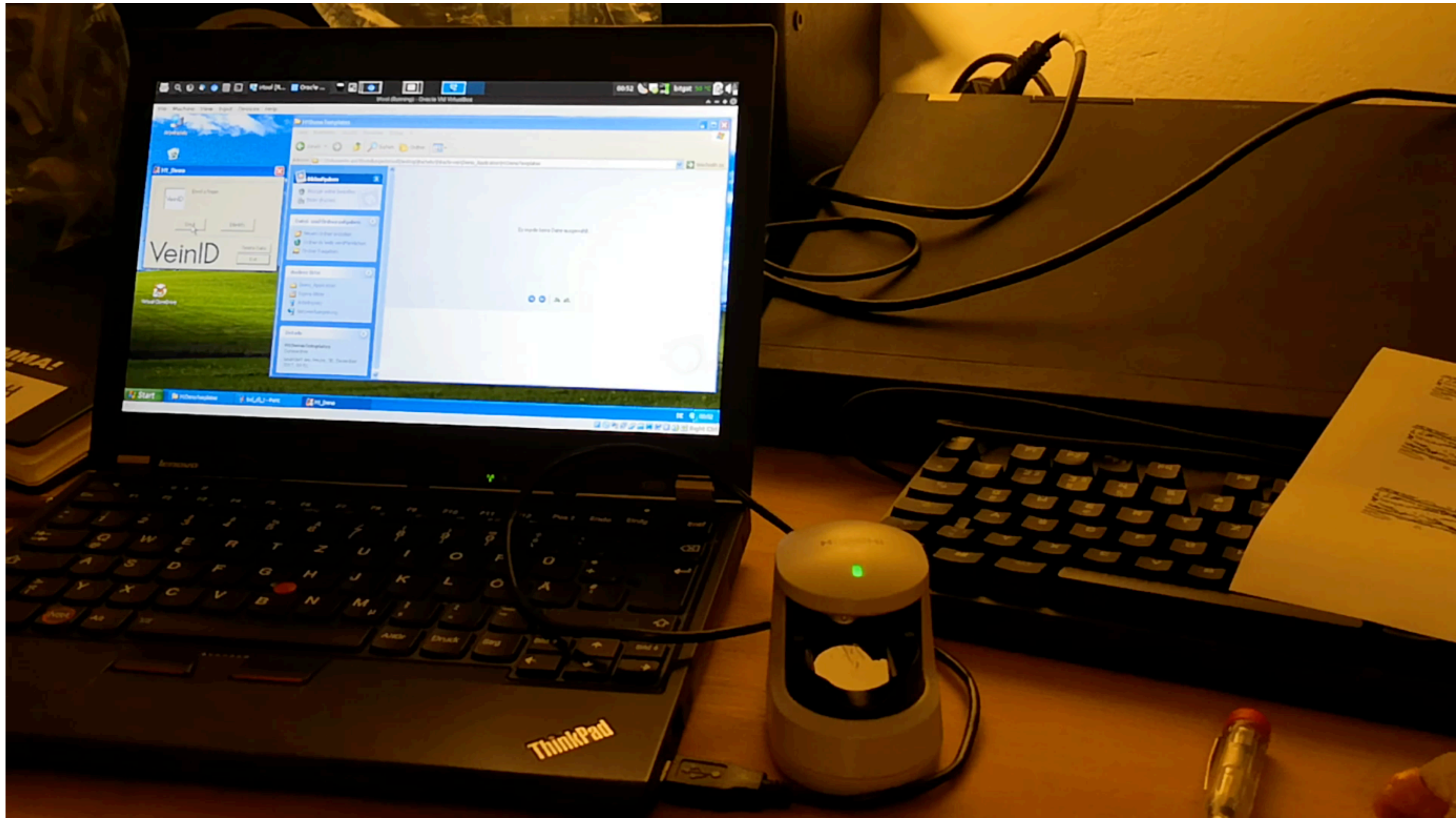
6. In Fujitsu's Palm Secure technology for biometrics, contact-less palm-vein sensing can be used to project a vein and hand contour image.



Junkie?



finally



conclusion

Password:

- neben der Länge zählt auch die Eingabeumgebung

Token:

- RFID ist convenient, birgt aber Risiken
- proprietäre Kryptoalgorithmen sind böse

Biometrie:

- man hinterlässt Spuren von fast allen biom. Merkmalen
- Lebenderkennung prüft nicht unbedingt Leben

vielen Dank



Fragen?

starbug@ccc.de