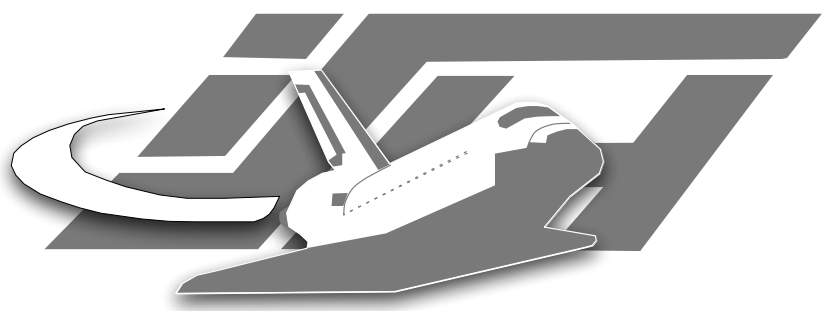
Hardware Attacks

2004-09-20

Summerschool Applied IT Security 2004

Maximillian Dornseif

See http://md.hudora.de/presentations/summerschool/

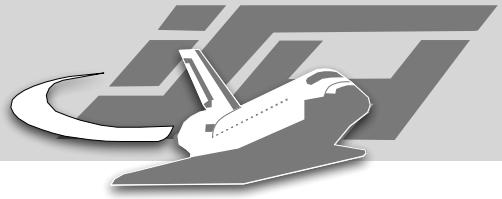


Laboratory for Dependable Distributed Systems

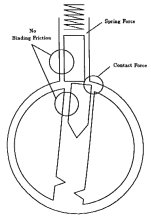
RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

RWTH

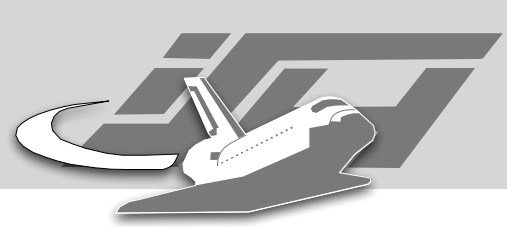
UNIVERSITY
OF TECHNOLOGY
AACHEN



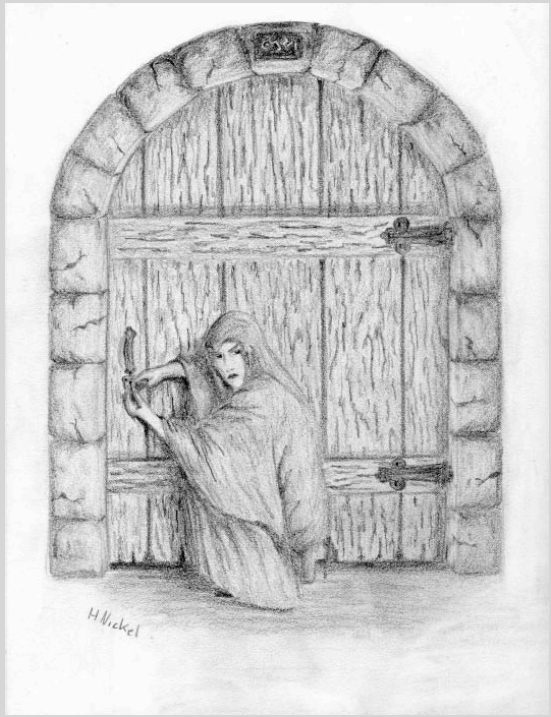
Agenda



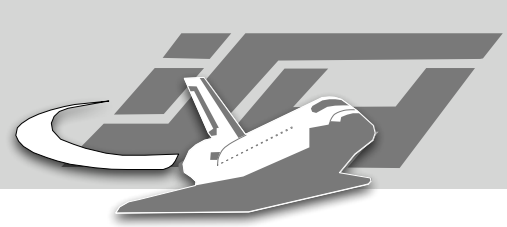
- Traditional hardware attacks: Locks
- Tampering: Looking into things you are not supposed to
- Tempest: Spooks are watching you
- Side-Channels 
- Fault-Injection
- Cracking 128 Bit in 128 Minutes 



The playing field

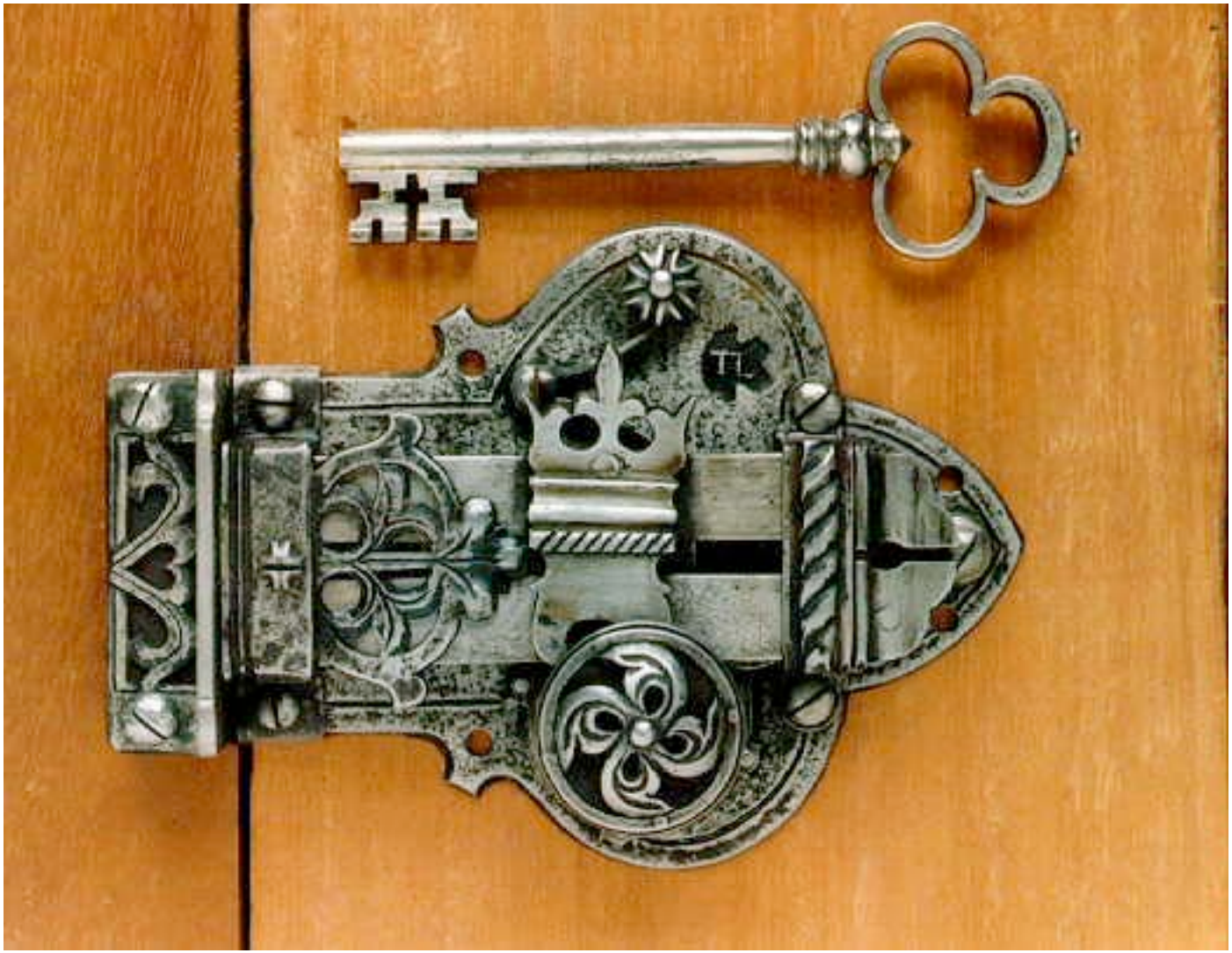


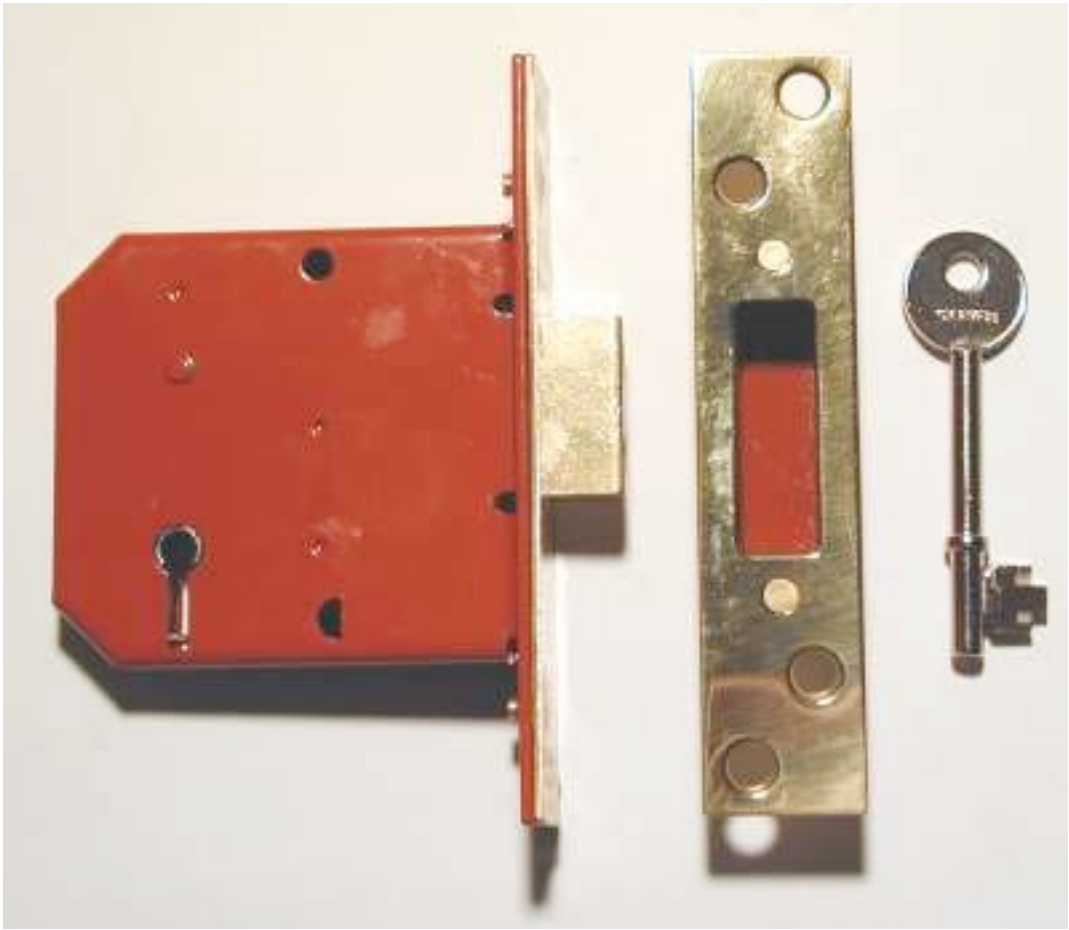
Locks

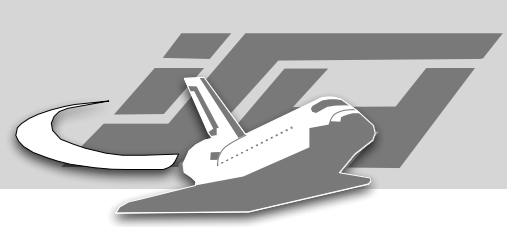


History of Locks

Traditional Locks







Modern locks

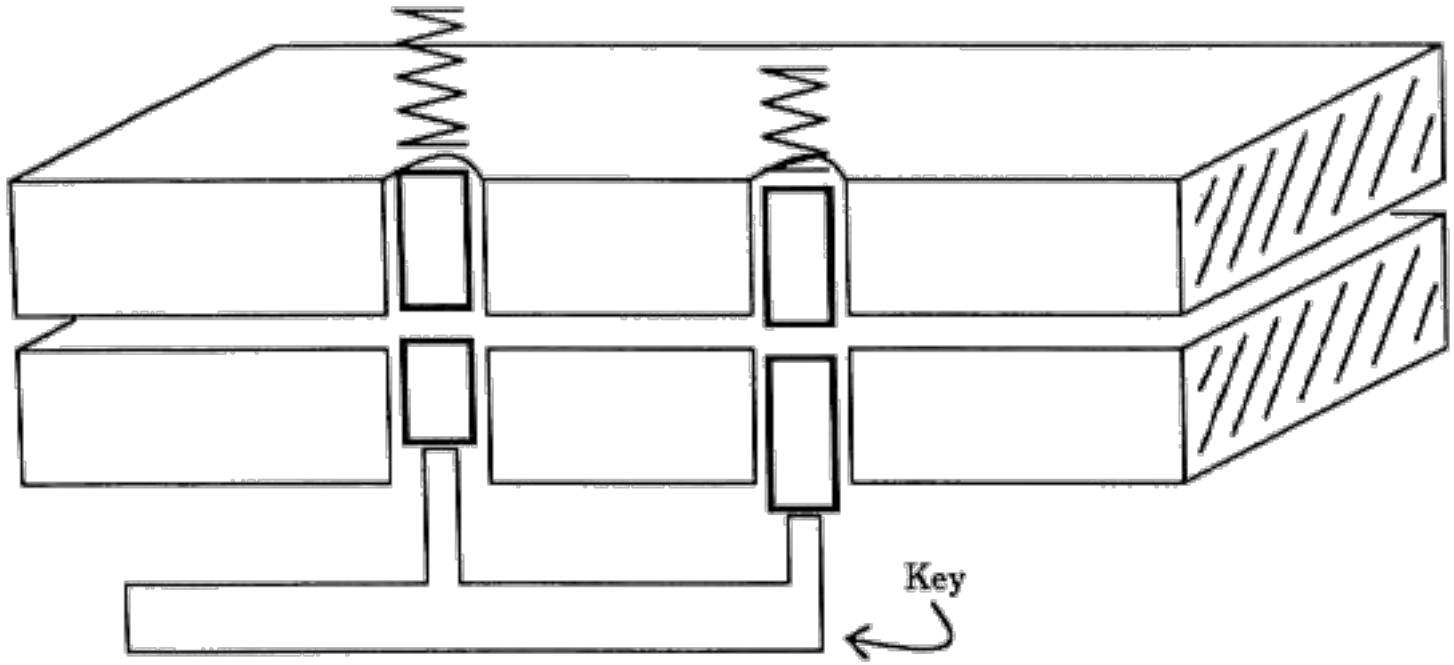


Figure 3.2: (a) Flatland key raises pins

Modern locks

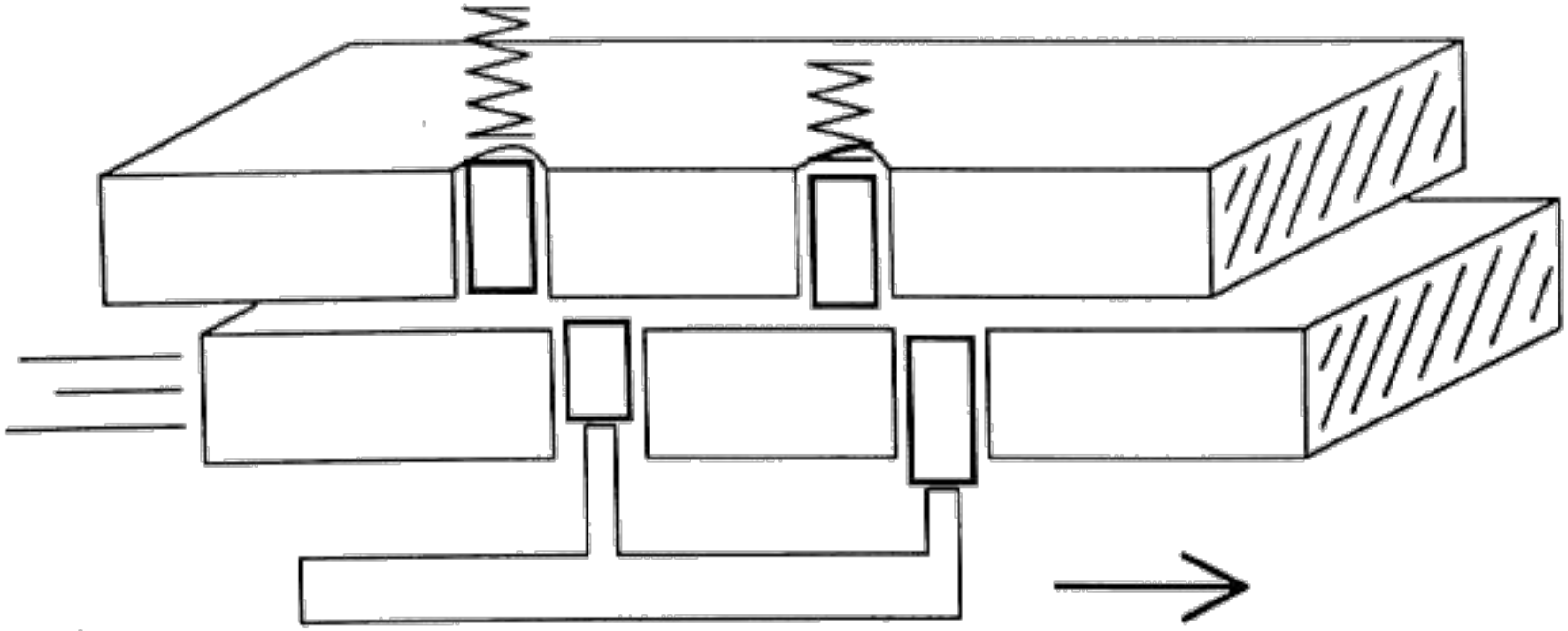
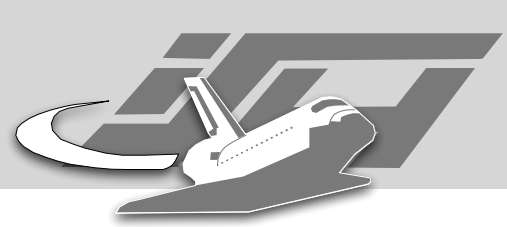


Figure 3.3: (b) Proper key allows plates to slide



Modern locks

Figure 4.2: (b) Pick lifts the binding pin

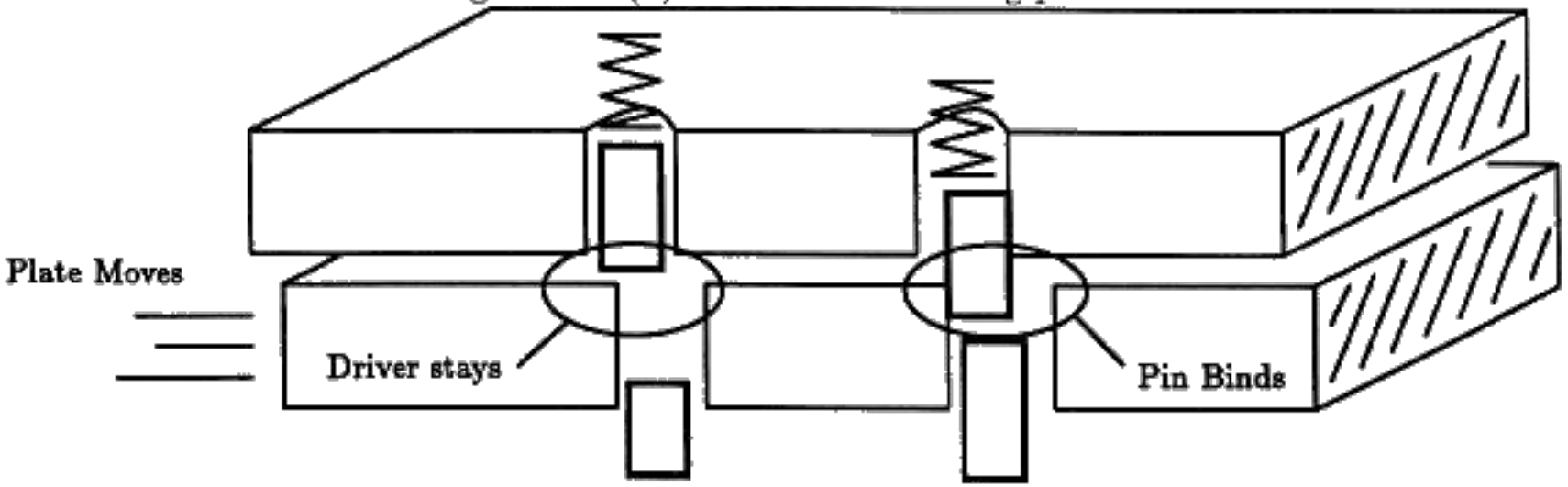
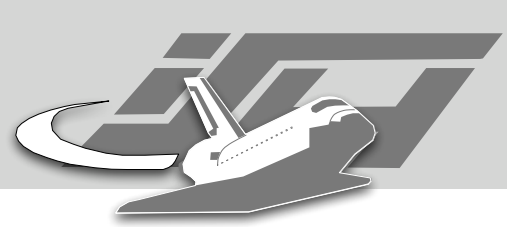
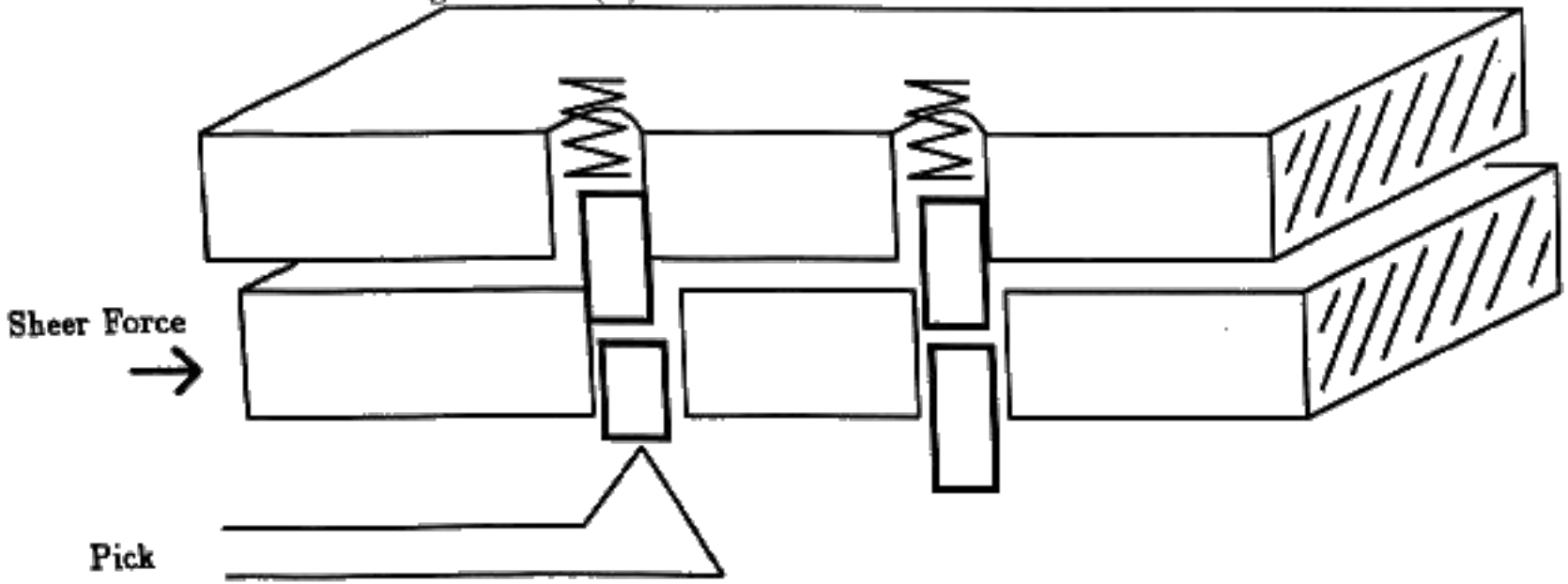


Figure 4.3: (c) Left driver sets and right driver binds



Modern locks

Figure 4.1: (a) Sheer force causes driver to bind



Modern Locks

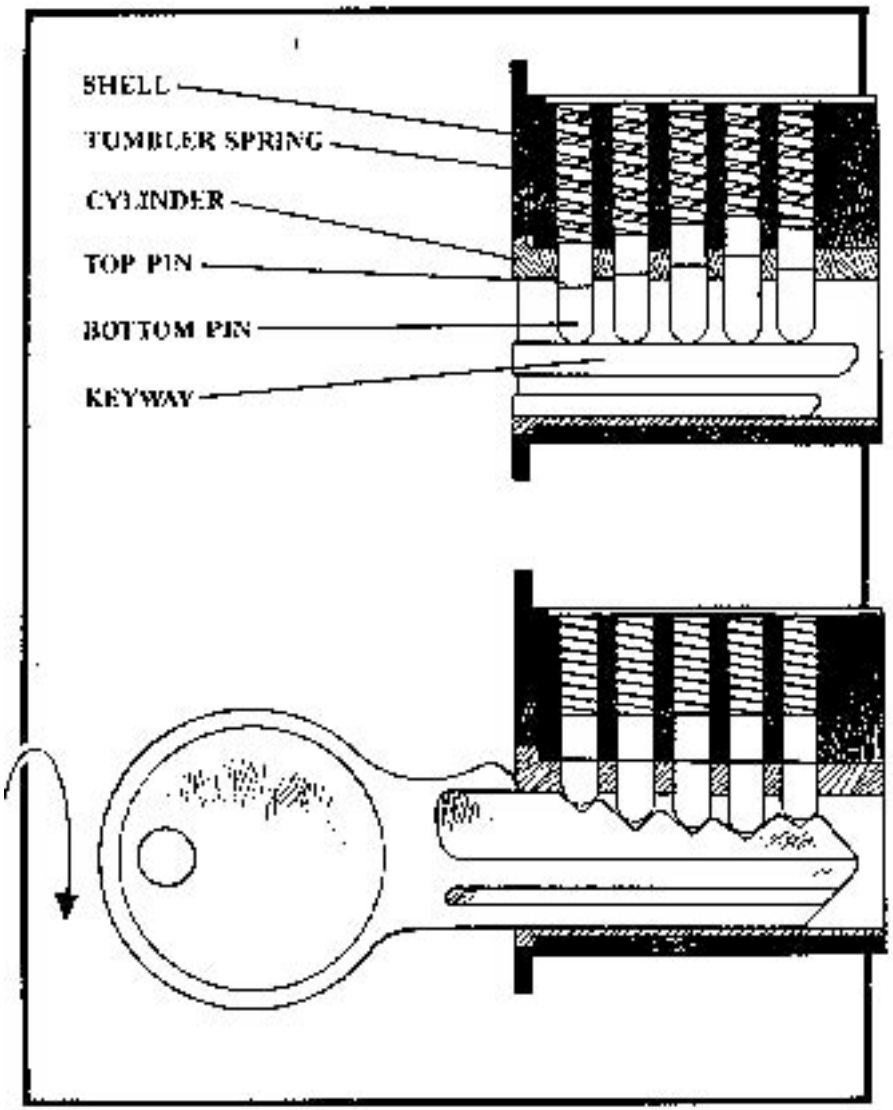
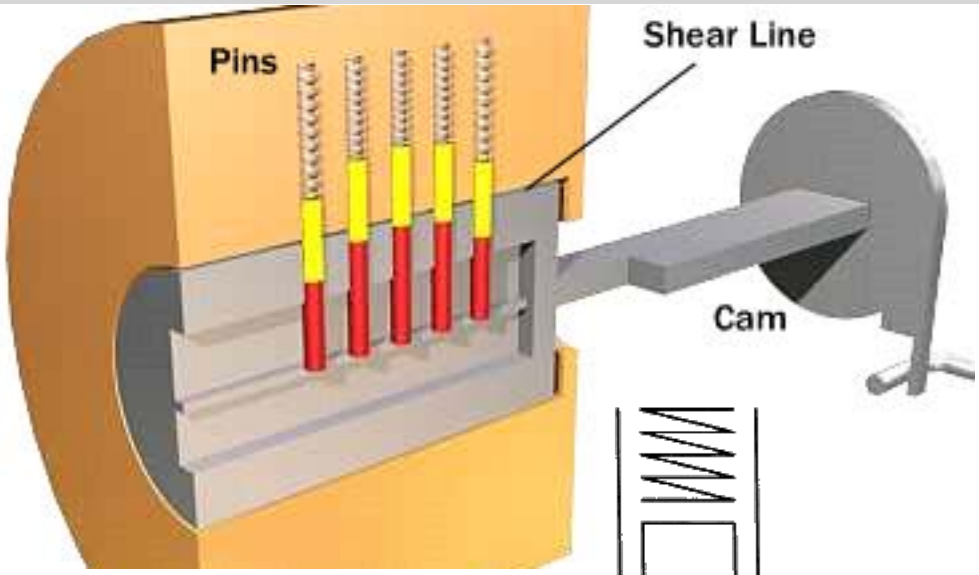
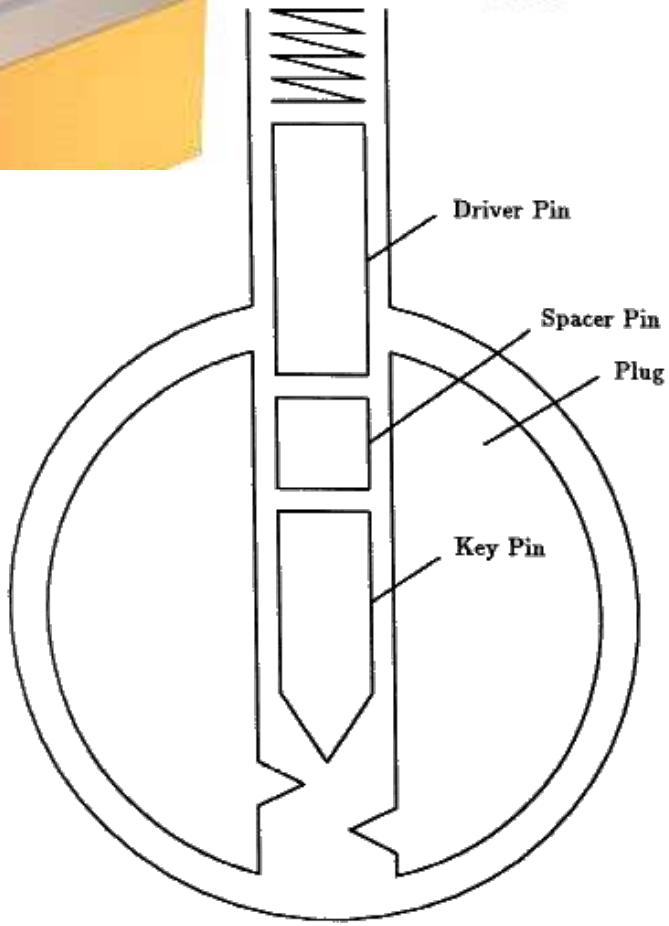
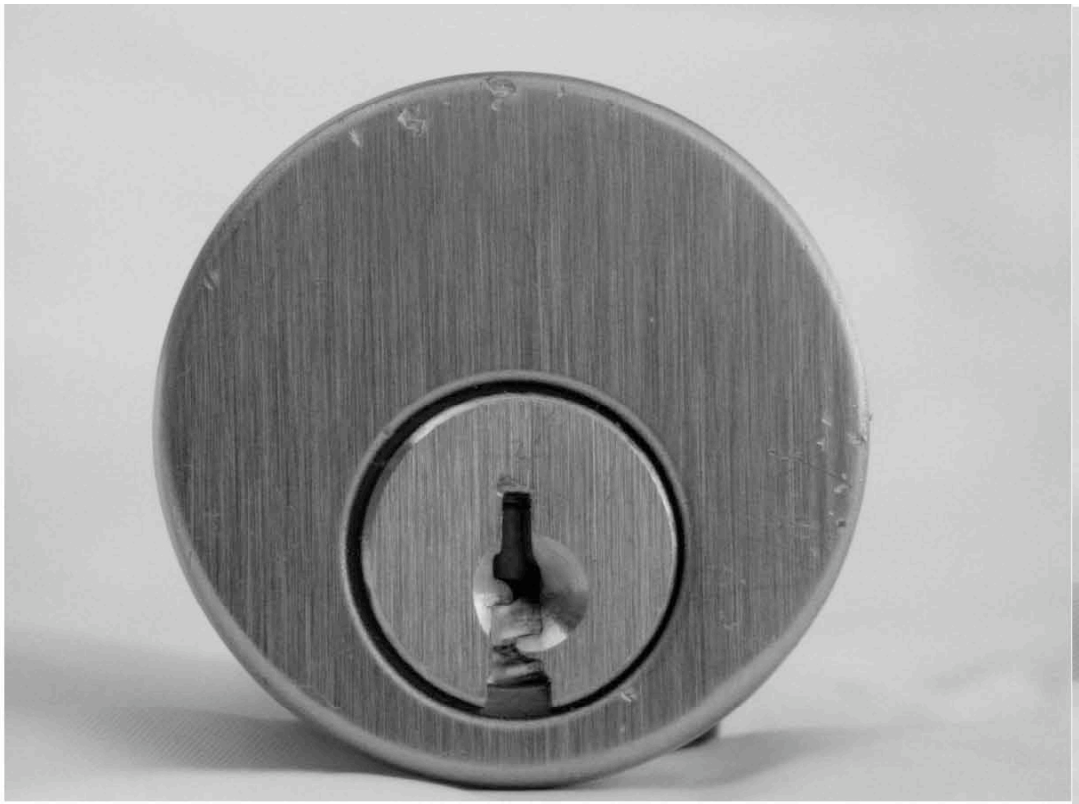
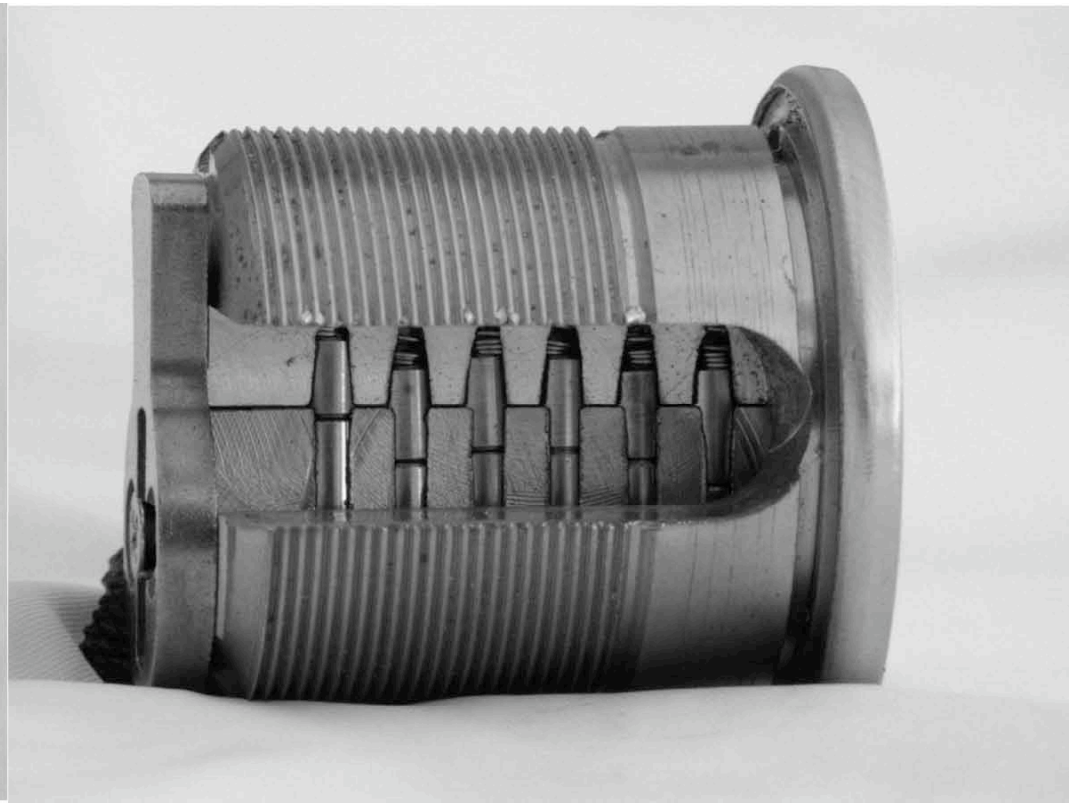


Figure 1. The pin tumbler lock, cutaway view.

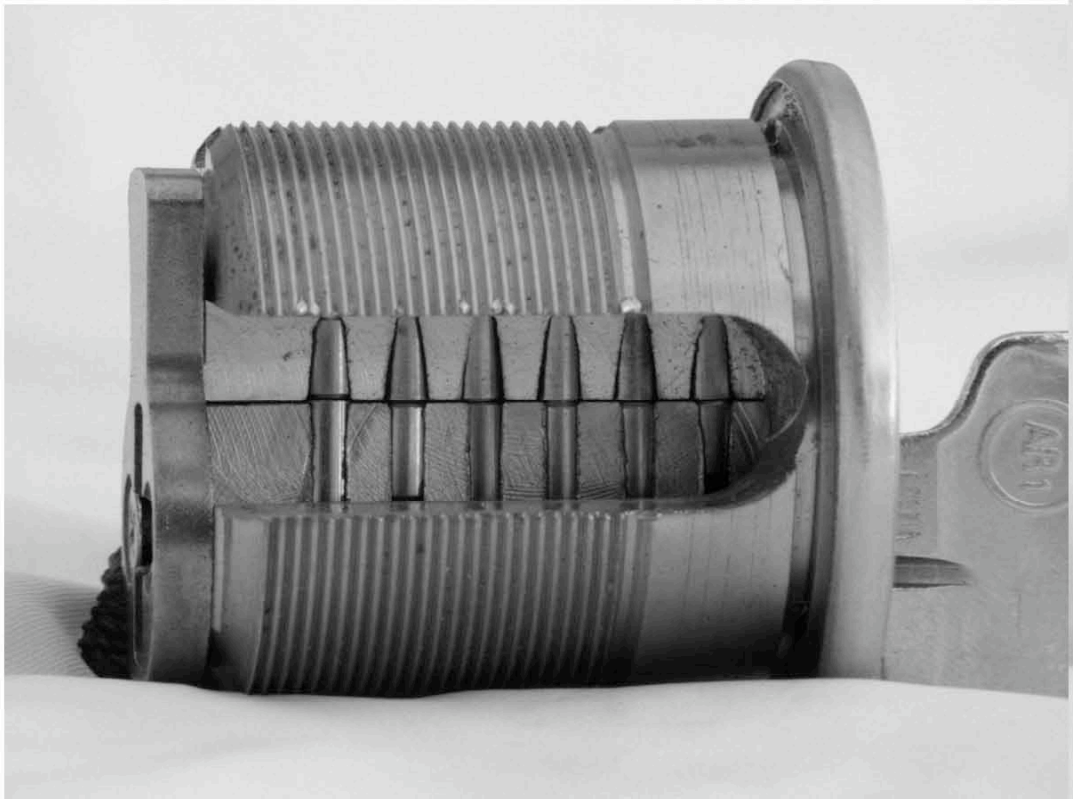


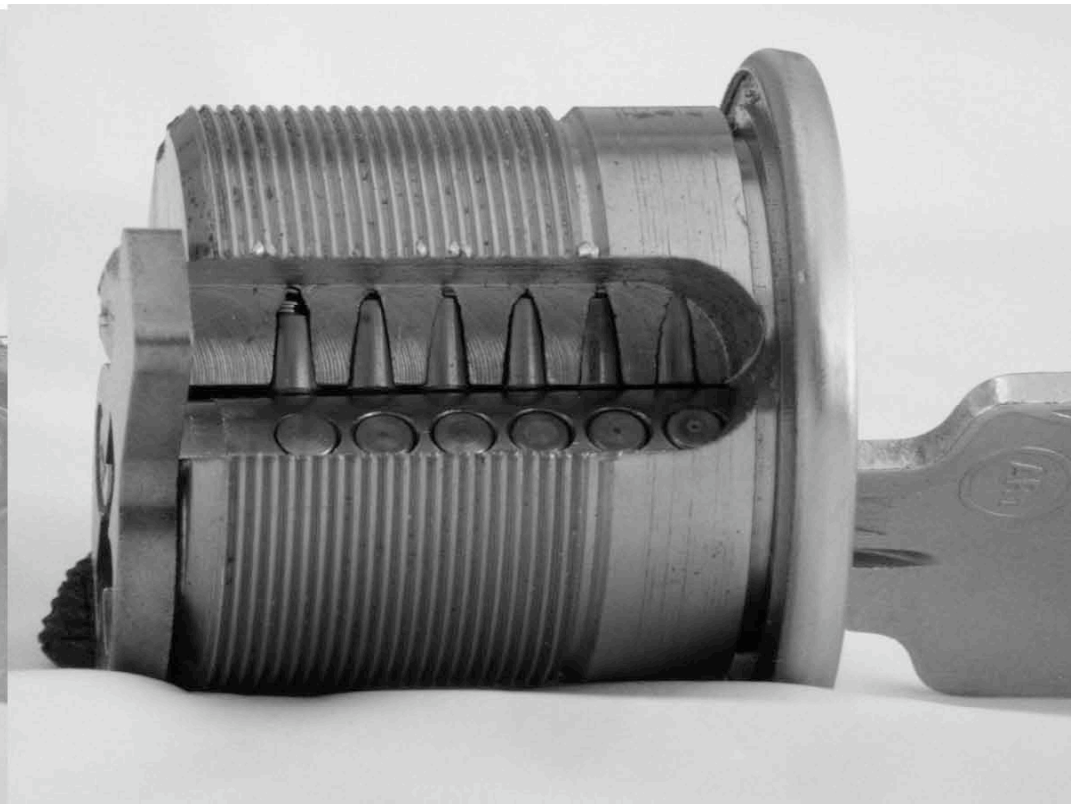




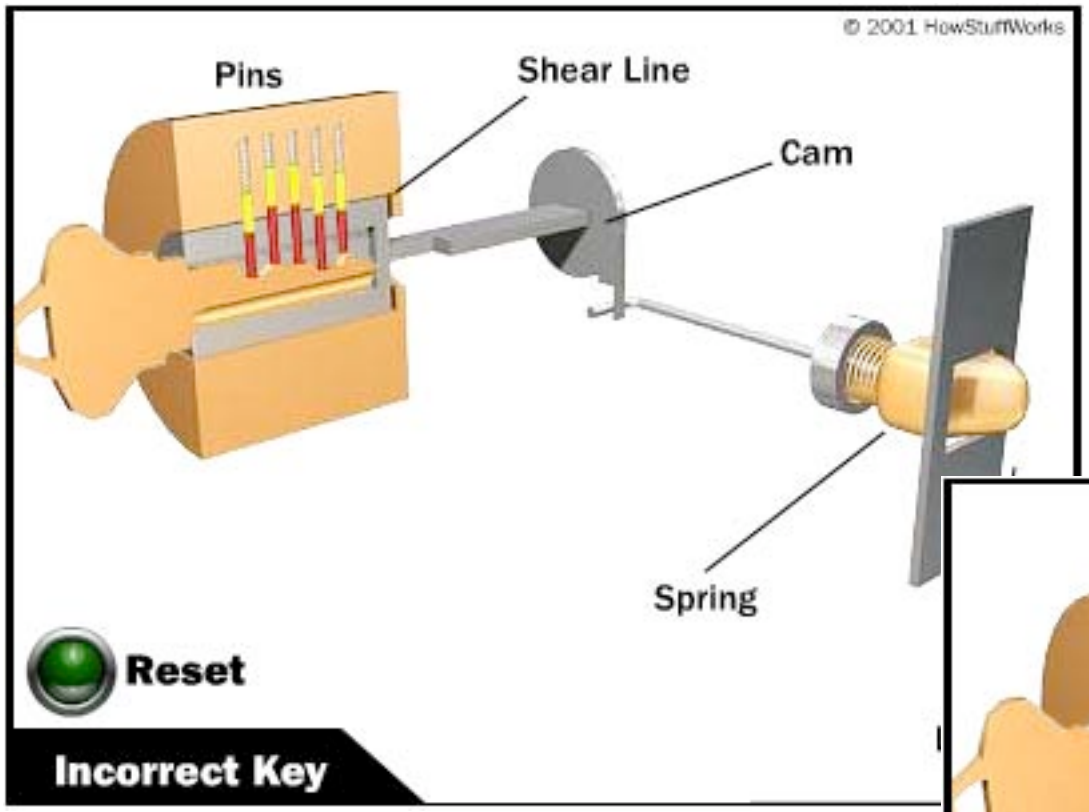


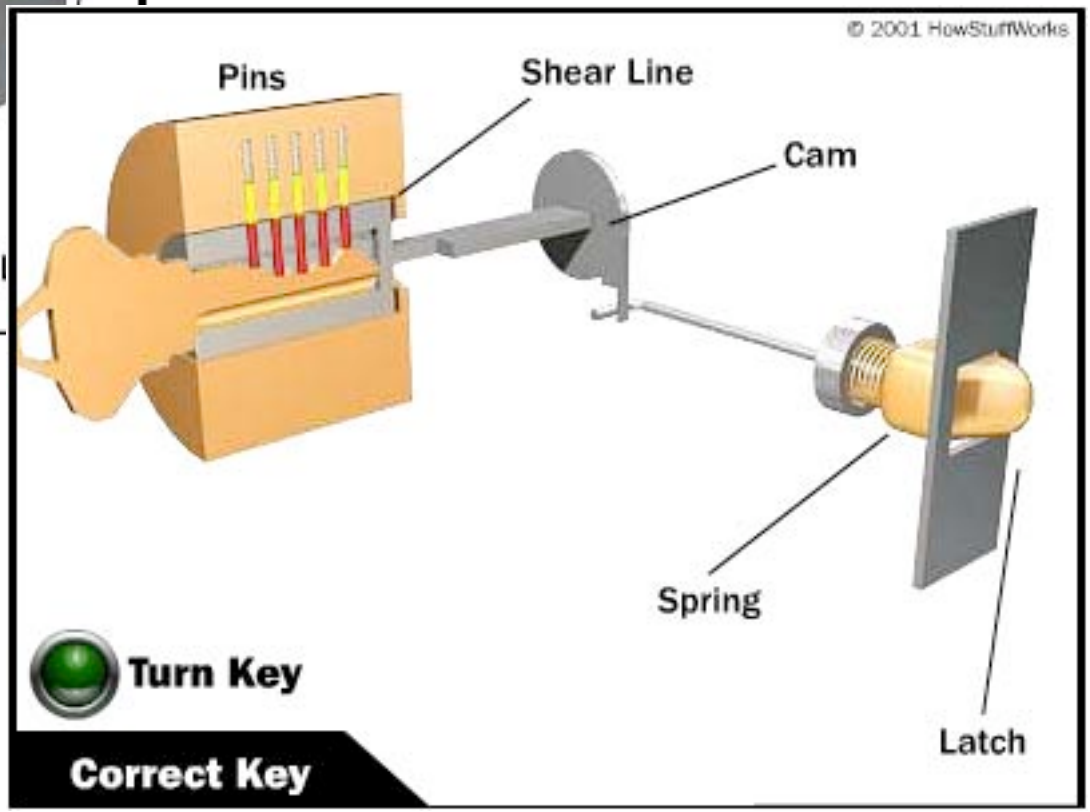
Matt Blaze: Rights Amplification in Master-Keyed Mechanical Locks



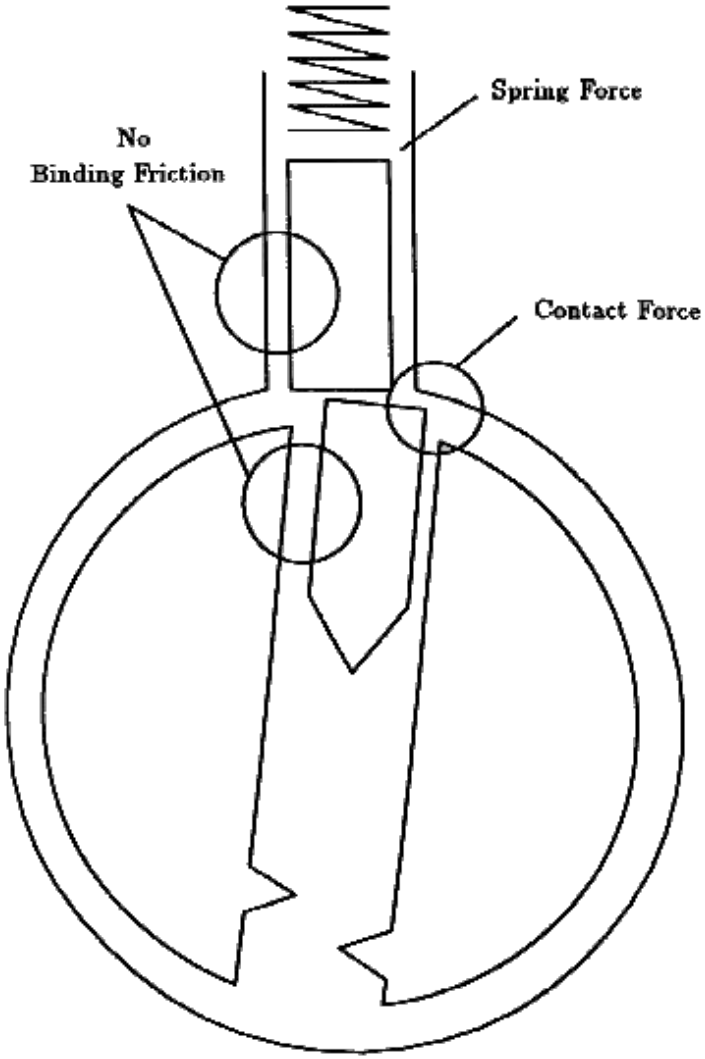


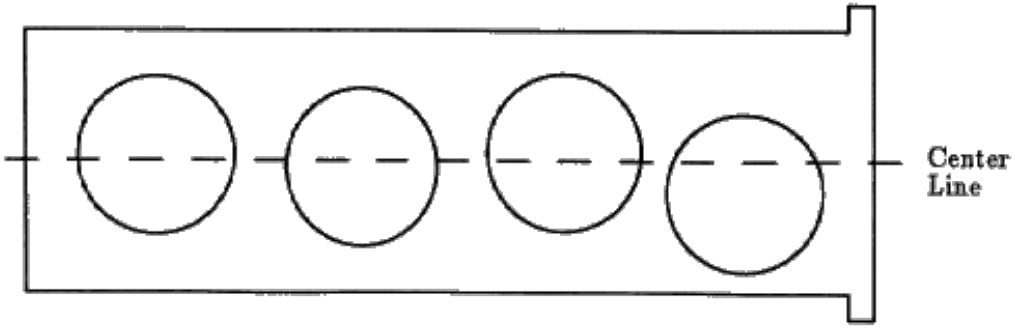
Matt Blaze: Rights Amplification in Master-Keyed Mechanical Locks


© 2001 HowStuffWorks
Pins
Shear Line
Cam
Spring
Reset
Incorrect Key

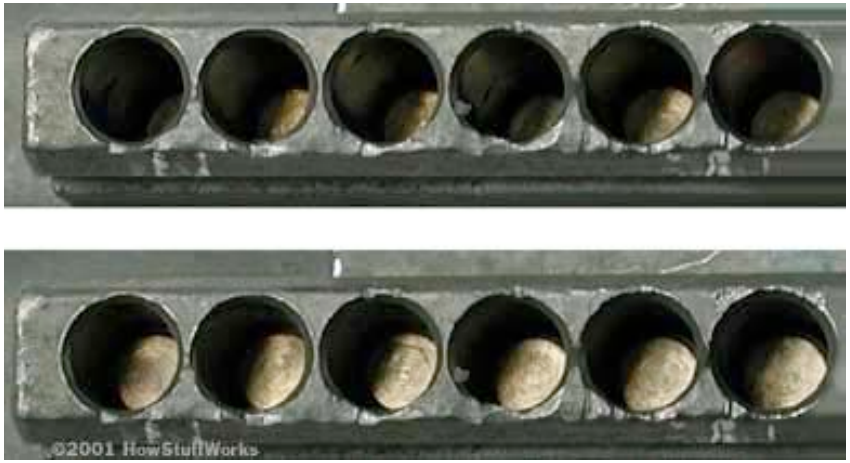

© 2001 HowStuffWorks
Pins
Shear Line
Cam
Spring
Latch
Turn Key
Correct Key

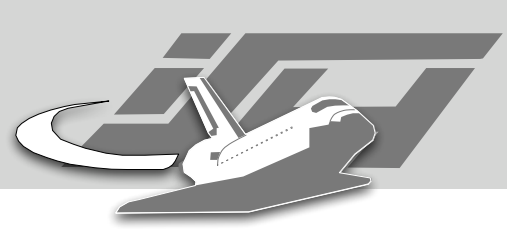
Picking Locks





Random Hole Alignment





Picking Locks

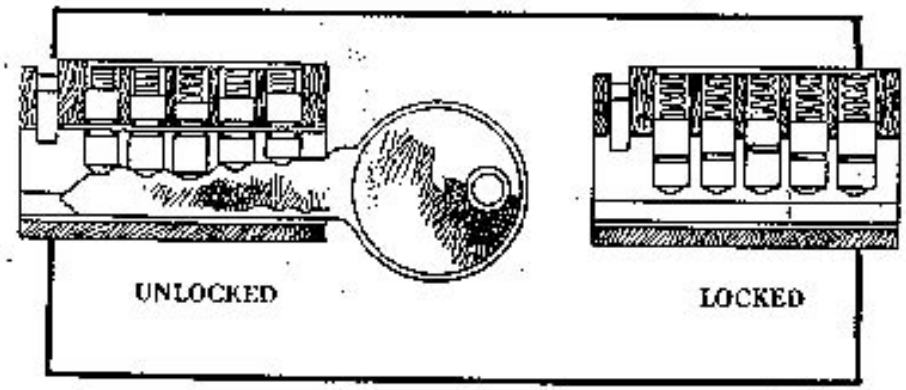


Figure 8. A pin tumbler lock.

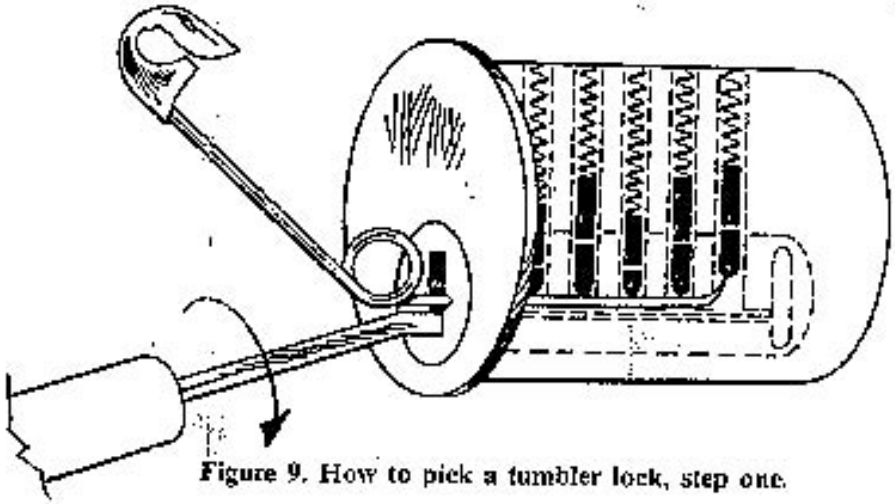


Figure 9. How to pick a tumbler lock, step one.

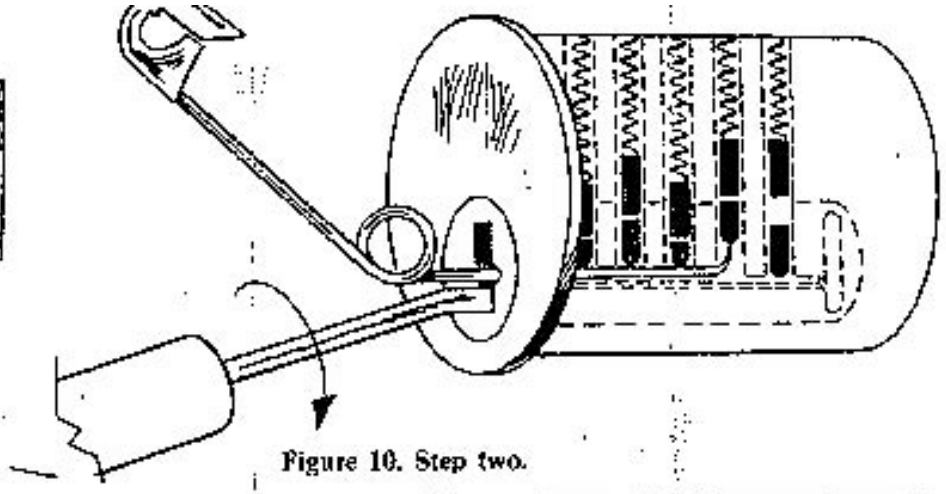


Figure 10. Step two.

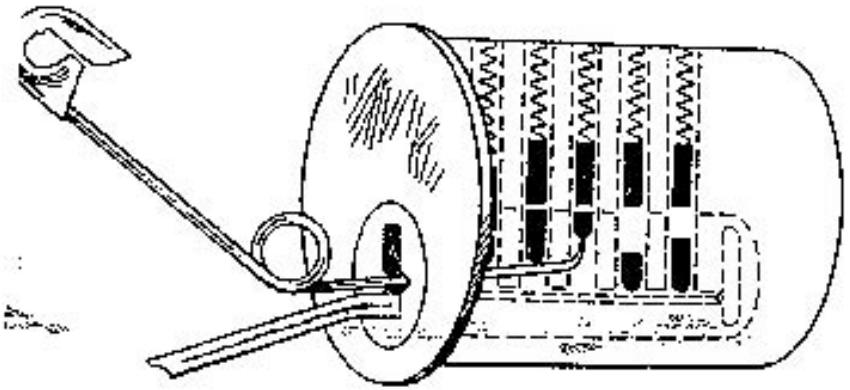


Figure 11. Step three.

Side-Bar/Disc Locks

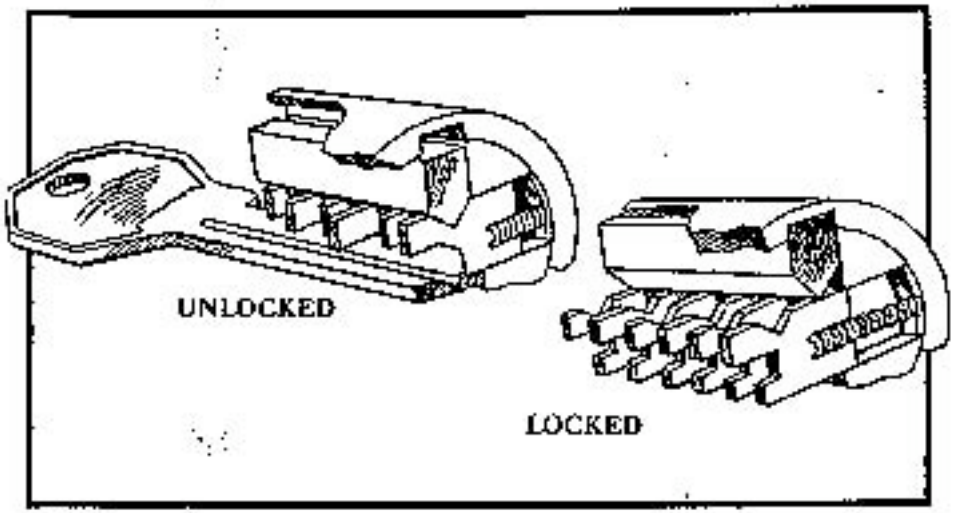


Figure 14. A side bar lock.

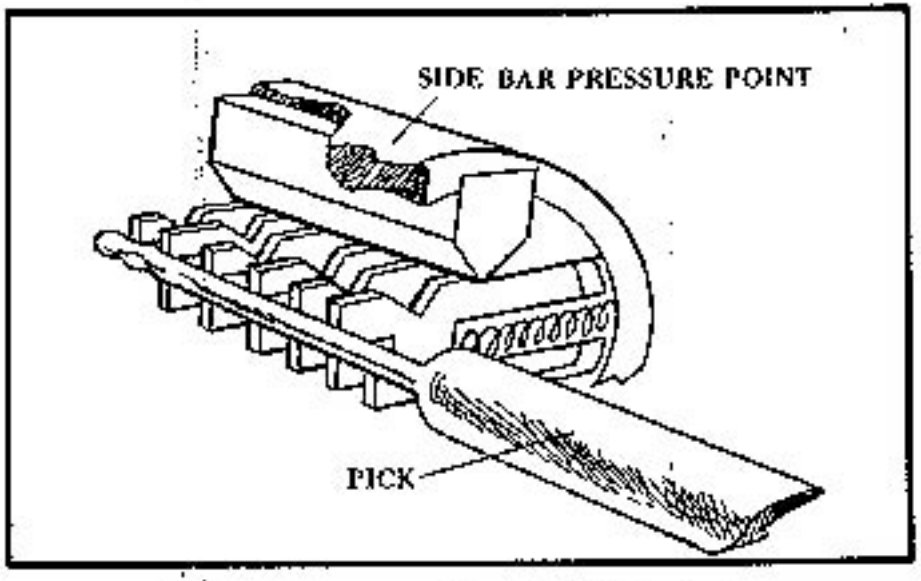


Figure 15. The rake pick inserted in the side bar lock.

Picking tools

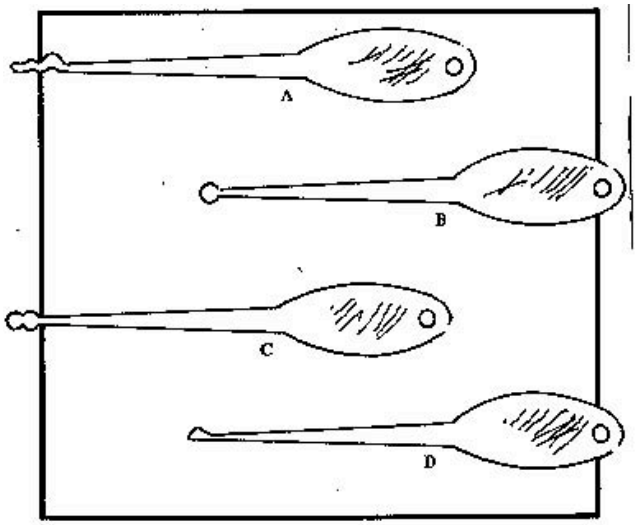


Figure 4. A: a rake pick; B: a ball pick; C: a double ball pick; D: a diamond pick.

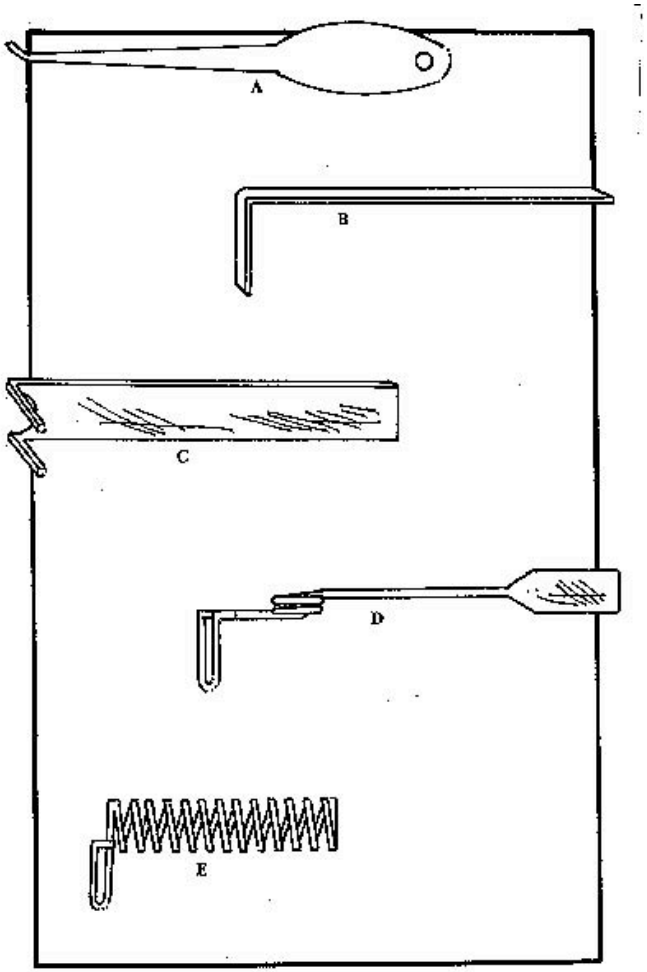
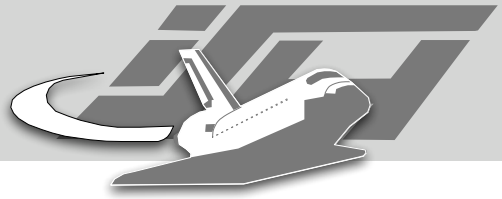
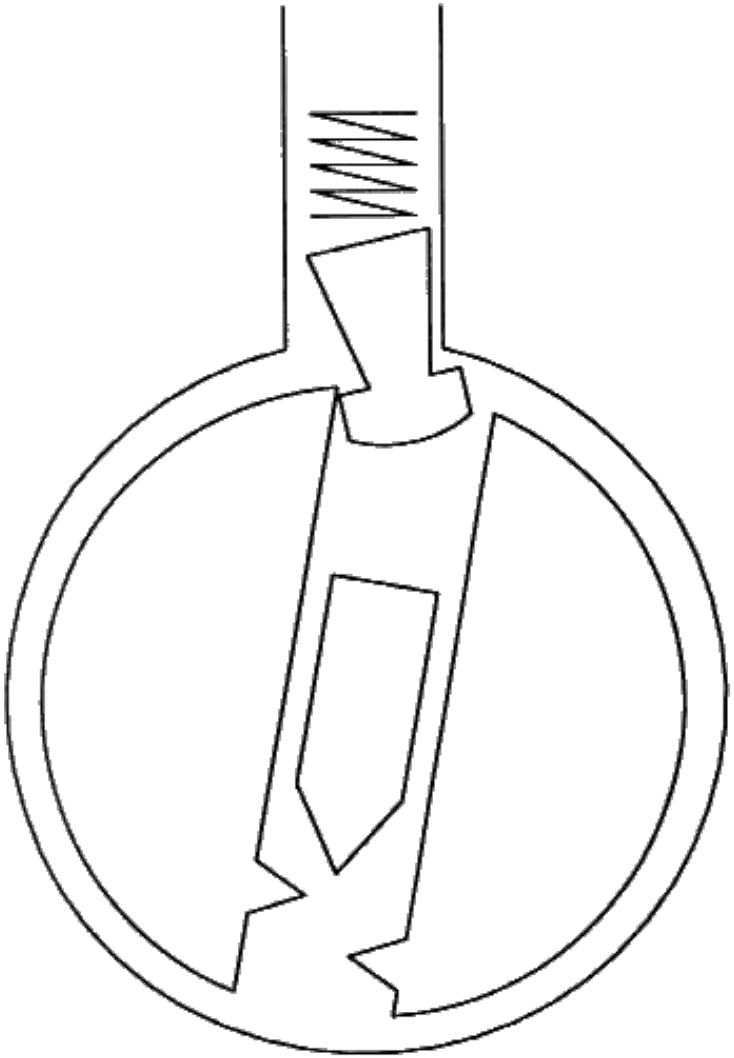


Figure 5. A: a hook pick; B: a pin and wafer lock tension wrench; C: a double-wafer tension wrench; D: a Feather Touch tension wrench; E: a homemade Feather Touch tension wrench.



Automatic Picking

Pick protection



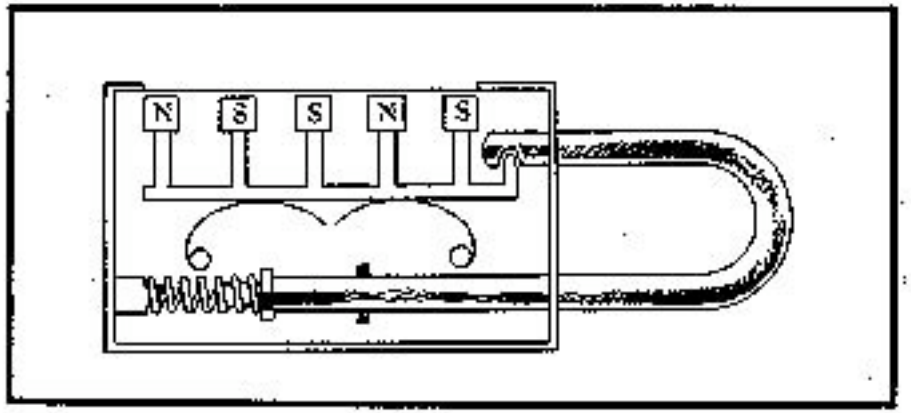


Figure 28. The inner mechanism of a magnetic lock is rather simple.

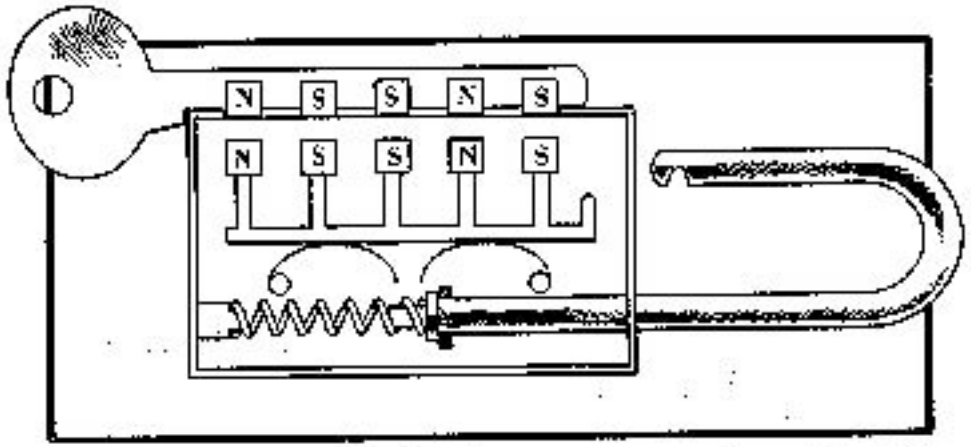


Figure 29. The magnetic key has the same sequence of magnets as the lock.

Magnetic Locks

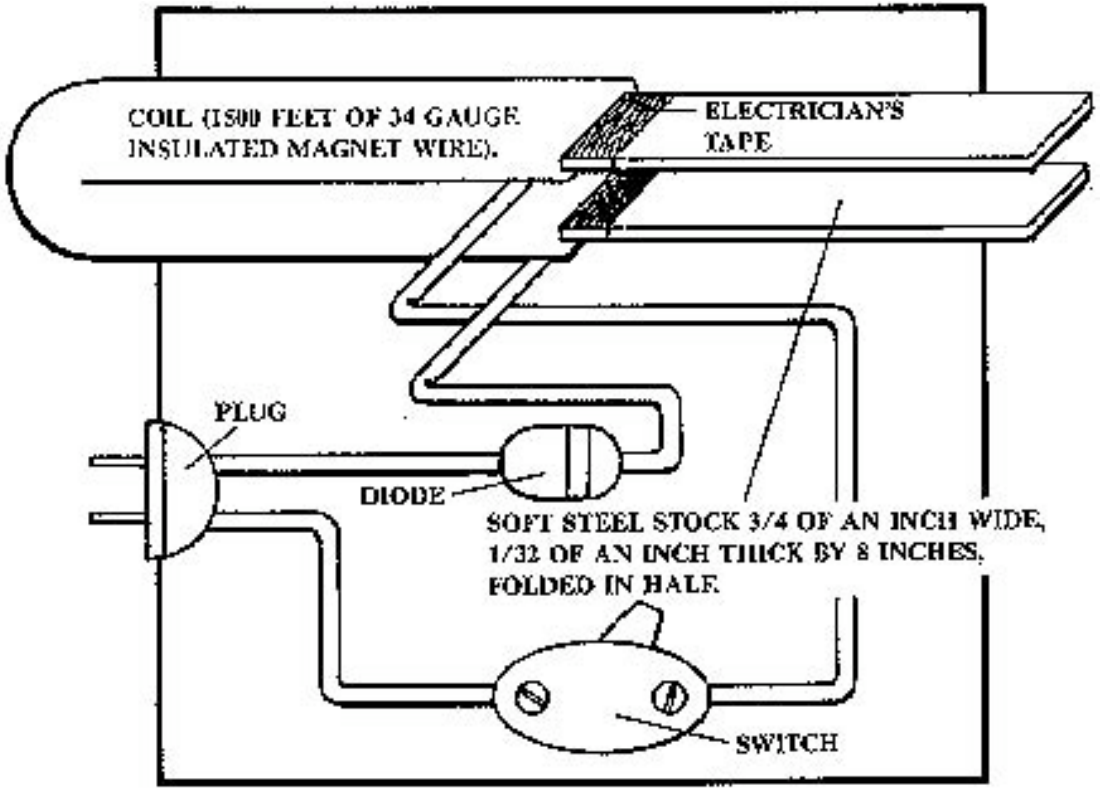
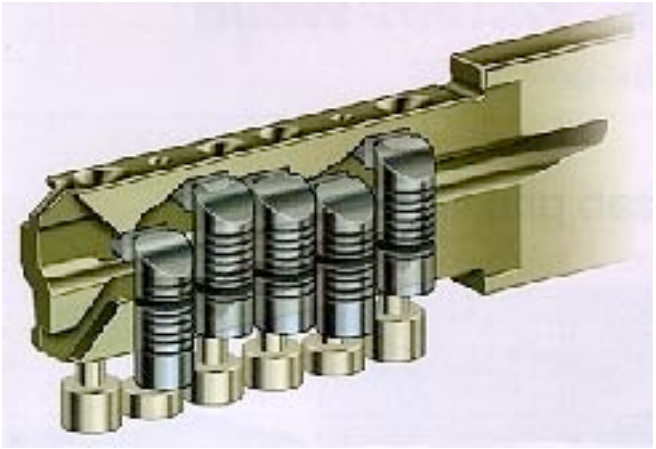
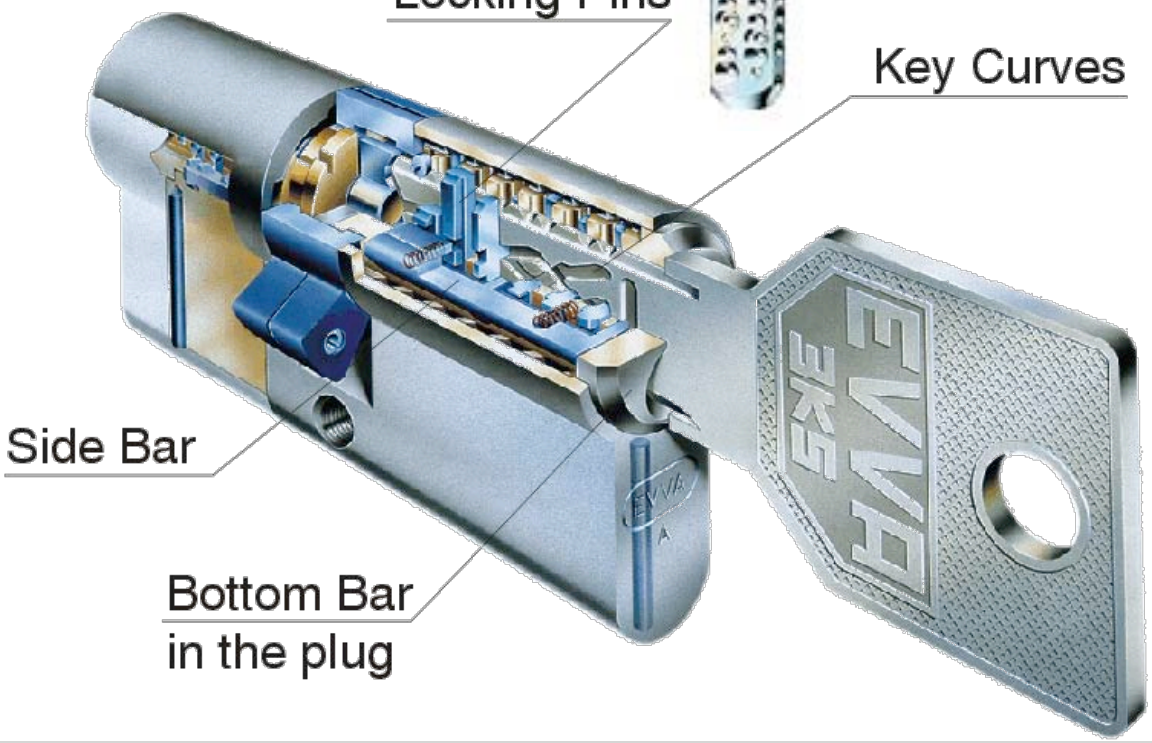


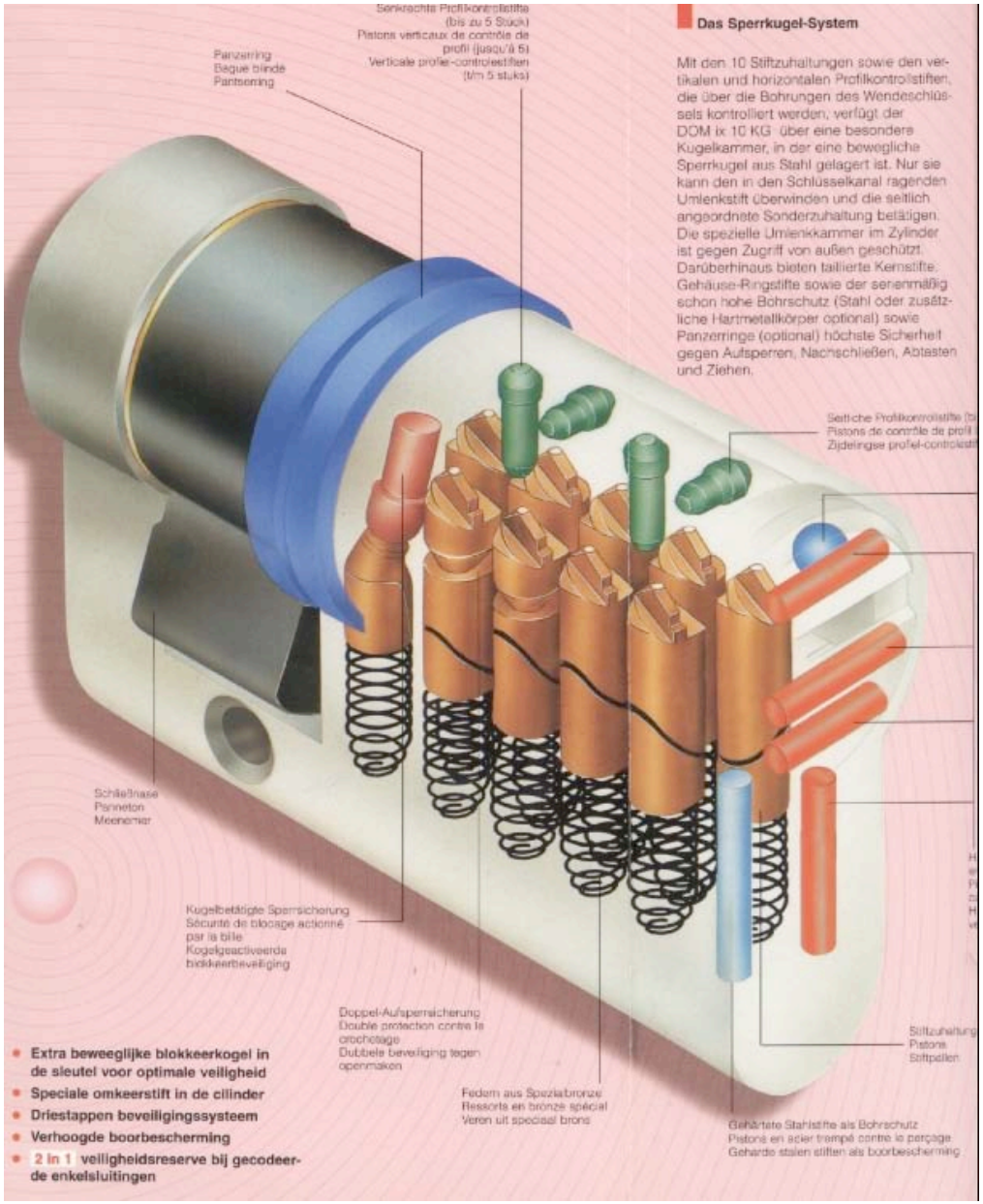
Figure 30. The magnetic pick is easy to construct.

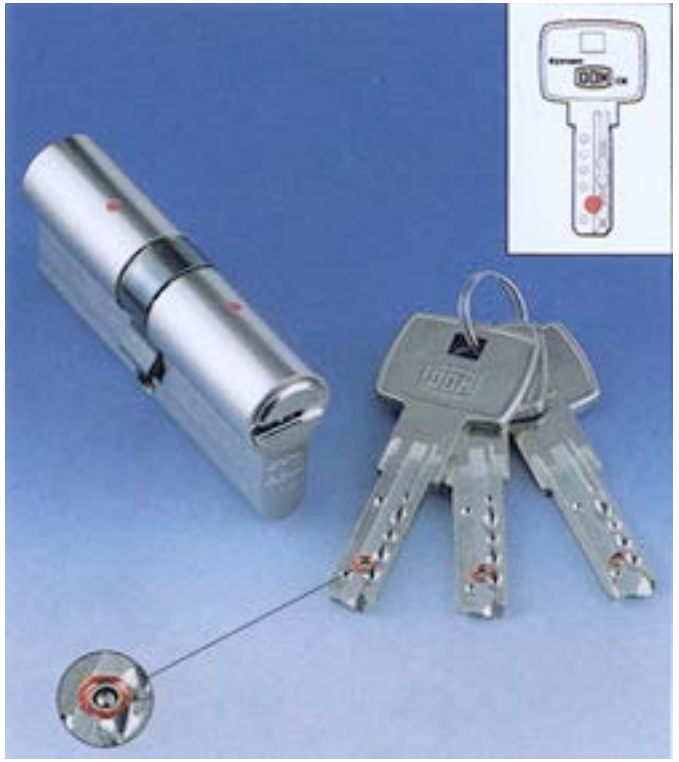
Figure 19-08. The Ikon magnetic lock is one of the most secure in the world The mechanism is comprised of eight rotating magnetic discs that control two sidebars, as well as secondary pin tumblers. If all of the discs are not in alignment, the sidebars are not able to retract, thus preventing plug rotation. Courtesy Ikon.

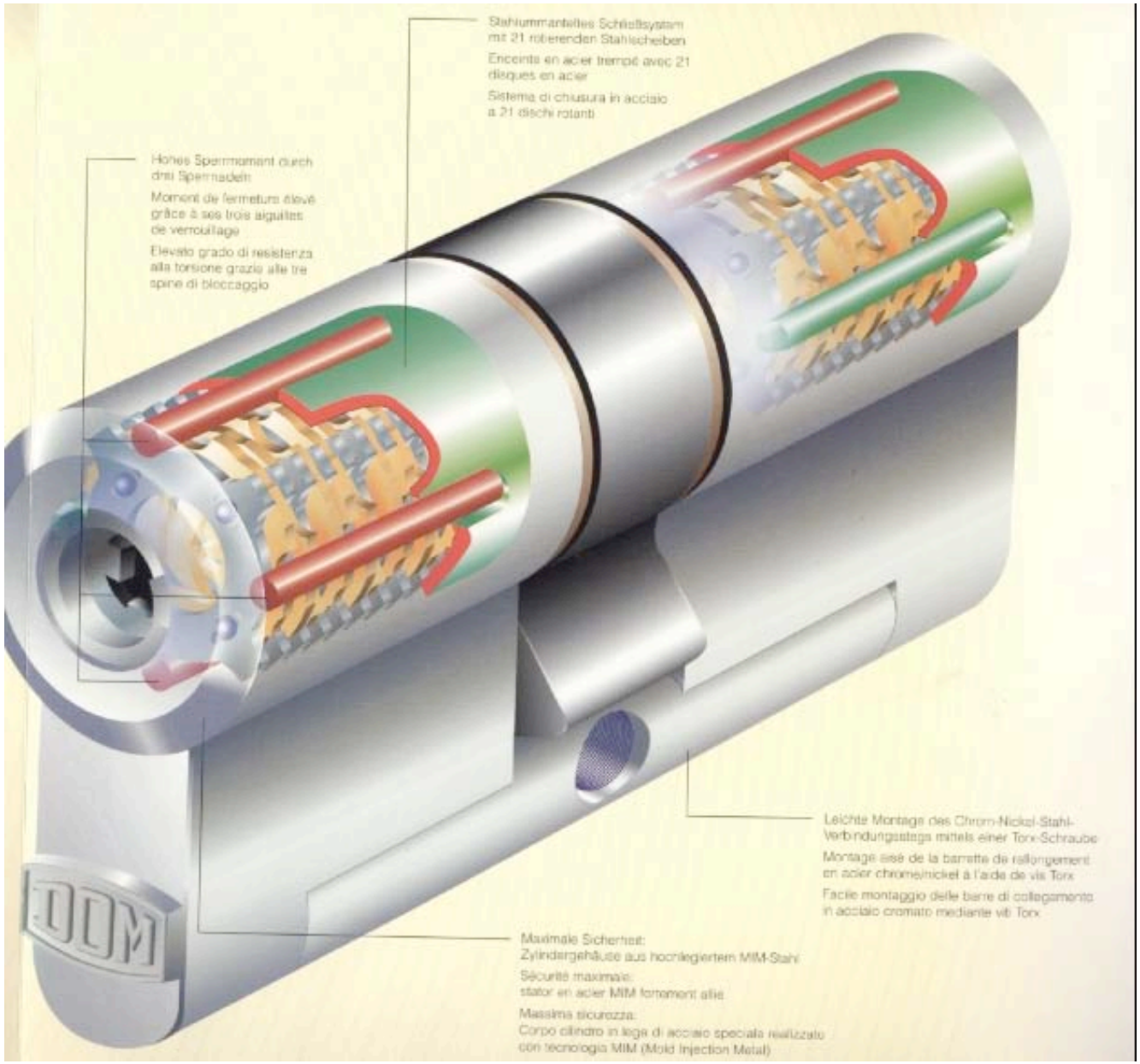
High Security Locks



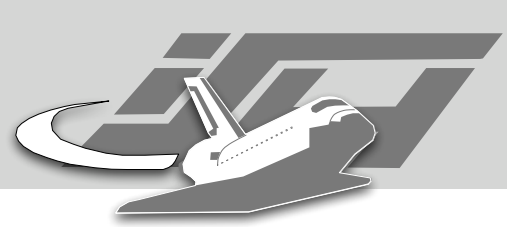



Das Sperrkugel-System
Mit den 10 Stiftzuhaltungen sowie den vertikalen und horizontalen Profilkontrollstiften, die über die Bohrungen des Wendeschlüssels kontrolliert werden, verfügt der DOM ix 10 KG über eine besondere Kugelkammer, in der eine bewegliche Sperrkugel aus Stahl gelagert ist. Nur sie kann den in den Schlüsselkanal ragenden Umlenkstift überwinden und die seitlich angeordnete Sonderzuhaltung betätigen. Die spezielle Umlenkkammer im Zylinder ist gegen Zugriff von außen geschützt. Darüberhinaus bieten taillierte Kernstifte, Gehäuse-Ringstifte sowie der serienmäßig schon hohe Bohrschutz (Stahl oder zusätzliche Hartmetallkörper optional) sowie Panzerringe (optional) höchste Sicherheit gegen Aufsperren, Nachschließen, Abtasten und Ziehen.
Panzerring
Bague blindé
Pantsering
Schließnase
Panneton
Meenemer
Kugelbetätigte Sperrsicherung
Sécurité de blocage actionné par la bille
Kogelgeactiveerde blokkeerbeveiliging
Doppel-Aufsperrsicherung
Double protection contre le crochetage
Dubbele beveiliging tegen openmaken
Federn aus Spezialbronze
Ressorts en bronze spécial
Veren uit speciaal brons
Stiftzuhaltung
Pistons
Stiftpallen
Gehärtete Stahlstifte als Bohrschutz
Pistons en acier trempé contre le perçage
Geharde stalen stiften als boorbescherming
Extra beweeglijke blokkeerkogel in de sleutel voor optimale veiligheid
Speciale omkeerstift in de cilinder
Driestappen beveiligingssysteem
Verhoogde boorbescherming
2 in 1 veiligheidsreserve bij gecodeerde enkelsluitingen



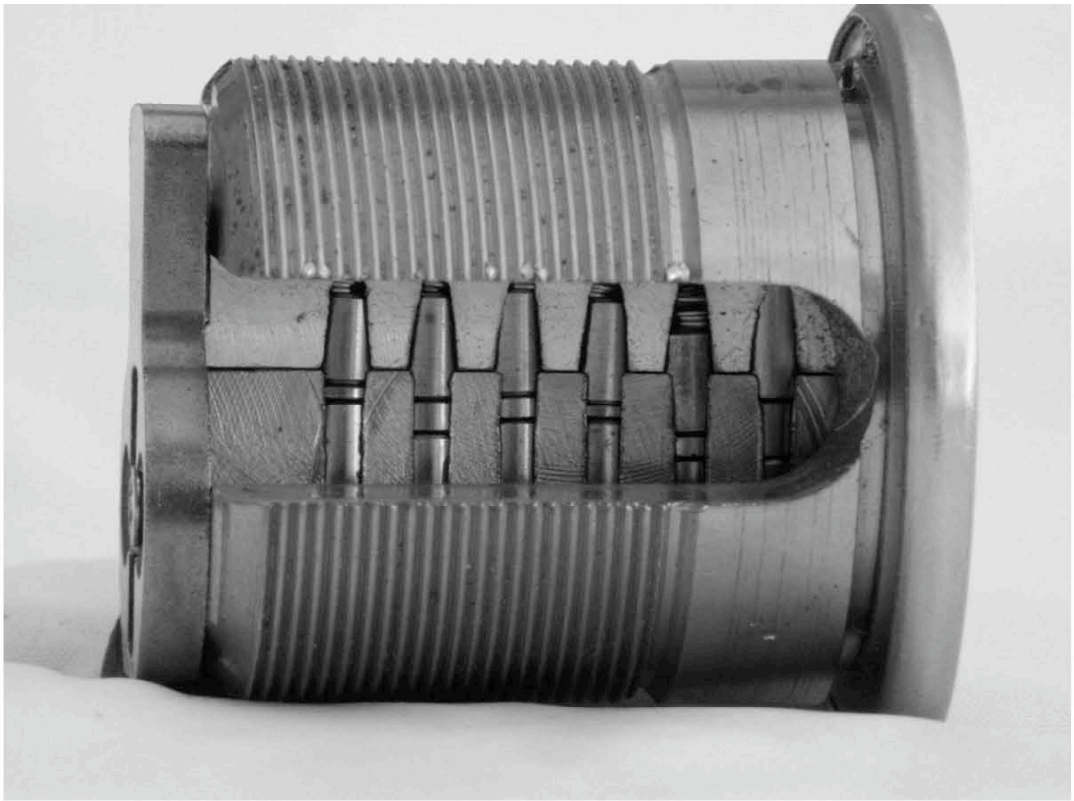

Stahlummanteltes Schließsystem mit 21 rotierenden Stahlscheiben
Enceinte en acier trempé avec 21 disques en acier
Sistema di chiusura in acciaio a 21 dischi rotanti
Hohes Sperrmoment durch drei Sperrnadeln
Moment de fermeture élevé grâce à ses trois aiguilles de verrouillage
Elevato grado di resistenza alla torsione grazie alle tre spine di bloccaggio
Leichte Montage des Chrom-Nickel-Stahl-Verbindungssteges mittels einer Torx-Schraube
Montage aisé de la barrette de rallongement en acier chrome/nickel à l'aide de vis Torx
Facile montaggio delle barre di collegamento in acciaio cromato mediante viti Torx
Maximale Sicherheit:
Zylindergehäuse aus hochlegiertem MIM-Stahl
Sécurité maximale:
stator en acier MIM fortement allié
Massima sicurezza:
Corpo cilindro in lega di acciaio speciale realizzato con tecnologia MIM (Mold Injection Metal)
DOM

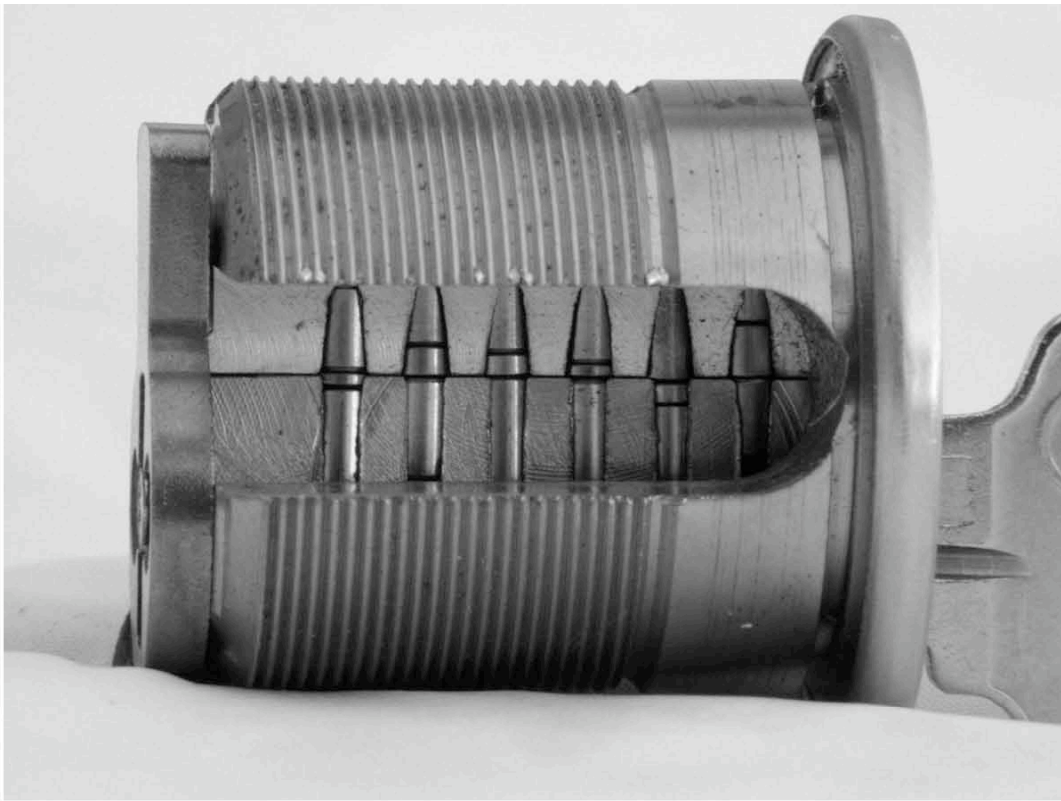

DOM



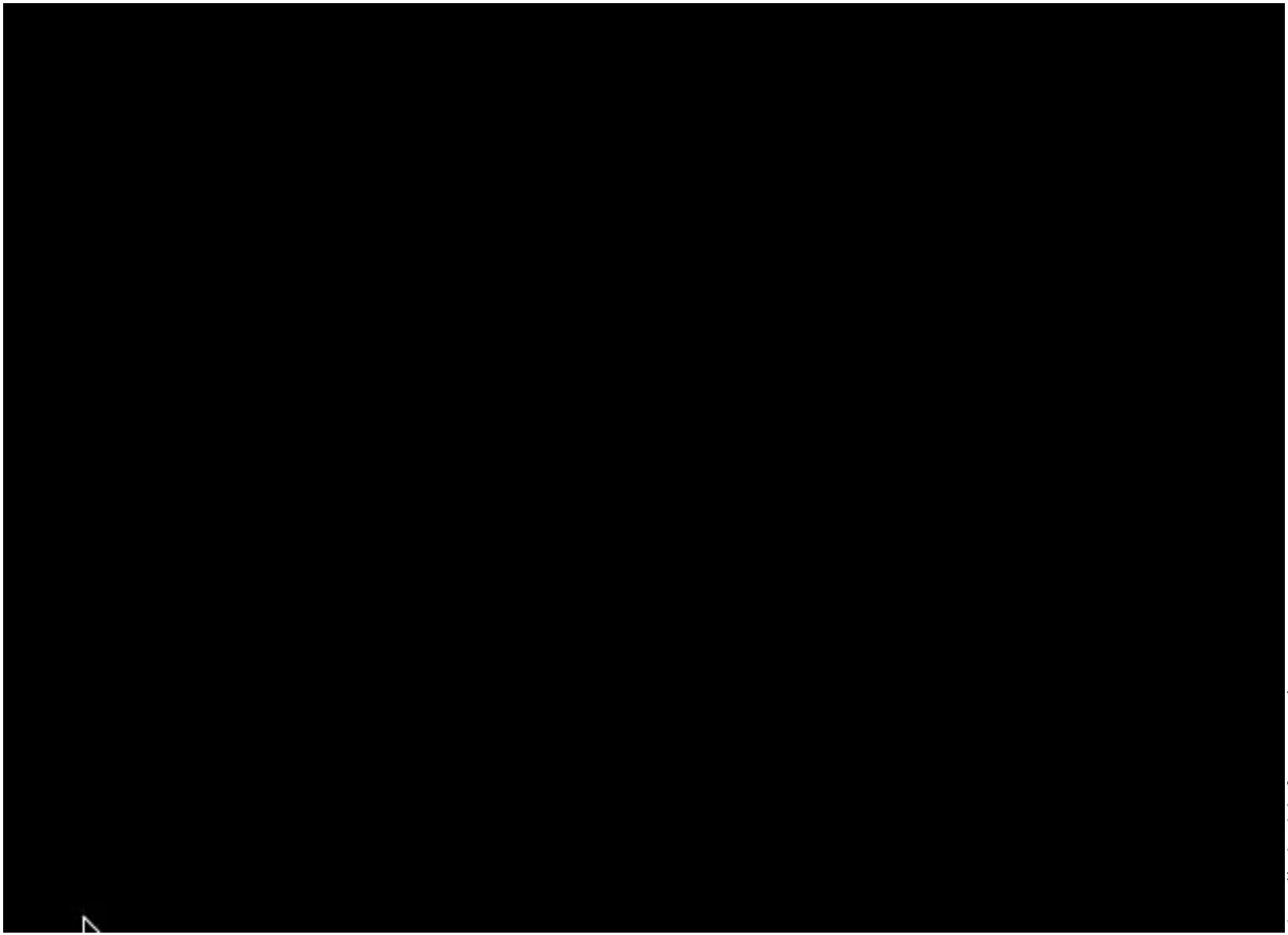
The Crypto Attack

- Matt Blaze: Rights Amplification in Master-Keyed Mechanical Locks, IEEE Security & Privacy, March/April 2003

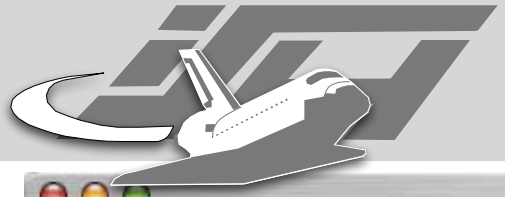




Matt Blaze: Rights Amplification in Master-Keyed Mechanical Locks



http://video.bikeforums.net/



SSDeV – Lockpicking in Germany

http://www.ssdev.org/

Google

Inhalt

Infos zum Sportverein
Vorwort / Einleitung
Satzung, Beitragsordnung, Sportordnung
Beitrittserklärung

Adressen & Sportgruppen
Kontakte zum SSDeV
Sport-Gruppen: Berlin: OST / WEST, Bochum, Darmstadt, Düsseldorf, Frankfurt, Freiburg, Hamburg, Karlsruhe, Köln, Marburg, Moers, München, Nordbaden, Stuttgart, Ulm.
SpG-Unterwasser

Sport-Shop
Literatur
Sportgeräte

Deutsche Meisterschaften
Meisterschaften 2004
Listung der Meister
Nachlese 1997
Schlossliste 1999
Die Wettkampfregeln 2004
Handöffnung, Freestyle, Hangöffnung, Blitz-Öffnung, Impressionstechnik.

Sonstiges
Handbuch zur Schlossöffnung
Bilder vom Camp2003
Tips zur Sicherheit
Workshop in Köln

Sportenthusiasts of Lockpicking - Europe
www.lockpicking.org

Das Buch "Geheimwissen Schlüsseldienst" von Michael Bübl ist verfügbar !

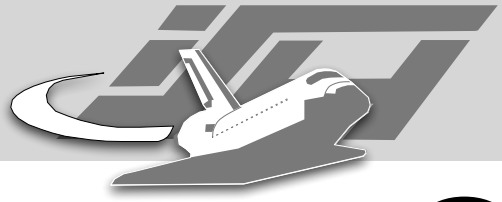
SPORTSFREUNDE DER SPERRTECHNIK - DEUTSCHLAND e.V.

Sportsfreunde der Sperrtechnik - Deutschland e.V.
Mission of the Sportenthusiasts of Lockpicking - Germany

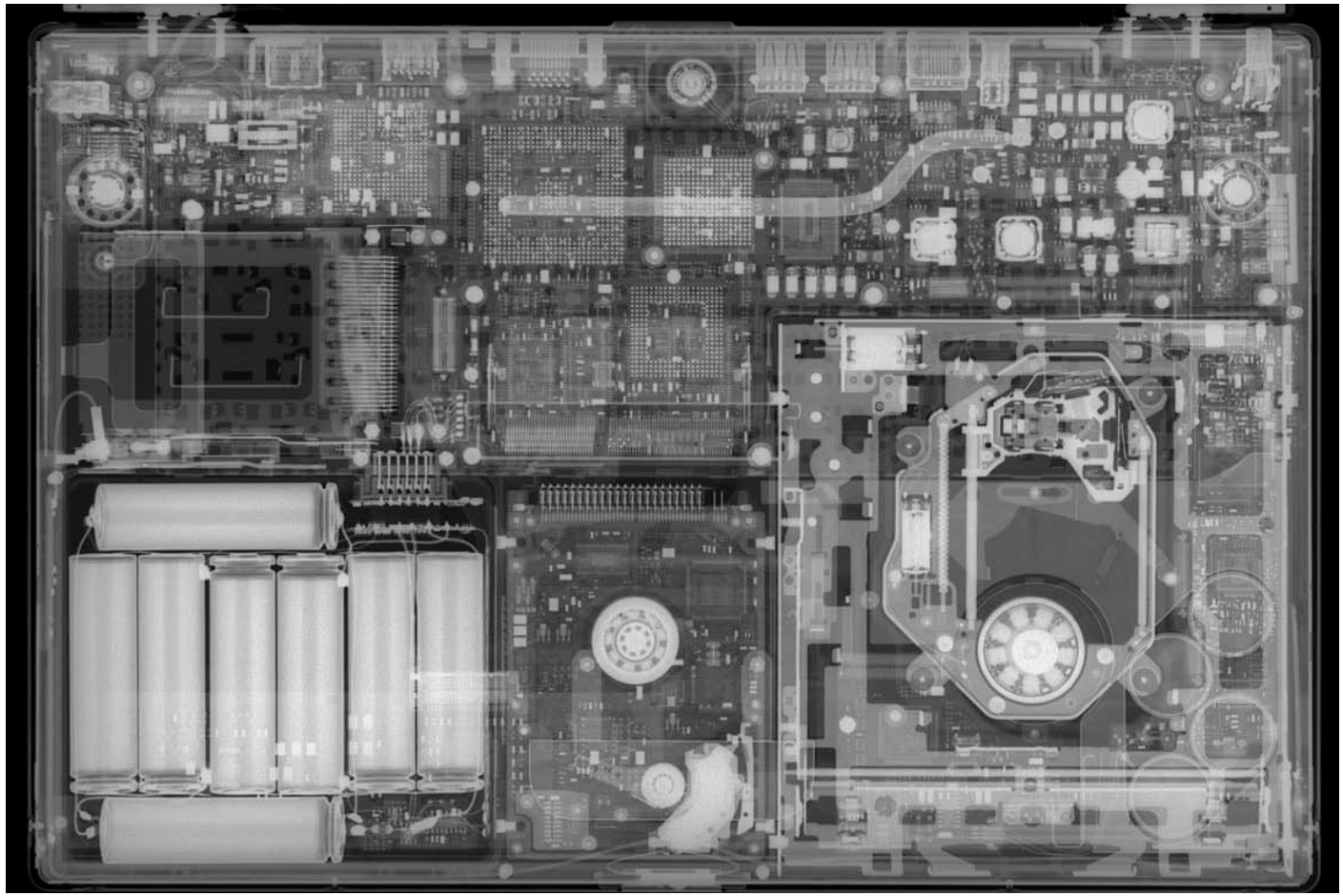
The Open Organisation Of Lockpickers (Nederland)
Lockpickers in UK (United Kingdom)
Guide de Crochetage des serrules a Gouplilles (France)

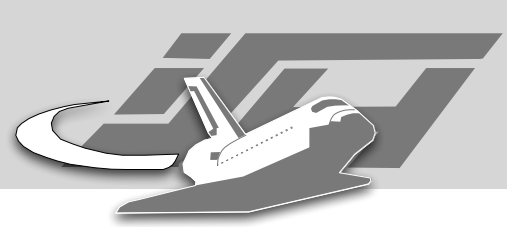
No Lockpicking ...

Tampering

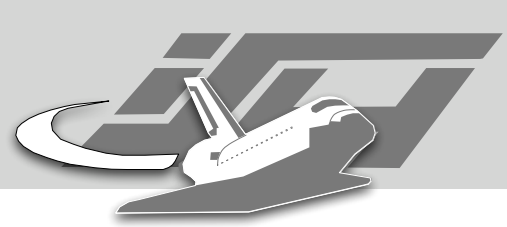


Opening things you shouldn't

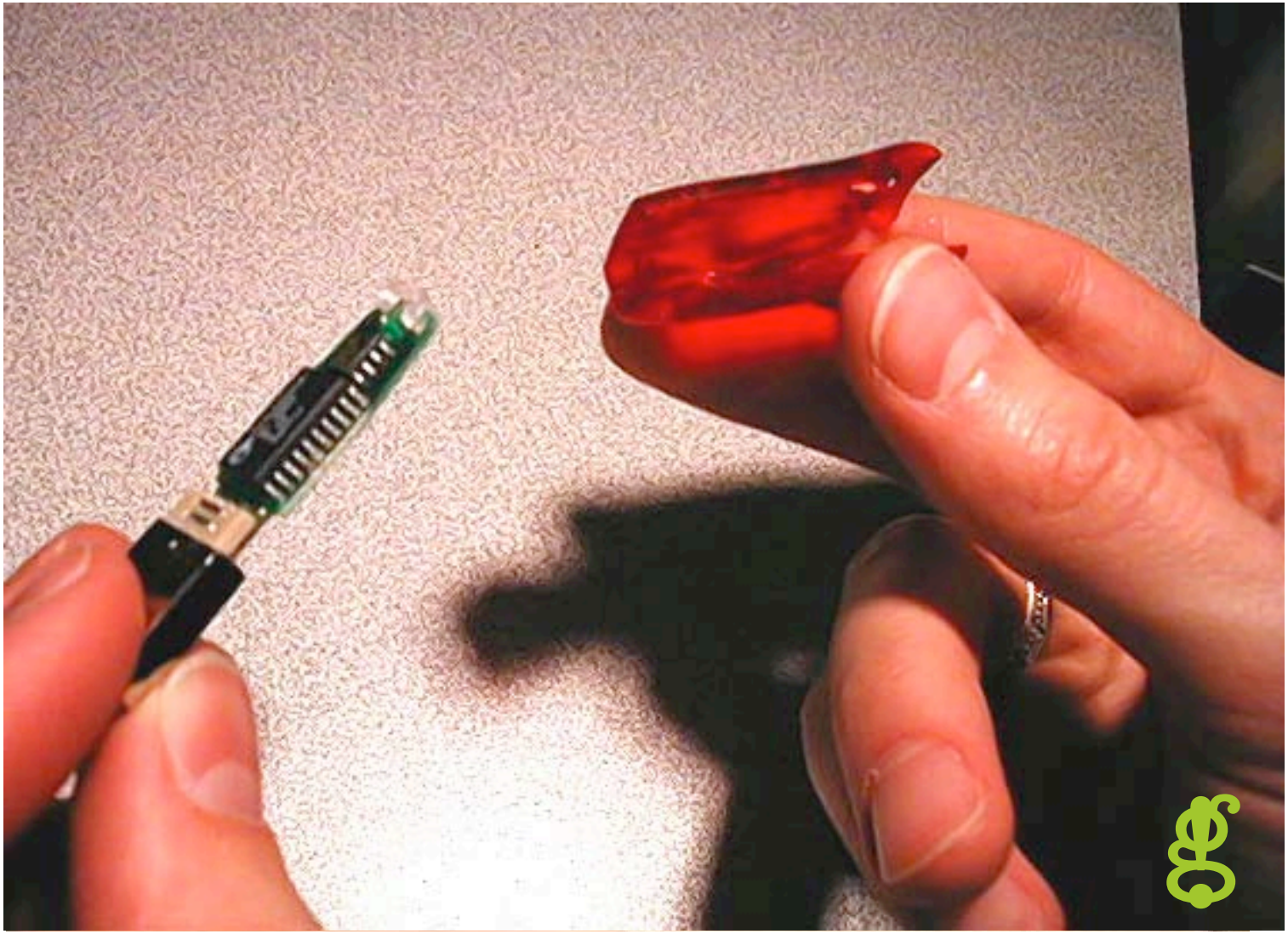


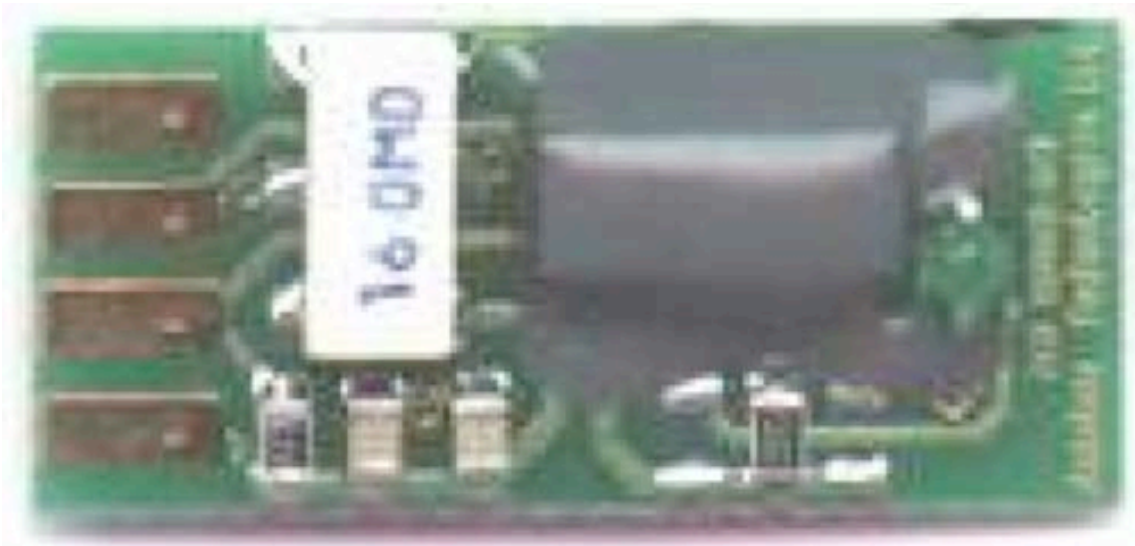


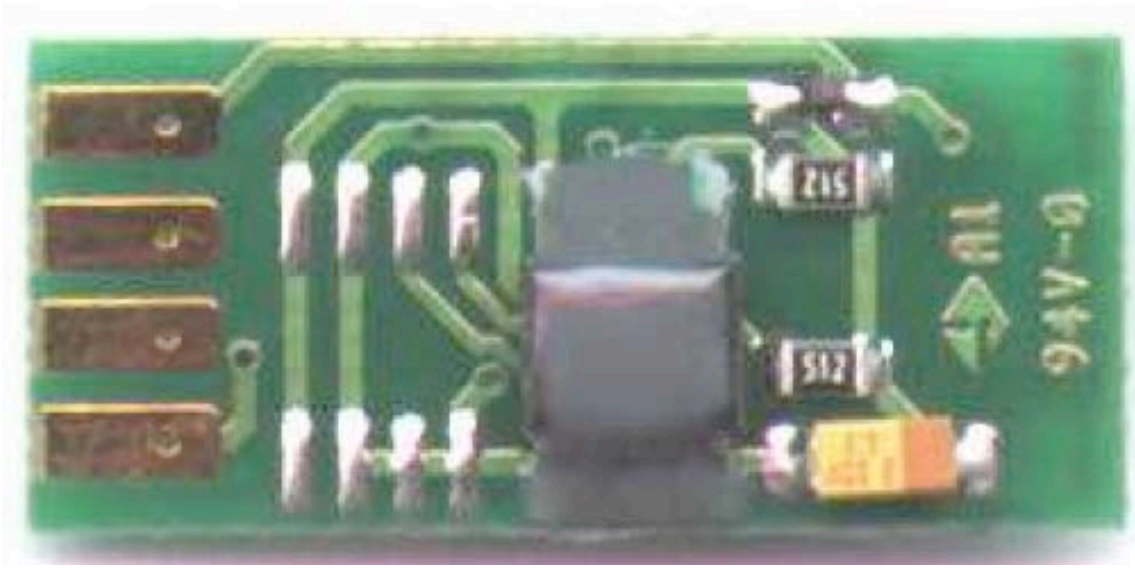
iPod

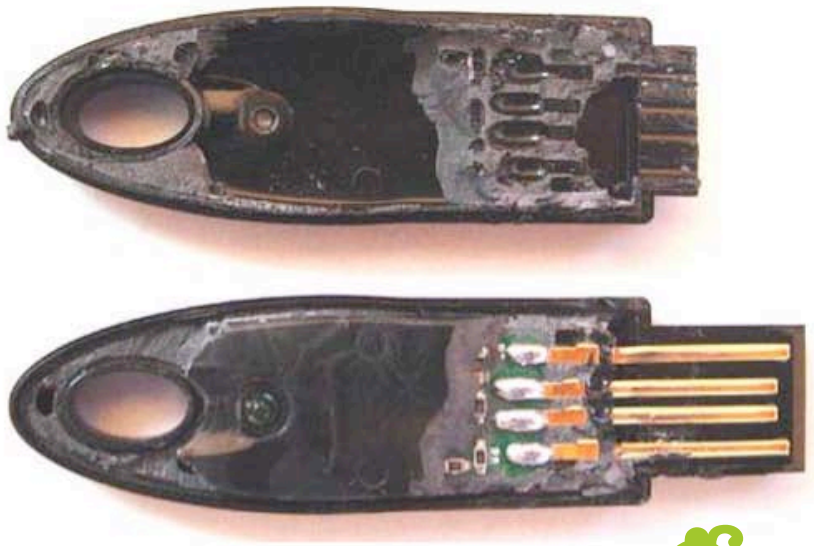


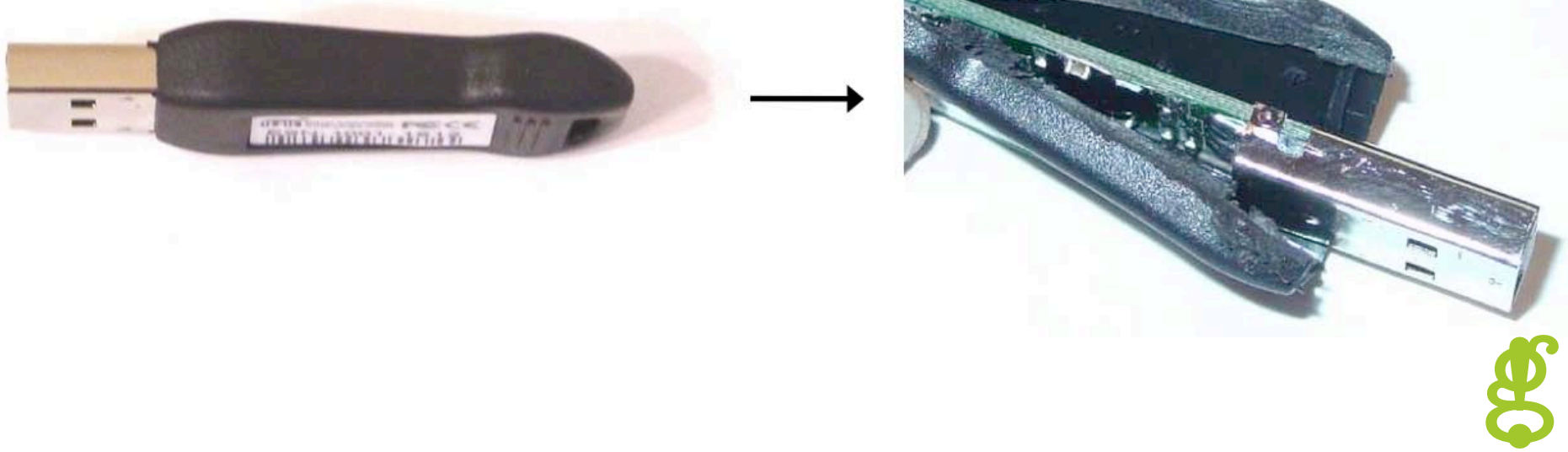
USB Devices




16 DMD

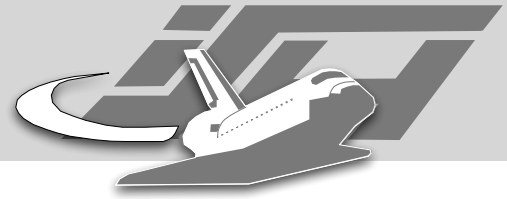

94V-0





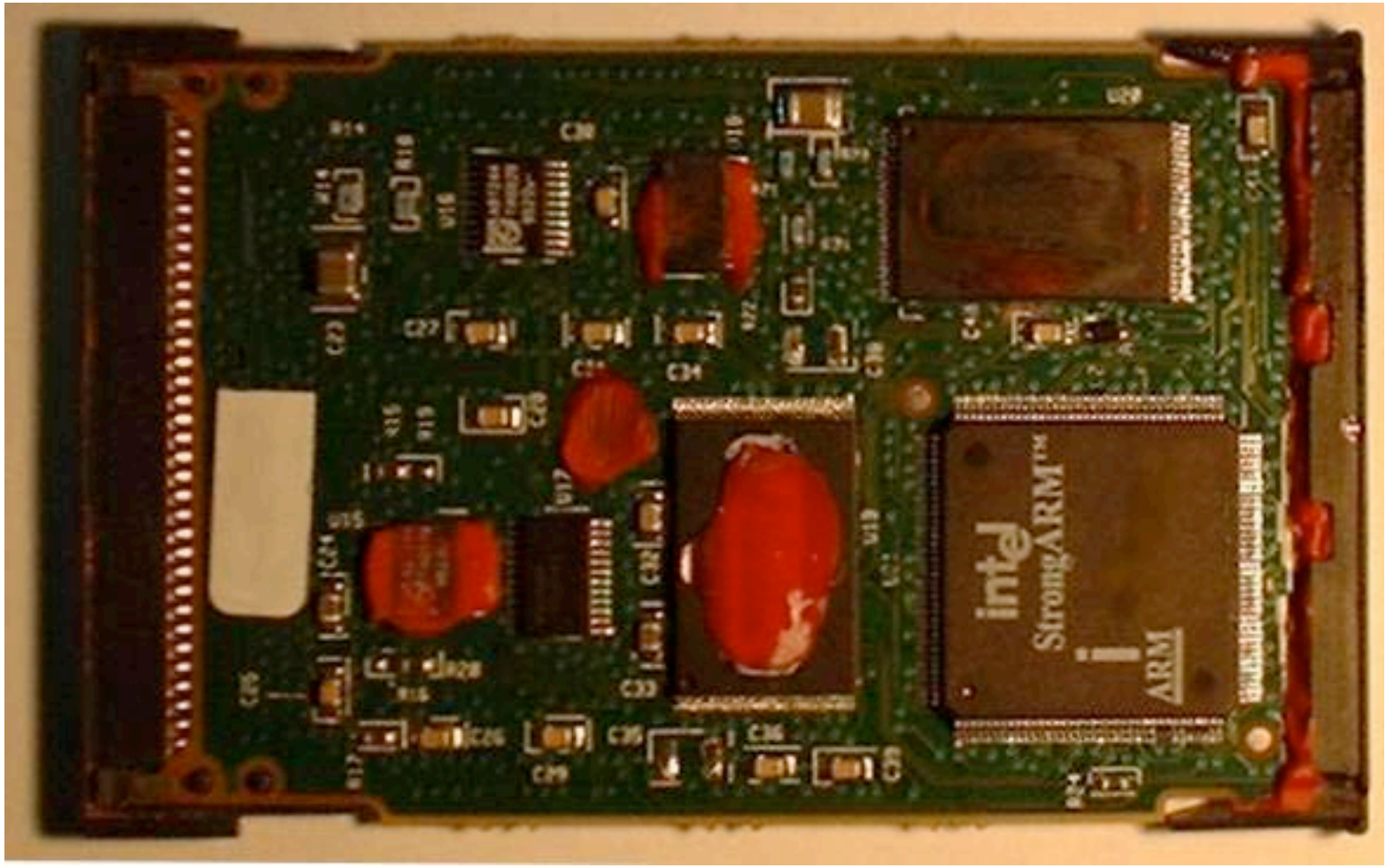

DALLAS
C2
02
00D0007B04E6


JAVA

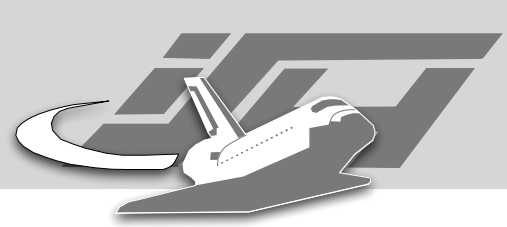


- Chrysalis-ITS Luna CA3 Cryptographic Token
- Mike Bond, Daniel Cvrček, Steven J. Murdoch: Unwrapping the Chrysalis

Bond / Cvrček /Murdoch:Unwrapping the Chrysalis

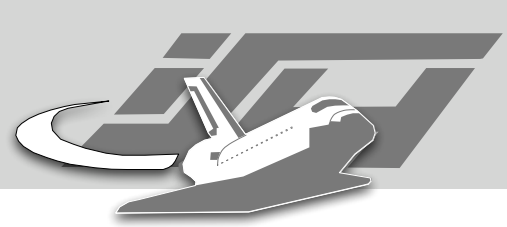


Bond / Cvrček /Murdoch:Unwrapping the Chrysalis

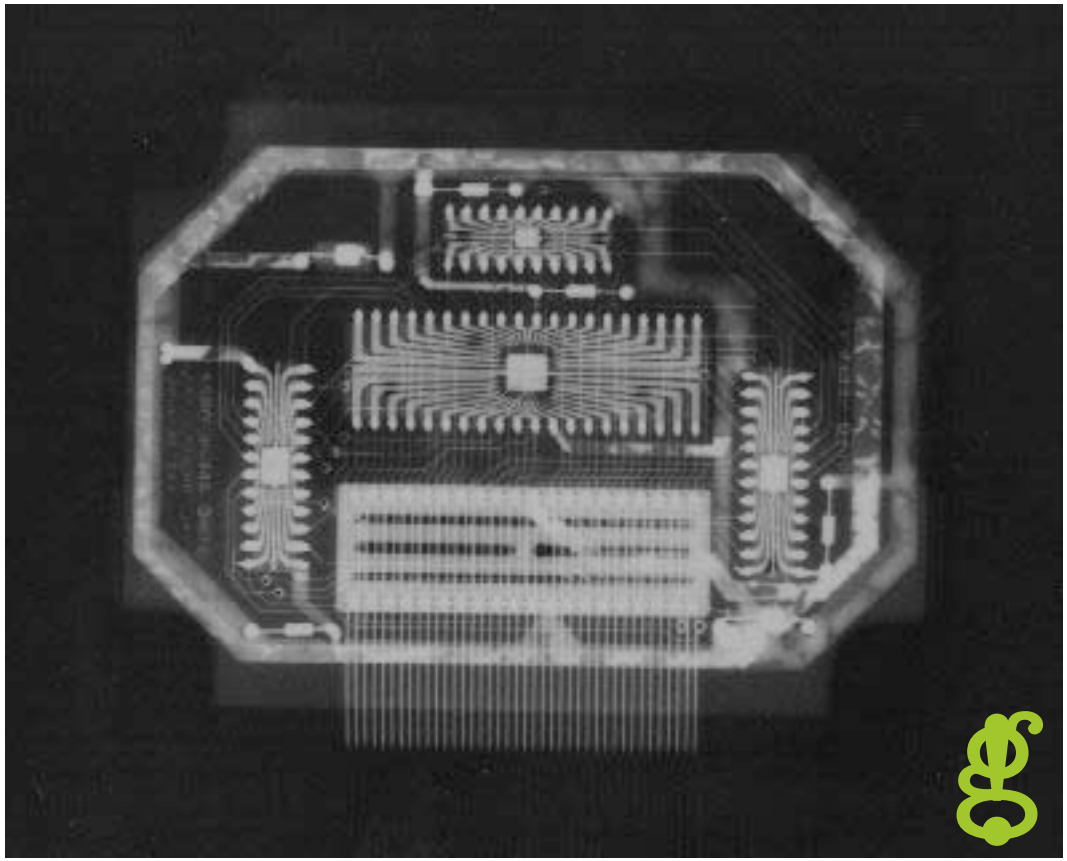


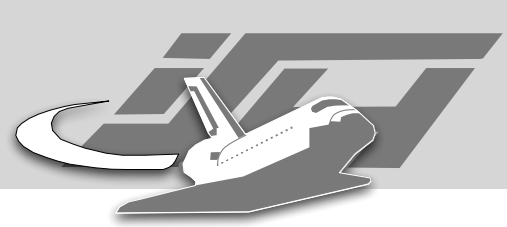
Looking inside

Super Pacman

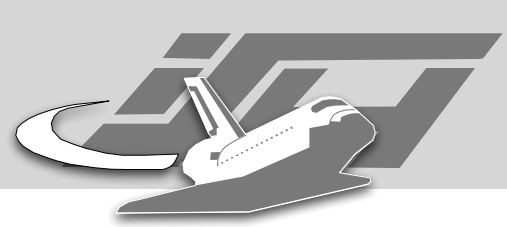


Super Pacman

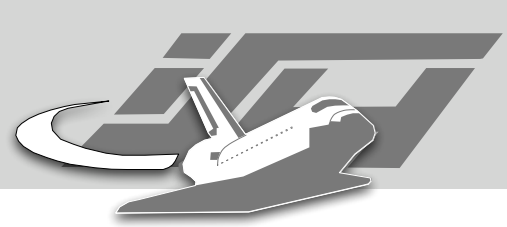




iPod

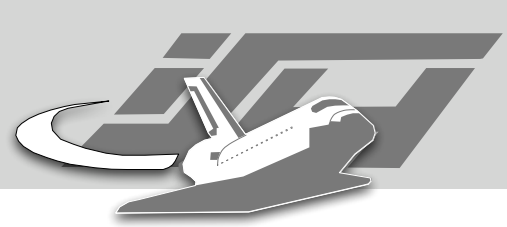


iPod

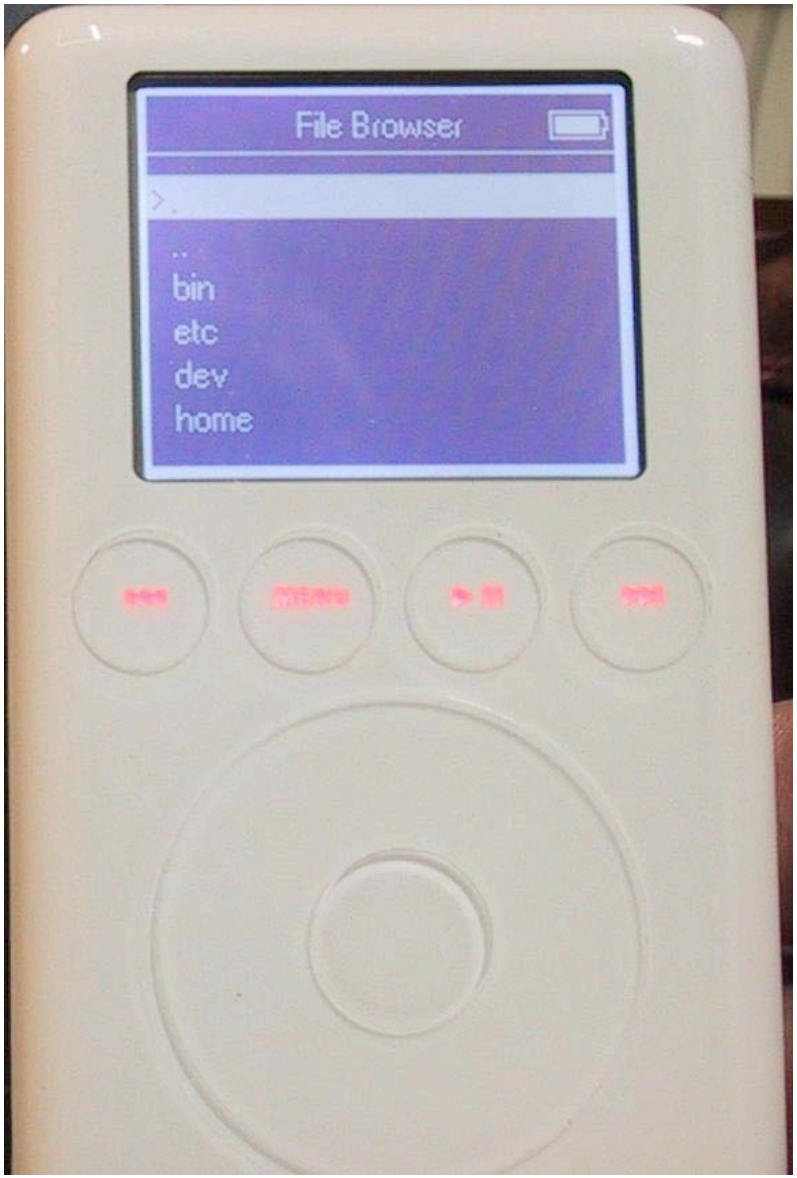


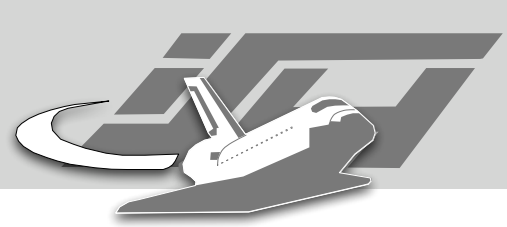
iPod


Linux version 2.4.20
-uc0 (leachbj@xenon)
(gcc version 2.95.3
20010315 (release)(
ColdFire patches - 2
0010318 from http://
fiddes.net/coldfire/
)(-msep-data patches
)) #12 Wed Jan 29 12
:47:34 CET 2003
Processor: ARM/VLSI
ARM 7 TDMI revision
0
Architecture: iPod
reserve_bootmem_core
: address 28008000 b
menu



iPod



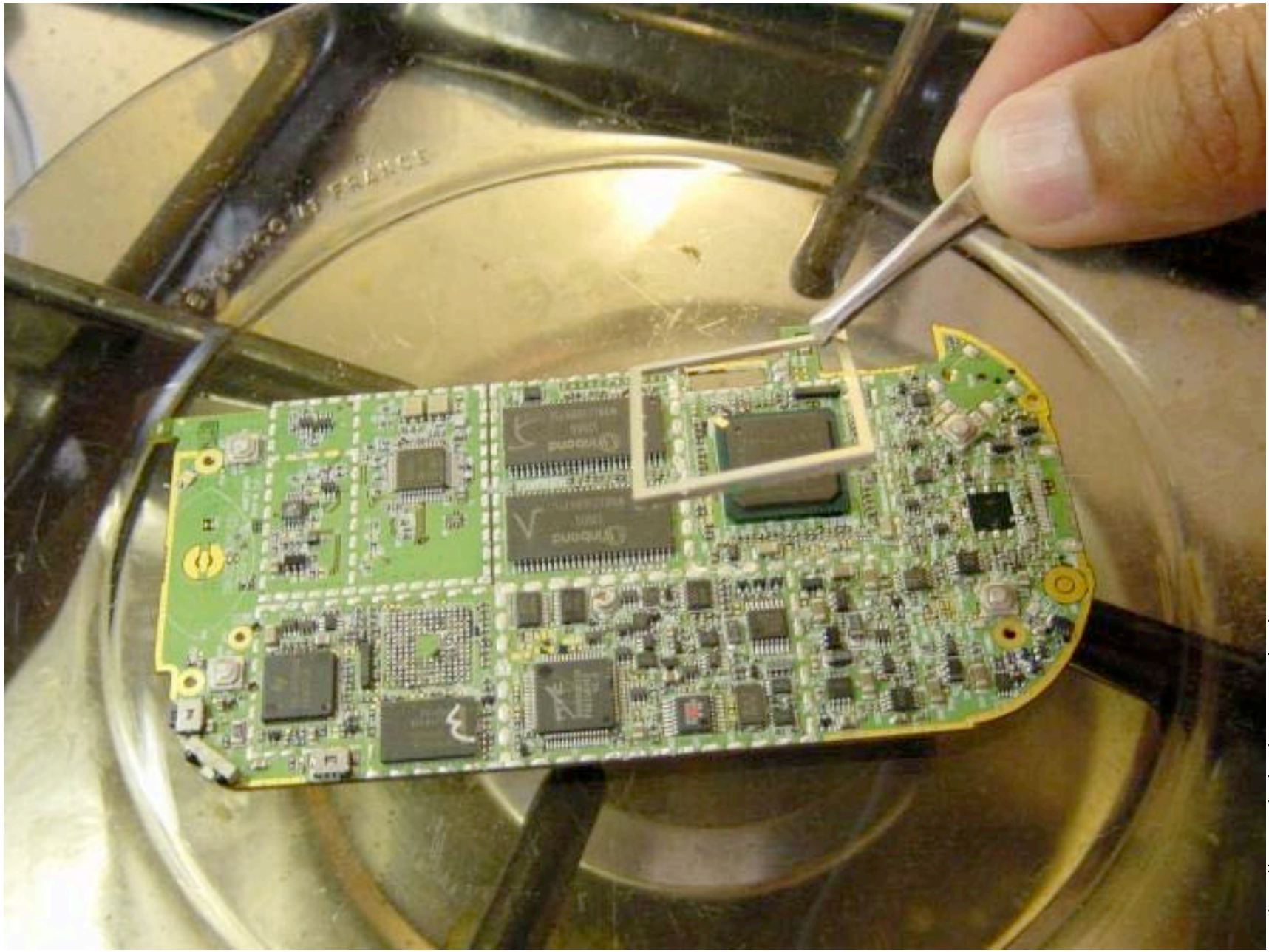


JTAG

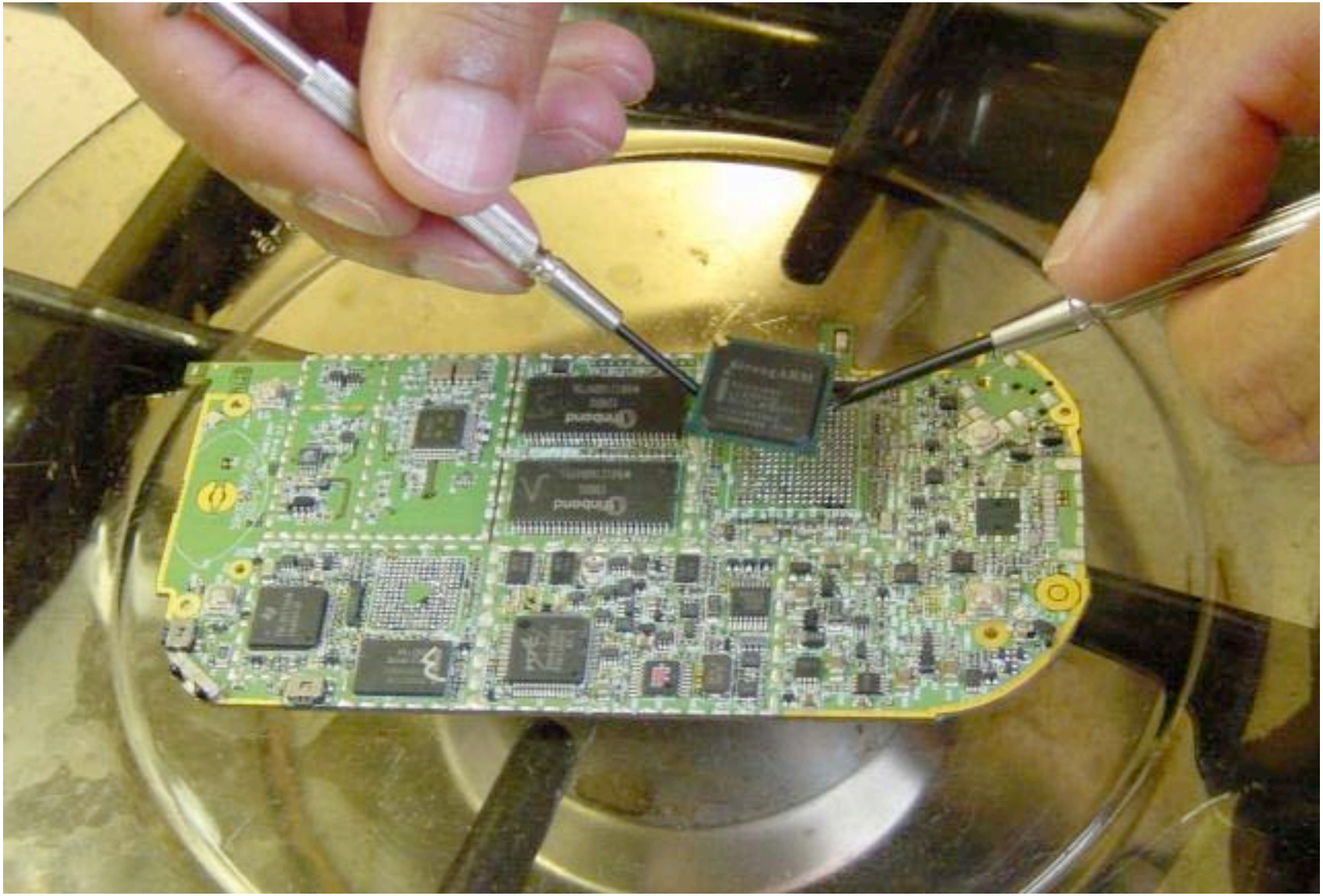

Security Dynamics
20 Crosby Dr.
Bedford, MA 01730


P/N: ASY-02657-001 REV A
LOT NO: 510PS 080
Lithium-Ion rechargeable battery. Must be disposed of properly. Do not short circuit, mutilate, crush, heat, overcharge, nail penetration, reverse polarity, or disassemble. High temperatures resulting from abuse of battery could present a burn hazard. Use approved battery chargers only.
© 2000 RIML
MADE IN CANADA
pfc 320-00

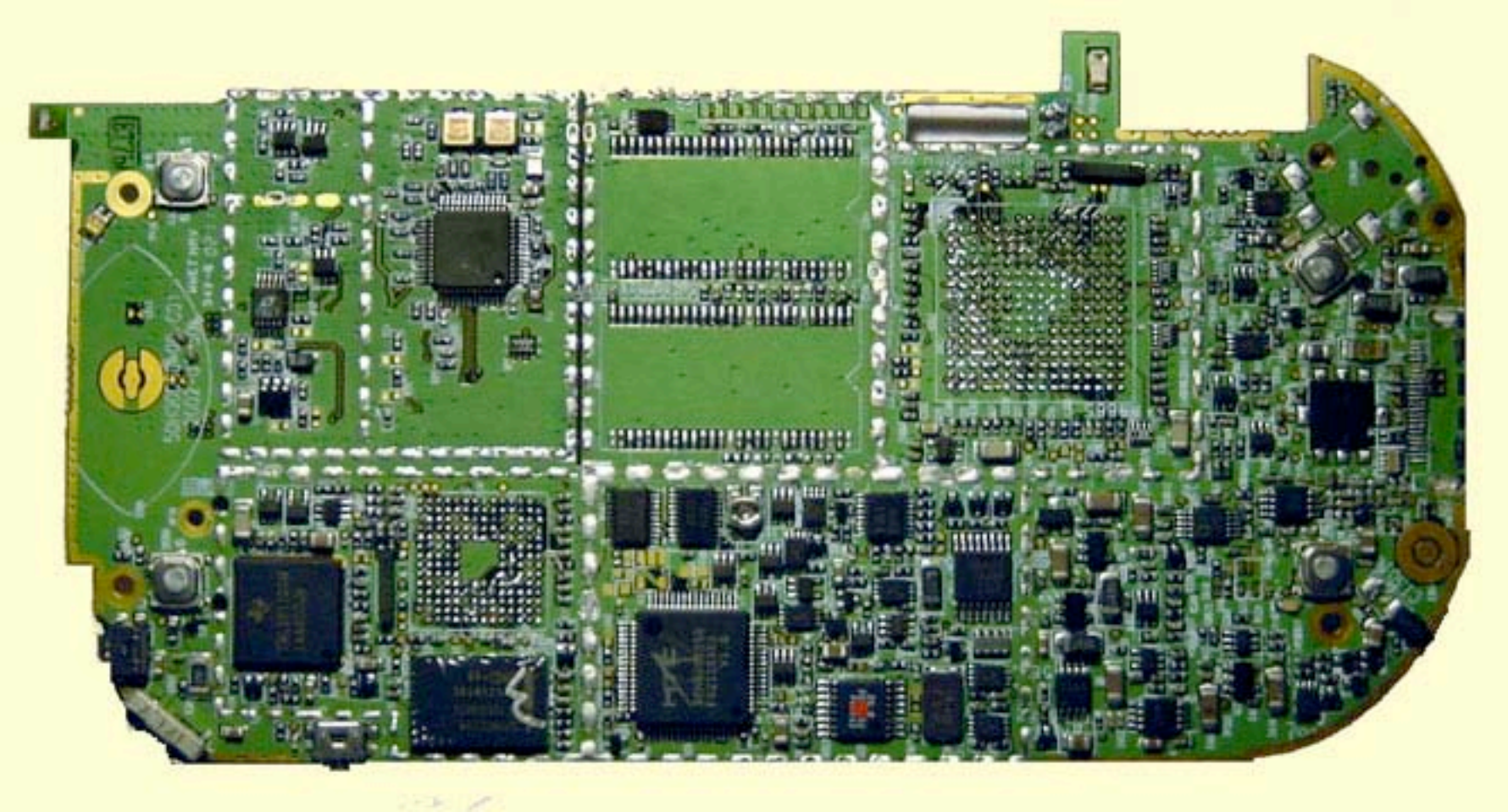
http://www.xda-developers.com/jtag/



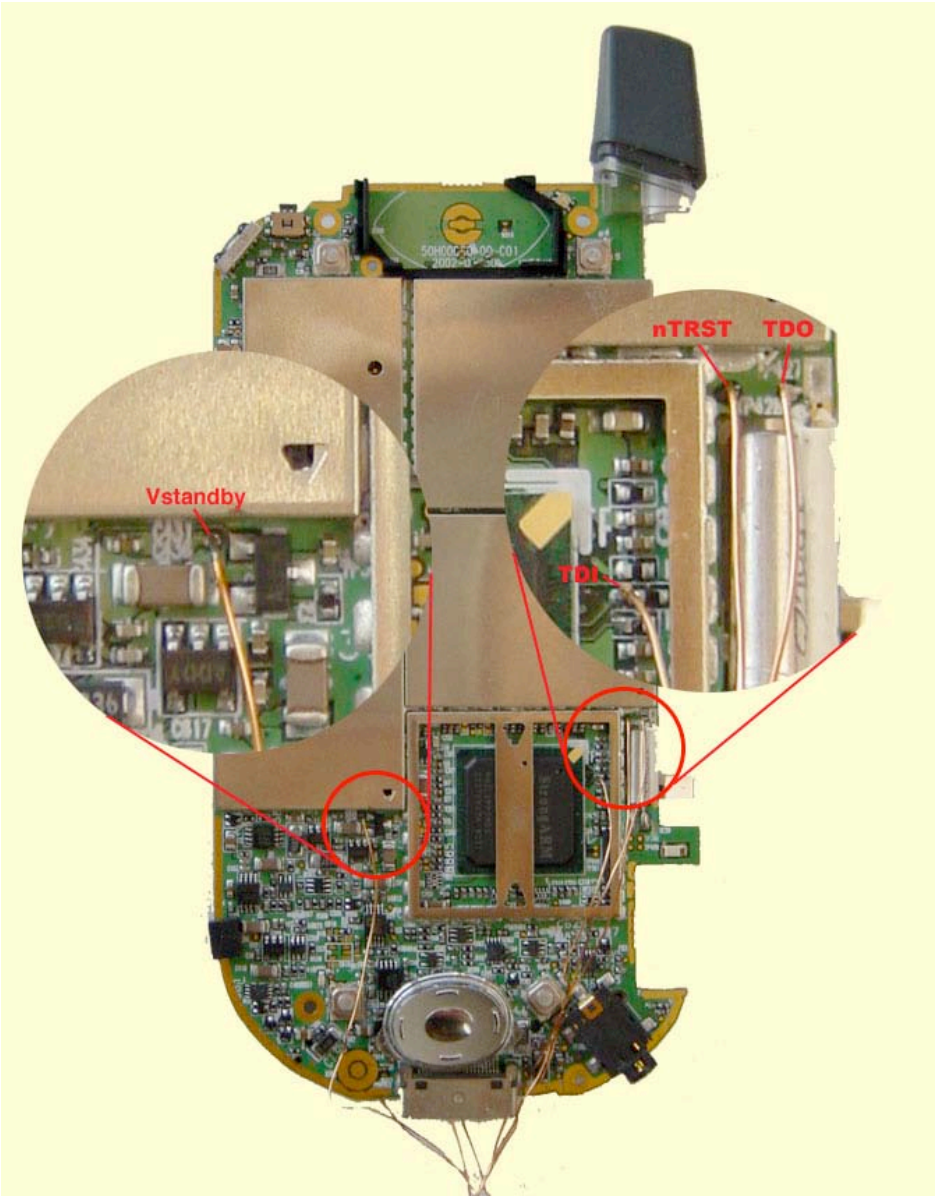
http://www.xda-developers.com/jtag/

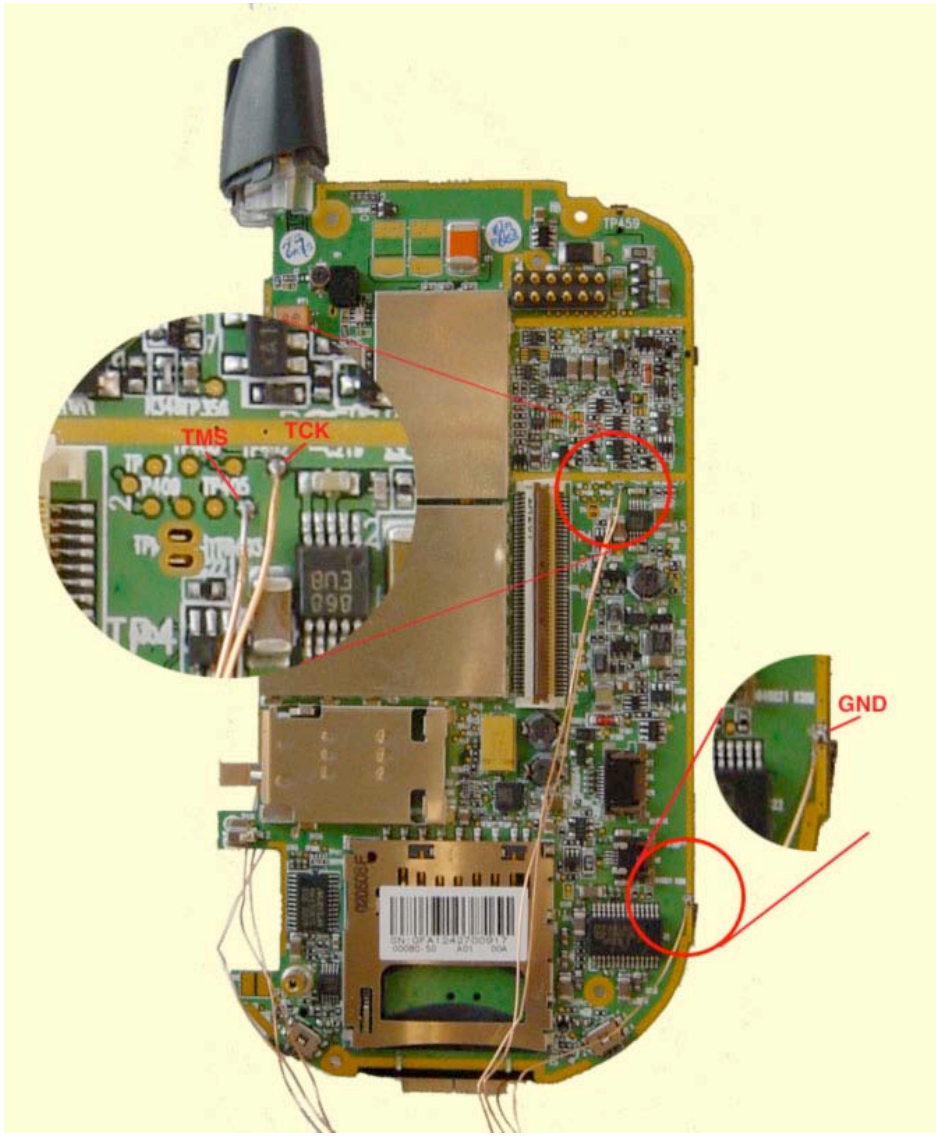


http://www.xda-developers.com/jtag/

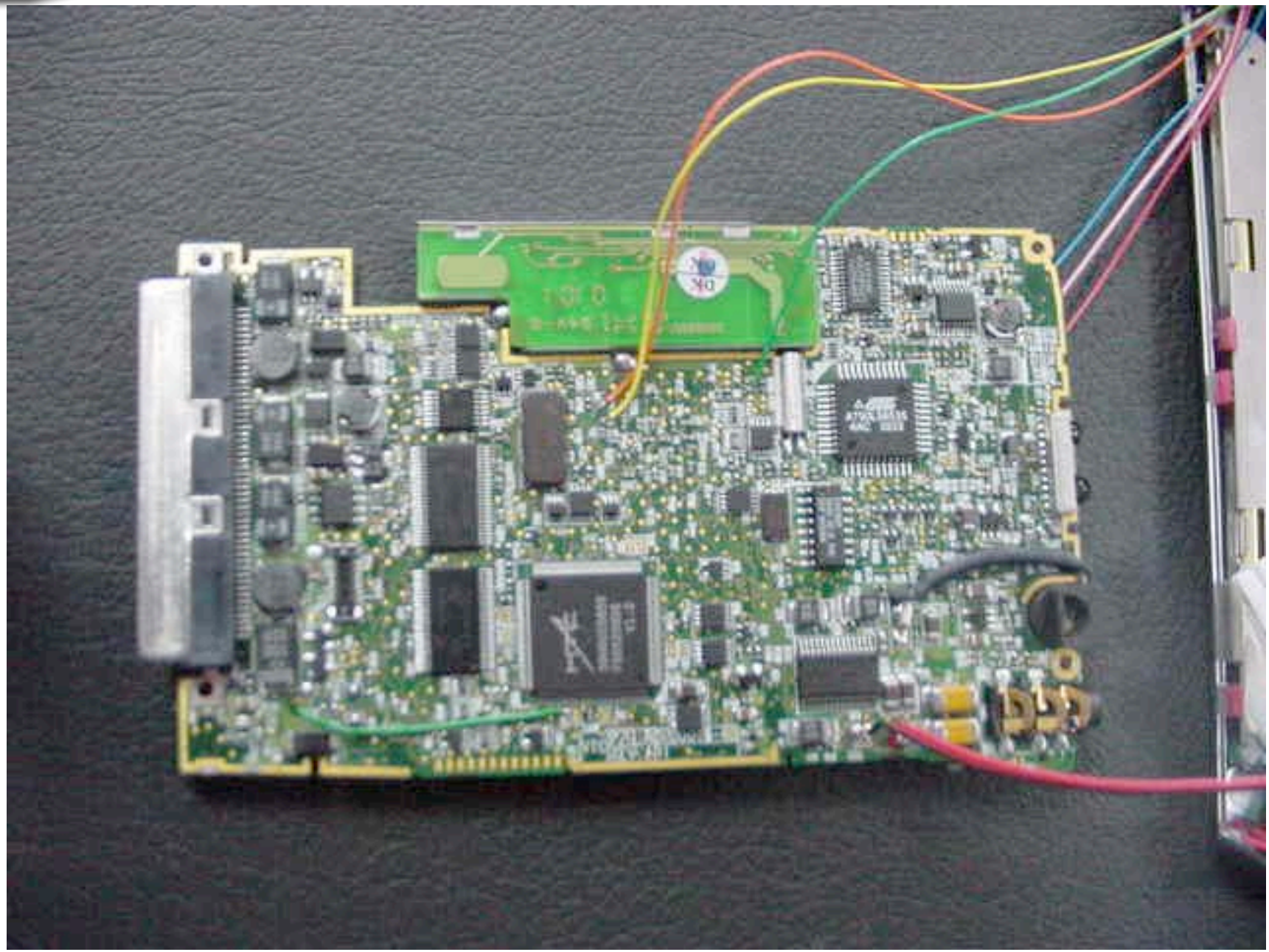


http://www.xda-developers.com/jtag/

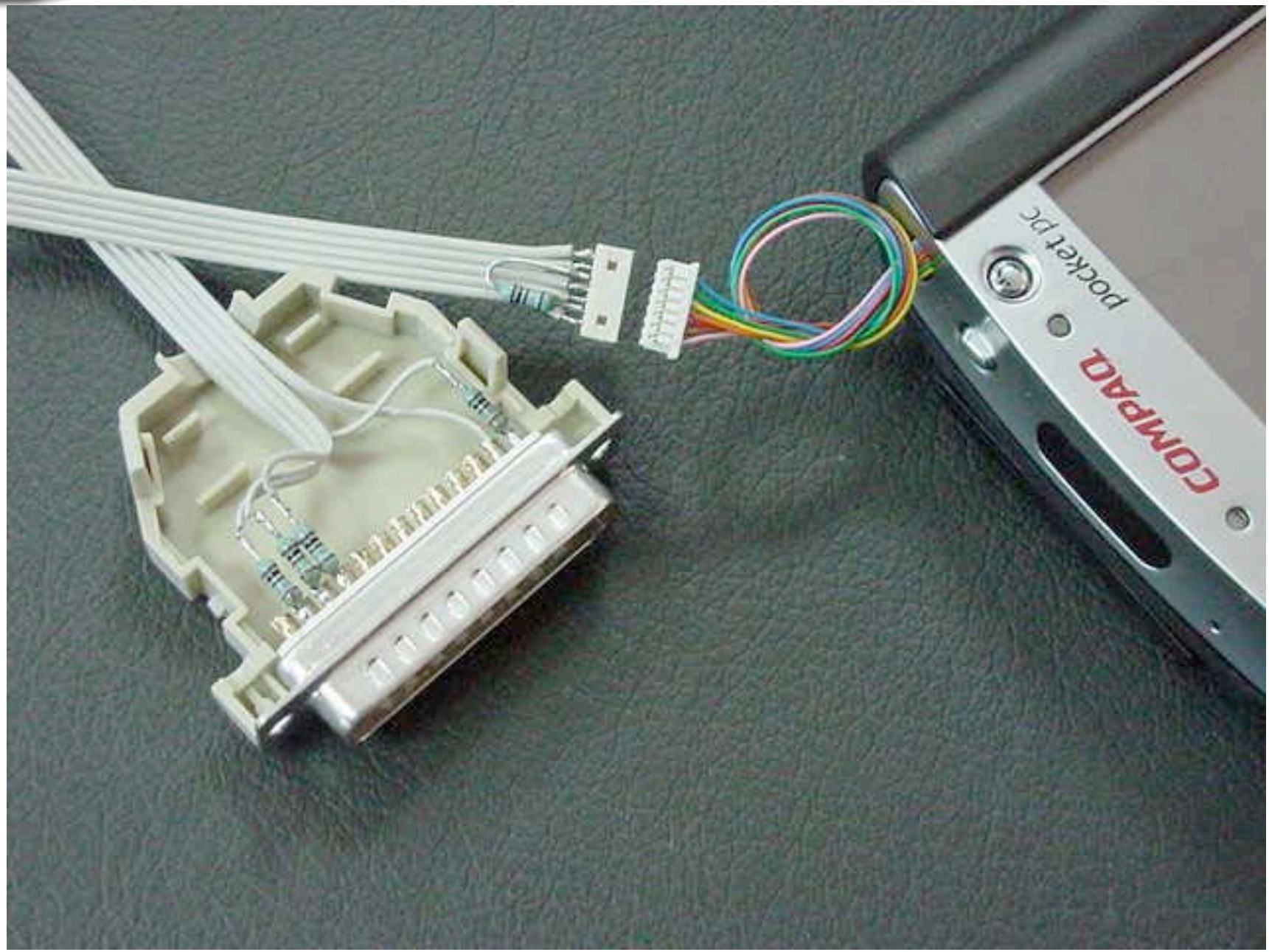




http://www.xda-developers.com/jtag/



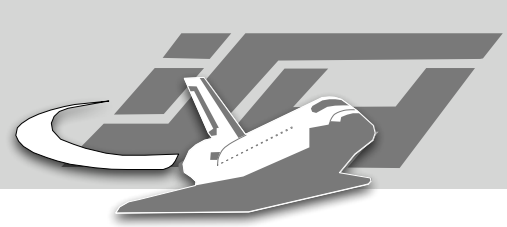
http://openwince.sourceforge.net/jtag/iPAQ-3600/



http://openwince.sourceforge.net/jtag/iPAQ-3600/

Terminal

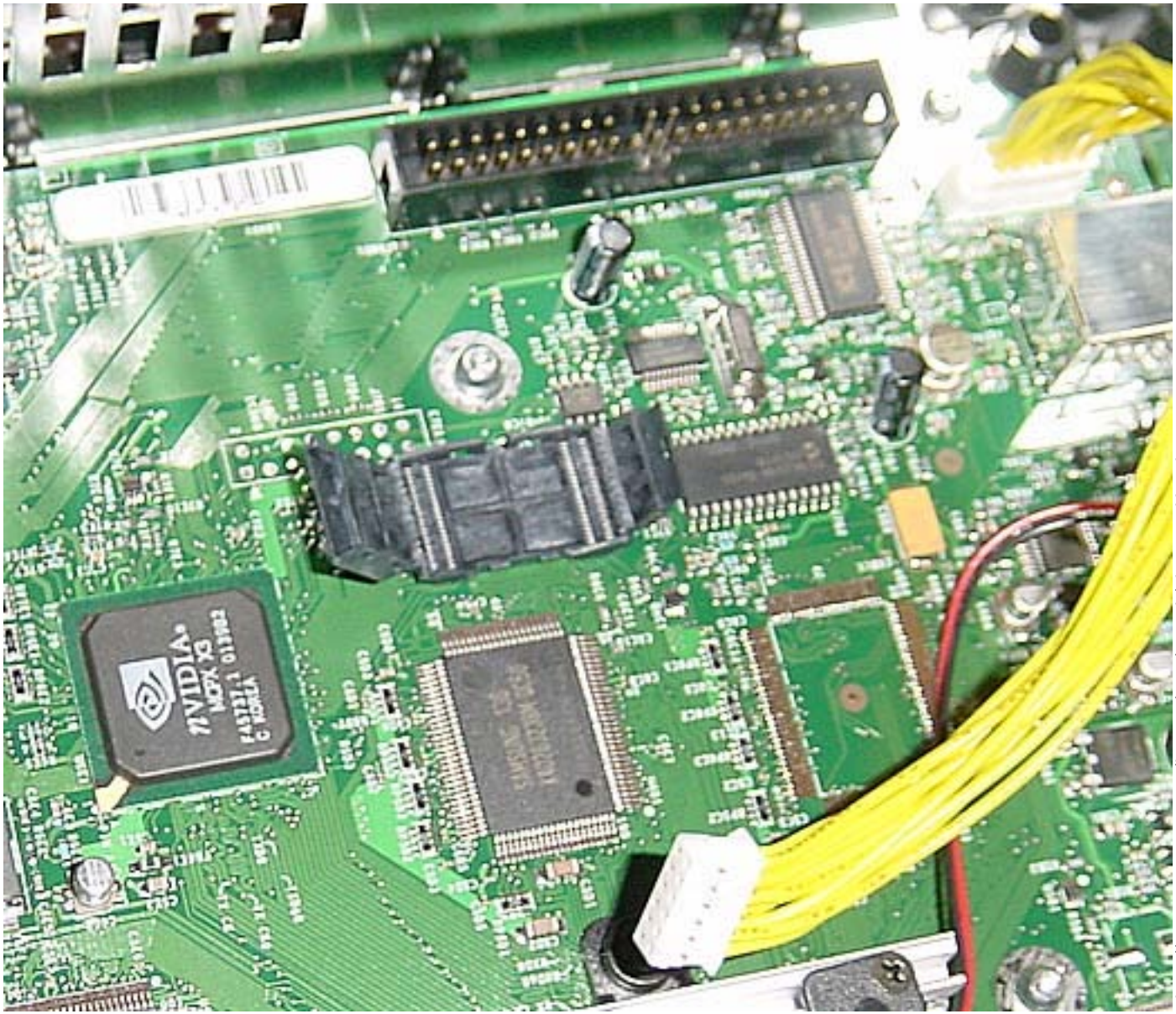
```
jtag> detectflash
Note: Supported configuration is 2 x 16 bit only
ROM_SEL: 32 bits

2 x 16 bit CFI devices detected (QRY ok)!

CFI Query Identification String:
        Primary Vendor Command Set and Control Interface ID Code: 0x0001 (Intel/Sharp Extended Command Set)
        Address of Primary Algorithm extended Query table: P = 0x????
        Alternate Vendor Command Set and Control Interface ID Code: 0x0000 (null)
        Address of Alternate Algorithm extended Query table: A = 0x????
[...]
Manufacturer: Intel
Chip: 28F640J3A
jtag> print
 No. Manufacturer         Part                 Stepping Instruction          Register
-------------------------------------------------------------------------------------
   0 Intel                SA1110               B4       EXTEST               BSR
jtag> flashmem 0 /home/bootldr-2.18.54.bin
0x00000000
Note: Supported configuration is 2 x 16 bit only
ROM_SEL: 32 bits

2 x 16 bit CFI devices detected (QRY ok)!

program:
block 0 unlocked
erasing block 0: 0
addr: 0x00033500
verify:
addr: 0x00033500
Done.
```



XBox

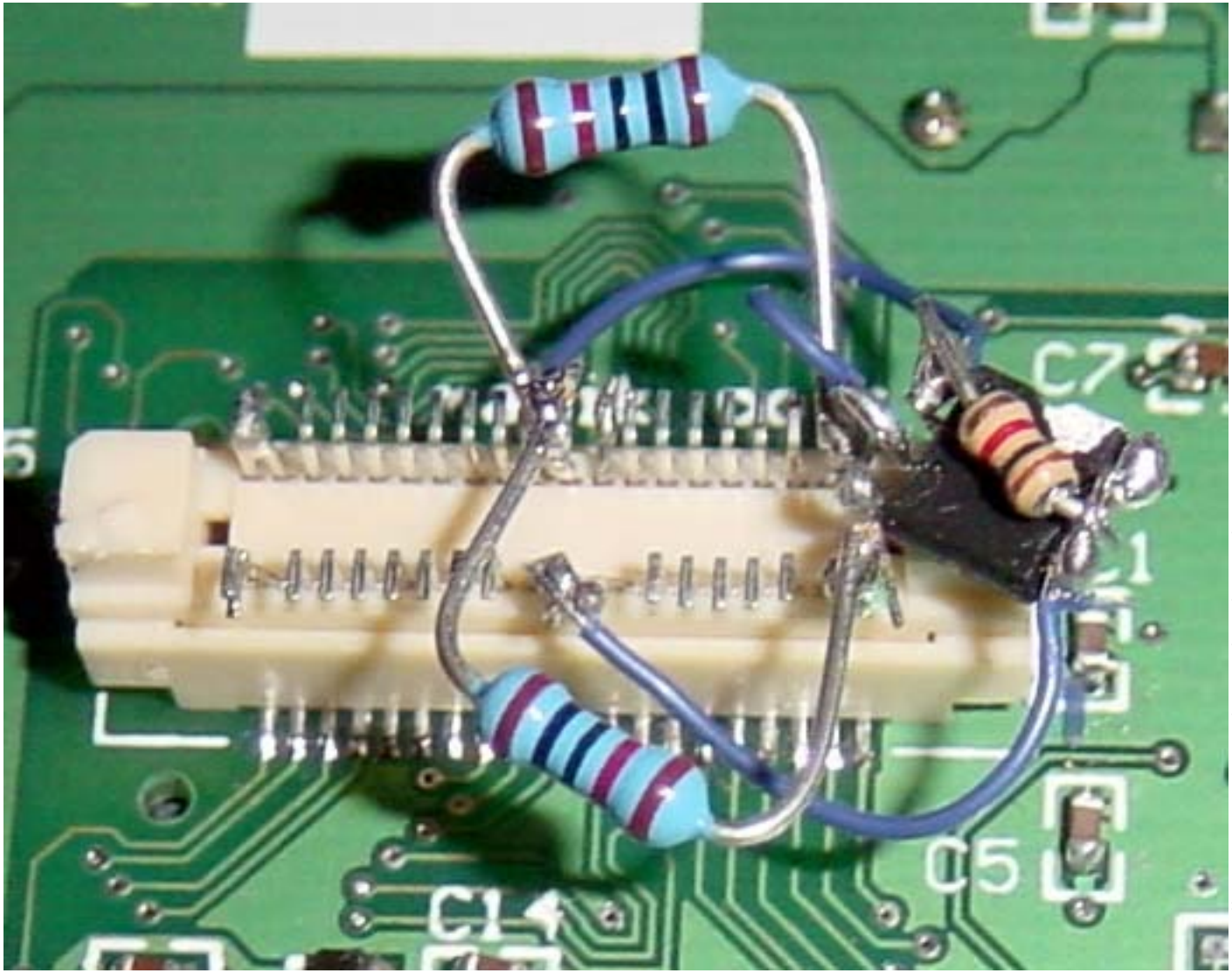
- Andrew “bunnie” Huang: Keeping Secrets in Hardware: the Microsoft XBox Case Study (2002)

http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html

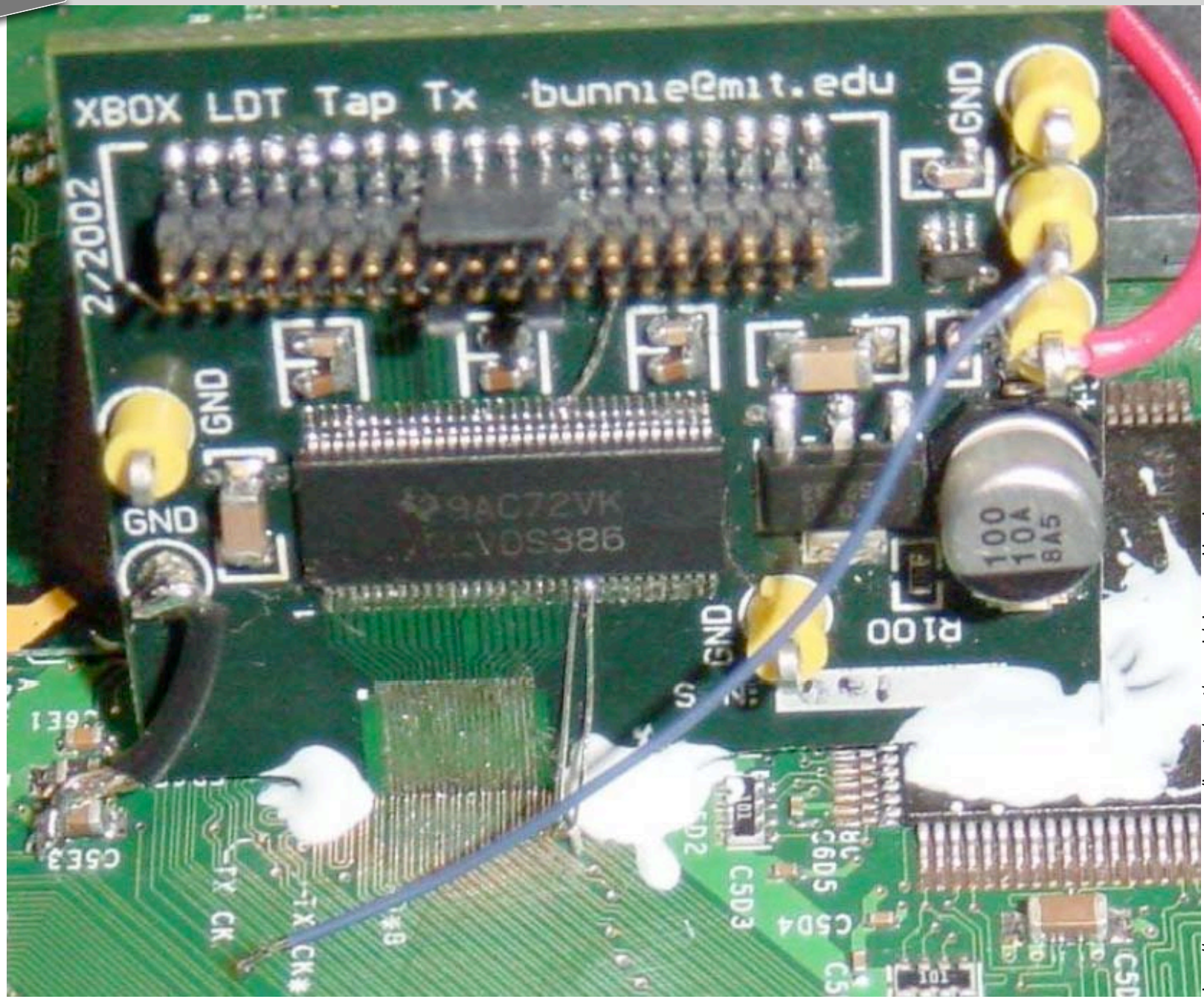


http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html

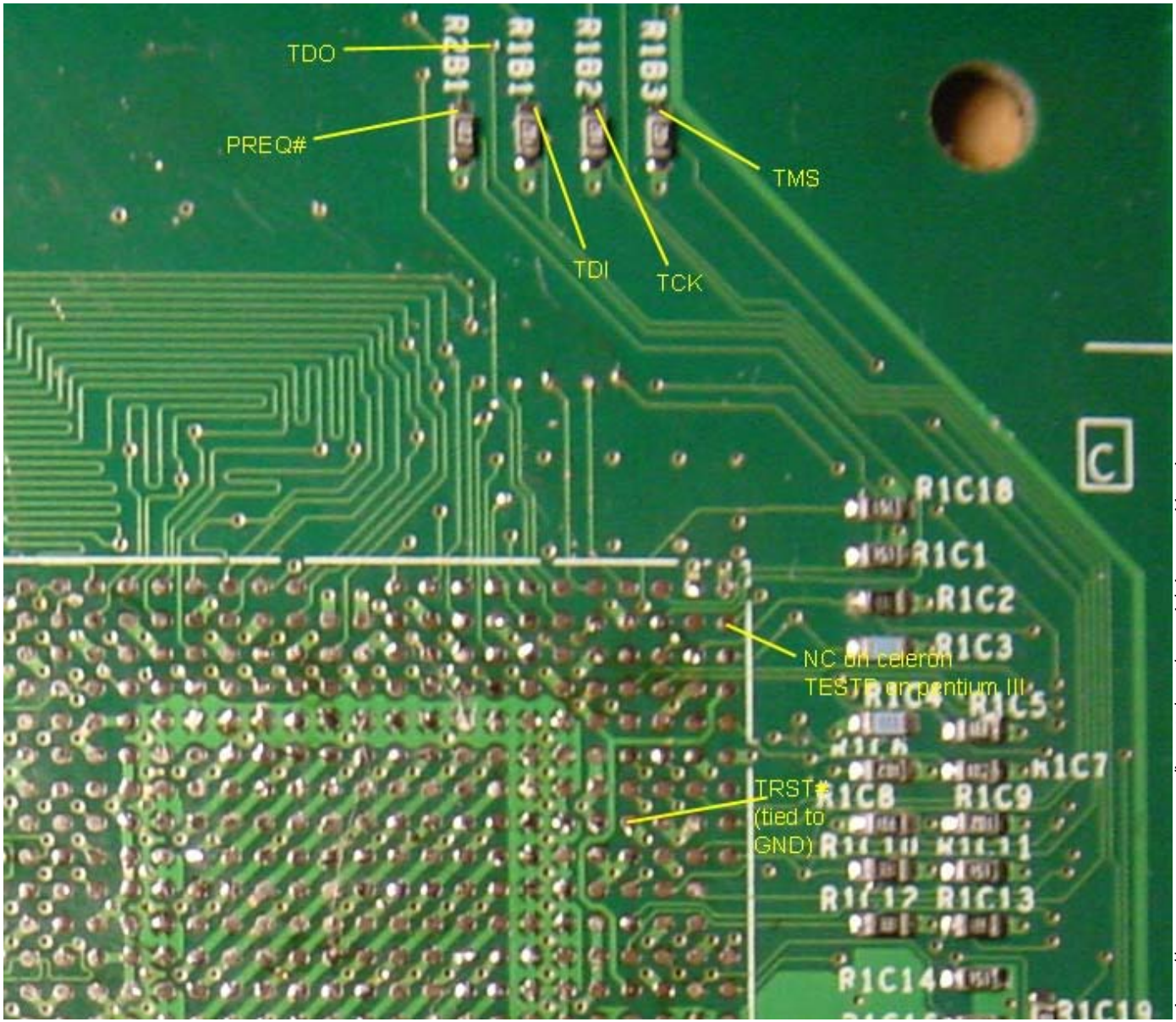
http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html



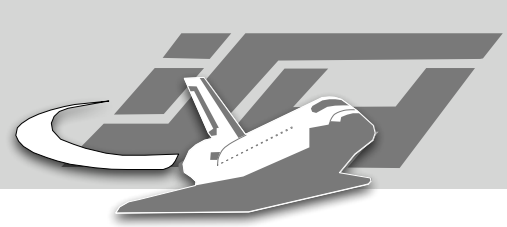
http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html



http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html

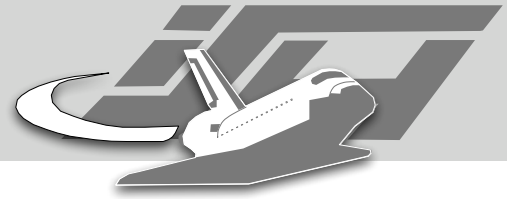


http://www.xenatera.com/bunnie/proj/anatak/xboxmod.html



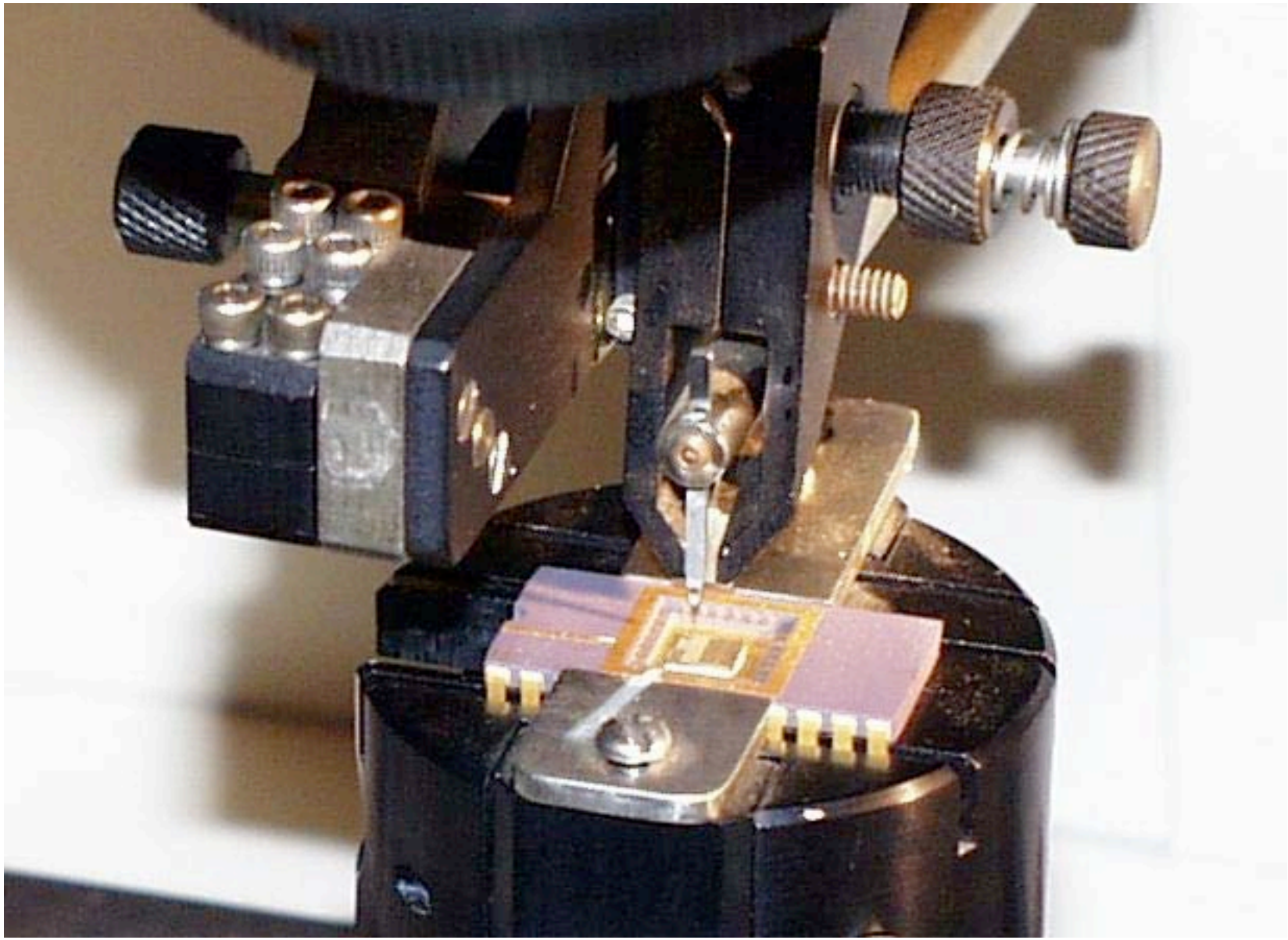
Tampering with Chips

- Ross Anderson, Markus Kuhn: Low Cost Attacks on Tamper Resistant Devices (Security Protocols, 1997)
- Oliver Kömmerling, Markus G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors (Smartcard '99)

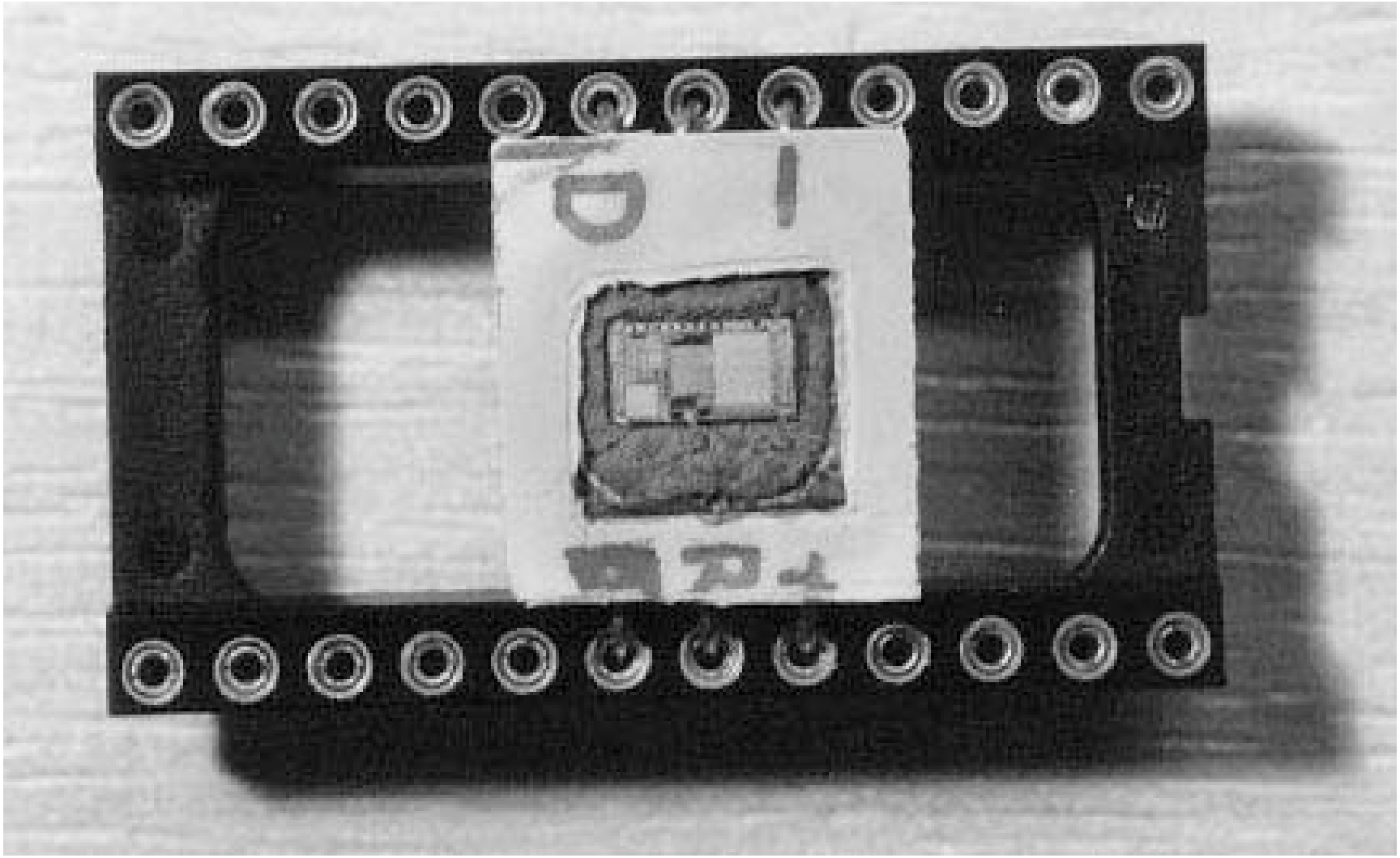


Tampering

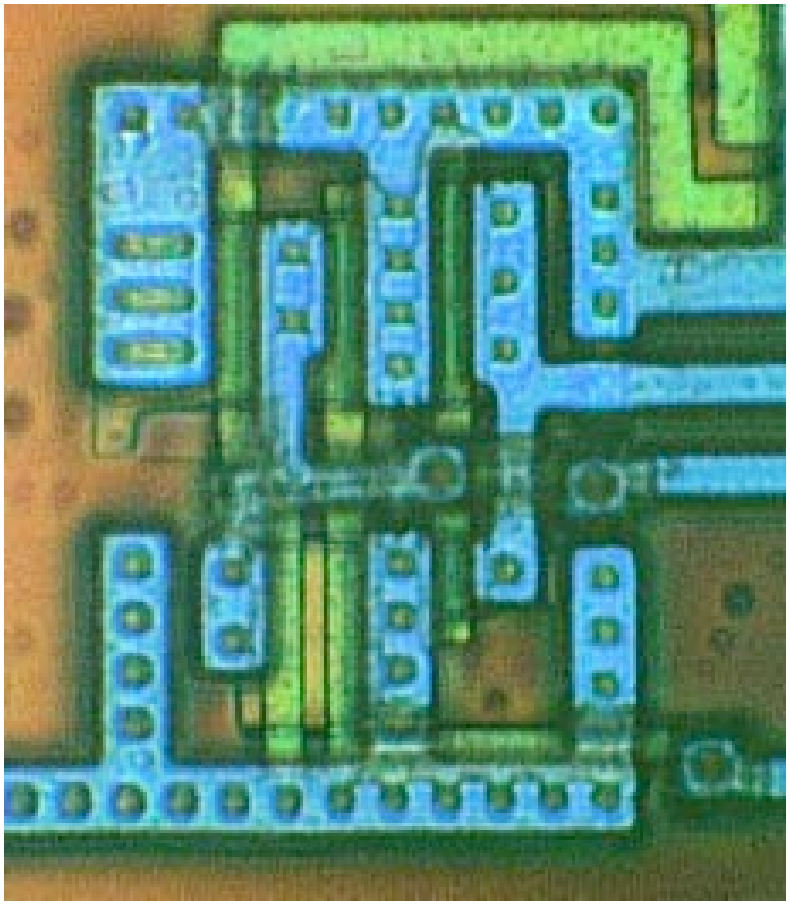
Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors

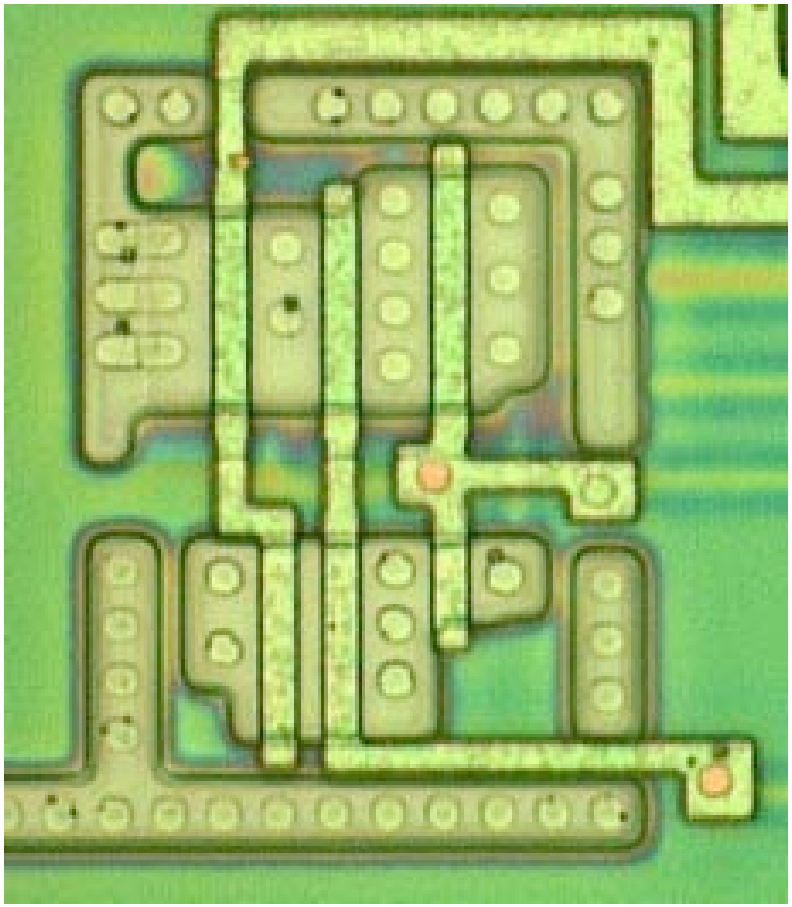


Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors

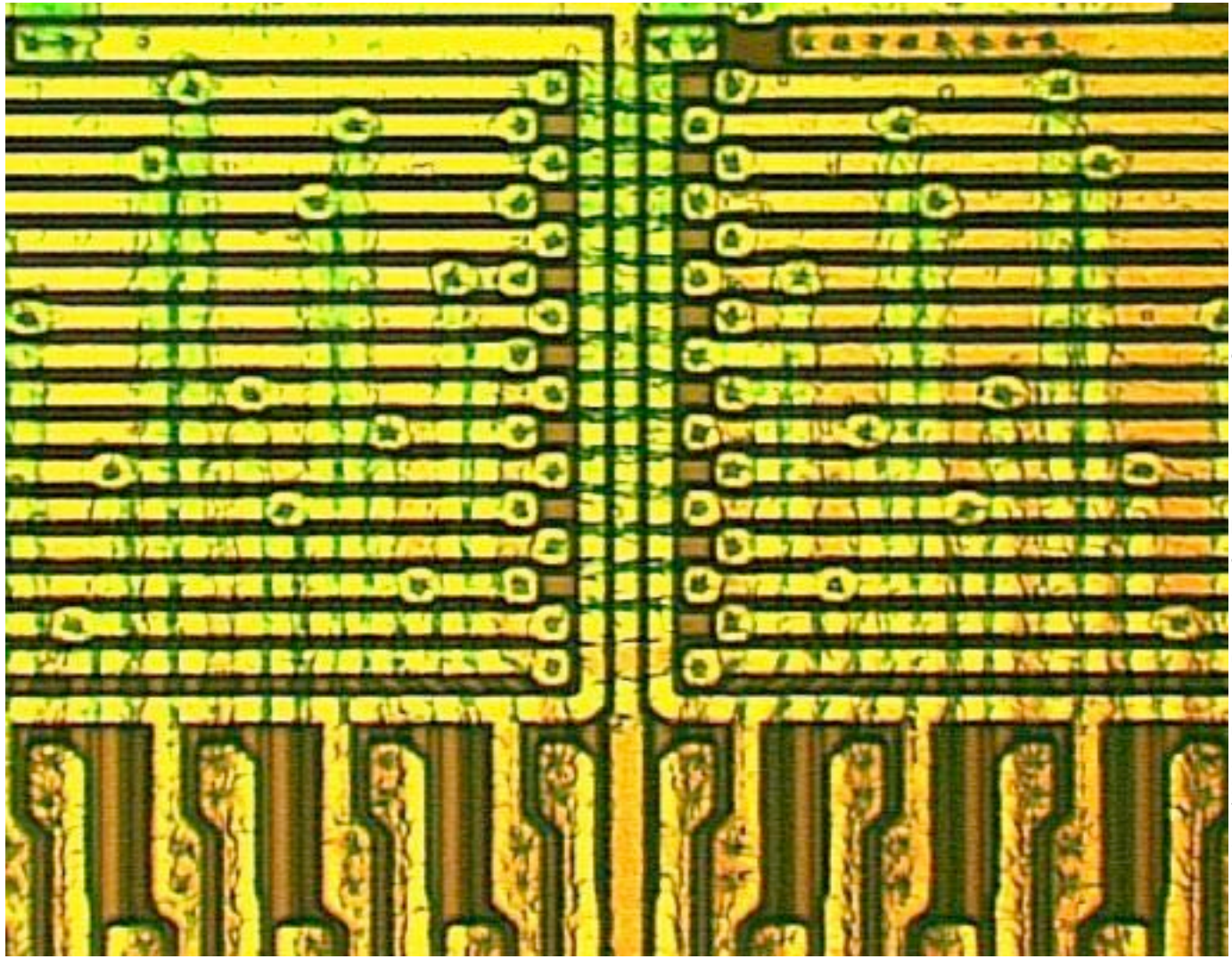


Anderson: On the Security of Digital Tachographs

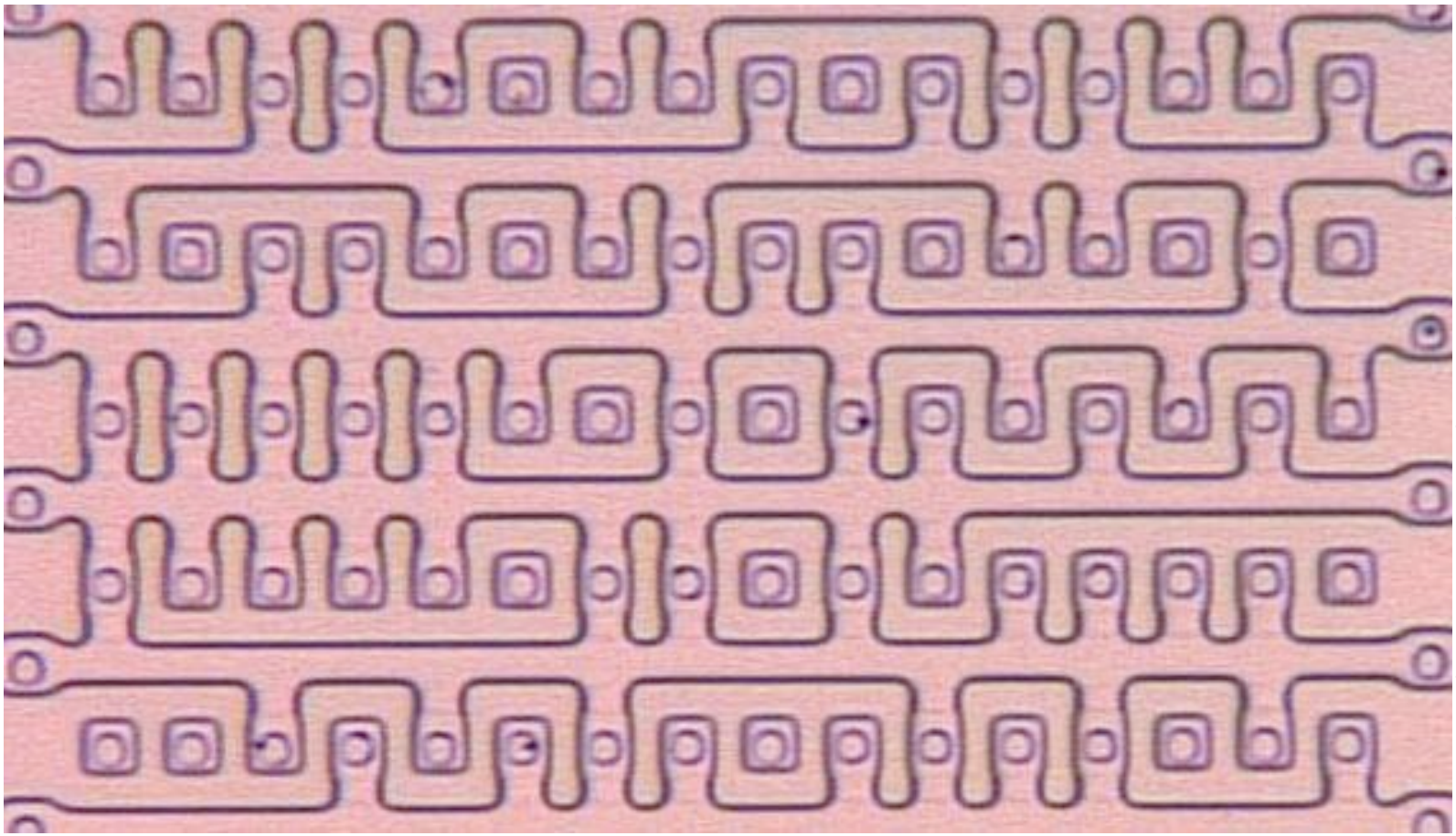




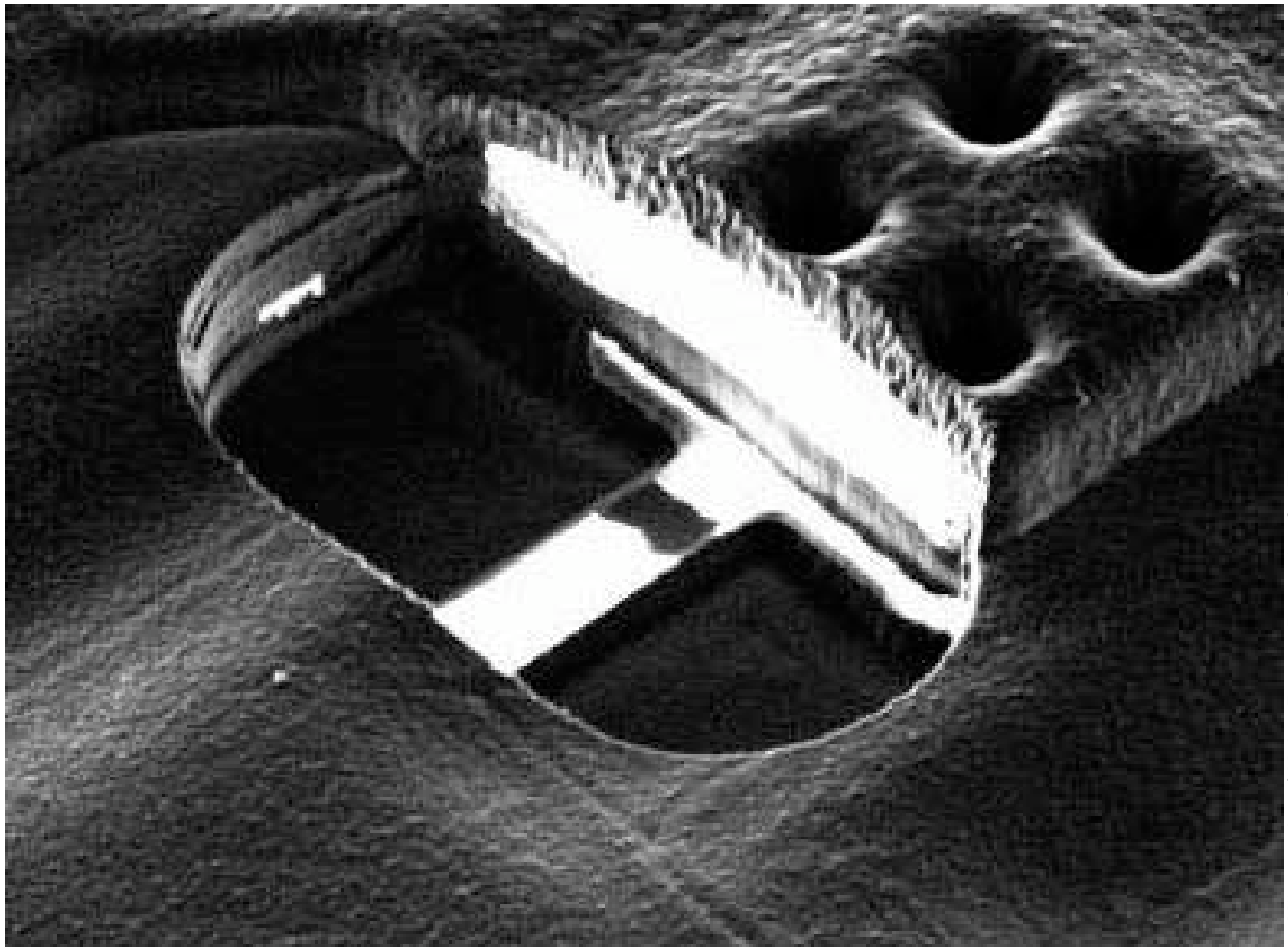
Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors



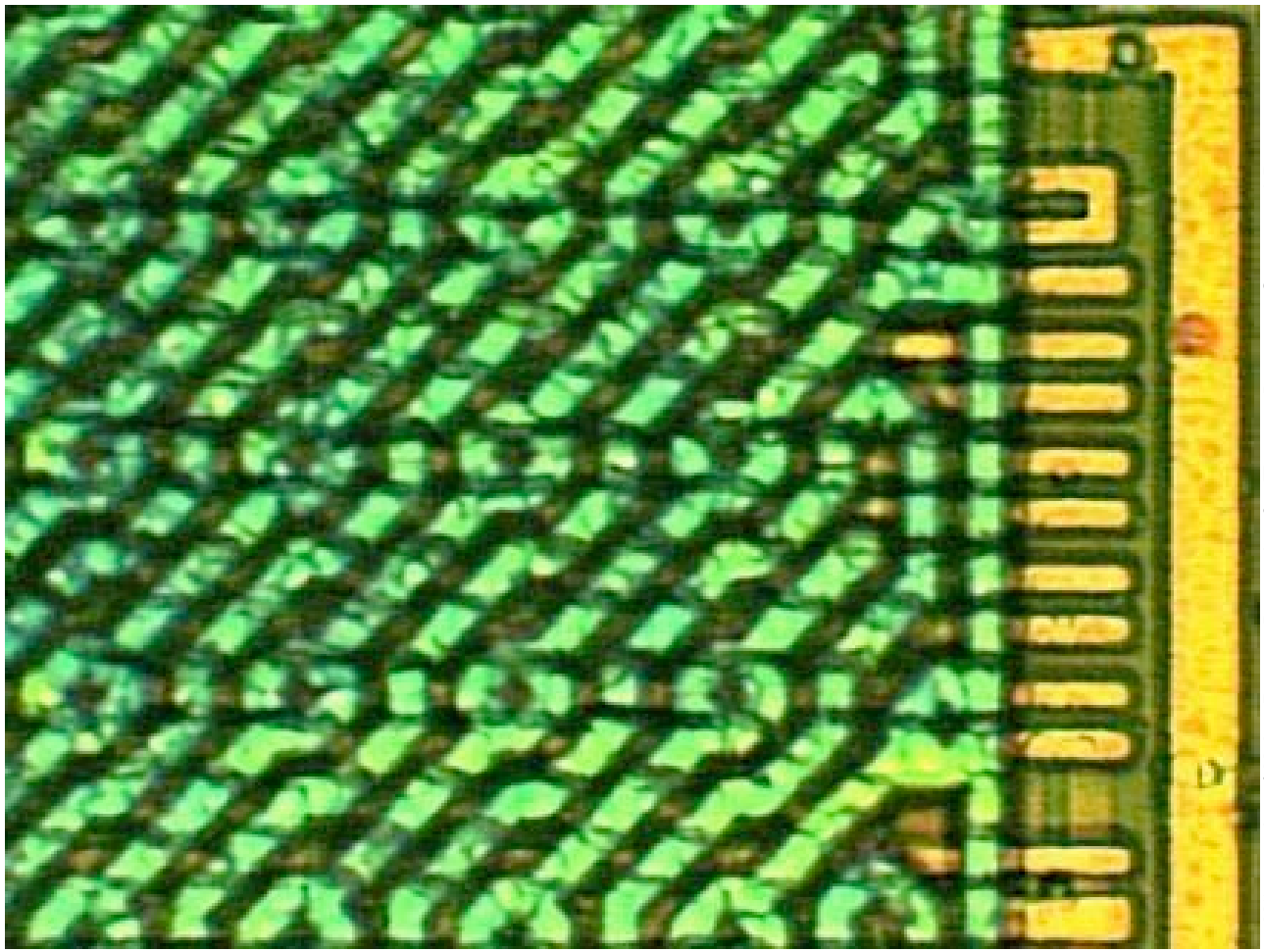
Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors



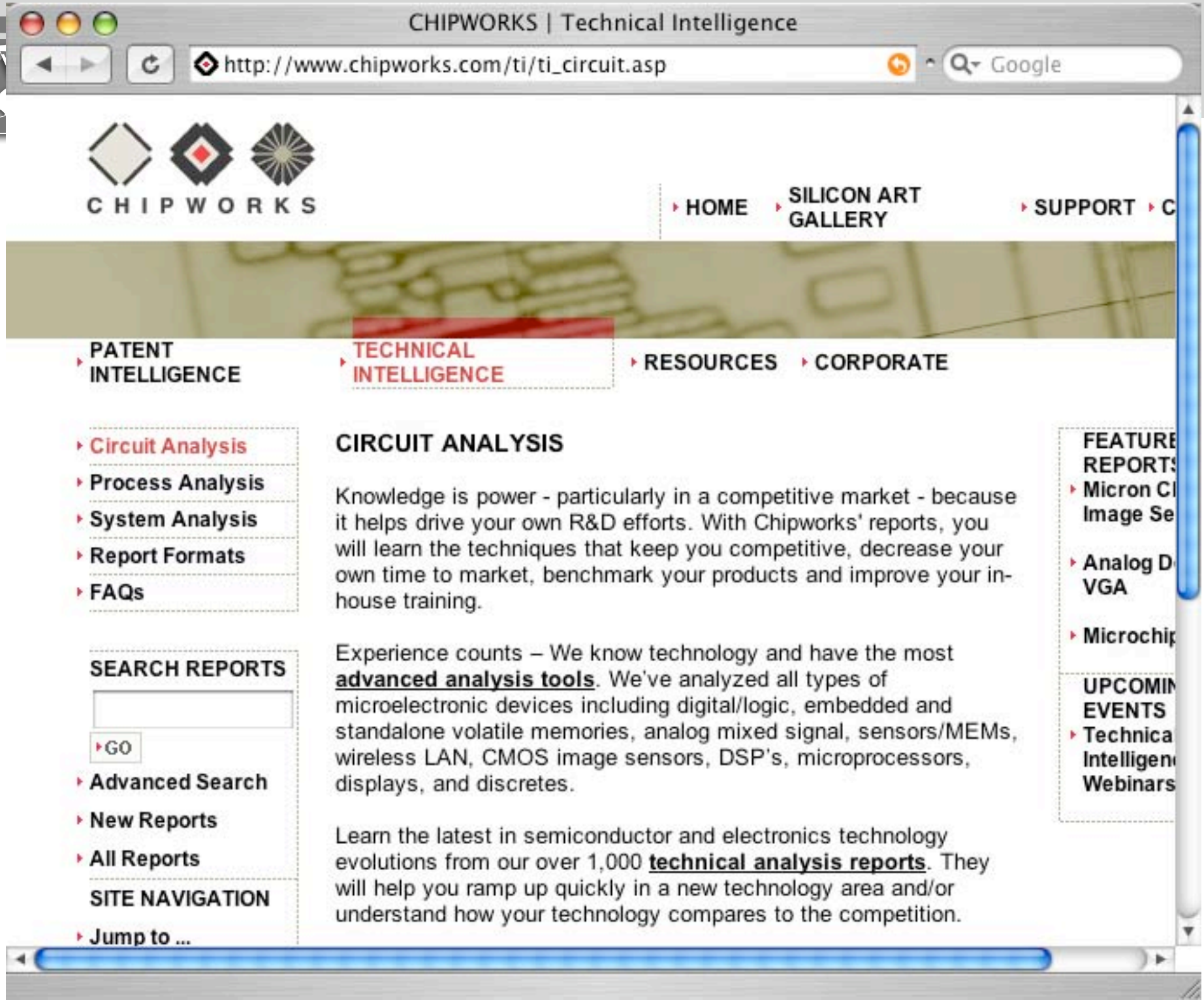
Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors



Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors



Kömmerling / Kuhn: Design Principles for Tamper-Resistant Smartcard Processors

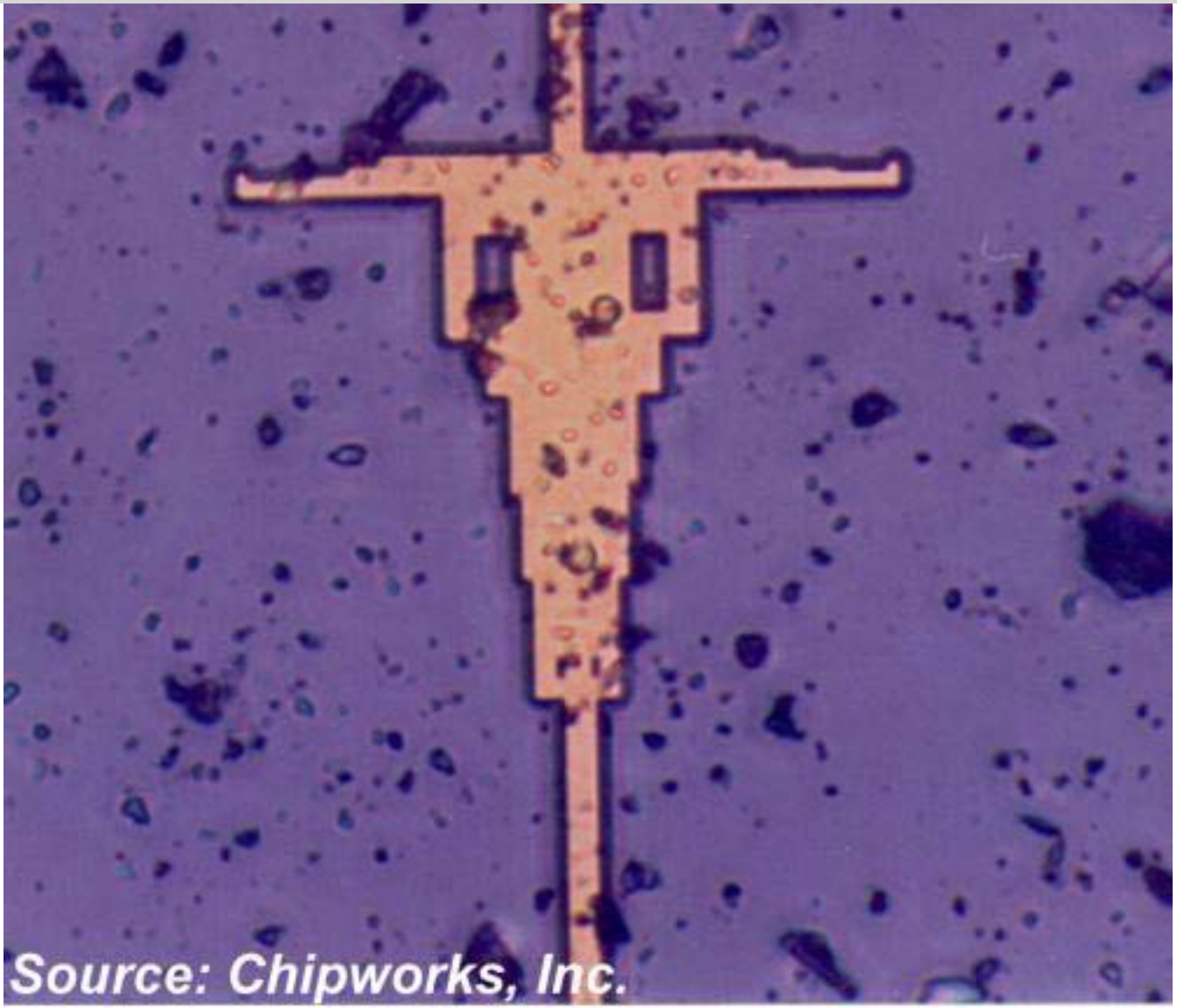

CHIPWORKS | Technical Intelligence
http://www.chipworks.com/ti/ti_circuit.asp
Google
CHIPWORKS
HOME
SILICON ART GALLERY
SUPPORT
PATENT INTELLIGENCE
TECHNICAL INTELLIGENCE
RESOURCES
CORPORATE
Circuit Analysis
Process Analysis
System Analysis
Report Formats
FAQs
SEARCH REPORTS
GO
Advanced Search
New Reports
All Reports
SITE NAVIGATION
Jump to ...
CIRCUIT ANALYSIS
Knowledge is power - particularly in a competitive market - because it helps drive your own R&D efforts. With Chipworks' reports, you will learn the techniques that keep you competitive, decrease your own time to market, benchmark your products and improve your in-house training.
Experience counts – We know technology and have the most advanced analysis tools. We've analyzed all types of microelectronic devices including digital/logic, embedded and standalone volatile memories, analog mixed signal, sensors/MEMs, wireless LAN, CMOS image sensors, DSP's, microprocessors, displays, and discretes.
Learn the latest in semiconductor and electronics technology evolutions from our over 1,000 technical analysis reports. They will help you ramp up quickly in a new technology area and/or understand how your technology compares to the competition.
FEATURE REPORTS
Micron C
Image Se
Analog D
VGA
Microchip
UPCOMIN EVENTS
Technica
Intelligen
Webinars

From: Silicon Image
Sil154CT64
Digital Transmitter

CHIPWORKS

From: Qualcomm
Q5312I-3S2
ASIC

CHIPWORKS

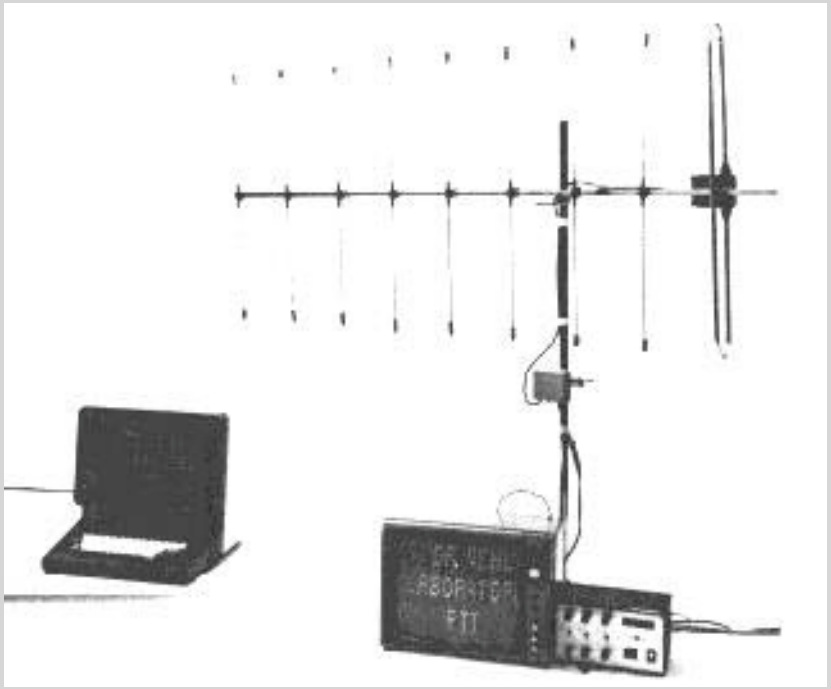


From: AMD A80486DX4-120SV8B
32-bit Microprocessor

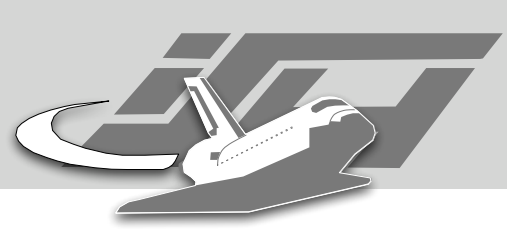
CHIPWORKS

From: Siemens SAB80C535-N
8-bit Microcontroller

CHIPWORKS

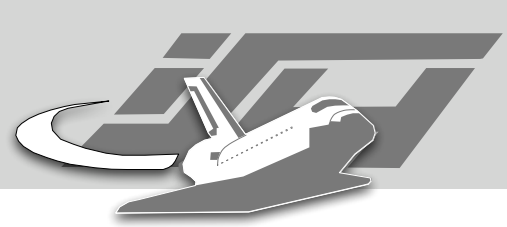


Tempest



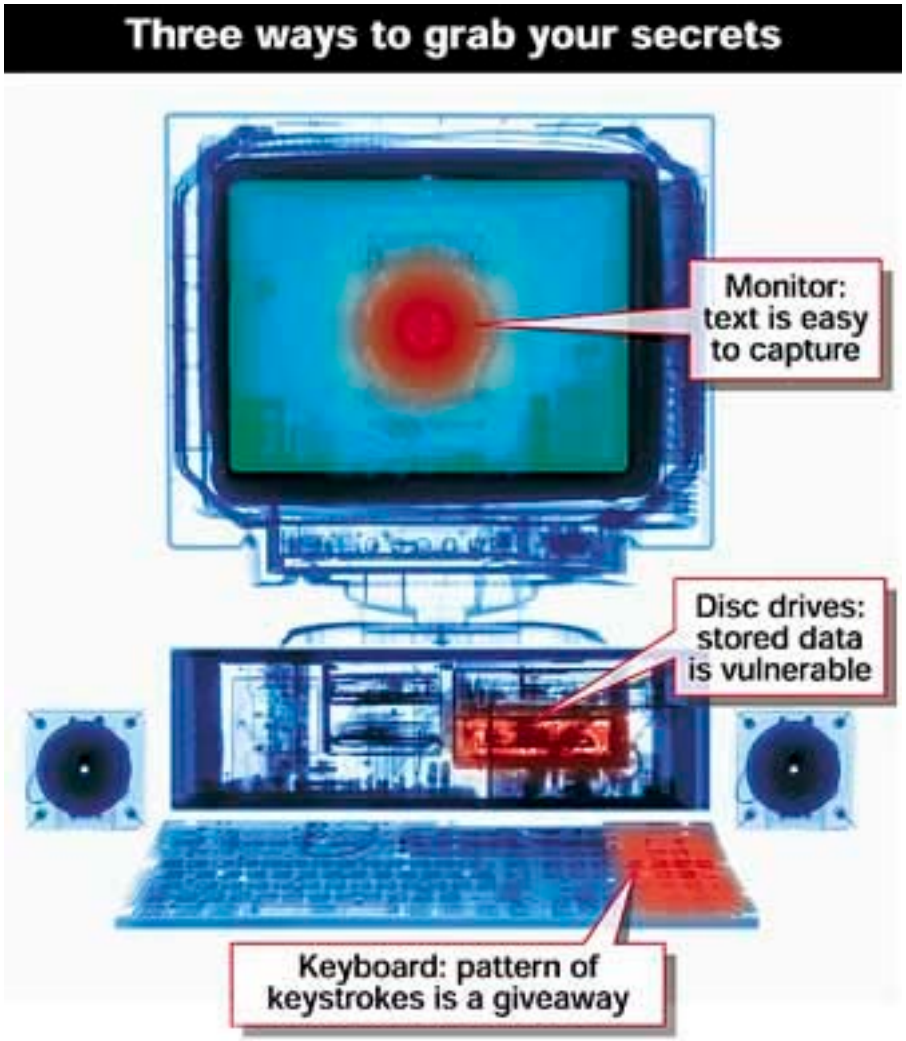
Tempest

- "TEMPEST is a code word that relates to specific standards used to reduce electromagnetic emanations. In the civilian world, you'll often hear about TEMPEST devices (a receiver and antenna[...]) or TEMPEST attacks" (Joel McNamara)
- "Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?" Wim van Eck, PTT Dr. Neher Laboratories (1985 - http://www.shmoo.com/tempest/emr.pdf): "All it takes to do so is a little knowledge of the principles of TV reception and an investment of about $5."
- You can put together a emanation monitoring device for under $100 worth of Radio Shack and surplus parts. Perhaps for a dumb video display terminal (VDT), but certainly not for a VGA or SVGA monitor. (TEMPEST Urban Folklore - Joel McNamara)



Old sch00l

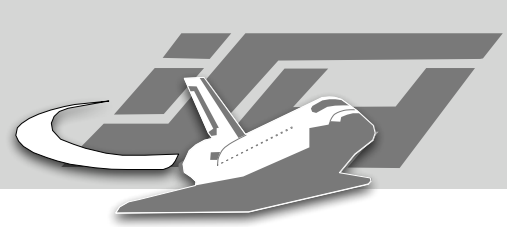
- "The Threat of Information Theft by Reception of Electromagnetic Radiation from RS-232 Cables." Peter Smulders - Computers & Security vol 9, pp 53-58, 1990
- "Protective Measures Against Compromising Electro Magnetic Radiation Emitted by Video Display Terminals", Professor Erhart Möller University of Aachen, Aachen, Germany - Phrack (!) Vol 4, Issue # 44, File 10 of 27



http://web.archive.org/web/20010606194803/
http://www.newscientist.com/ns/19991106/newsstory6.html

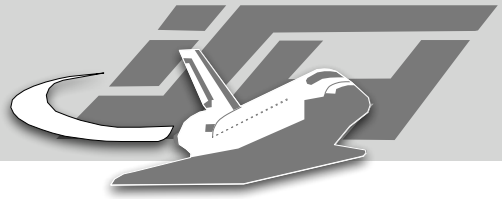
http://www.bemashield.com/

http://www.hollandshielding.be/tempest_equipment.htm

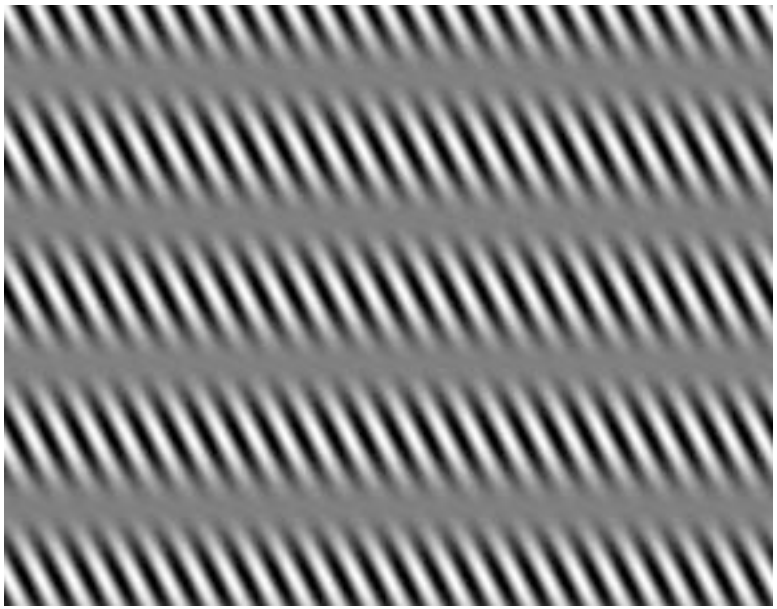


Soft Tempest

- Soft Tempest: Hidden Data Transmission Using Electromagnetic Emanations Markus G. Kuhn and Ross J. Anderson (Information Hiding Workshop, 1998)
- Soft Tempest - An Opportunity for NATO Ross J. Anderson and Markus G. Kuhn (1999)
- Patents
  - Markus Günther Kuhn, Ross John Anderson: Low cost countermeasure against compromising electromagnetic computer emanations. UK Patent GB2333883, granted 2002-09-17, filed 1998-01-28
  - Markus Günther Kuhn, Ross John Anderson: Software piracy detector sensing electromagnetic computer emanations. UK Patent GB2330924, granted 2003-08-06, filed 1997-10-29
  - Ross John Anderson, Markus Günther Kuhn: Low cost countermeasures against compromising electromagnetic computer emanations. US Patent US6721423, granted 2004-04-13, filed 1999-01-28



Broadcasting AM



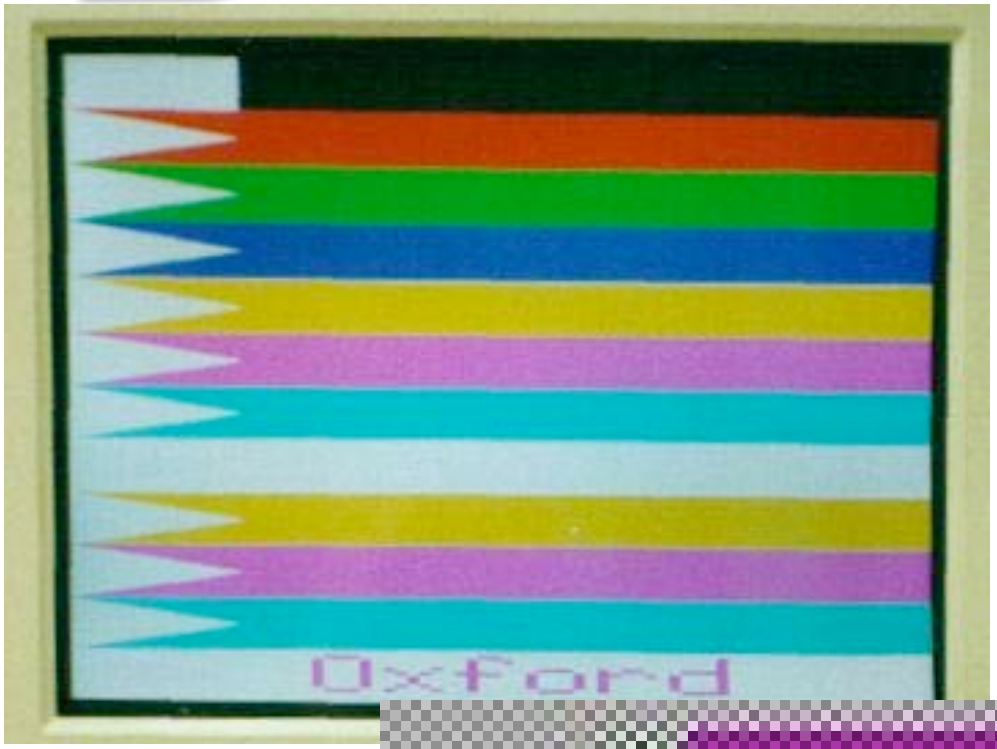
300 kHz

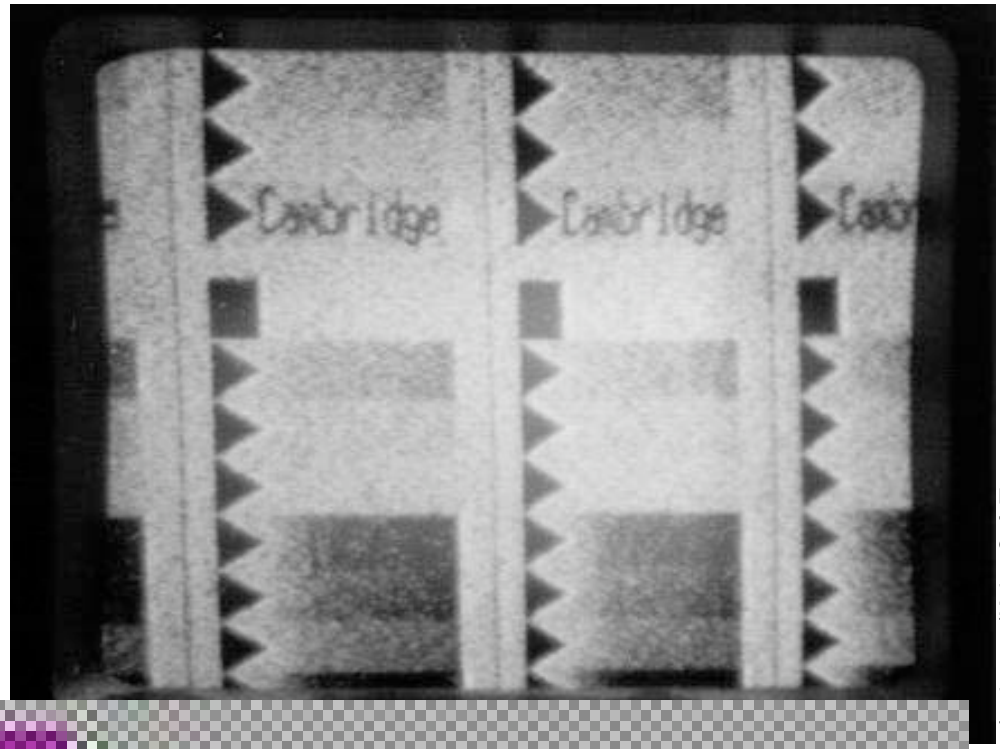
1200 kHz

Anderson/Kuhn: Soft Tempest

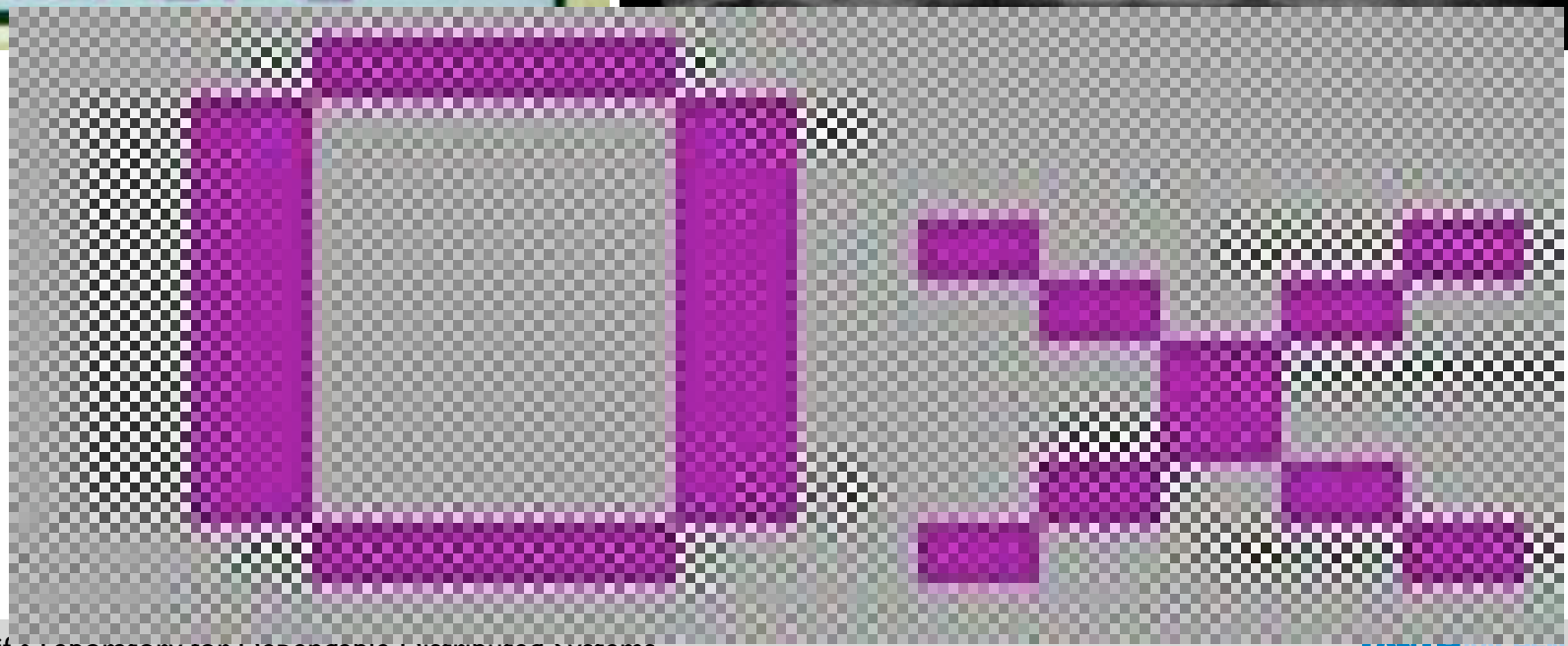
Anderson/Kuhn: Soft Tempest

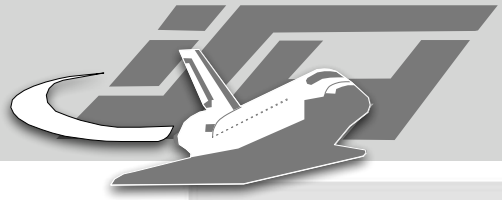
DataSafe/ESL Model 400 Tempest Emission Monitor





Anderson/Kuhn: Soft Tempest





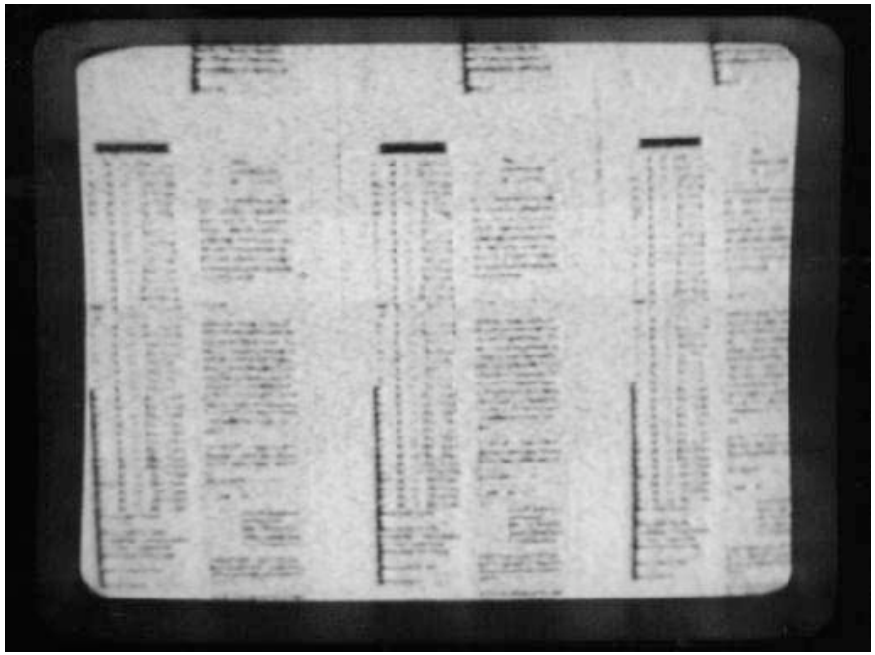
Tempest Fonts

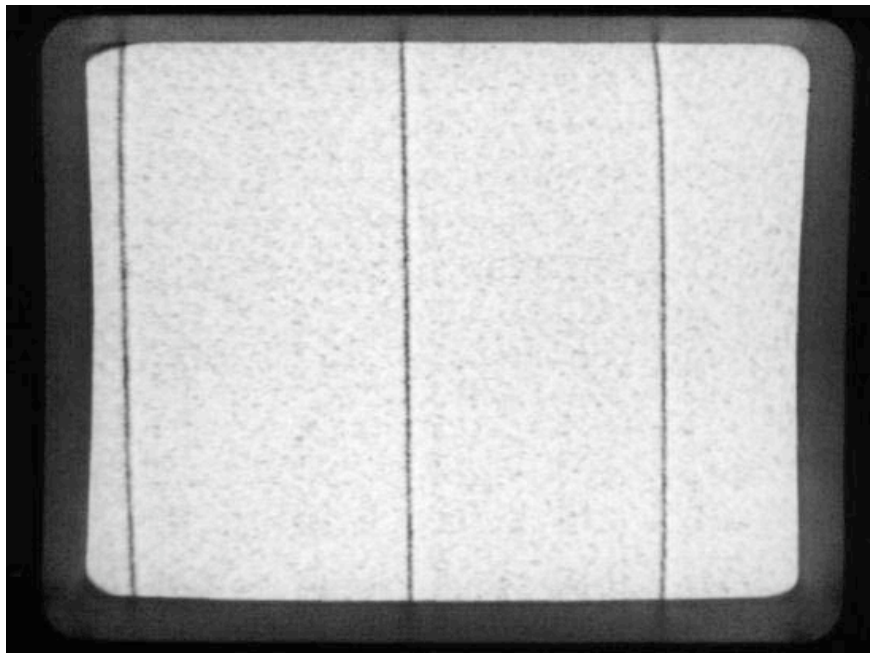
TrustNo1

TrustNo1

TrustNo1

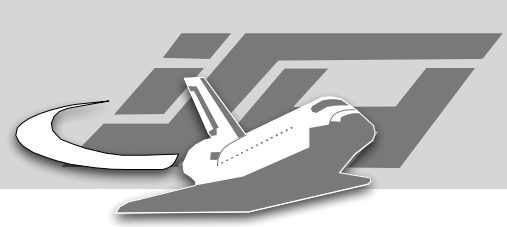
TrustNo1





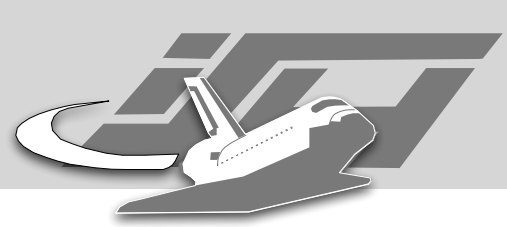
Tempest For Eliza
by Erik Thiel (2001)

http://www.erikyyy.de/tempest/



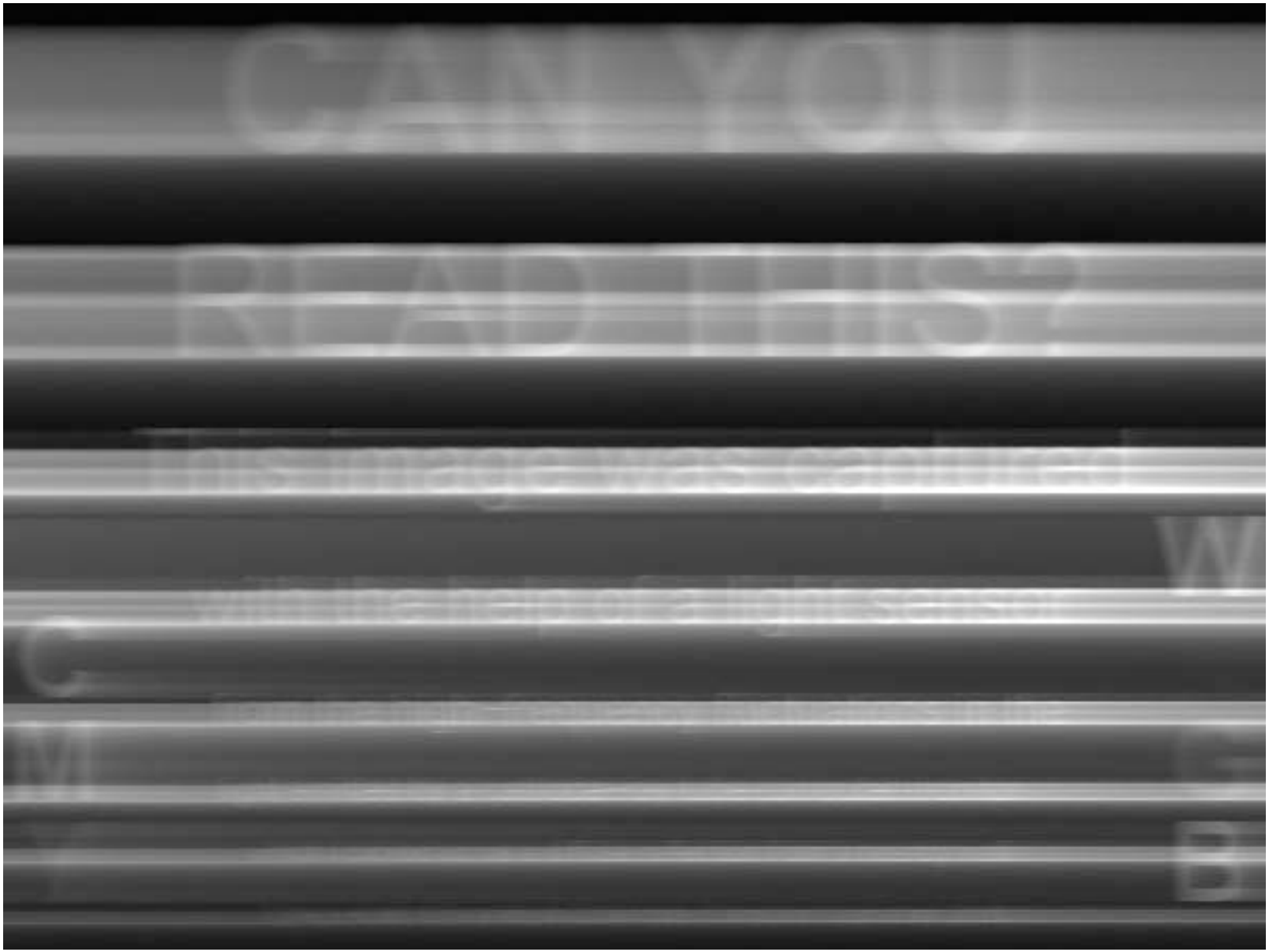
Optical Tempest

- CRT
- LED

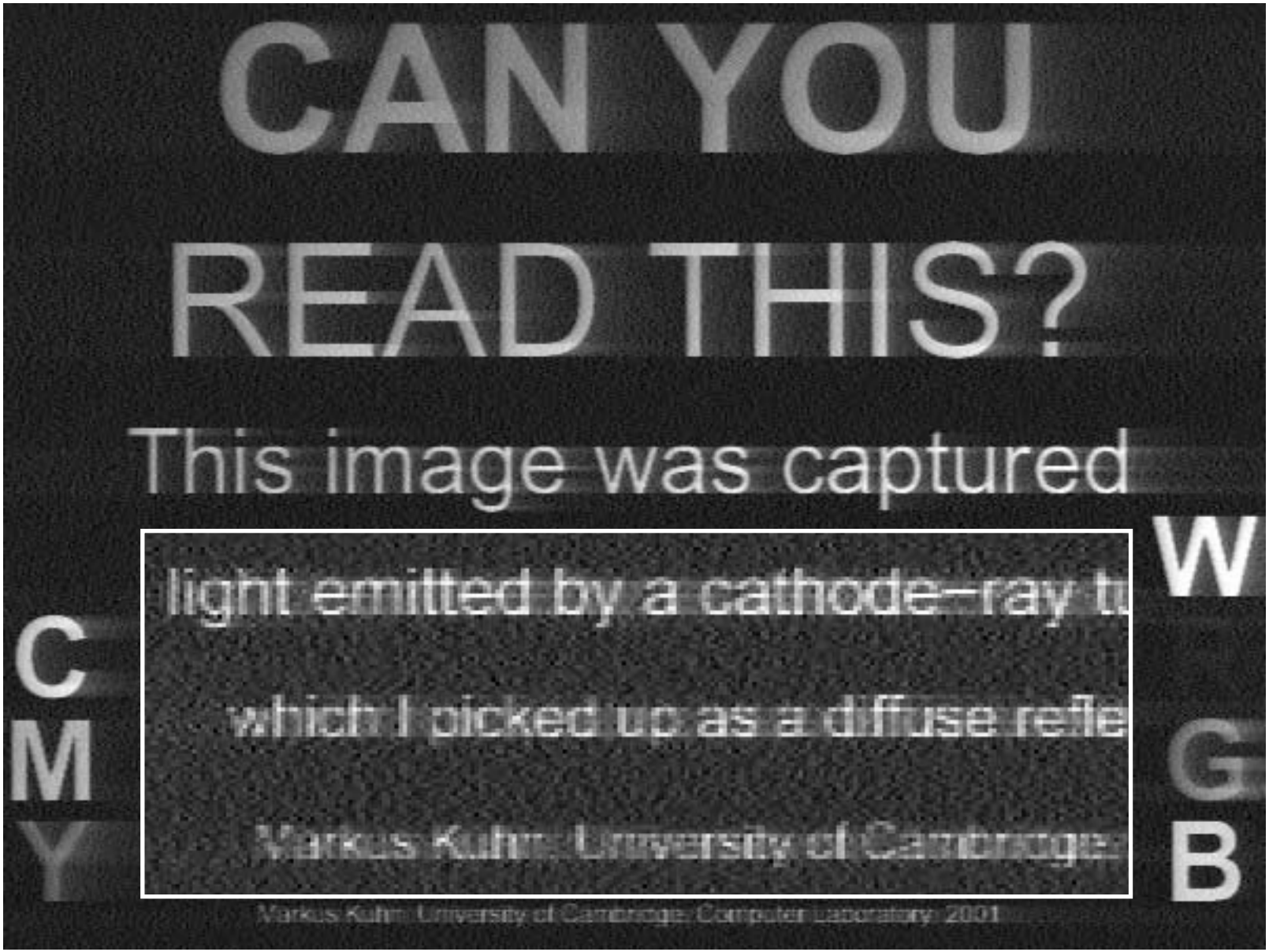


Monitors

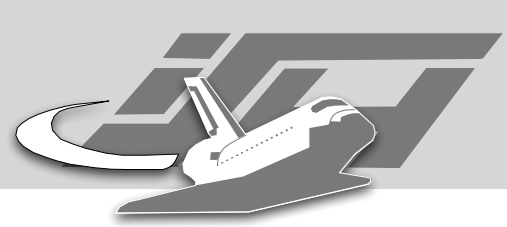
- Markus G. Kuhn: Optical Time-Domain Eavesdropping Risks of CRT Displays, Proceedings 2002 IEEE Symposium on Security and Privacy, Berkeley, California, 2002



http://www.cl.cam.ac.uk/~mgk25/emsec/optical-faq.html

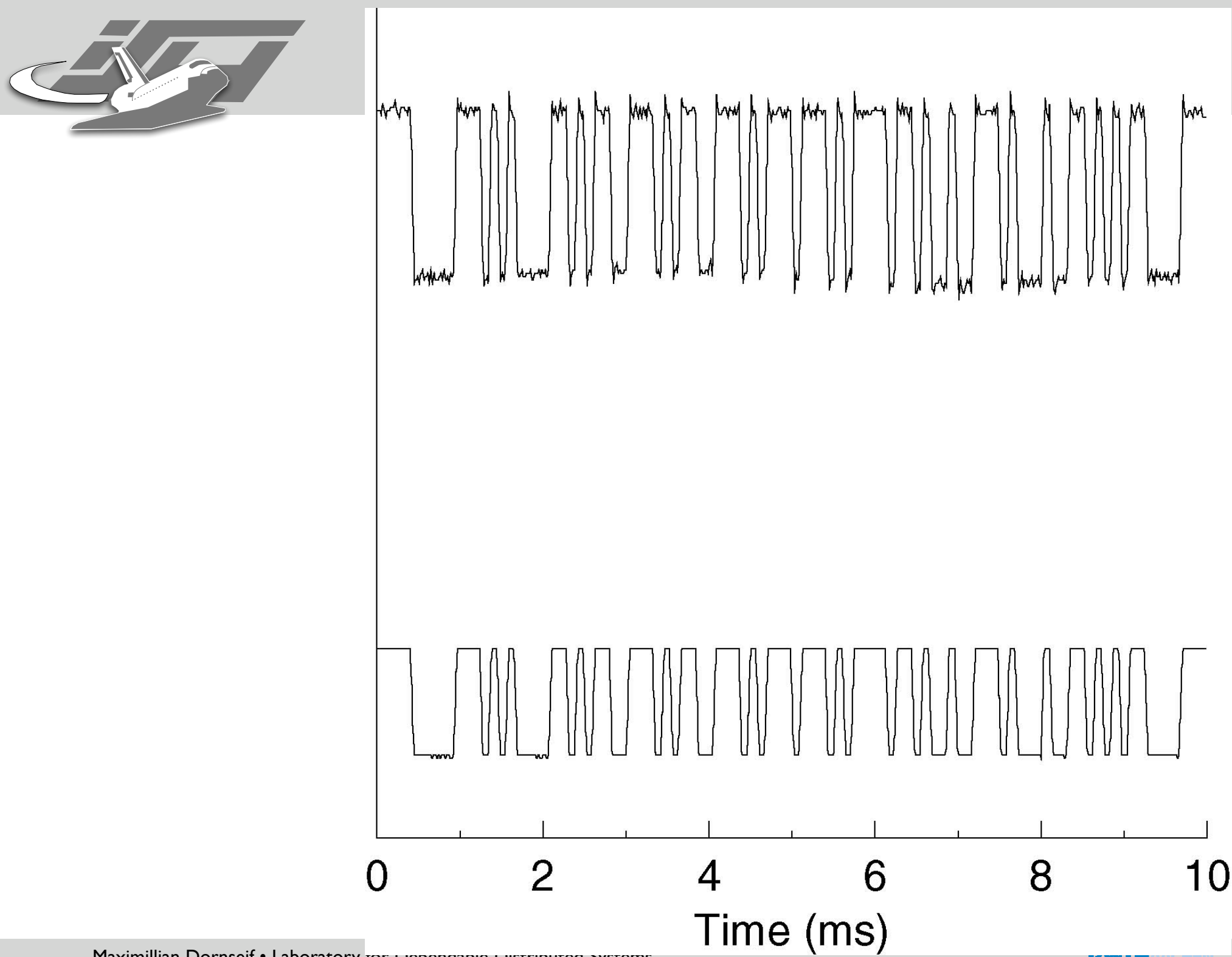


http://www.cl.cam.ac.uk/~mgk25/emsec/optical-faq.html

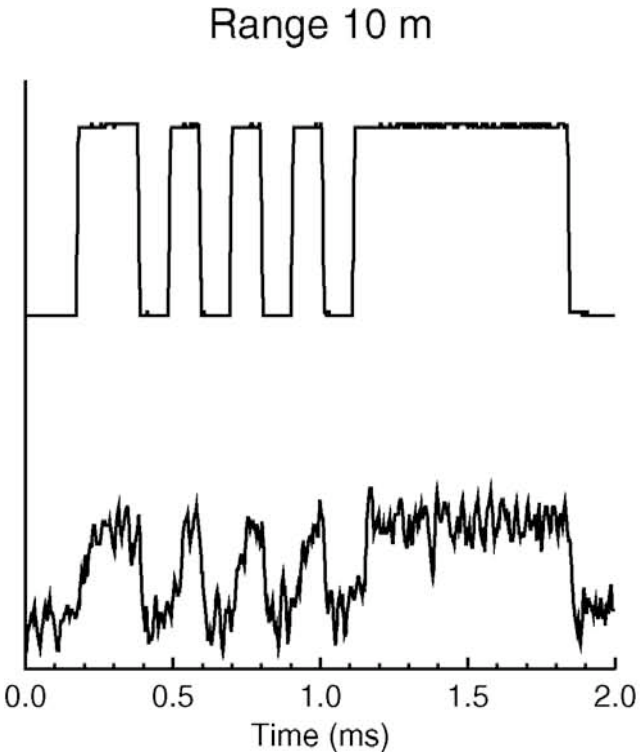


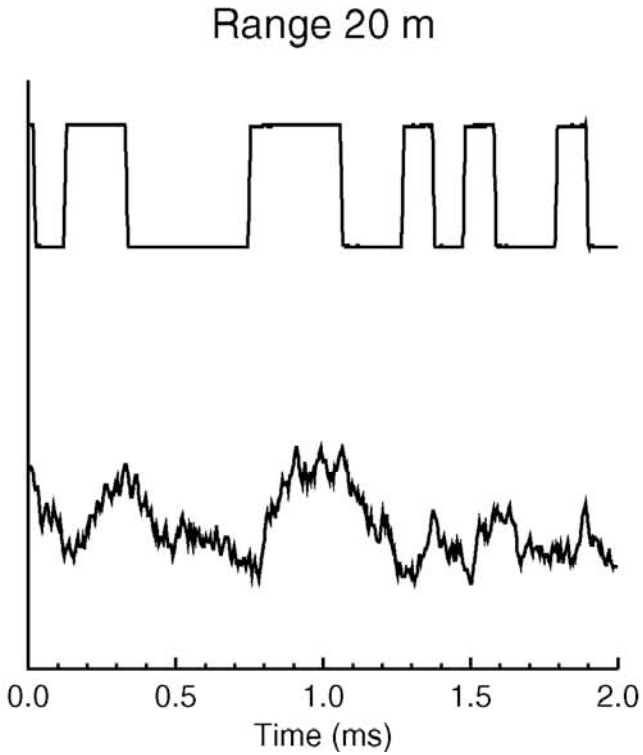
LEDs

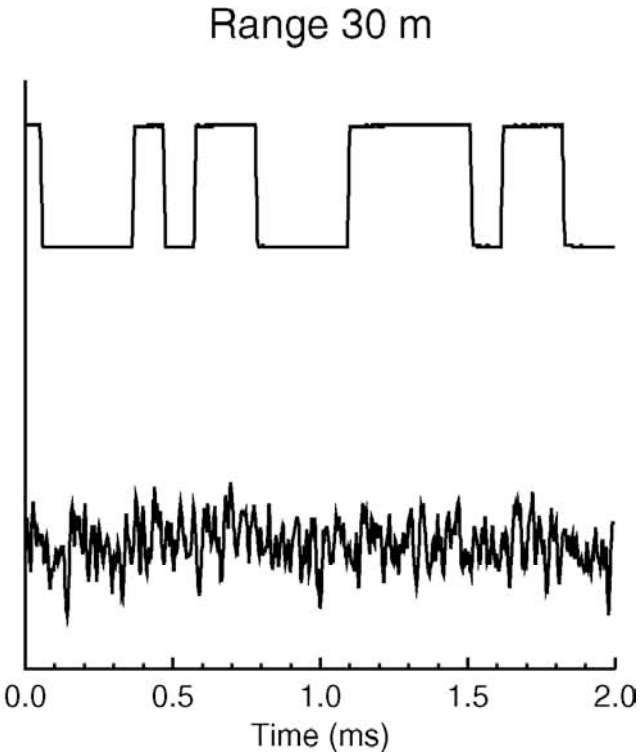
- Information Leakage from Optical Emanations JOE LOUGHRY Lockheed Martin Space Systems and DAVID A. UMPHRESS Auburn University -ACM Transactions on Information and System Security, Vol. 5, No. 3, August 2002, Pages 262–289.



Loughry/Umphress: Information Leakage from Optical Emanations

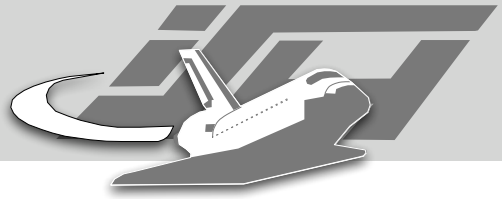






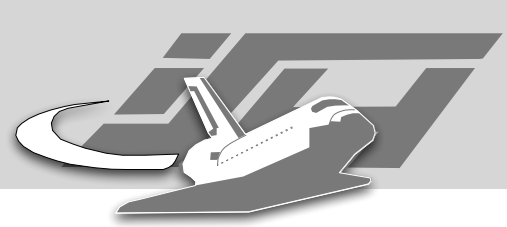
Loughry/Umphress: Information Leakage from Optical Emanations

Side-Channels

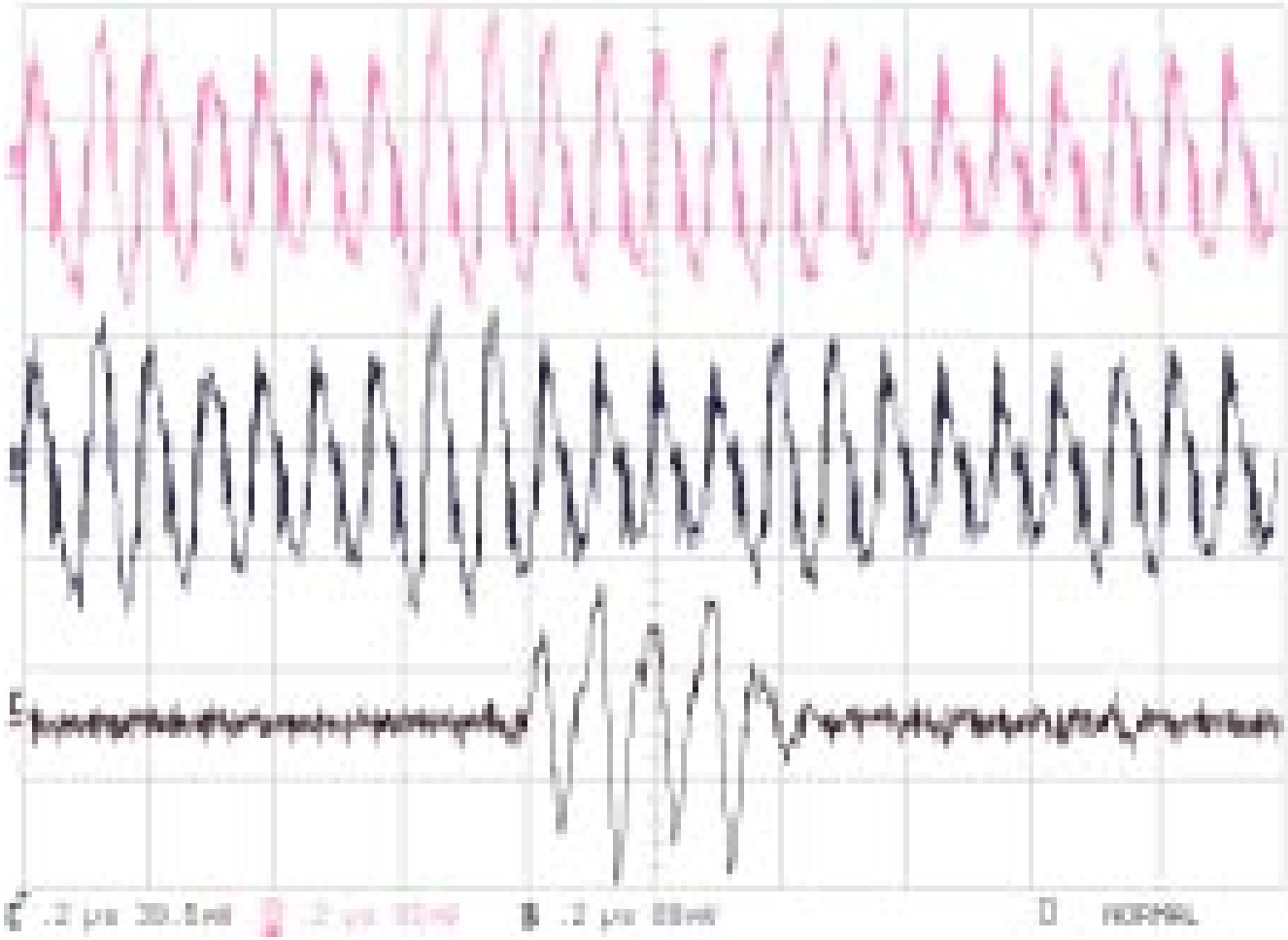


Side Channels

- Simple Power Analysis (SPA)
- (Differential) Timing Analysis.
- Differential Power Analysis (DPA)
- Overview:
  - N. P. SMART: PHYSICAL SIDE-CHANNEL ATTACKS ON CRYPTOGRAPHIC SYSTEMS
  - Manfred Aigner and Elisabeth Oswald: Power Analysis Tutorial



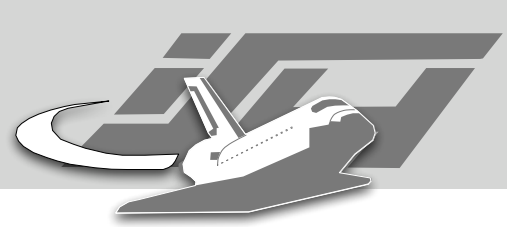
DPA



Aigner / Oswald: Power Analysis Tutorial

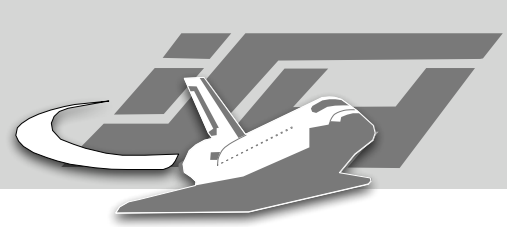
MOV 0 vs. MOV FF

Fault-Injection



Fault Injection

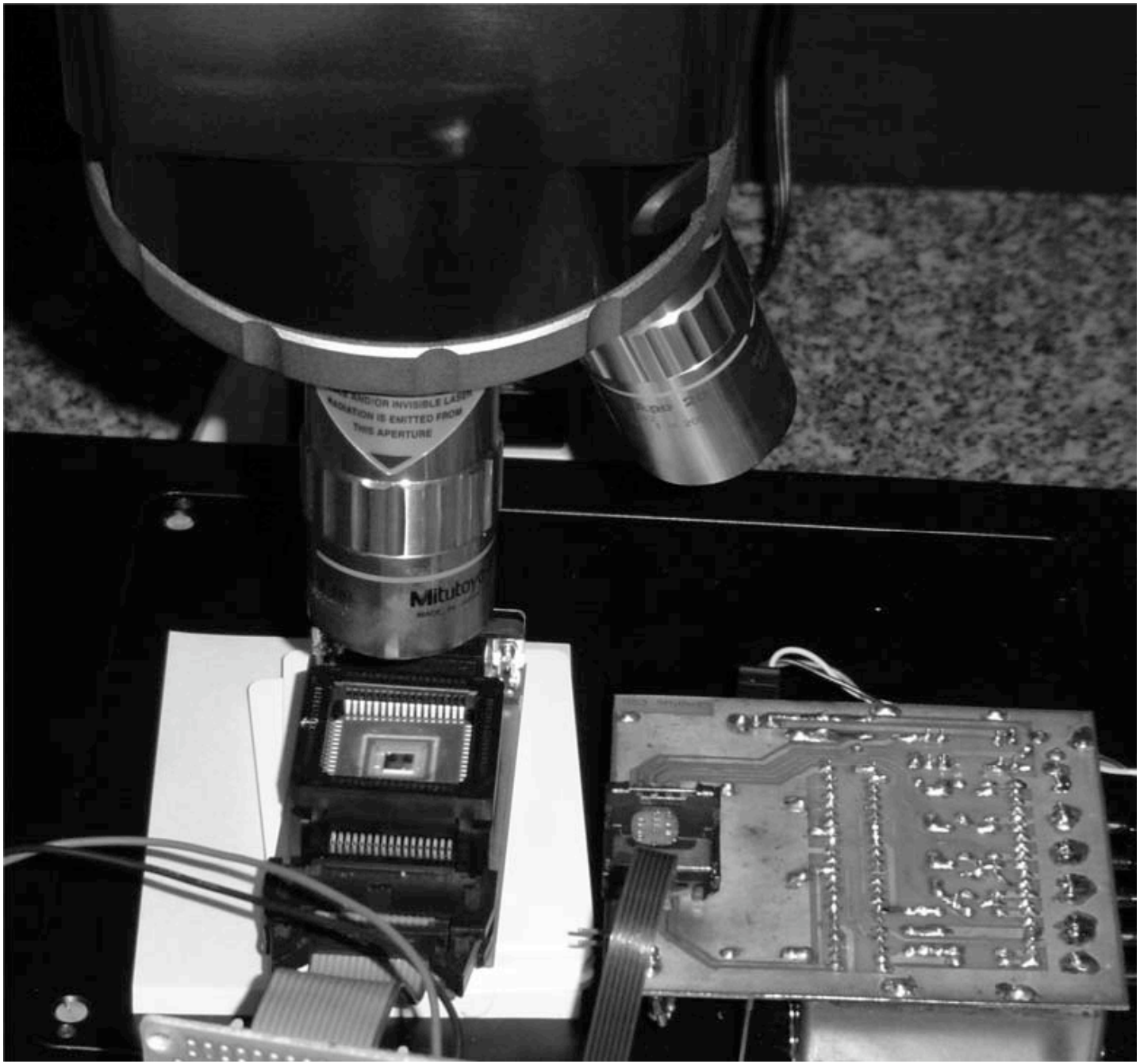
- Often called “glitching”.
- Overview
  - Hagai Bar-El, Hamid Choukri, David Naccache, Michael Tunstall, Claire Whelan: The Sorcerer’s Apprentice Guide to Fault Attacks (2004)



Fault Injection

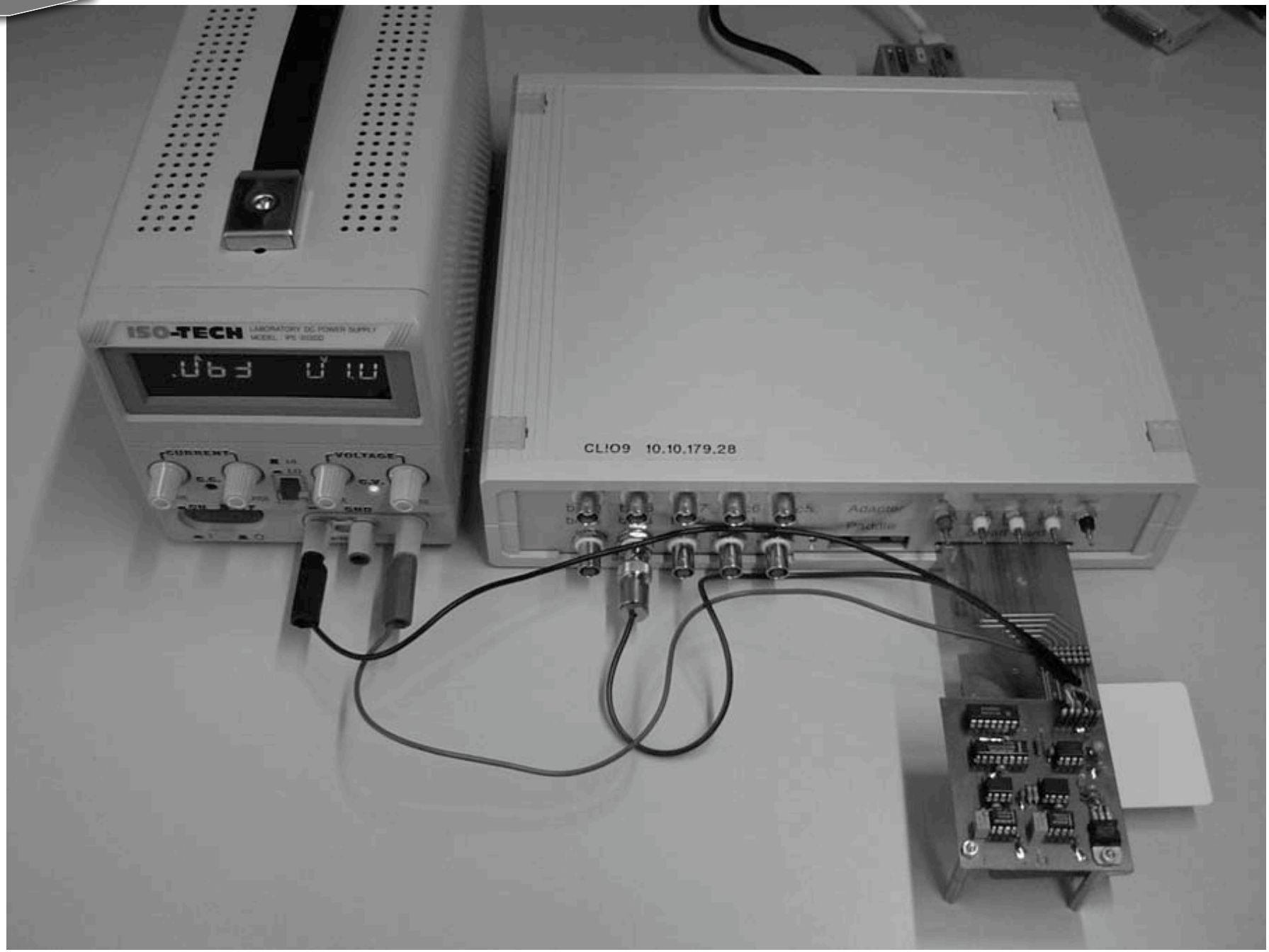
- Electrical perturbation on the standard ISO contact of the smart card
- Vcc glitch
- Clock duty cycle and/or frequency alteration
- Light-beam perturbation
- Global light-beam (wide spectrum)
- Focused light-beam (wide spectrum)
- Laser-beam (single wavelength)
- Electro-Magnetic Field perturbation (contact-less
- Temperature

Optical Fault Injection

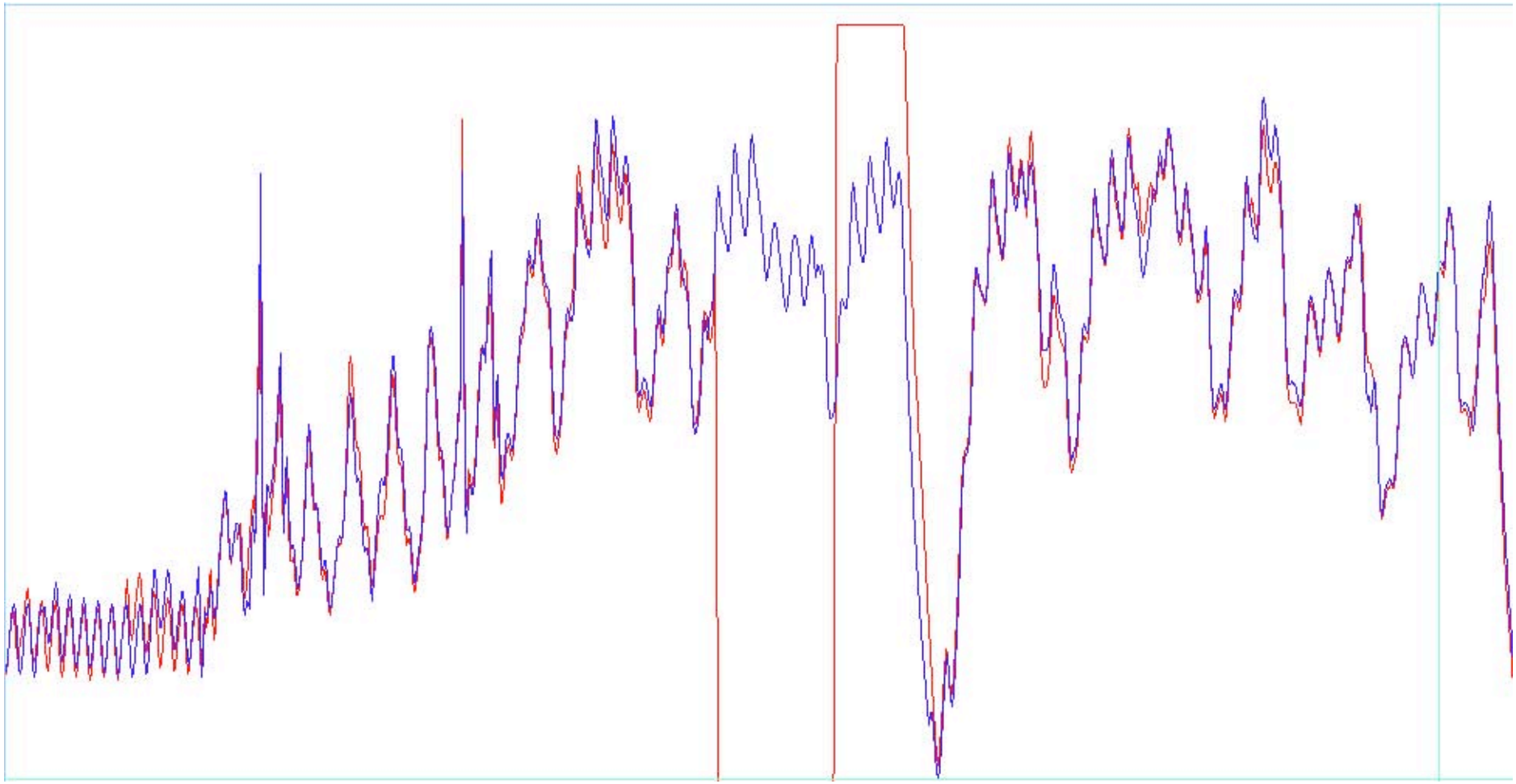


Bar-El/Choukri et.al.: The Sorcerer's Apprentice Guide to Fault Attacks

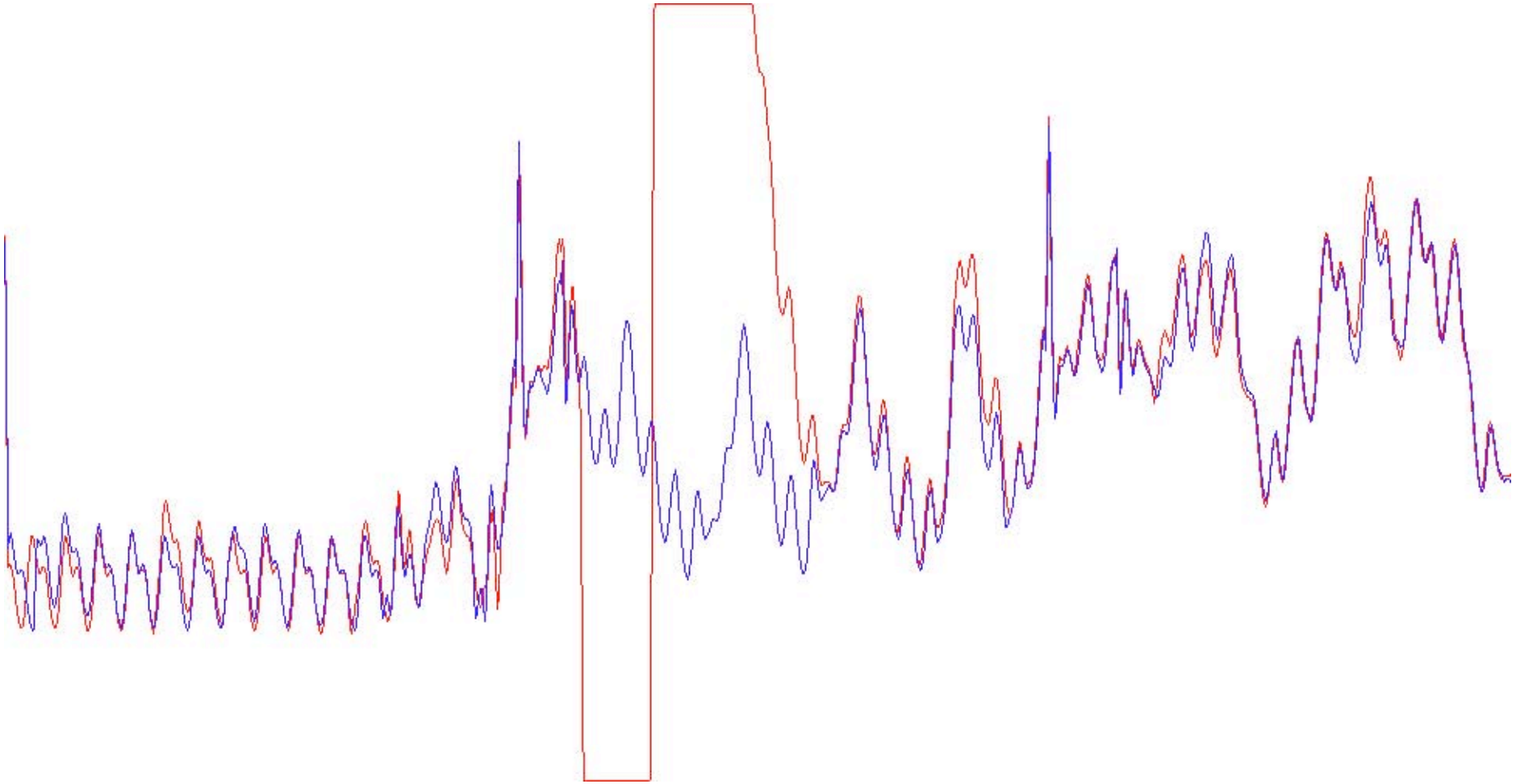
Electrical Fault Injection



Bar-El/Choukri et.al.: The Sorcerer's Apprentice Guide to Fault Attacks

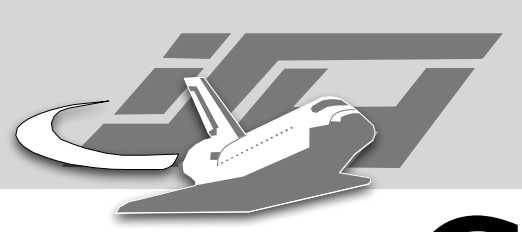


Bar-El/Choukri et.al.: The Sorcerer's Apprentice Guide to Fault Attacks



Bar-El/Choukri et.al.: The Sorcerer's Apprentice Guide to Fault Attacks

Cracking 128 Bit in 128 Minutes

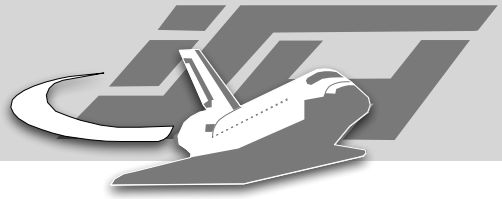


Cracking 128 Bit in 150 Minutes

- Embedded Systems are often underpowowered
- This allows all kinds of timing attacks
- Example: comparing a 128 bit key on an 8 bit Processor

Terminal

```
def checkAccess(k):
    for i in range(8):
        ktest = k[i]
        kcorrect = correct_key[i]
        if ktest != kcorrect:
            return False
    return True
```



Checking ...

-	>	S	e	c	r	e	t	!	u	n	G	u	e	S	s

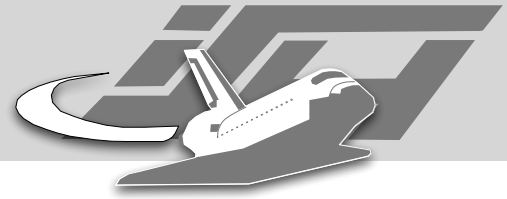
- Check for ->GeheimPassWord
- Check for ->SecretPassWord

Terminal

```
def cracker():
    known = ''
    while 1:
        tests = [0] * 256
        for c in range(256):
            k = pad(16, known + chr(c))
            s = time.time()
            if checkAccess(k):
                print "done: %r" % known
                return
            tests[c] = time.time() - s
        known += chr(tests.index(max(tests)))
        print repr(known)
```

Terminal

```
% python latency.py
0.51 '-'
136.97 '->'
402.24 '->S'
799.69 '->Se'
1326.48 '->Sec'
1996.37 '->Secr'
2664.01 '->Secre'
3319.87 '->Secret'
3980.39 '->Secret!'
4638.58 '->Secret!u'
5302.46 '->Secret!un'
5964.47 '->Secret!unG'
6620.07 '->Secret!unGu'
7295.35 '->Secret!unGue'
7954.96 '->Secret!unGueS'
8616.71 '->Secret!unGueSs'
```



Credits

- Joe Grand for Inspiration and Images
- Google Images and respective page owners for lock-picking images.

Cryptographic Processors and Algorithms 2

- Do NOT roll-your-own crypto
  - Possibly the most common problem in engineering
  - Easily broken, no matter what you may think
  - Usually just "security through obscurity"
  - Ex.: Palm OS system password decoding [1], US authentication tokens [8], iButton Dictionary Attack vulnerability [11]

Cryptographic Processors and Algorithms 2

- Do NOT roll-your-own crypto
  - Possibly the most common problem in engineering
  - Easily broken, no matter what you may think
  - Usually just "security through obscurity"
  - Ex.: Palm OS system password decoding [1], US authentication tokens [8], iButton Dictionary Attack vulnerability [11]