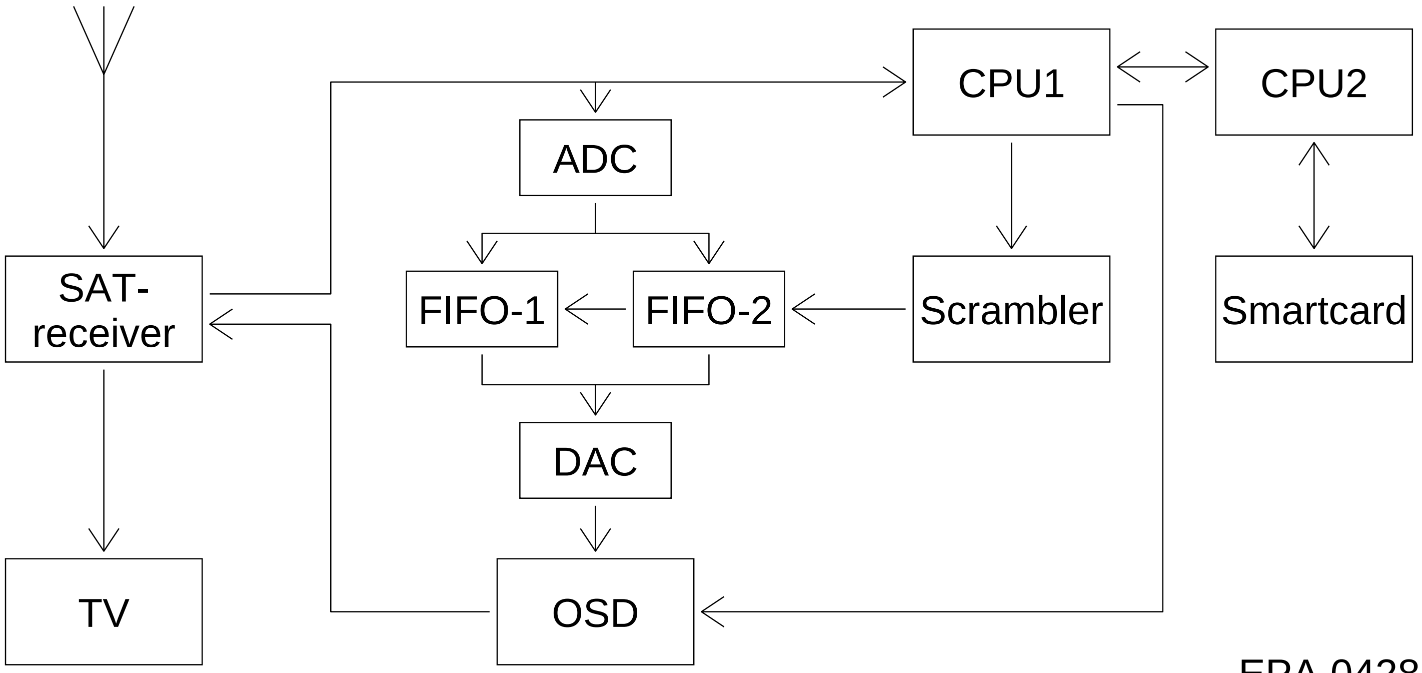
# Known cipher-text attack against a pay-TV image scrambler

# Example of a Hybrid System: VideoCrypt

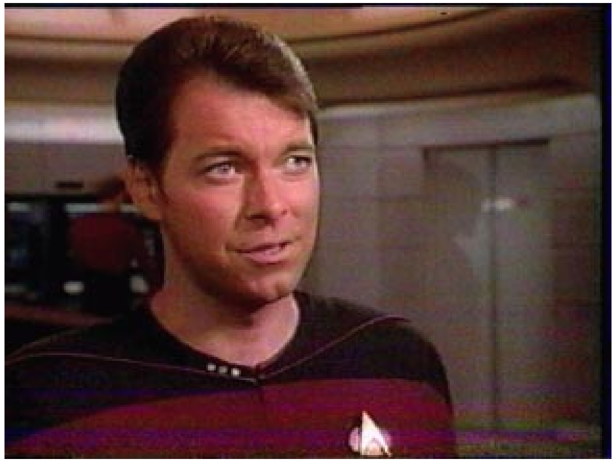


EPA 0428252 A2

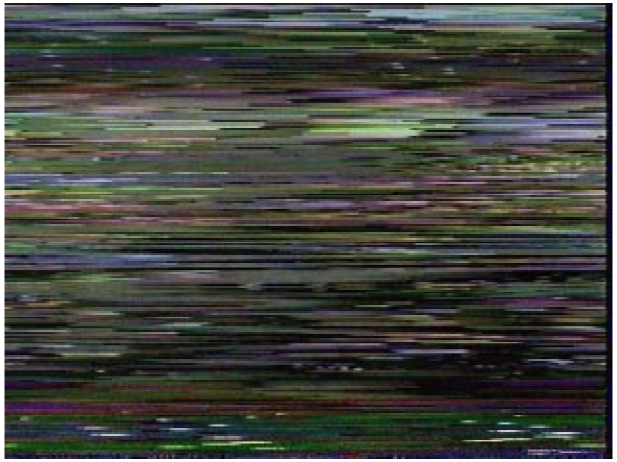
## Features:

- scrambling by active-line rotation, requires only memory for one single image line
- vertical-blank-interval data contains 32-byte messages with blacklist/whitelist data
- smartcard calculates 60-bit MAC as control word from 32-byte messages every 2.5 s
- CPU1 salts control word with frame counter to generate 60-bit PRNG seed per frame
- Scrambler uses 60-bit seed to generate cut-point sequence per frame

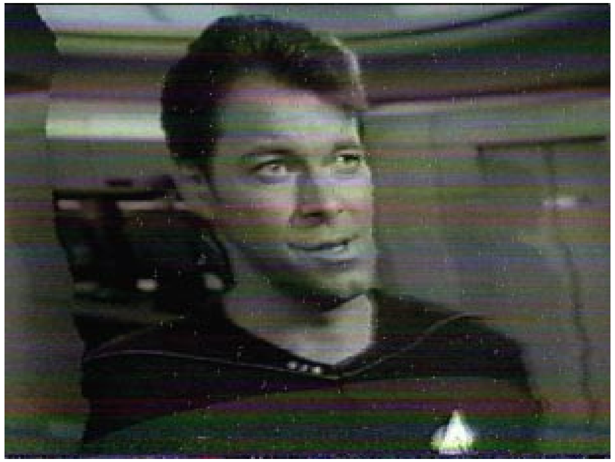
# An Image Processing Attack on VideoCrypt



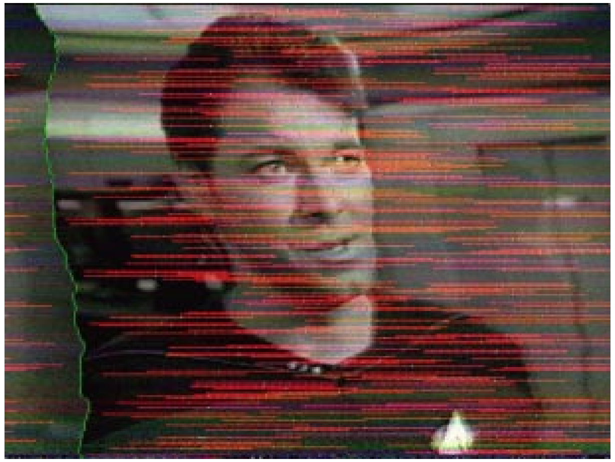
unscrambled source signal



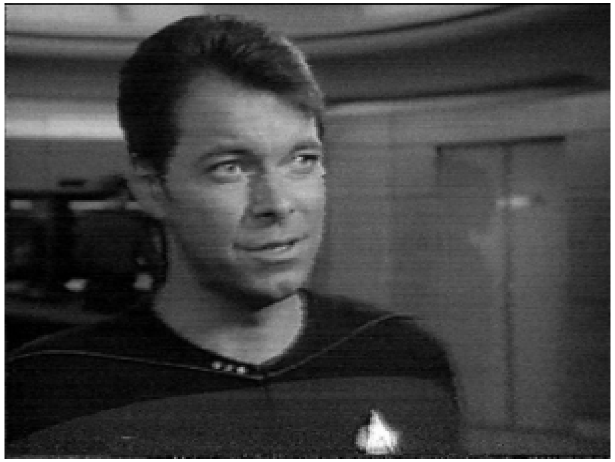
broadcasted scrambled signal



result of cross-correlation with cutpoints marked



edge detector avoids horizontal penalty zones around cut points

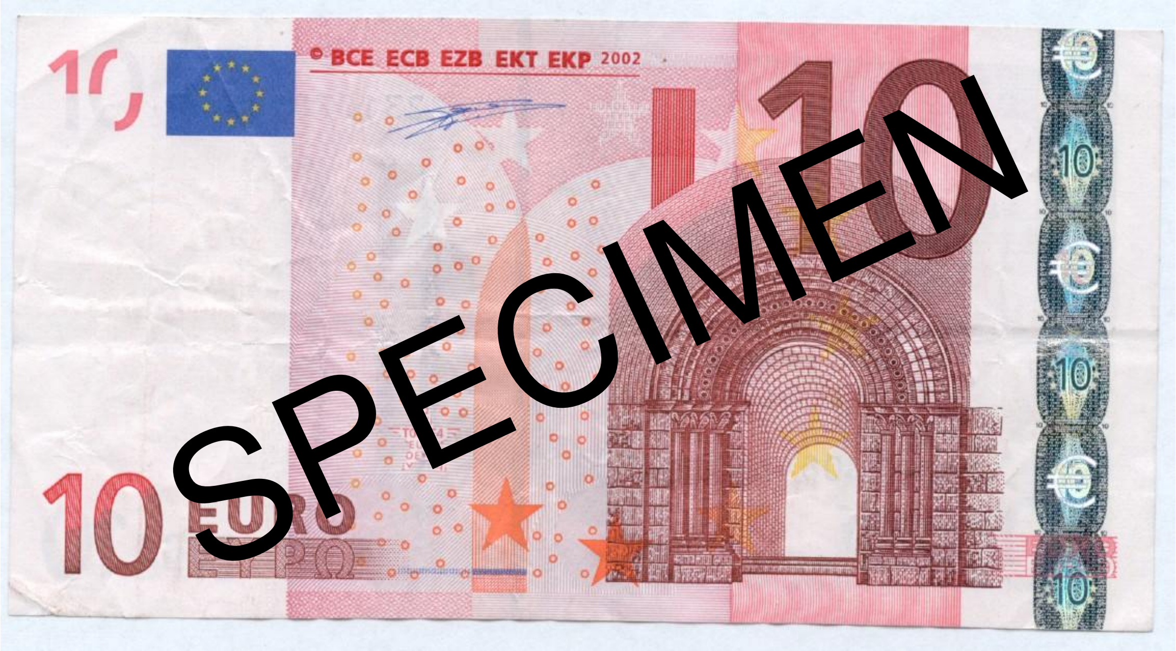


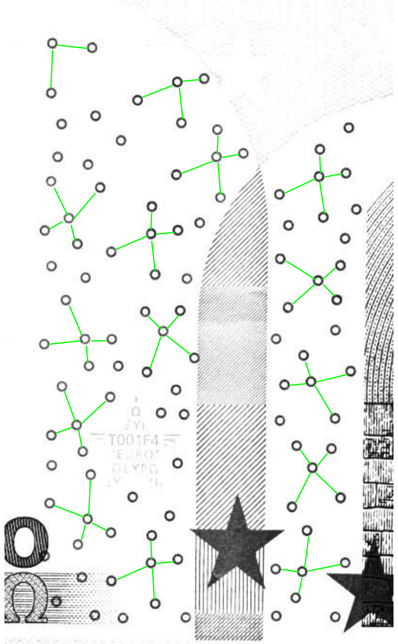
final b/w descrambling result obtained without knowledge of card secret

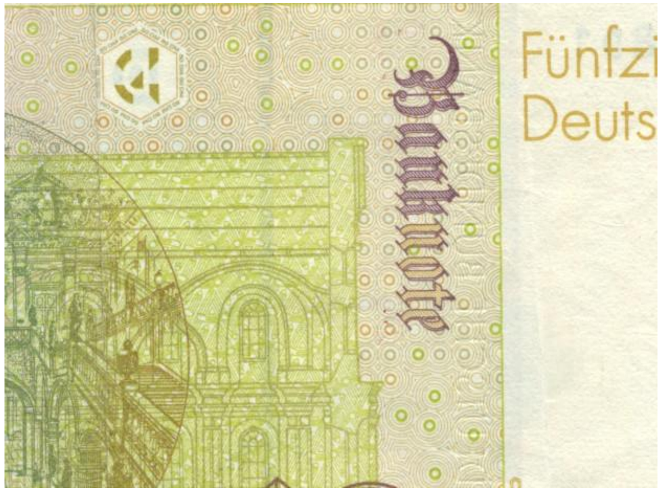
# Information hiding

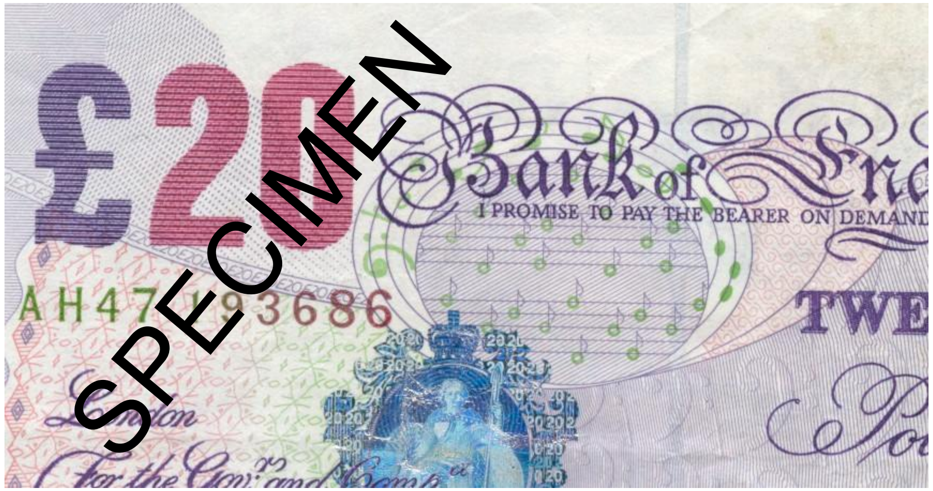
# The EURion Constellation

Markus Kuhn, Computer Laboratory, University of Cambridge, 2002–02–08







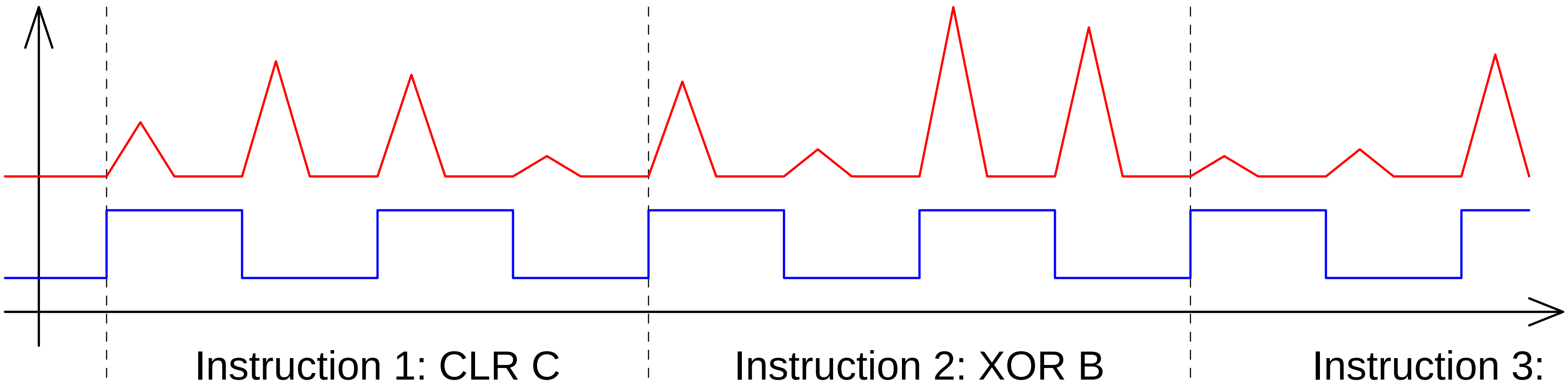


Modern colour photo–copying machines refuse to copy many of the more recent banknotes, such as the pound, mark or euro. But how do they decide, what is a banknote? They search for a simple geometric pattern, consisting of five 1 mm large circles that appears on many more recent banknotes, usually in yellow, but often also in green or orange. The circles are particularly well visible in the blue channel, can be easily detected with a matched filter and tested for the presence of the characteristic constellation.

# Side-channel attacks

# Power Supply Current Forms a Significant Covert Channel

Record current in VCC/GND connection with 12−bit, 30−MHz ADC, in order to reconstruct executed instruction sequence and observe cryptographic computations.

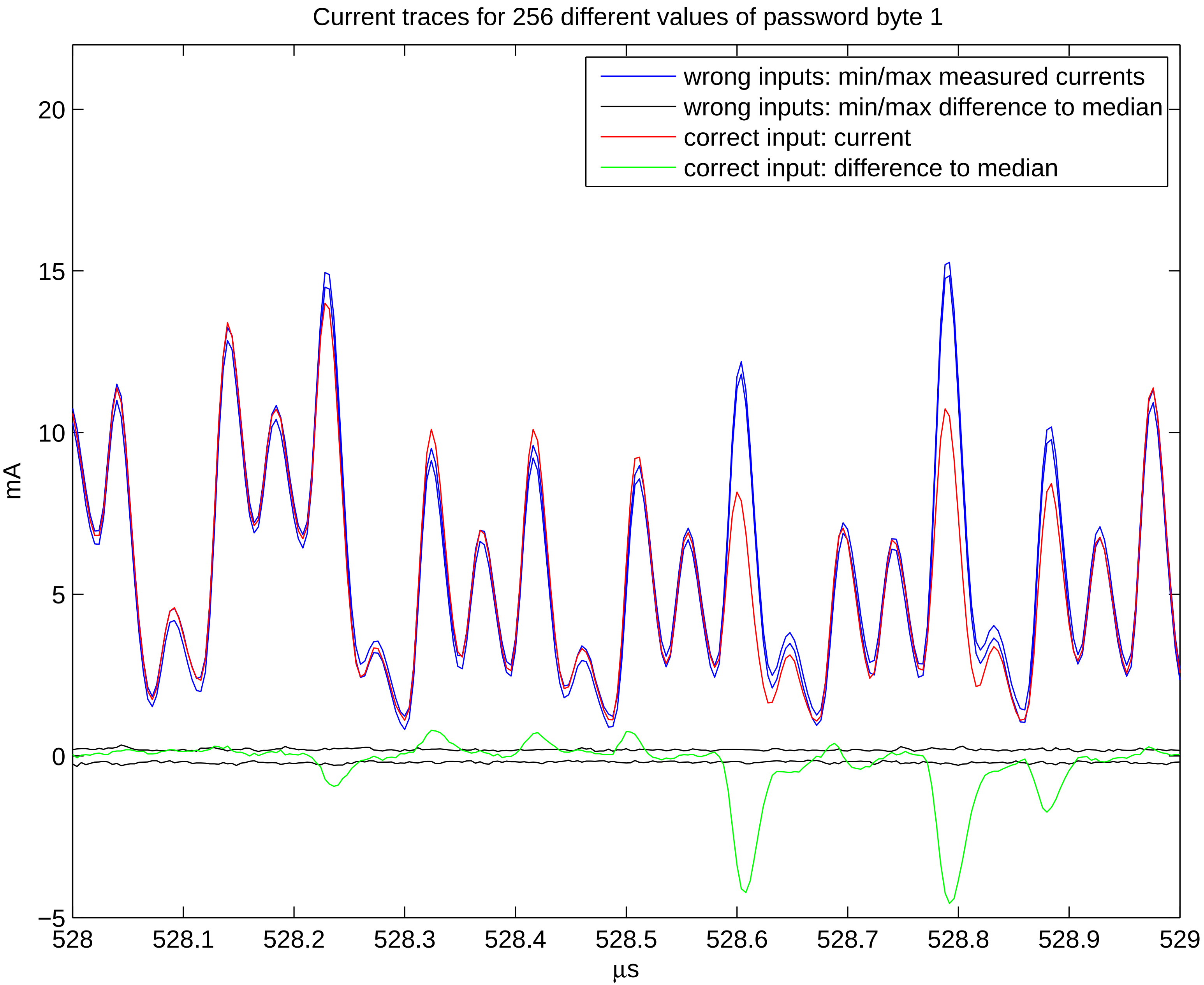


→ Characteristic current spikes can identify executed instruction

→ Data values appear in power profiles either as differential Hamming weights (~0.5−1 mA/bit) or as individual bits, e.g. with multiplication or shift instructions

→ Current signature depends on accessed memory type (SRAM−write short circuit, EEPROM read−out amplifier, etc.)

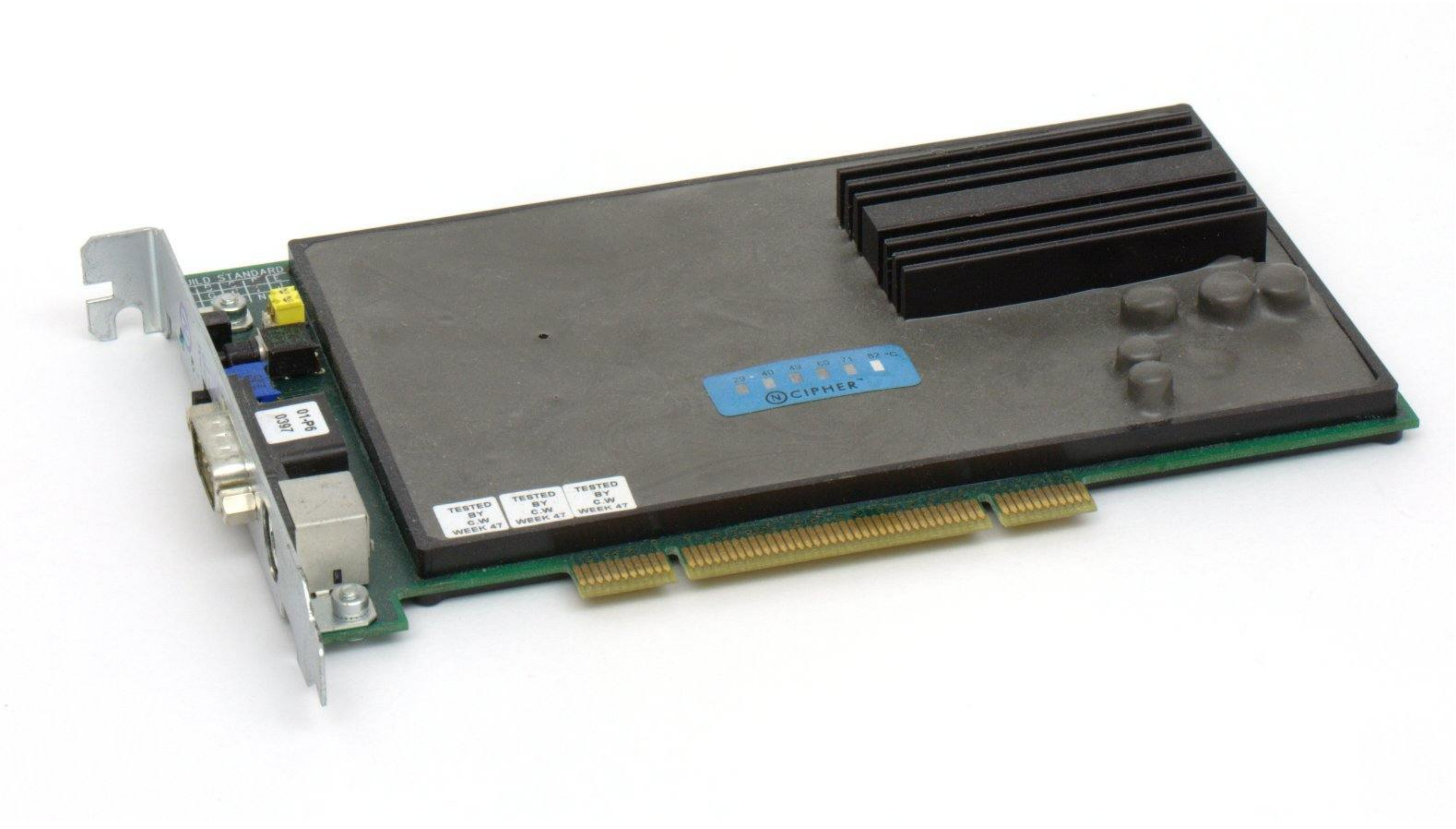
→ Activation of EEPROM programming−voltage charge pump observable, which allows to abort before state changes (e.g., with bad retry counters)



Single-shot power analysis to break the firmware password protection in a car microcontroller.

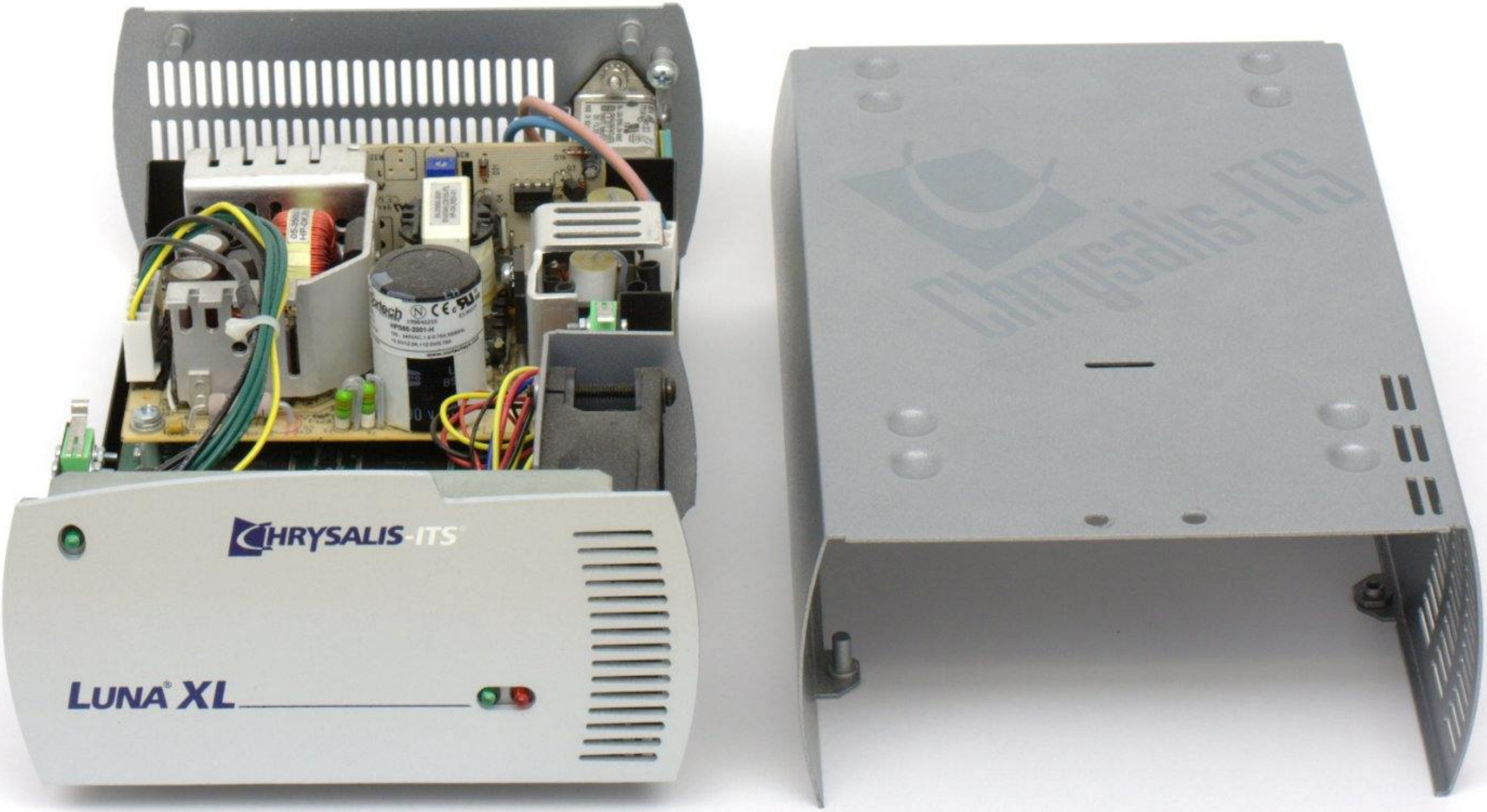
# Hardware security modules

# Potting



Encapsulating components into an obaque, hard resin discourages casual inspection and probing (requires mechanical or chemical removal).

# Lid switches



Lid-switches that zeroize keys stored in battery-backed SRAM require mechanical tools (e.g., milling machine) to penetrate chassis.

# Tamper-sensing membrane

WARNING: INCORRECT BATTERY REPLACEMENT OR
MISUSE WILL PERMANENTLY DISABLE THE CARD. REFER TO
IBM 4758 PCI CRYPTOGRAPHIC COPROCESSOR INSTALLATION MANUAL
CAUTION
IBM
BT1

IBM 4758

Penetration-tested tamper-sensing membrane in difficult-to-machine resin and SRAM zeroization can provide high to very high key protection.

# Cipher-instruction search attack against a security microcontroller

# Tamper-resistant modules

## 3) Bus encryption

The CPU chip incorporates a unit that encrypts both the data and address bus. The secret key used is stored on the CPU chip in a battery-backed SRAM register. External memory contains only encrypted data that is decrypted when fetched into the CPU cache.

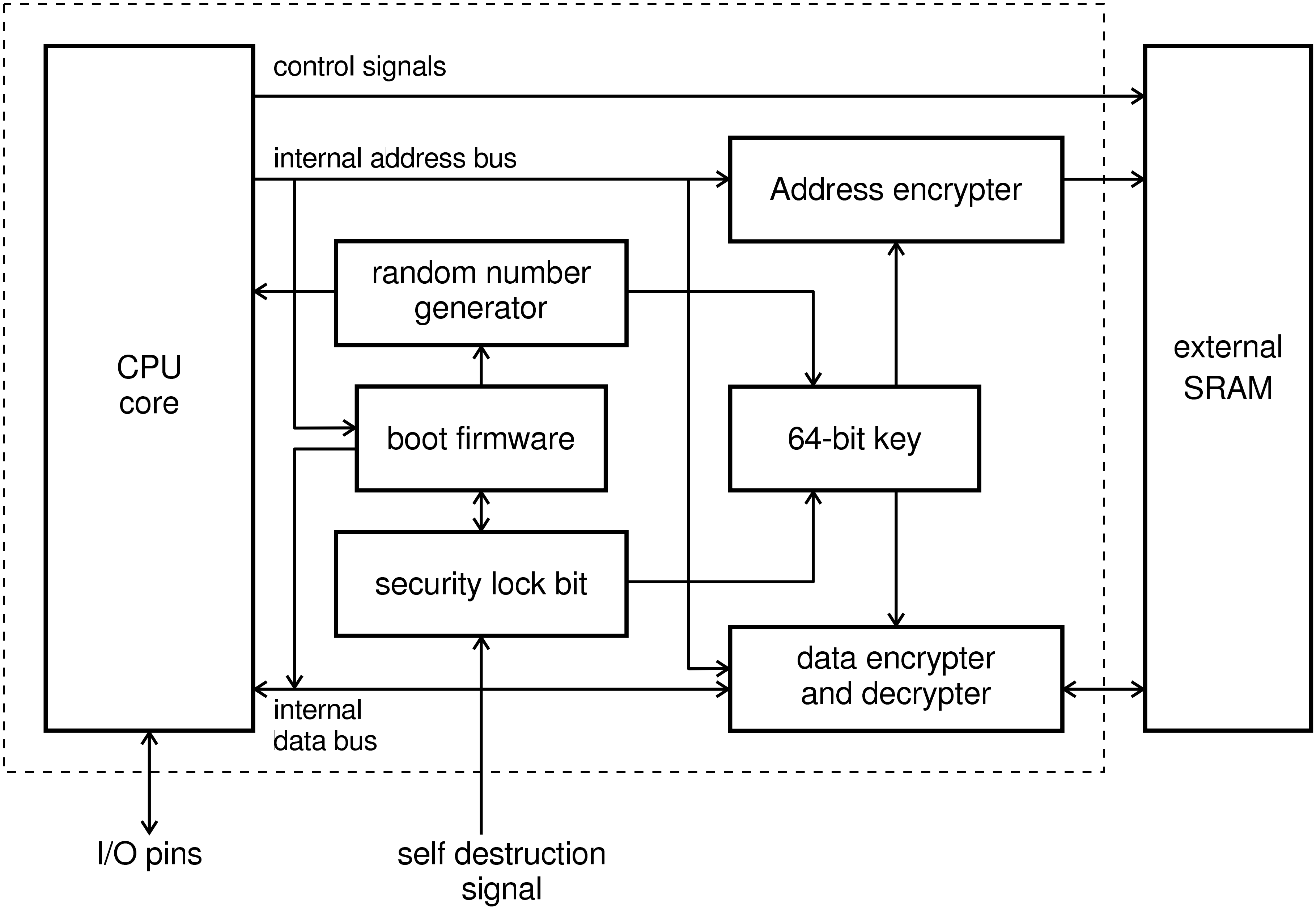
**Advantages:**

- → no capacity limit
- → SRAM registers are difficult to access for attackers
- → simple to manufacture (no off-chip alarm envelope)
- → can easily be combined with a secure package

**Disadvantages:**

- → design tradeoff between good cryptography and low bus latency
- → traces of external memory accesses lead to information leaks

# Bus Encryption in the DS5002FP:

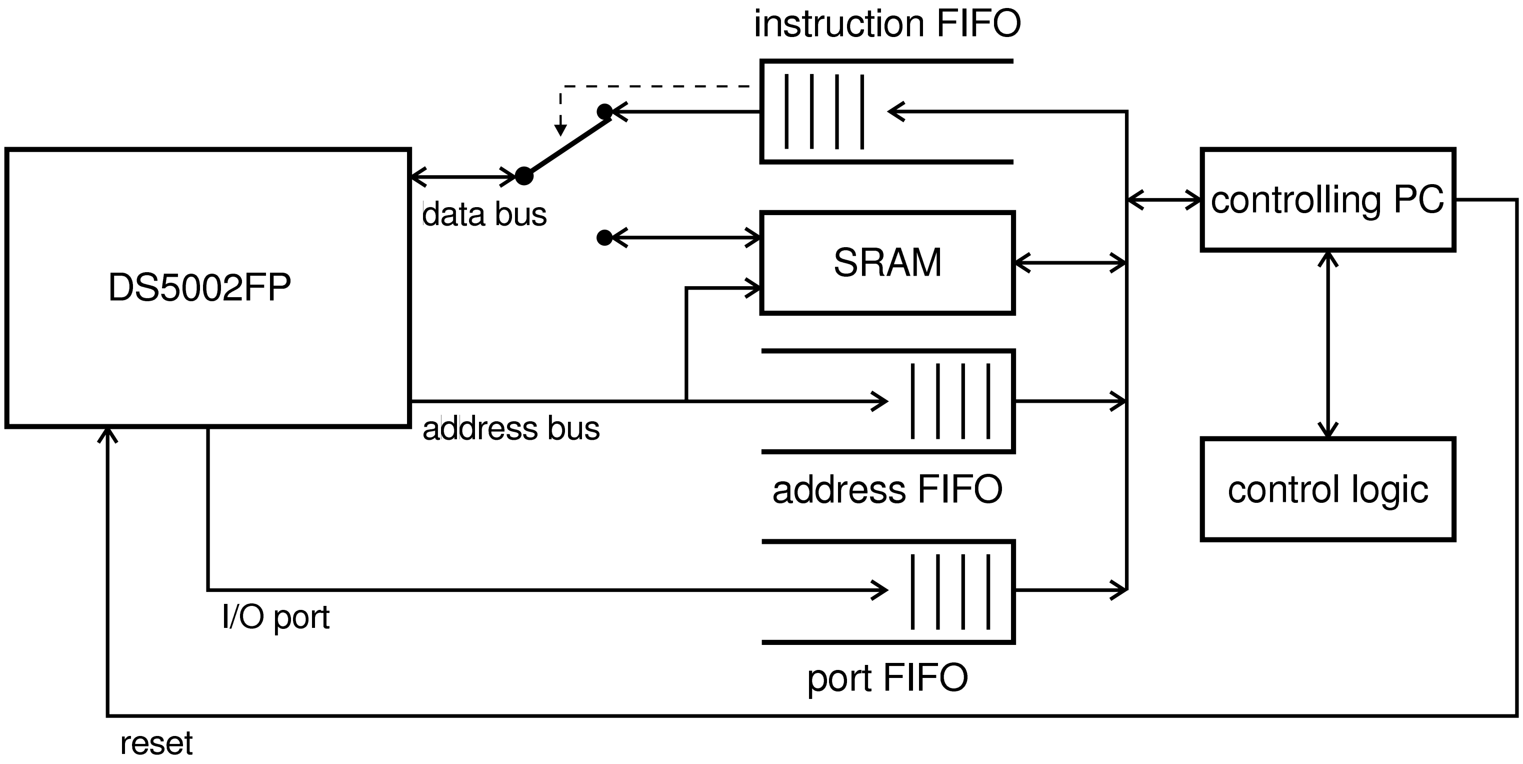


## Attack Concept:

Search systematically cipher bytes for the following instructions:

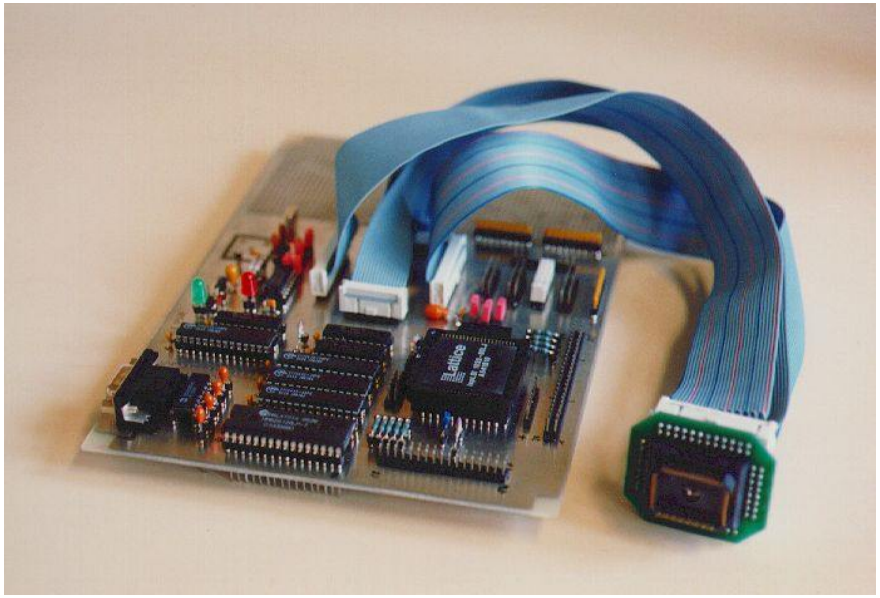
```
00         NOP              ; no operation
75 90 xx   MOV 90h, #xxh    ; output value xxh on port 1
```

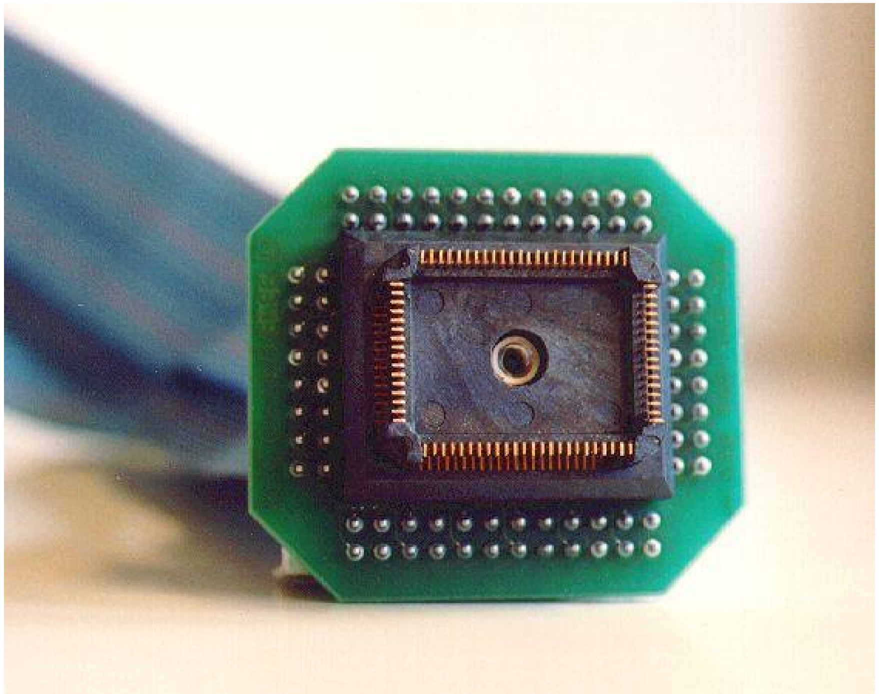
## Experimental Setup:



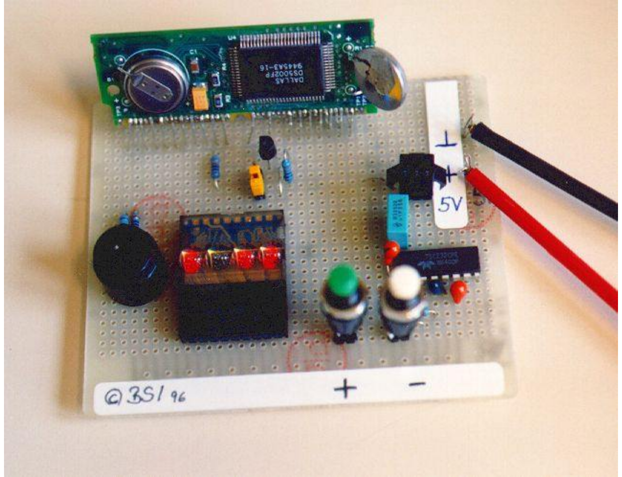
Details: M.G. Kuhn: *Cipher instruction search attack on the bus-encryption security microcontroller DS5002FP*. IEEE Trans. on Computers **47**(10), October 1998, pp. 1153–1157.

# The DS5002FP Attack Support Hardware

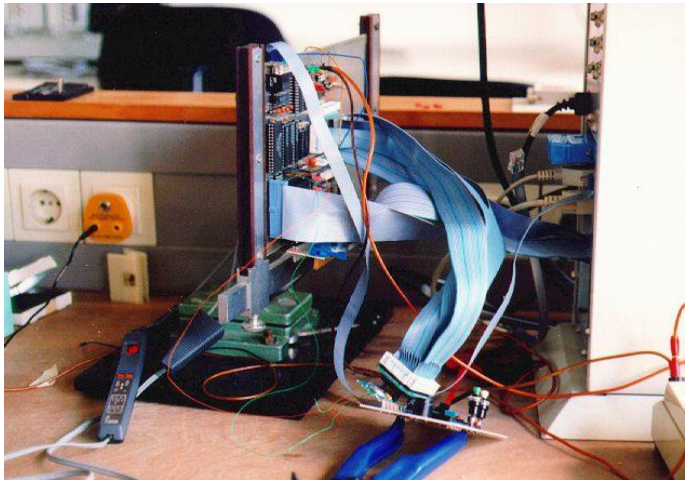




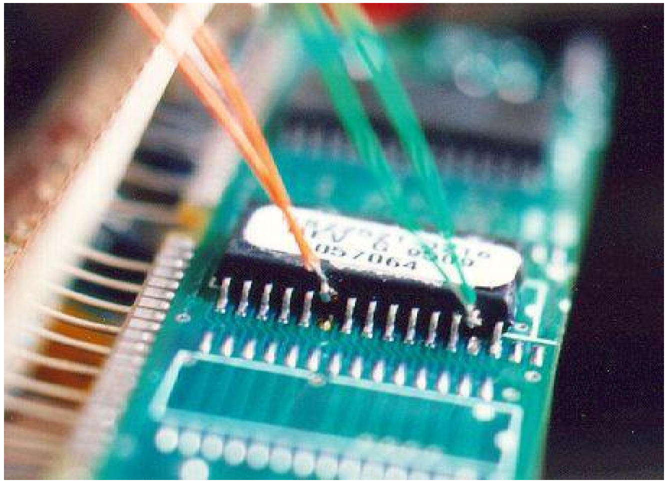
# Attack on a DS5002FP Based Demonstration System



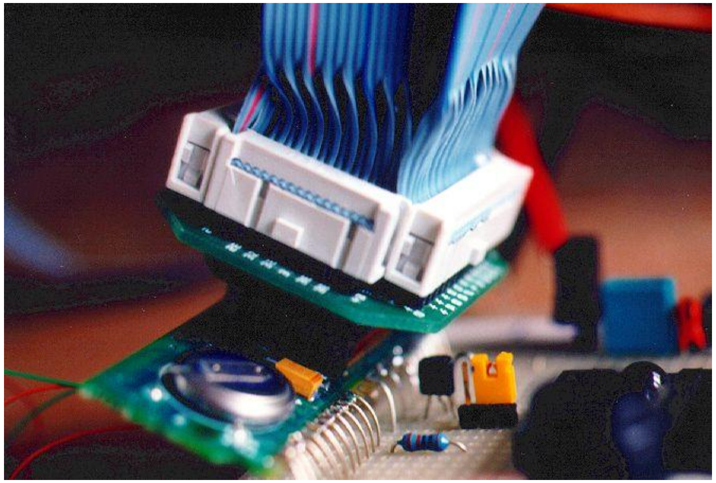
Code lock provided by the German Federal Agency for Information Technology Security (BSI)



Analyzed system connected to read−out circuit and controlling personal computer



Chip−select and read/write connection between SRAM and CPU rerouted through read−out circuitry



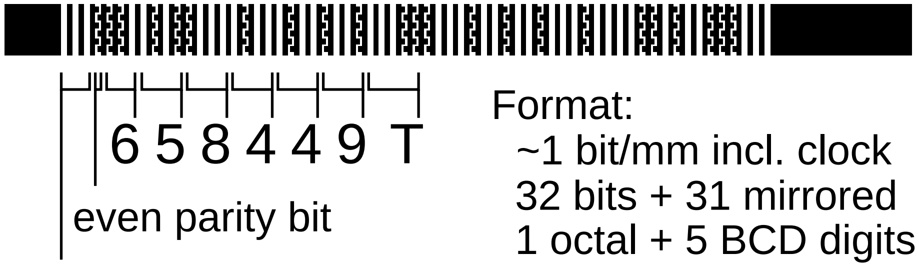
Easy access to all CPU signals is possible using an SMD test clip

# Changes in assumptions

# ENTACARD Demystified

Markus Kuhn, Computer Laboratory, University of Cambridge

*... or how to penetrate our door access control system in 20 minutes*



6 5 8 4 4 9 T

even parity bit

start code = 000

Format:

~1 bit/mm incl. clock
32 bits + 31 mirrored
1 octal + 5 BCD digits
5-bit letter code

Code Space:

800 000 numbers ×
32 letters = $2^{28}$

T658449

TDSi Microcard infra-red bar code

Patent US4538059 http://www.tdsi.co.uk/

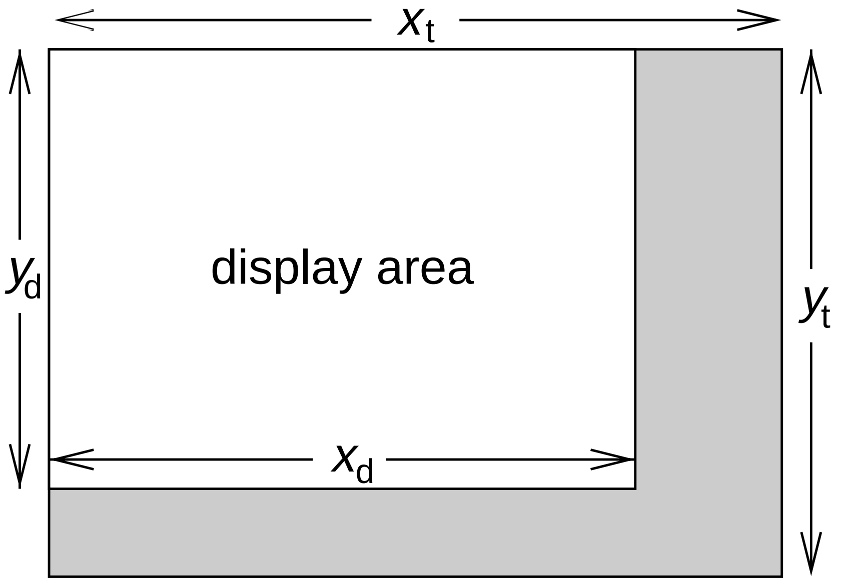
Security Analysis:

Clone cards trivial to generate from known valid card number (printed on each card!), or from IR bar code. Only standard office equipment necessary (graphics software, laser printer, transparencies, desk lamp). Cards issued in batches of consecutive numbers, therefore knowledge of cancelled card number allows attacker to guess a valid one. Penetration around one order of magnitude simpler/faster compared to standard cylinder lock.

# Optical eavesdropping of CRTs

# Time-domain observation of CRT light

Electron beam position of raster-scan CRT predictable:



Pixel frequency: $f_\mathrm{p}$

Deflection frequencies:

$$f_\mathrm{h} = \frac{f_\mathrm{p}}{x_\mathrm{t}}, \qquad f_\mathrm{v} = \frac{f_\mathrm{p}}{x_\mathrm{t} \cdot y_\mathrm{t}}$$

The 43 VESA standard modes specify $f_\mathrm{p}$ with a tolerance of $\pm 0.5\%$.

Overall light emitted by CRT is proportional to (gamma corrected) video signal $v_\gamma(t)$ convolved with phosphor impulse response $P(t)$:

$$I(t) = \int_0^\infty v_\gamma(t - t')\, P(t')\, \mathrm{d}t'$$

# CRT phosphor types

Monitor manual says “P22”, but this is just the generic designation for all RGB phosphor triplets designed for NTSC color TV.

Worldwide Type Designation System (WTDS): XXA, XXB, XBA, . . .

Substances:

- → Red: yttrium oxysulfide doped with europium ($Y_2O_2S$:Eu), zinc phosphate with manganese ($Zn_3(PO_4)_2$:Mn).
- → Green: zinc sulfide doped with copper (ZnS:Cu) and sometimes also with aluminium and/or gold, or zinc silicate doped with manganese and silver ($Zn_2SiO_4$:Mn,Ag).
- → Blue: The blue phosphor is usually zinc sulfide doped with silver (ZnS:Ag) and in some cases also aluminium or gallium.

# Light sensors

Requirements:

- $\longrightarrow$ very sensitive (to reduce preamp noise)
- $\longrightarrow$ very fast (bandwidth comparable to $f_{\mathrm{p}}/2$, ideally $>$100 MHz or $<$5 ns rise and fall time)

Options:

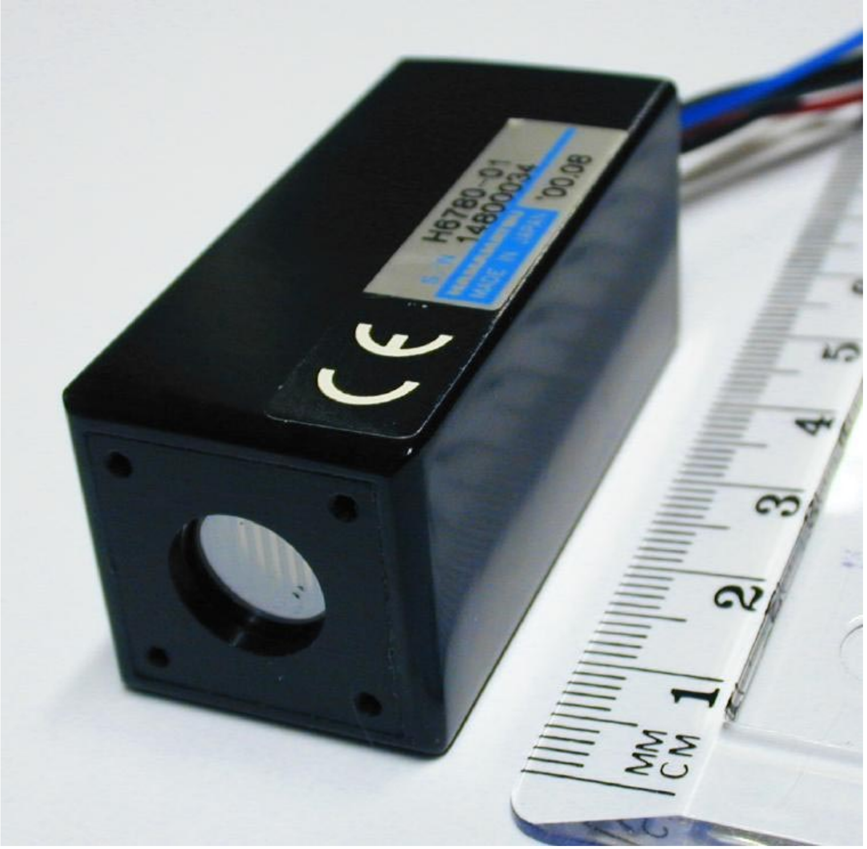
- $\longrightarrow$ PIN photodiode (typical sensitivity $0.2$–$0.6$ A/W, $\mu$s–ns)
- $\longrightarrow$ Avalanche photodiode (internal gain, typical sensitivity $10^2$ A/W, $< 1$ ns raise/fall time)
- $\longrightarrow$ Photomultiplier tube (significant internal gain, typical sensitivity $10^1$–$10^5$ A/W, $< 1$ ns raise/fall time)

# The photomultiplier tube (PMT)

Choice: Hamamatsu H6780-01 Photomultiplier tube module with integrated high-voltage circuit allows easy operation from 12 V lab power supply.

Control voltage $0.25 < U_\mathrm{c} < 0.9$ V adjusts radiant sensitivity to

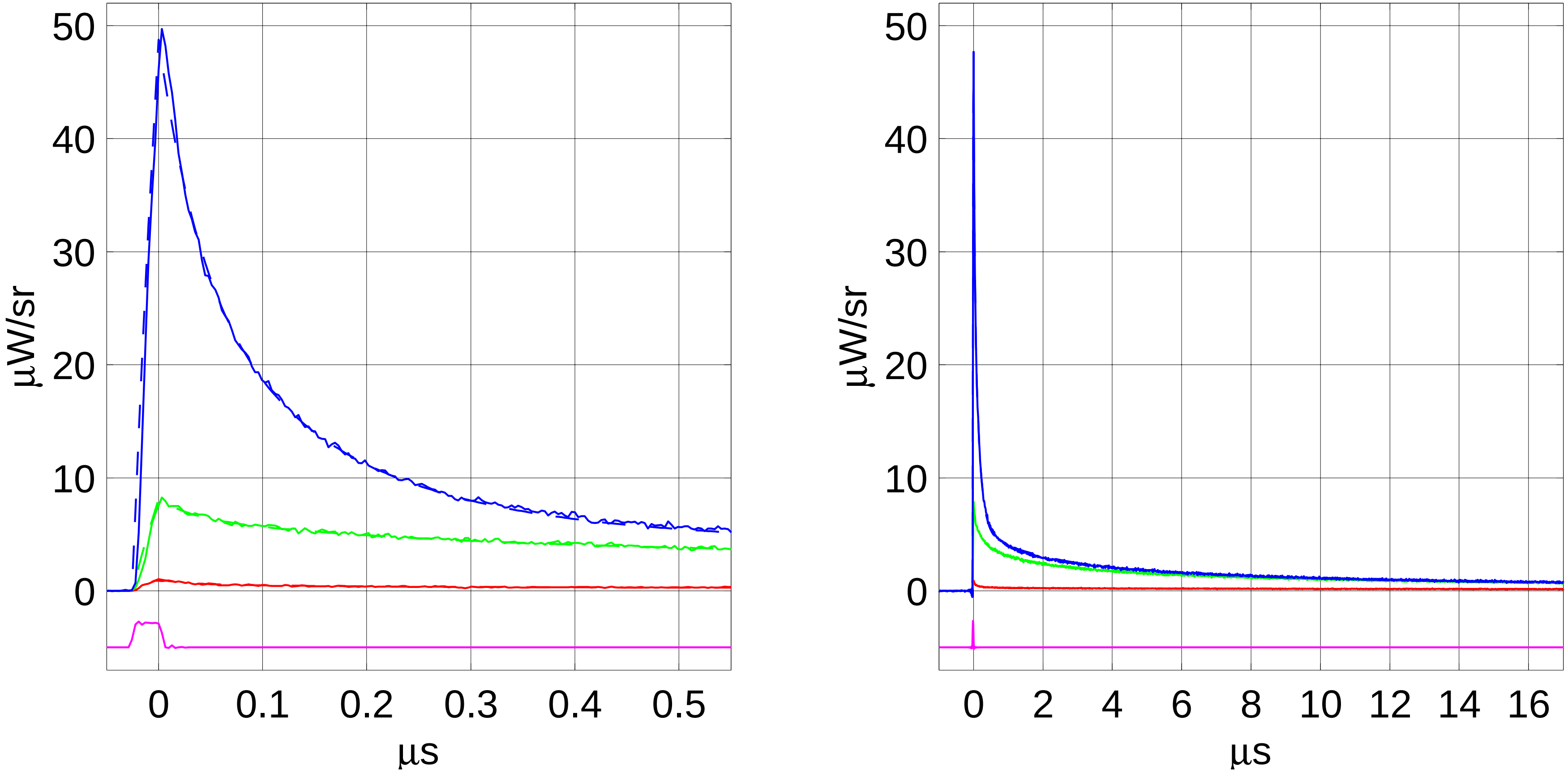
$$1.5 \times 10^5\ \mathrm{A/W} \cdot \left(\frac{U_\mathrm{c}}{1\ \mathrm{V}}\right)^{7.2}$$



Thanks to high internal gain no need for video pre-amplifier, allowing direct connection to 50 $\Omega$ DC input of digital storage oscilloscope.

# Measured P22 intensity decay curves

(a) Emission decay of a single pixel ($f_p$ = 36 MHz)



The sensor output voltage is shown here as the equivalent radiant intensity (power per solid angle) of the light source.

# Modeling phosphor impulse responses

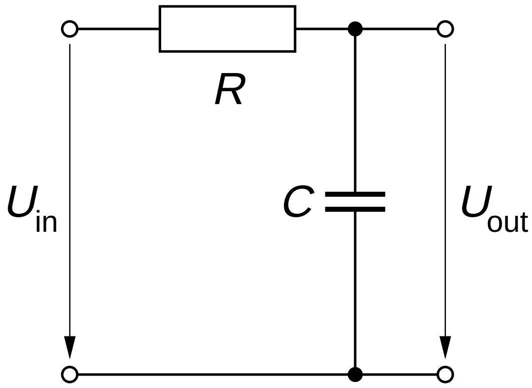
→ Exponential decay curve of a typical phosphorescent substance:

$$I_\mathrm{e}(t) = I_0 \cdot \mathrm{e}^{-\frac{t}{\tau}}$$

Note that this is for

$$\tau = \frac{1}{2\pi f} = RC$$

the impulse response of a first-order Butterworth low-pass filter.

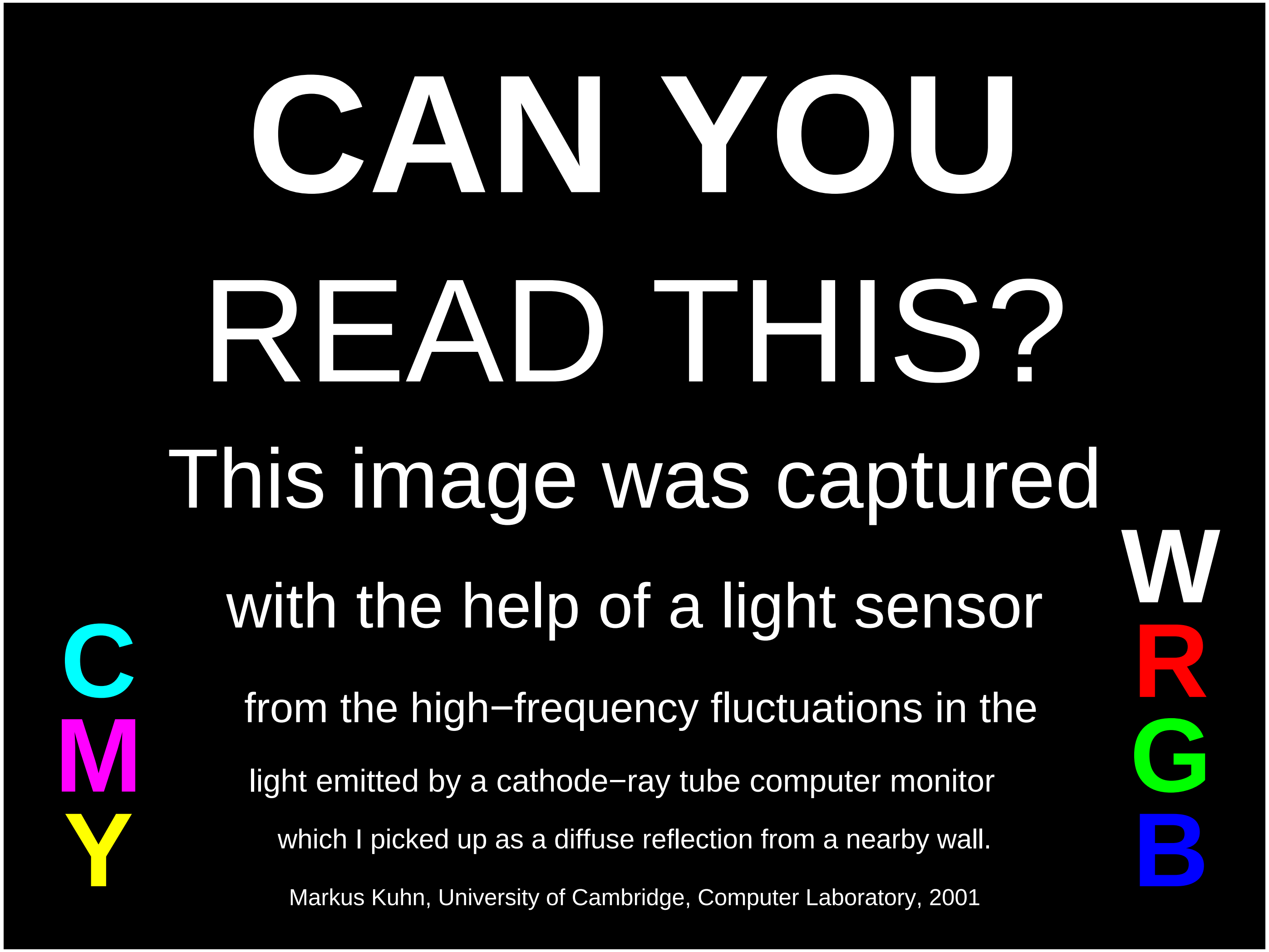


→ Power-law decay curve of zinc-sulfide based phosphors:

$$I_\mathrm{p}(t) = \frac{I_0}{(t+\alpha)^\beta}.$$

(Results in asymptotically straight line on loglog scale.)

# Test image shown on target monitor



CAN YOU

READ THIS?

This image was captured

with the help of a light sensor

from the high−frequency fluctuations in the

light emitted by a cathode−ray tube computer monitor

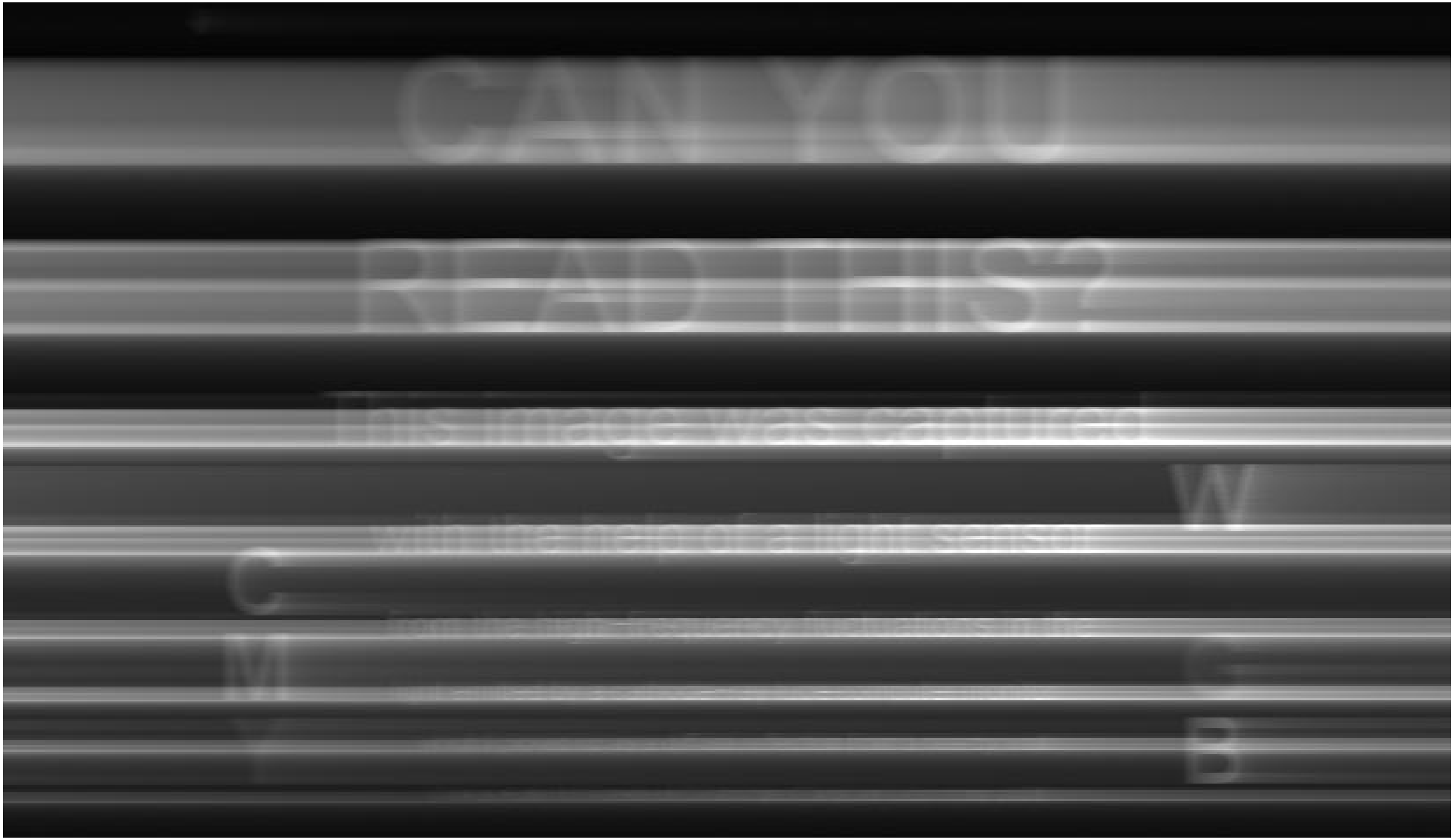
which I picked up as a diffuse reflection from a nearby wall.

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

C
M
Y

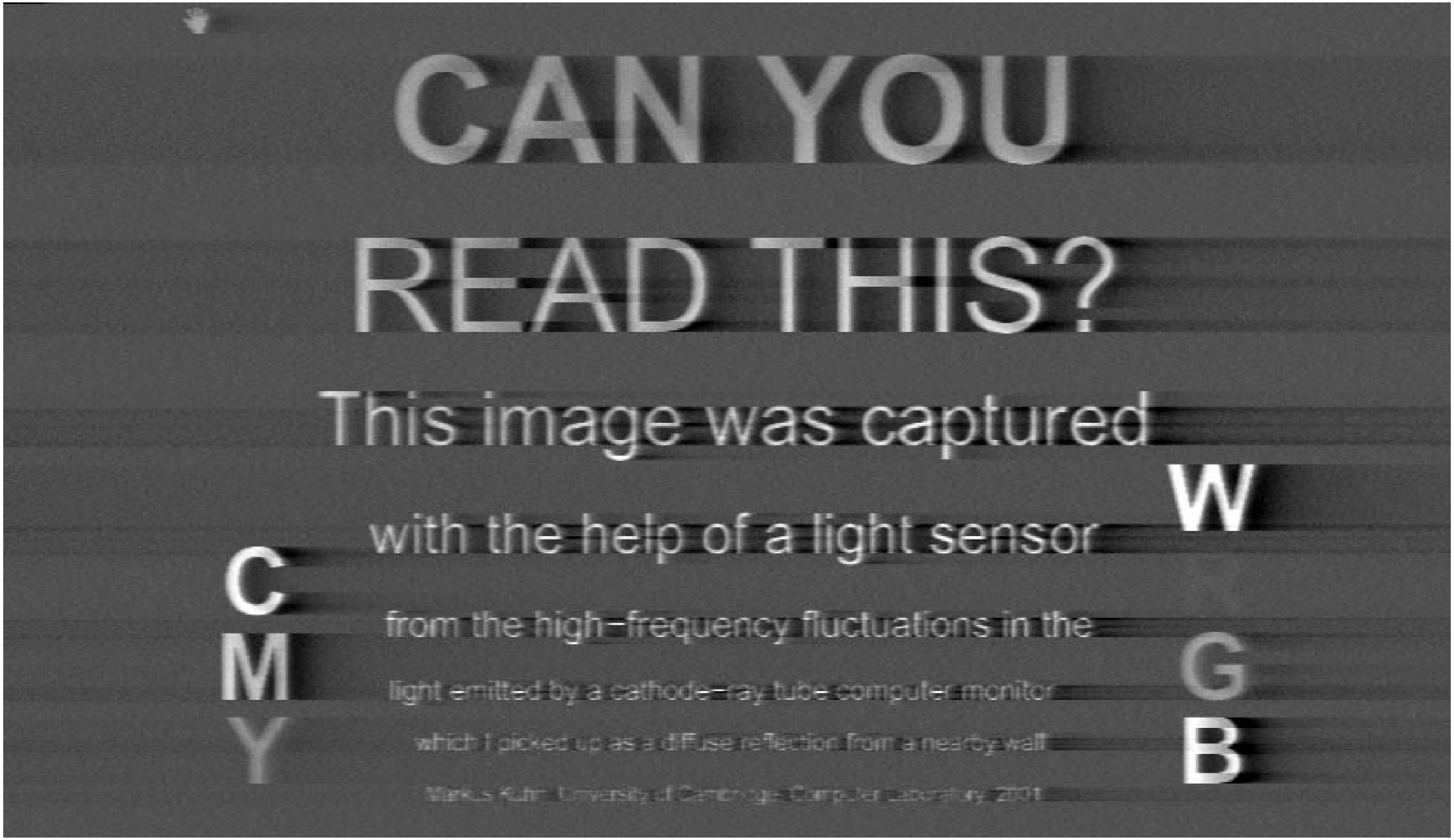
W
R
G
B

# Rasterized raw signal from PMT



VESA mode 640×480@85 Hz, 8-bit sampled at 250 MHz, 256 frames (3.0 s, 753 MB) averaged, scaled to 0.1% saturation

# High-pass filtering result



CAN YOU READ THIS?

This image was captured

with the help of a light sensor

from the high−frequency fluctuations in the

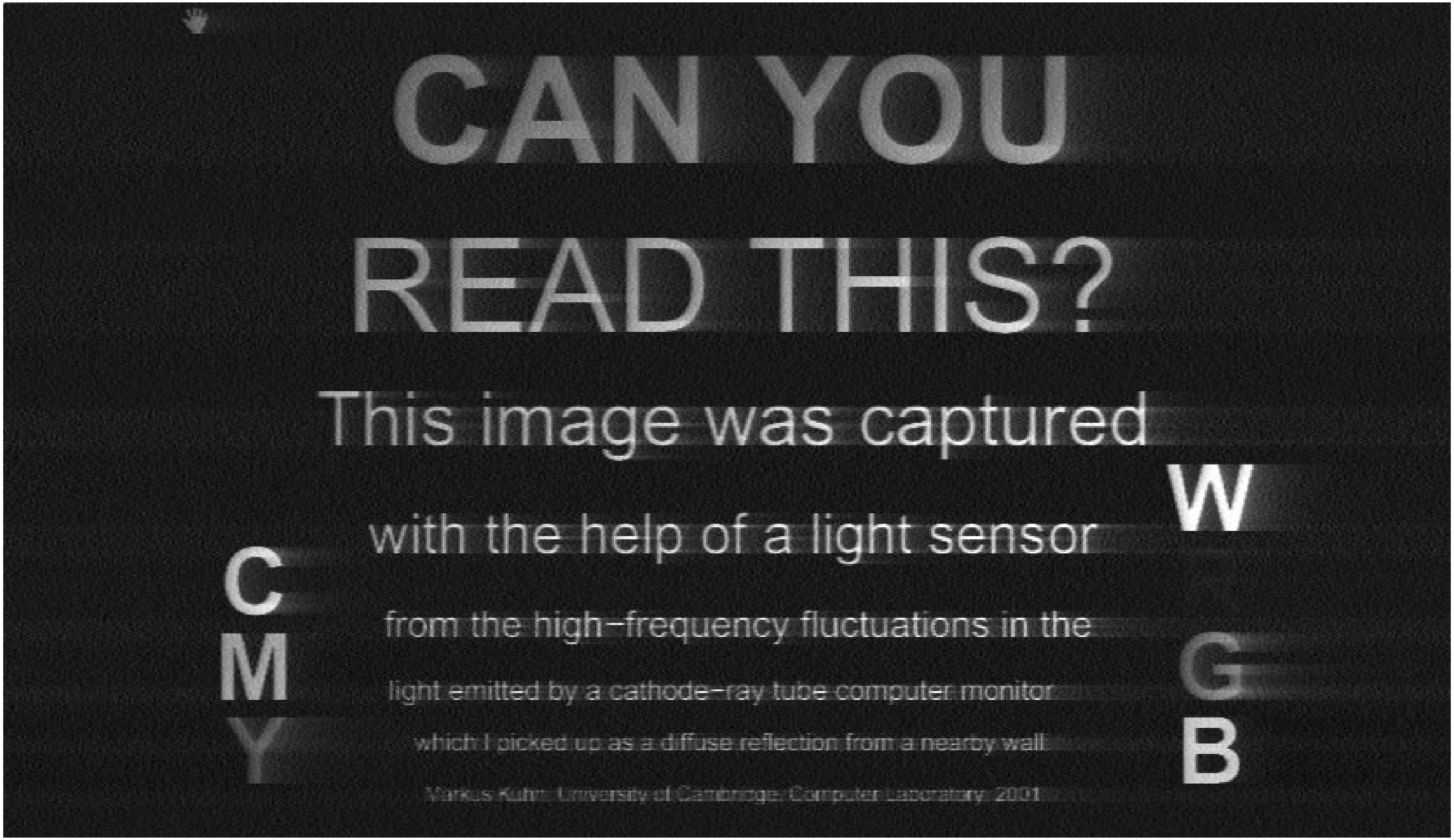
light emitted by a cathode−ray tube computer monitor

which I picked up as a diffuse reflection from a nearby wall

Markus Kuhn, University of Cambridge Computer Laboratory, 2001

First-order Butterworth high-pass filter applied, 3 dB cutoff at 4 MHz.

# Deconvolution result



CAN YOU READ THIS?

This image was captured with the help of a light sensor from the high–frequency fluctuations in the light emitted by a cathode–ray tube computer monitor which I picked up as a diffuse reflection from a nearby wall

Markus Kuhn, University of Cambridge, Computer Laboratory, 2001

# Deconvolution

We can model highly accurately the sensor signal blurred by the phosphor afterglow as the convolution of the beam current $v_\gamma$ and the impulse-response function $P_{\mathrm{P22}}$

$$I(t) = \int_0^\infty v_\gamma(t-t')\, P_{\mathrm{P22}}(t')\, \mathrm{d}t'$$

which a Fourier transform turns into a multiplication of frequency-domain signals:

$$\mathcal{F}\{I\} = \mathcal{F}\{\tilde{v}_\gamma\} \cdot \mathcal{F}\{P_{\mathrm{P22}}\}.$$

Deconvolution can be accomplished simply by division in the frequency domain, followed by an inverse FFT, leading to the shown estimate of the original beam current:

$$\tilde{v}_\gamma = \mathcal{F}^{-1}\left\{\frac{\mathcal{F}\{I\}}{\mathcal{F}\{P_{\mathrm{P22}}\}}\right\}$$

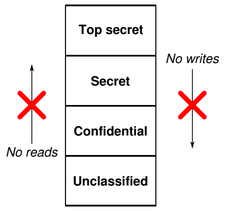
# Thermal covert channel

# Covert channels and anonymity

Steven J. Murdoch

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group

## Covert channels

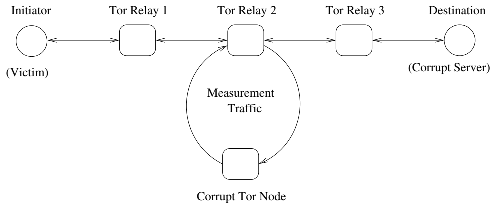


When military and intelligence organisations computerised their operation, they were concerned that confidential data might leak out. To reduce this risk, they required that computers enforce their existing document handling rules. In the simplest case, files are classified as either *top secret*, *secret*, *confidential* or *unclassified*. Users are assigned to levels and the operating system forbids *reading* information above a user's clearance. The system also prevents *writing* information from a high-level file to a lower-level one.

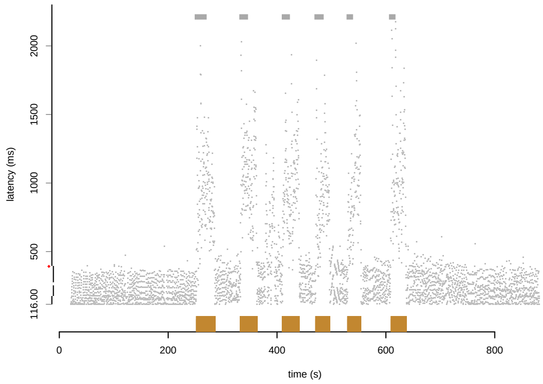
Normal storage and communication mechanisms, such as files and networks, can be made to respect these restrictions. But there are other ways to transmit information that the system designer might not have considered, called *covert channels*. For example, a high-level program could send data by changing its CPU usage while a low-level one observes CPU load to recover the data.

## Attacking Tor

Covert channels can be used to learn along which path messages are sent through the anonymising network Tor. Here, the attacker operates a webserver (corrupt server) that the user (victim) is accessing. The webserver inserts a distinctive load pattern into the network, and a second server (corrupt Tor node), controlled by the attacker, measures the performance of each Tor relay in turn:

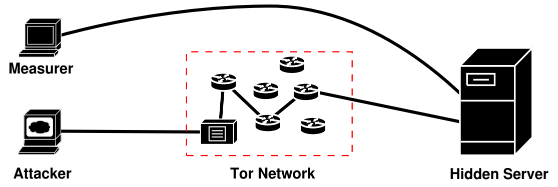


When the corrupt Tor node connects to one of the Tor relays carrying the victim's traffic, the attacker will see the pattern, and so learns that the path goes through the node being measured.

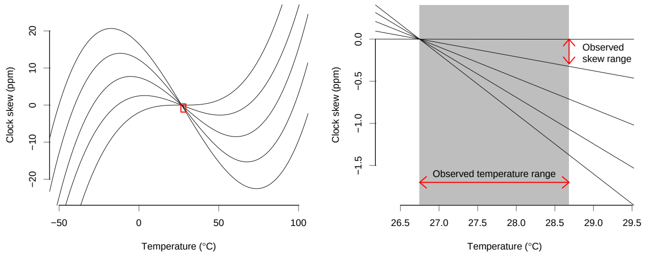


## CPU temperature as a covert channel

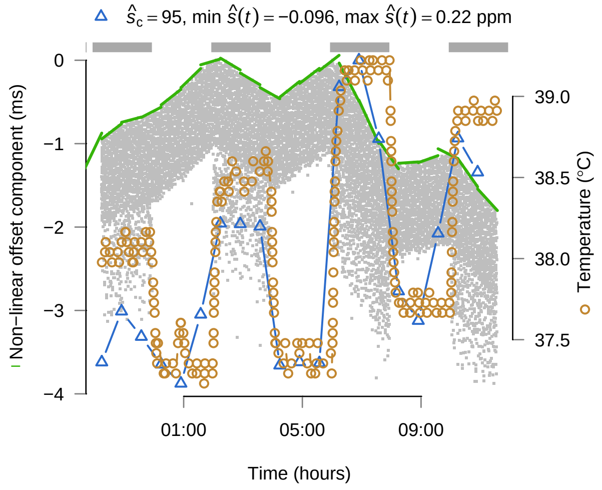
In addition to anonymous web browsing, Tor allows users to run servers without giving away their identity. To find out who is operating a particular hidden server, an attacker could increase its CPU load by connecting through the Tor network, while simultaneously connecting to each hidden server directly and measuring load:



The frequency of clock crystals, as used in computers for measuring time, varies with temperature. As the load of a computer increases, the temperature will too, so by remotely measuring changes in clock frequency, the CPU load of a system can be estimated, even if it cannot be measured directly.



If the attacker can see a match between the load pattern induced and the clock frequency, he knows that the correct hidden server has been found. In the graph below, the grey bars show the load pattern, the brown circles show the temperature and the blue triangles the clock frequency. The load pattern can be seen to alter the clock frequency, so here the attacker has identified the server.



For more information see `http://www.cl.cam.ac.uk/users/sjm217/projects/anon/`

2006-07-06