# When Organized Crime Applies Academic Results
# A Forensic Analysis of an In-Card Listening Device

Houda Ferradi
Information Security Group
Ecole Normale Supérieure

# Goal of This Presentation

- Illustrate to what length white collar criminals can go to hack embedded electronic devices.

- To date, the following is the most sophisticated smart card fraud encountered in the field.

**Goal: raise awareness to the level of resistance that IoT devices must have to resist real attacks in the field.**

# Context

A forensic assignments.

# Context

**In May 2011:** The French's bankers Economic Interest Group (GIE Cartes Bancaires) noted that a dozen EMV cards, stolen in France a few months before, were being used in Belgium.

The net loss caused by this fraud is estimated to stand below 600,000€, stolen over 7,000 transactions using 40 modified cards.

A forensic investigation was hence ordered by Justice

# The Judicial Seizure

# The Judicial Seizure

- What appears as an ISO/IEC 7816 smart card.
- The plastic body indicates that this is a VISA card issued by Caisse d'Épargne (a French bank).
- Embossed details are:
  - PAN5= 4978**********89;
  - expiry date in 2013;
  - and a cardholder name, hereafter abridged as P.S.
  - The forgery's backside shows a normally looking CVV.
- PAN corresponds to a Caisse d'Épargne VISA card.

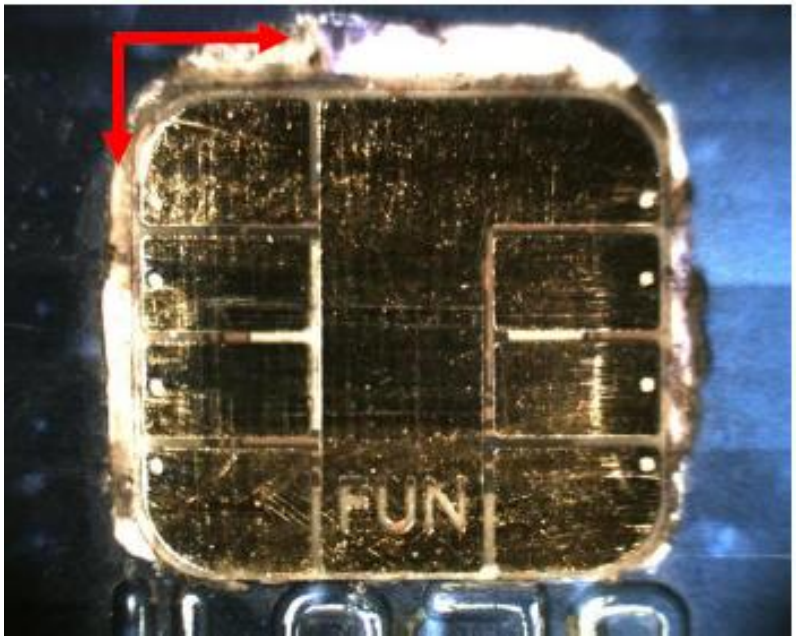
PAN=Permanent Account Number (partially anonymized here).
CVV=Card Verification Value.

# Visual Inspection

The backside is deformed around the chip area.

Such a deformation is typically caused by heating.
Heating (around 80°C) allows melting the potting glue to detach the card module.

# Visual Inspection




The module looks unusual in two ways:

1) it is engraved with the inscription "FUN";

2) glue traces (in red) clearly show that a foreign module was implanted to replace the **89 card's original chip

# FUNCards

Home

Kanda Blog

All Chips ICs and Modules

Smart Cards

Starter Kits Programmers Debugging Chips.ICs.Modules Training PC Interf

**Selected Category and Product:**

Chips ICs and Modules » Smart Cards » SC-YELLOW

Secure Payment by Bank Transfer VISA VISA Maestro MasterCard VISA PayPal

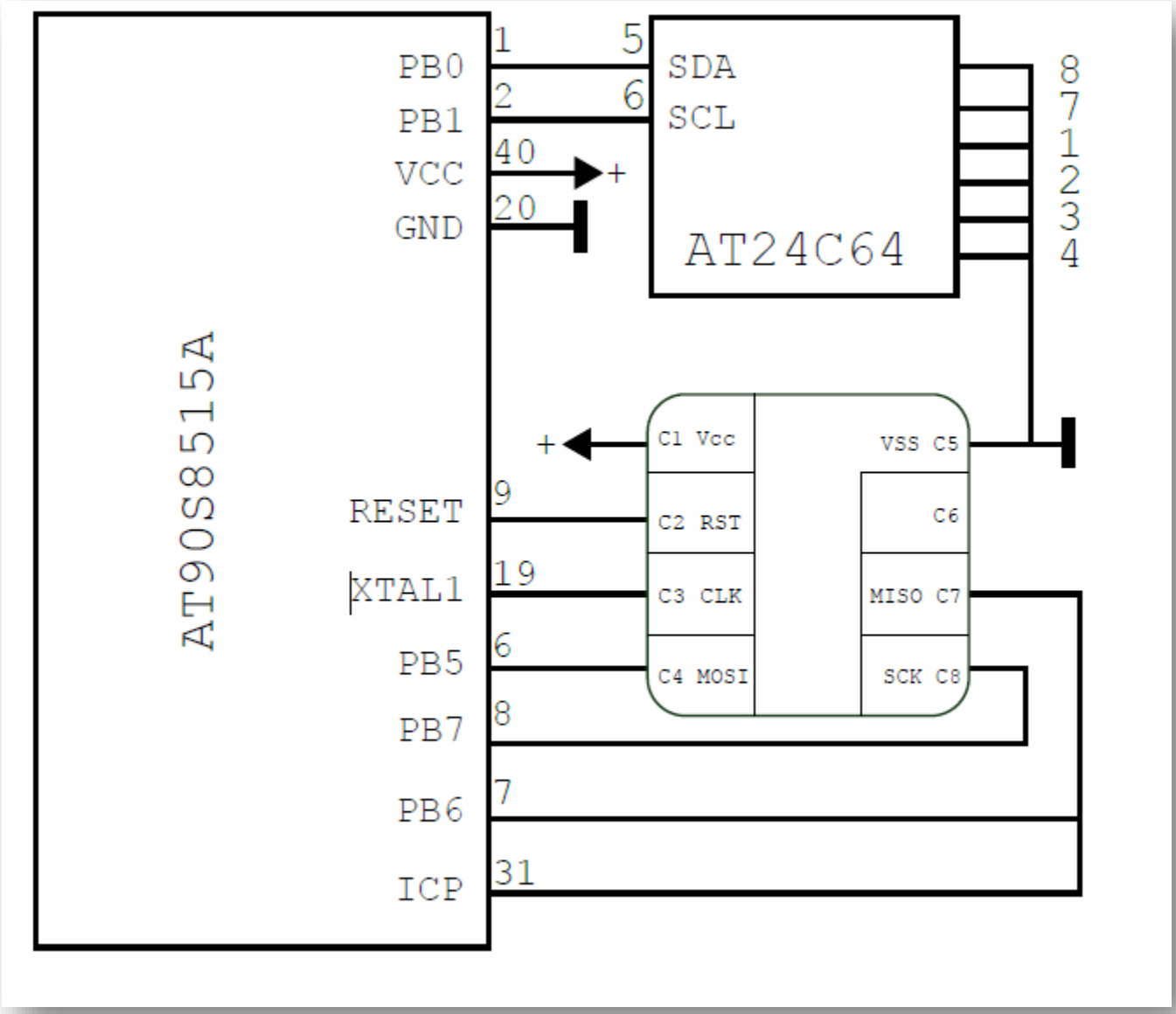
**Yellow Smart Card**

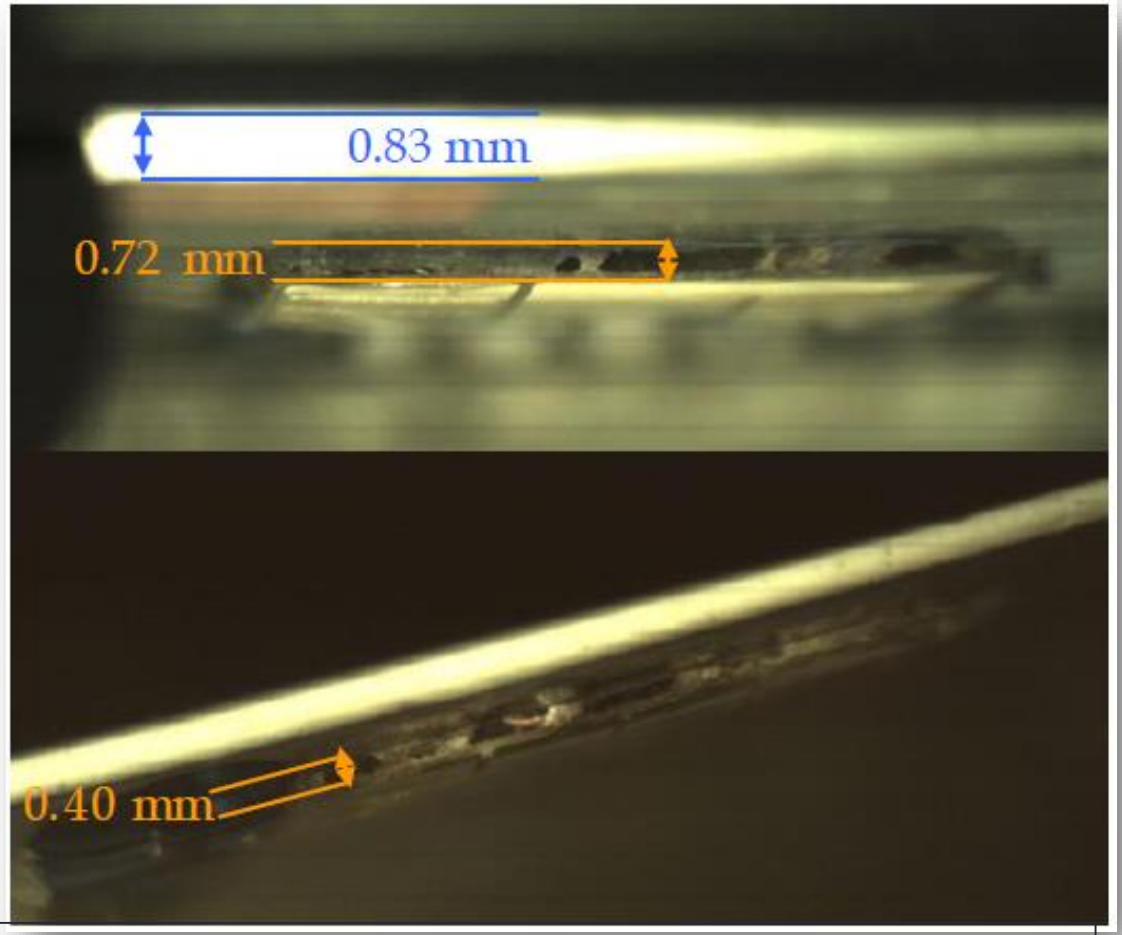
**Yellow Smart Card**
**The Smart Card YELLOW, also known as a Funcard 4, is a field programmable, ISO-7816-1 pin-out compatible multi-chip Smart Card featuring the ATMEL ATmega8515 + 24C64 die.**

Product Details

Shipping to France
Recorded Airmail: €8.95
Express: €19.00

# FUNCard's Inner Schematics



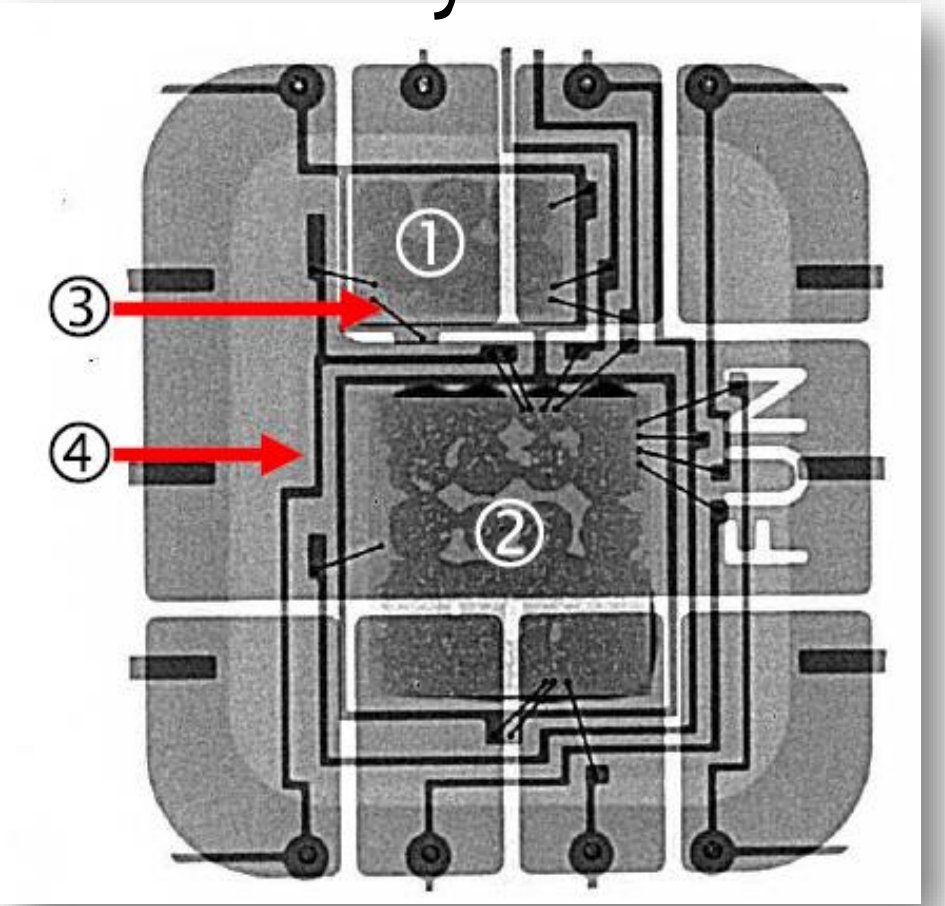


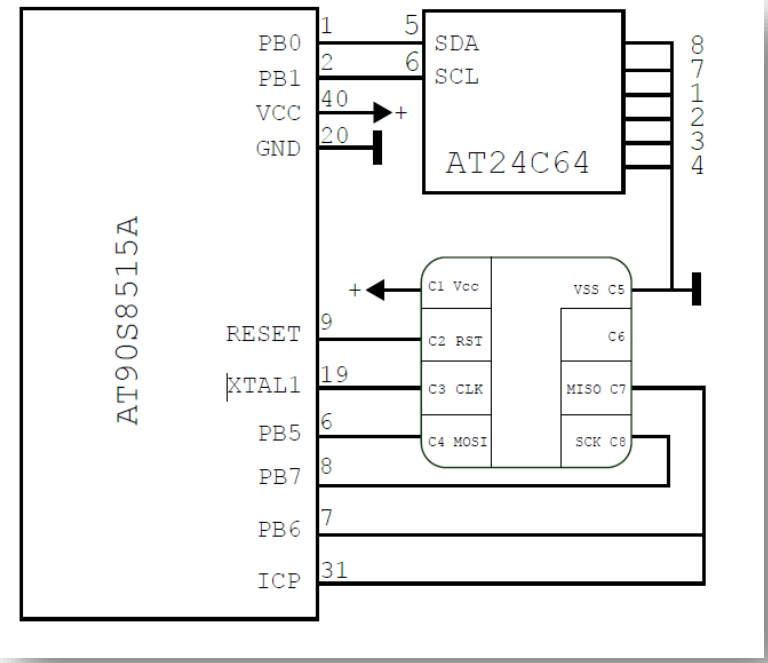

Side-views show that forgery is somewhat thicker than a standard card (0.83mm).

Extra thickness varies from 0.4 to 0.7mm suggesting the existence of more components under the card module, besides the FUNcard.

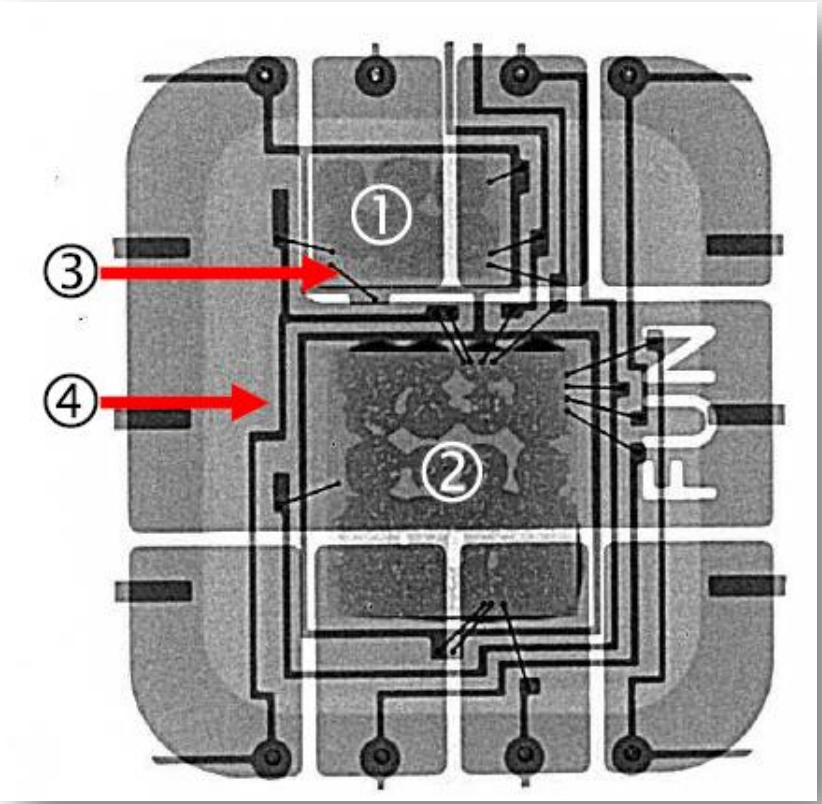
# FUNCard Under X-Ray

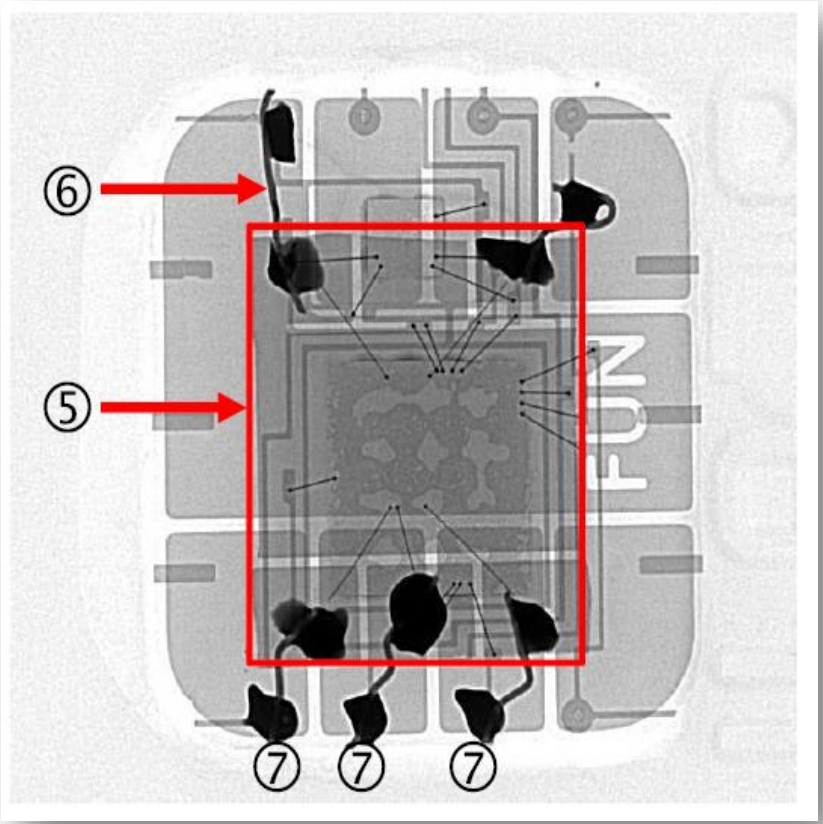
① External memory (AT24C64)
② μ-controller (AT90S85515A)
③ Connection wires
④ Connection grid



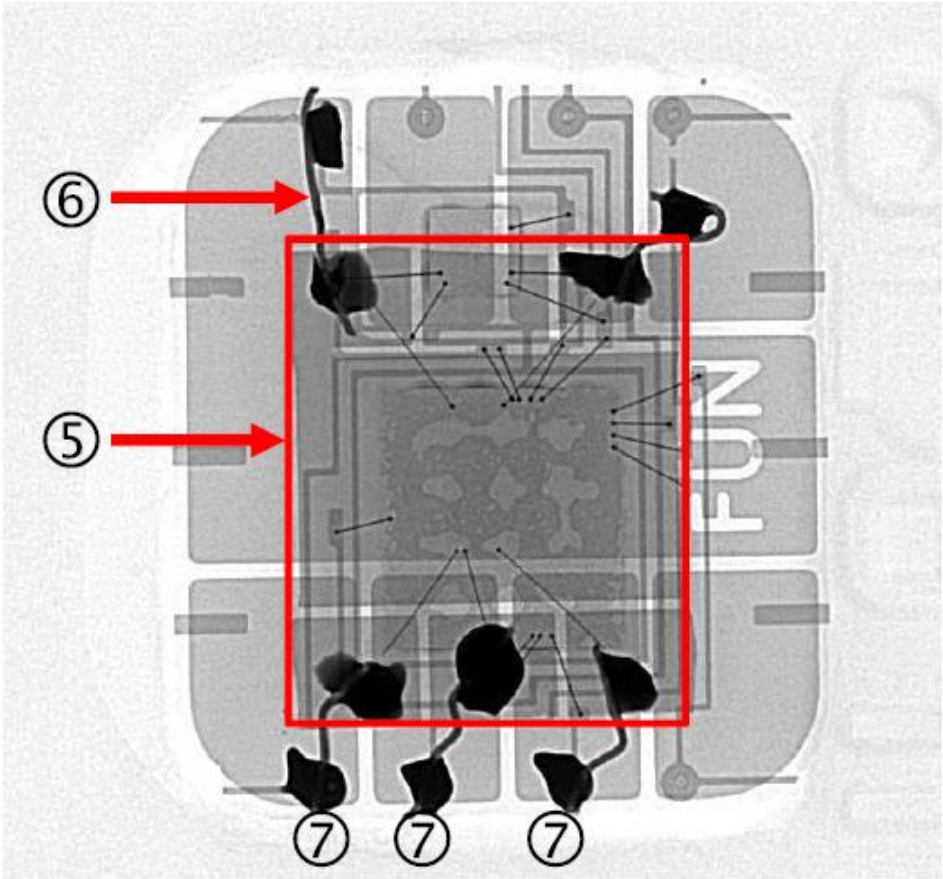



# FunCard vs. Forgery under X-Ray



# Forgery vs. FunCard




⑤ Stolen card module

⑥ Connection wires added by fraudster

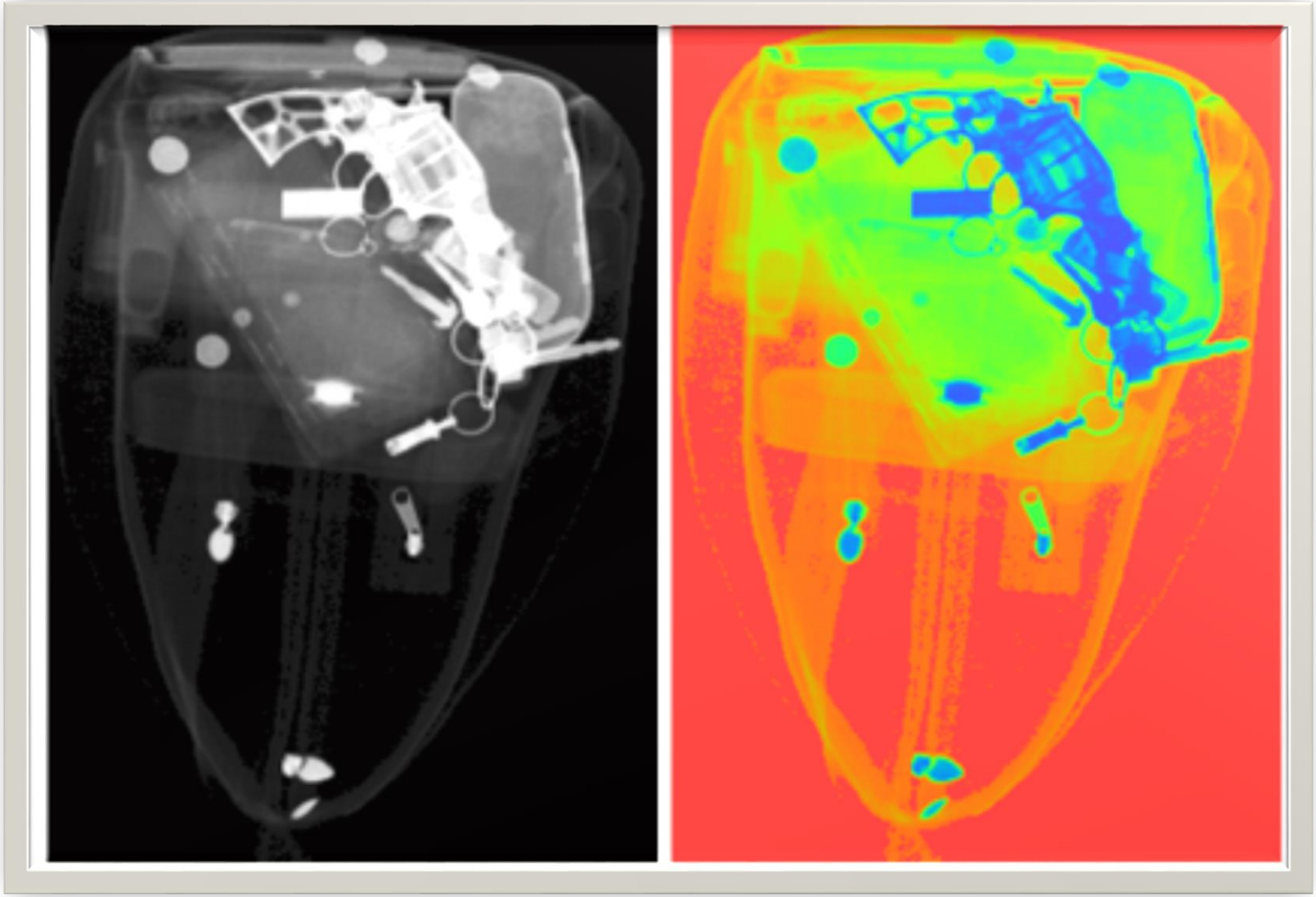
⑦ Welding points added by the fraudster

# Pseudo-Color Analysis

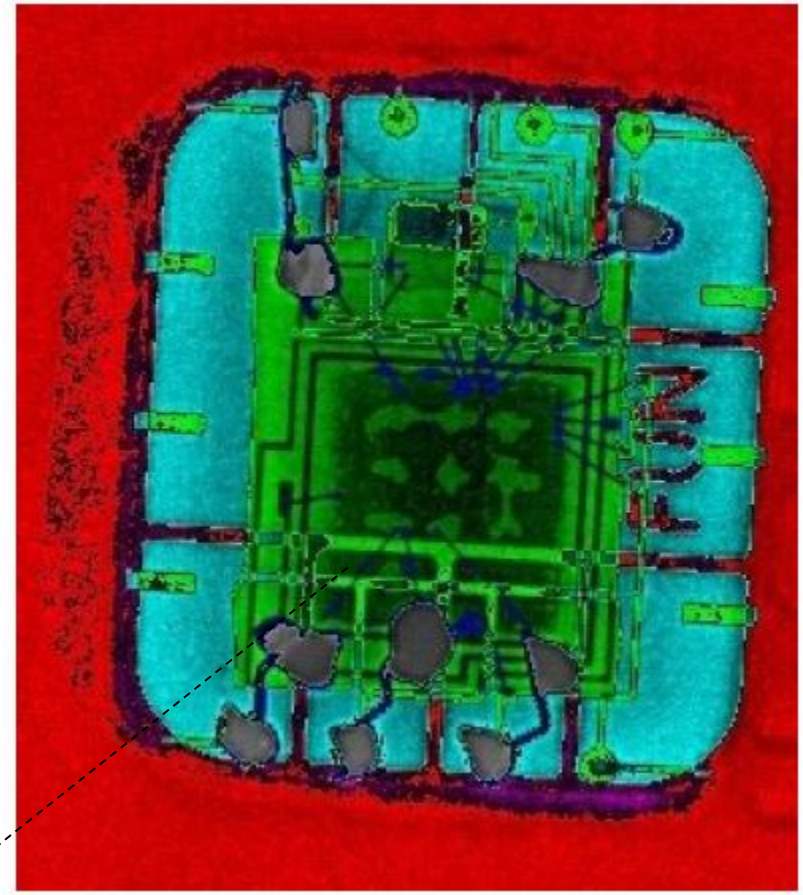
Definition: Materials may have the same color in the visible region of the EM spectrum and thus be indistinguishable to the Human eye. However, these materials may have different *properties* in other EM spectrum parts. The reflectance or transmittance spectra of these materials may be similar in the visible region, but ***differ in other regions.***

Pseudo-coloring uses information included in the near-infrared region (NIR) i.e. 800-1000nm to discriminate materials beyond the visible region.

# Pseudo-Color Analysis

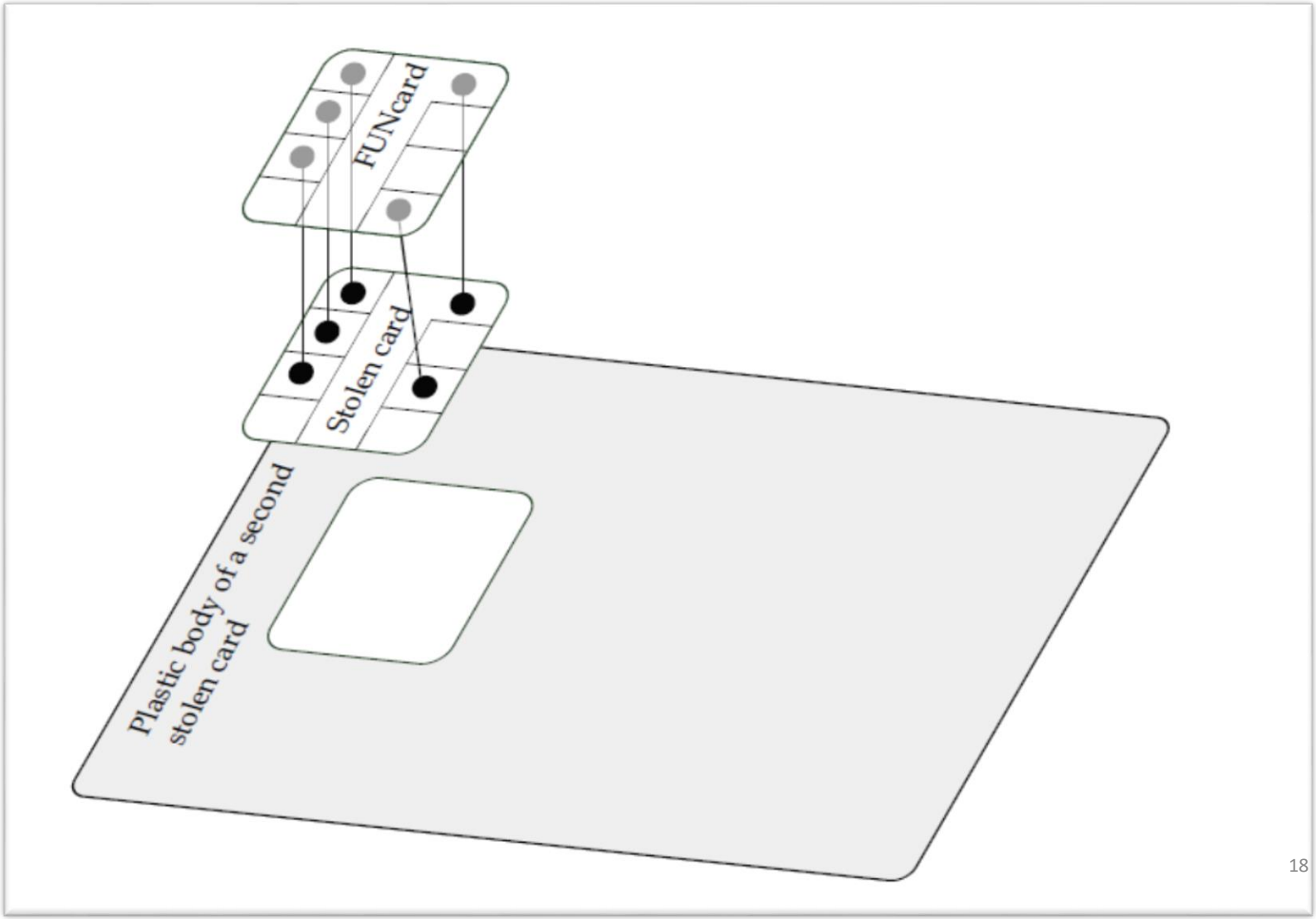


# Pseudo-Color Analysis

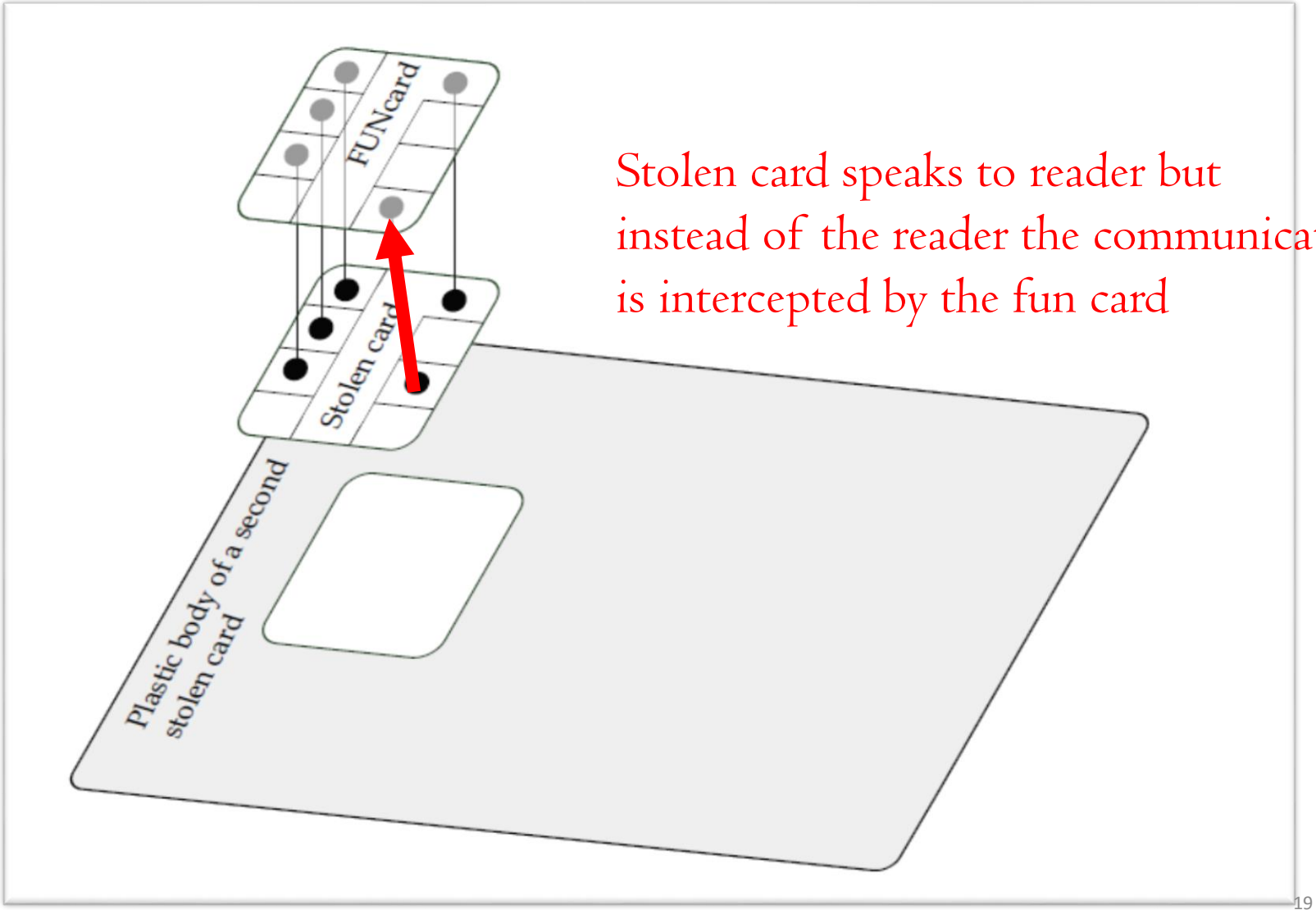


Stolen chip

# Forgery Structure Suggested so Far

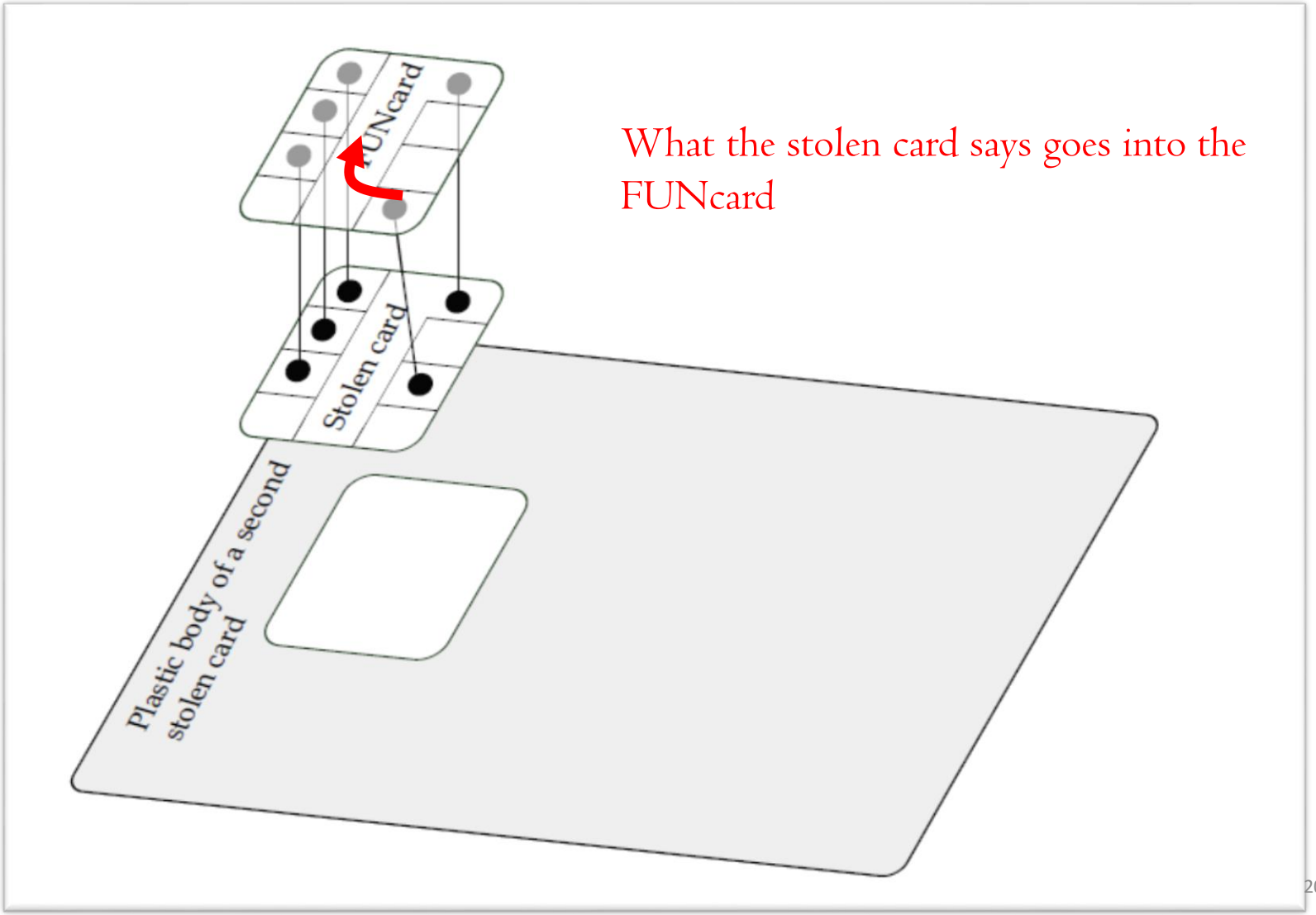


# Forgery Structure Suggested so Far

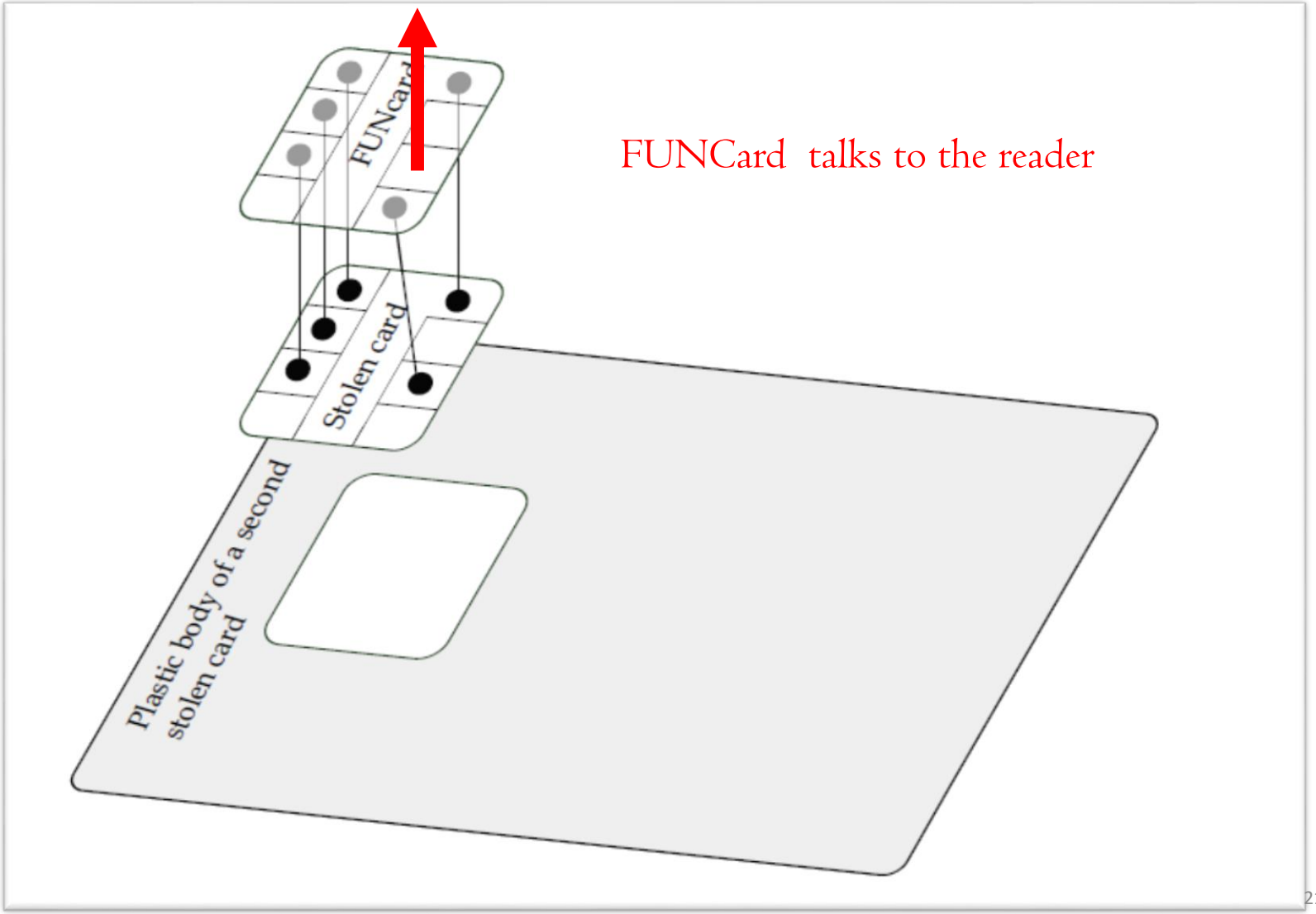



Stolen card speaks to reader but instead of the reader the communication is intercepted by the fun card

# Forgery Structure Suggested so Far



# Forgery Structure Suggested so Far



# Electronic Analysis Attempt

It is possible to read-back FunCard code if the card is not locked.

Attempted read-back failed. Device locked.

Anti-forensic protection by fraudster.

# Magnetic Stripe Analysis

The magnetic stripe was read and decoded.

ISO1 and ISO2 tracks perfectly agree with embossed data.

ISO3 is empty, as is usual for European cards.

# Electronic Information Query

Data exchanges between the forgery and the PoS were monitored.

- The forgery responded with the following information:
- PAN = 4561**********79;
- expiry date in 2011;
- cardholder name henceforth referred to as H.D.

All this information is in blatant contradiction with data embossed on the card.

The forgery is hence a combination of two genuine cards

# Flashback 2010

2010 IEEE Symposium on Security and Privacy

## Chip and PIN is Broken

Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond
*University of Cambridge*
*Computer Laboratory*
*Cambridge, UK*
*http://www.cl.cam.ac.uk/users/{sjm217,sd410,rja14,mkb23}*

***Abstract*—EMV is the dominant protocol used for smart card payments worldwide, with over 730 million cards in circulation. Known to bank customers as "Chip and PIN", it is used in Europe; it is being introduced in Canada; and there is pressure from banks to introduce it in the USA too. EMV secures credit and debit card transactions by authenticating both the card and the customer presenting it through a combination of cryptographic authentication codes, digital signatures, and the entry of a PIN. In this paper we describe and demonstrate a protocol flaw which allows criminals to use a genuine card to make a payment without knowing the card's PIN, and to remain undetected even when the merchant has an online connection to the banking network. The fraudster performs a man-in-the-middle attack to trick the terminal into believing the PIN verified correctly, while telling the card that no PIN was entered at all. The paper considers how the flaws arose, why they remained unknown despite EMV's wide deployment for the best part of a decade, and how they might be fixed. Because we have found and validated a practical attack against the core functionality of EMV, we conclude that the protocol**

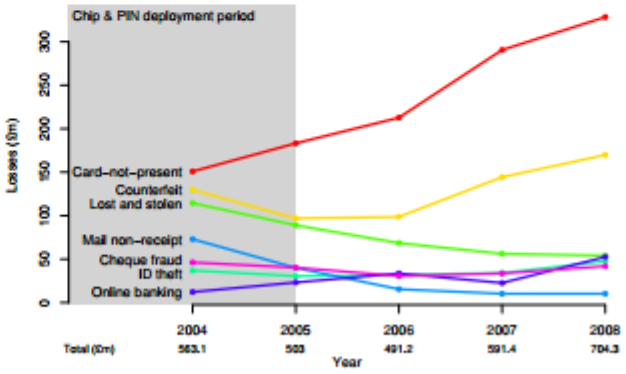
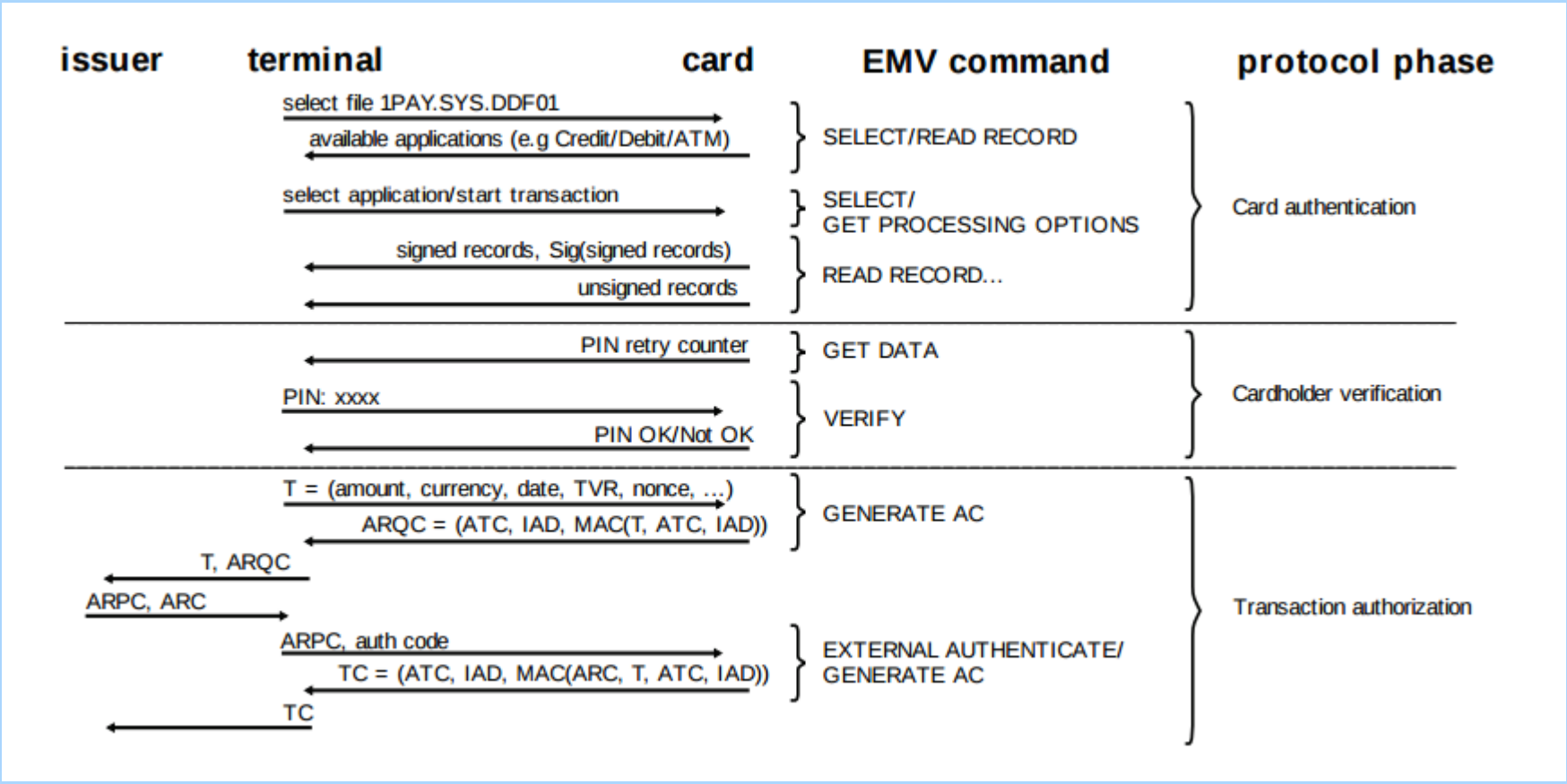
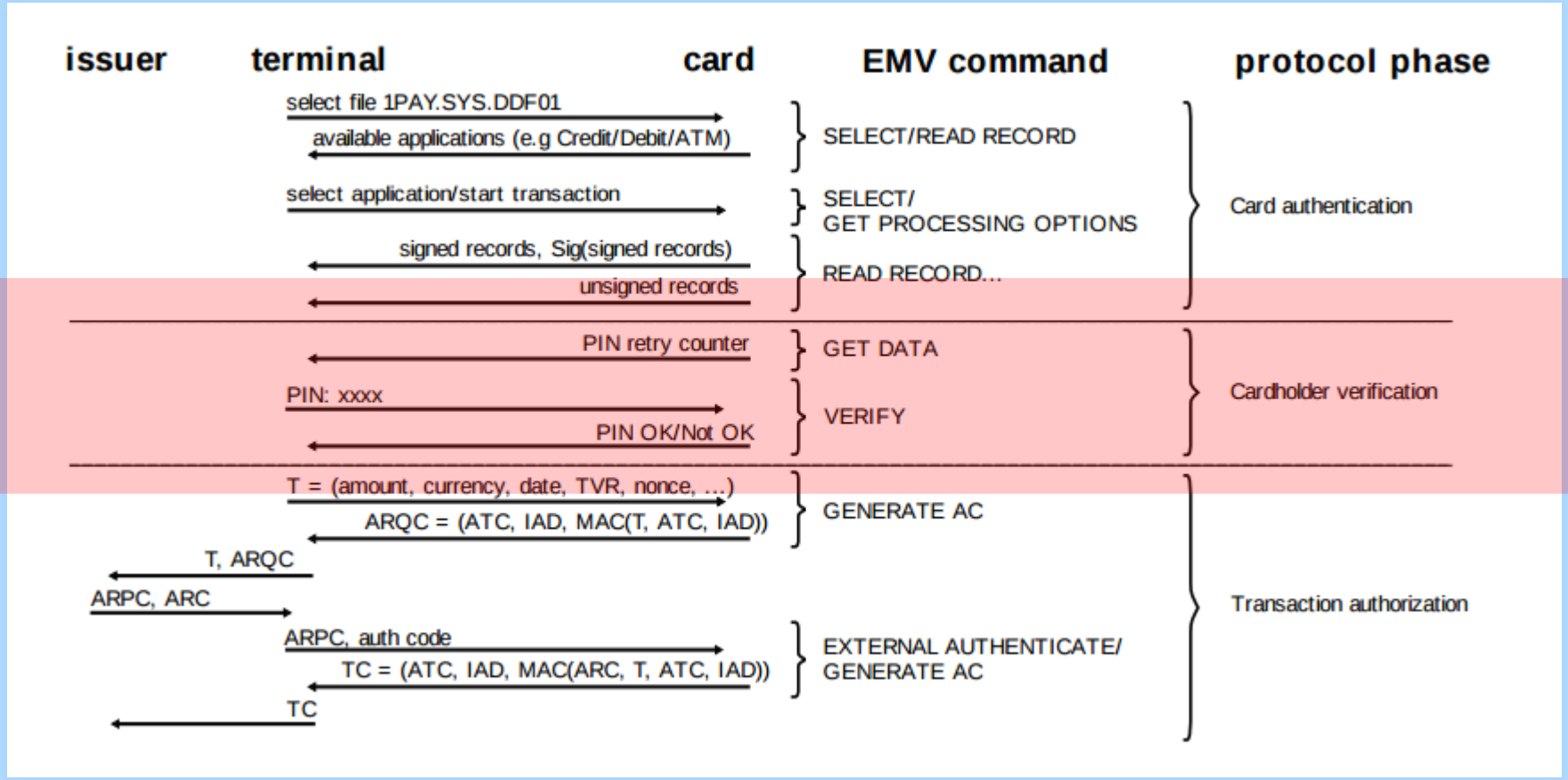



Figure 1. Fraud statistics on UK-issued cards [6]

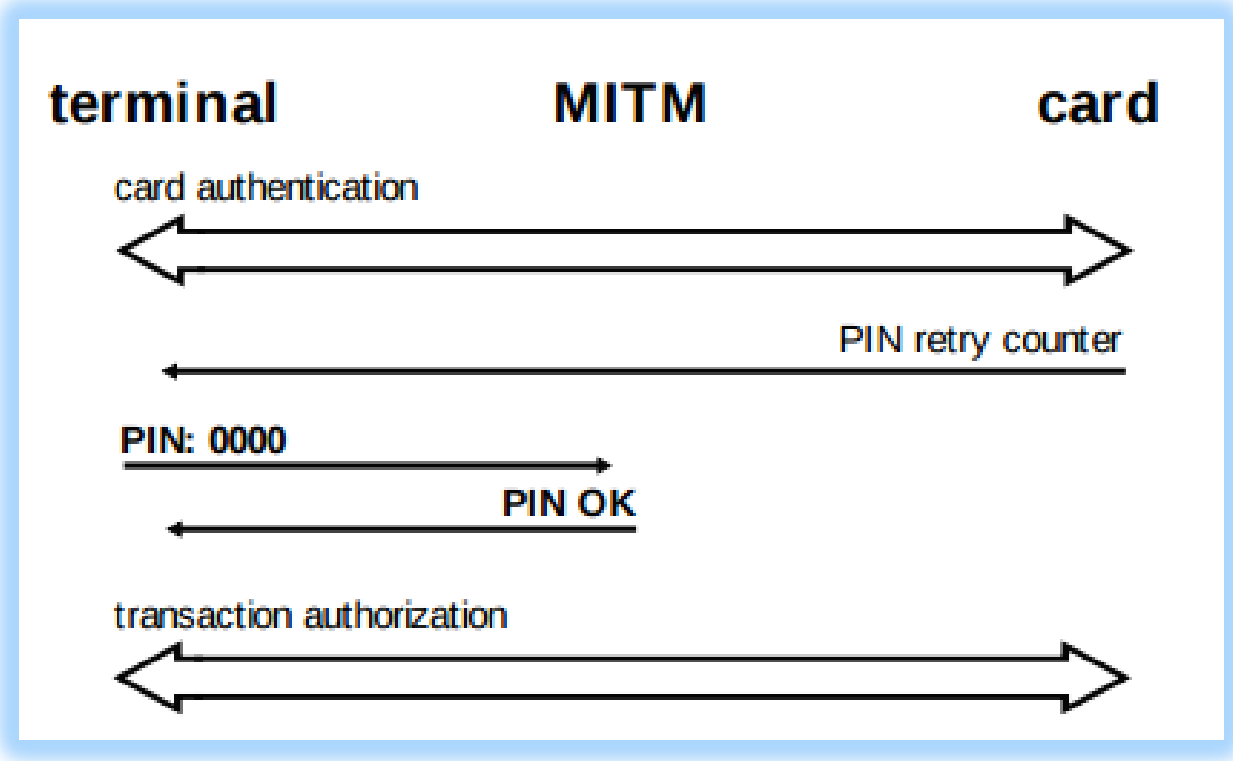
# Flashback 2010



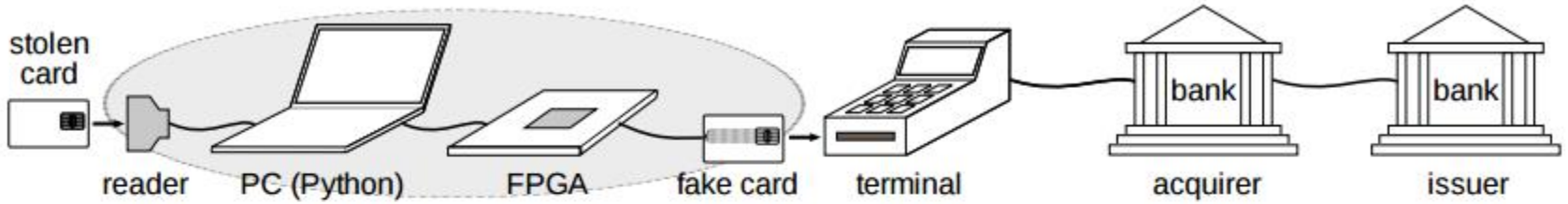
# The problem is here!



# Flashback 2010



# Flashback 2010




# Flashback 2010

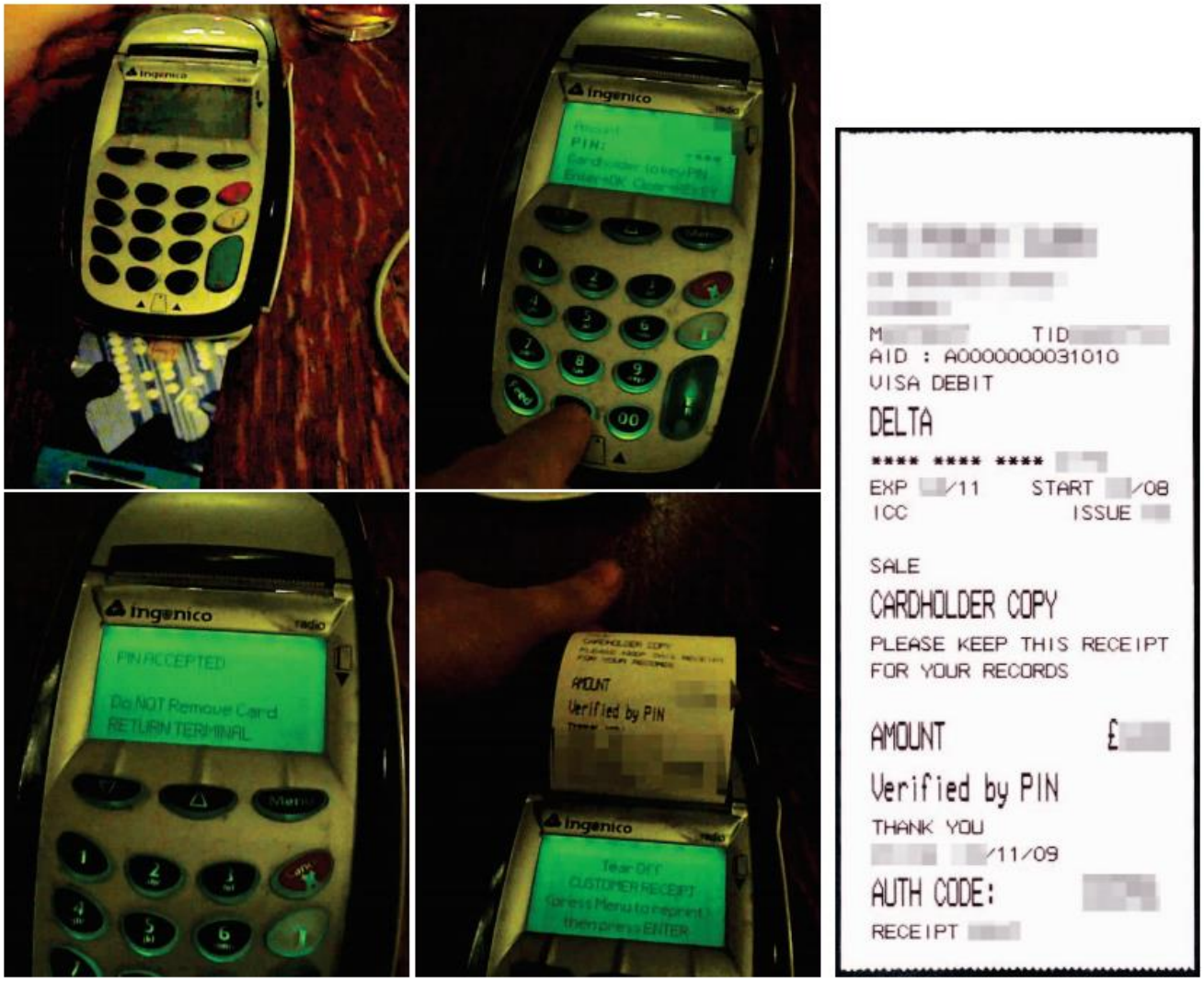
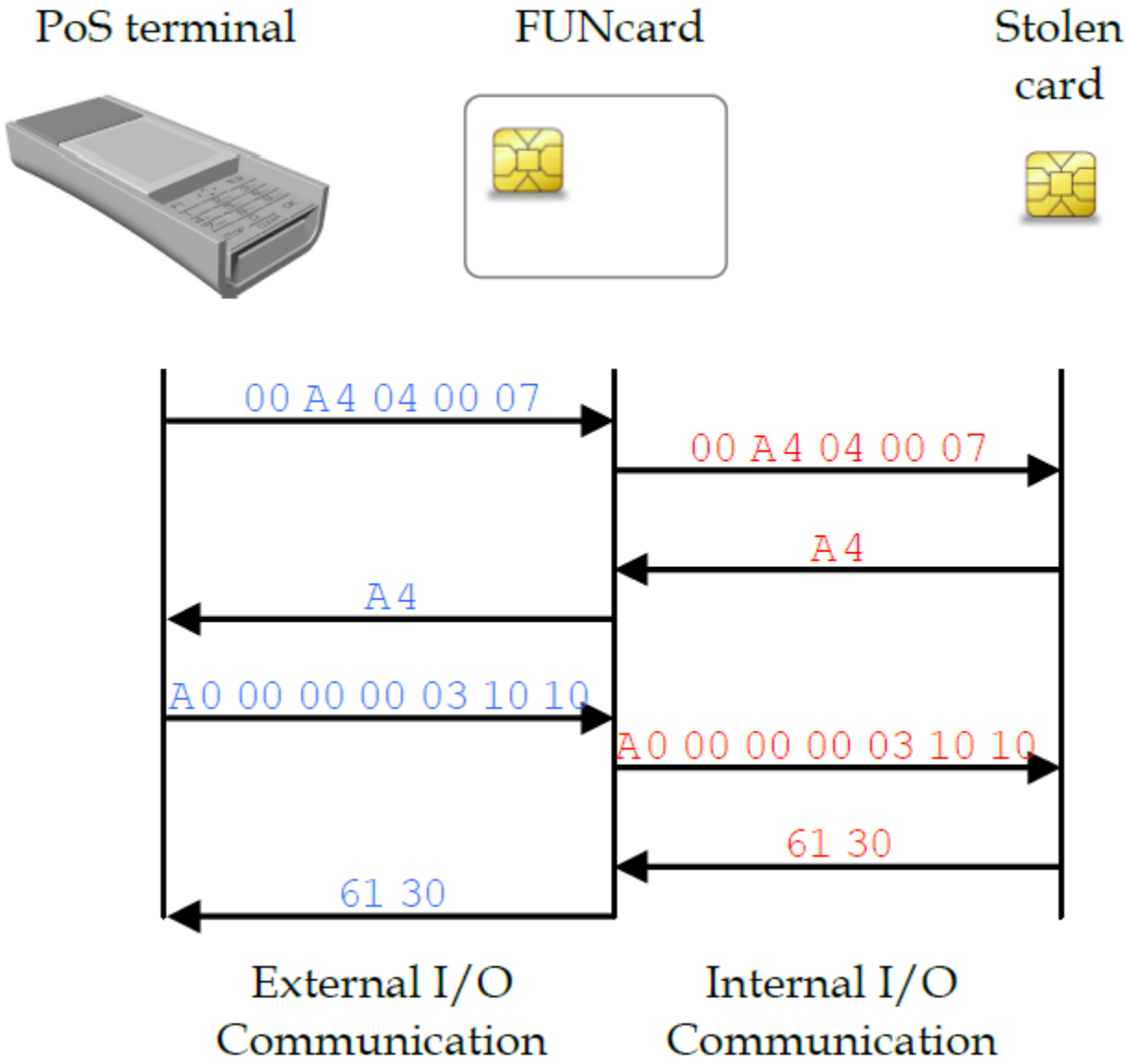
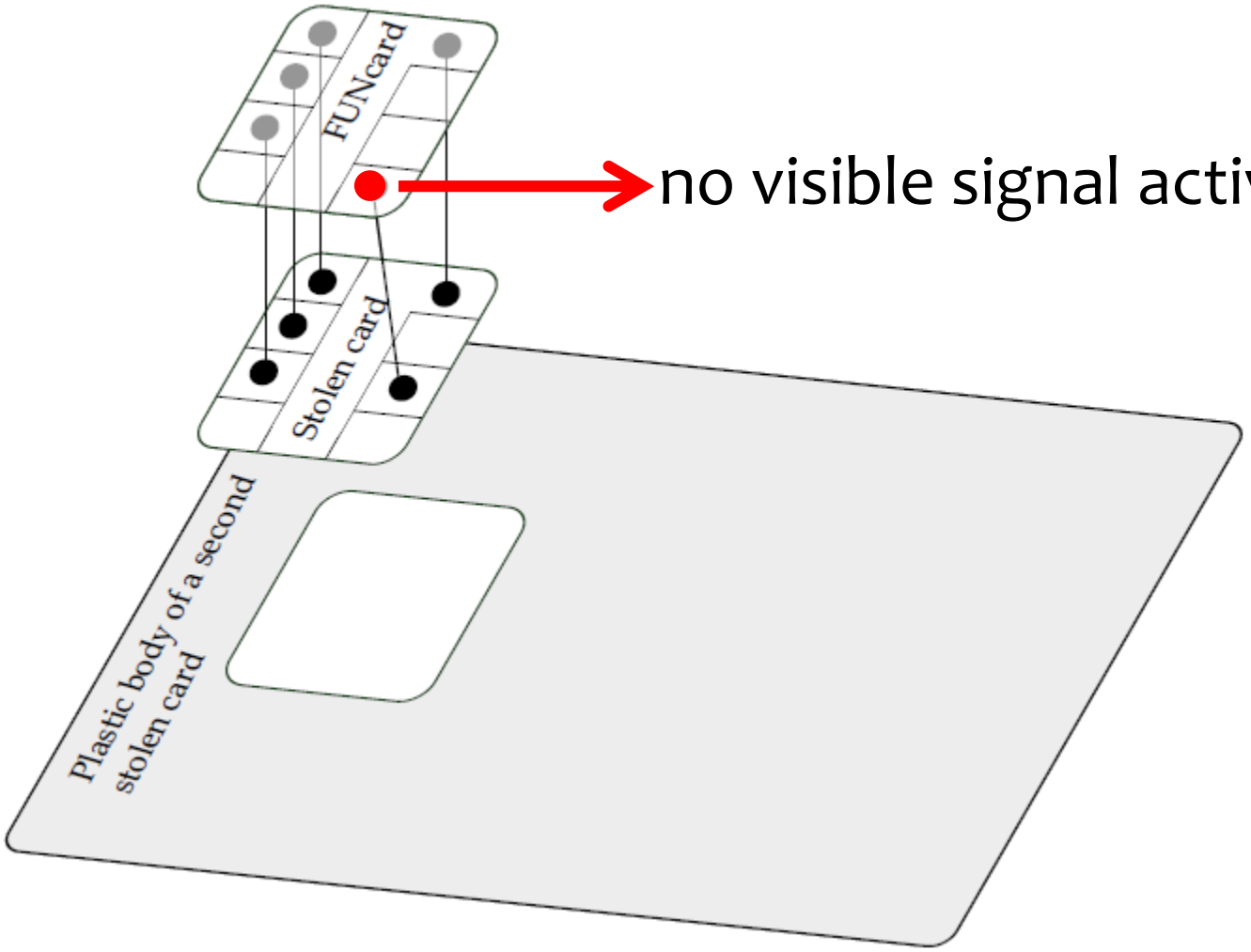



Figure 5. Carrying out the attack. Although we entered the wrong PIN, the receipt indicates that the transaction was "Verified by PIN".

# Modus Operandi Hypothesis

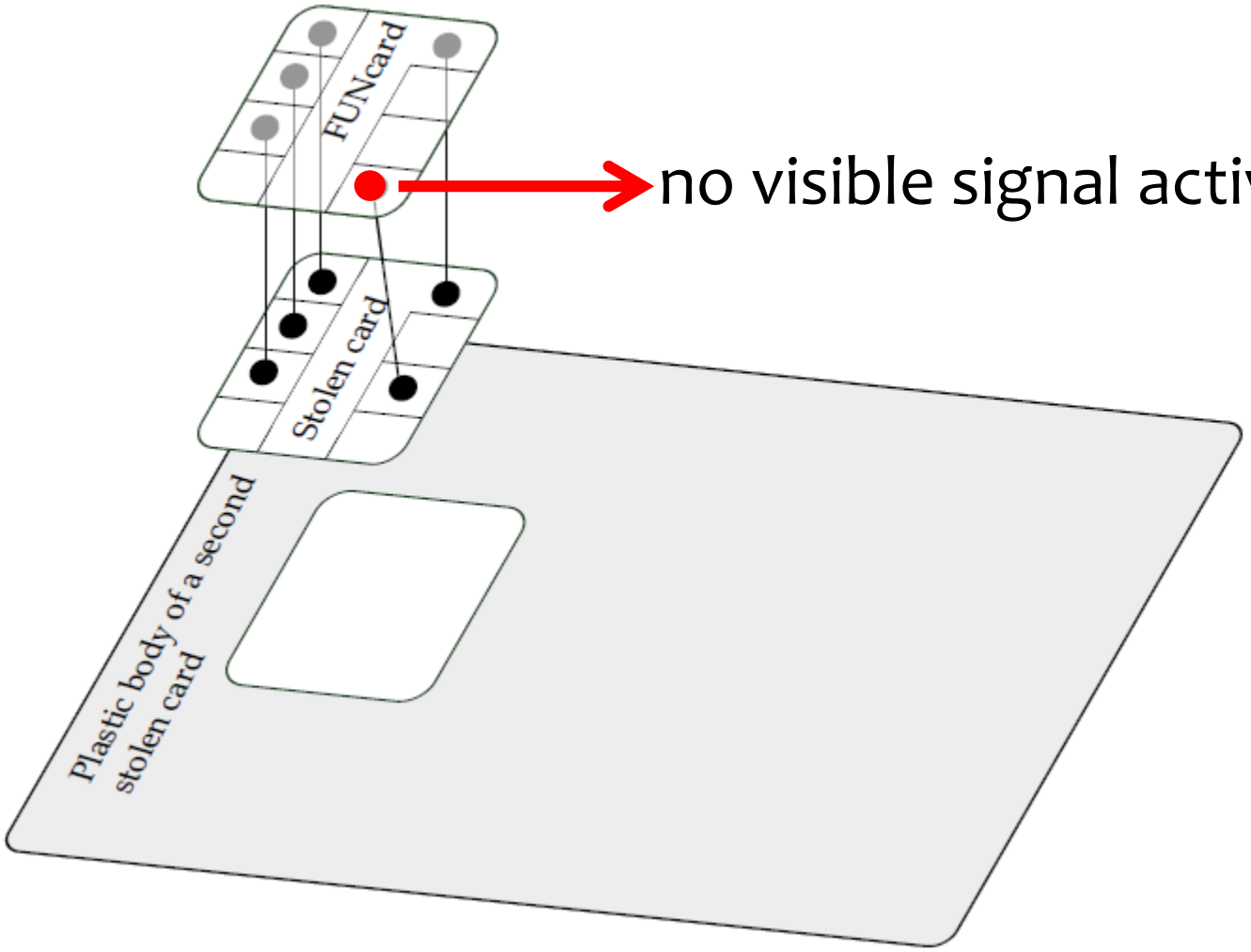


# Problem with Hypothesis!

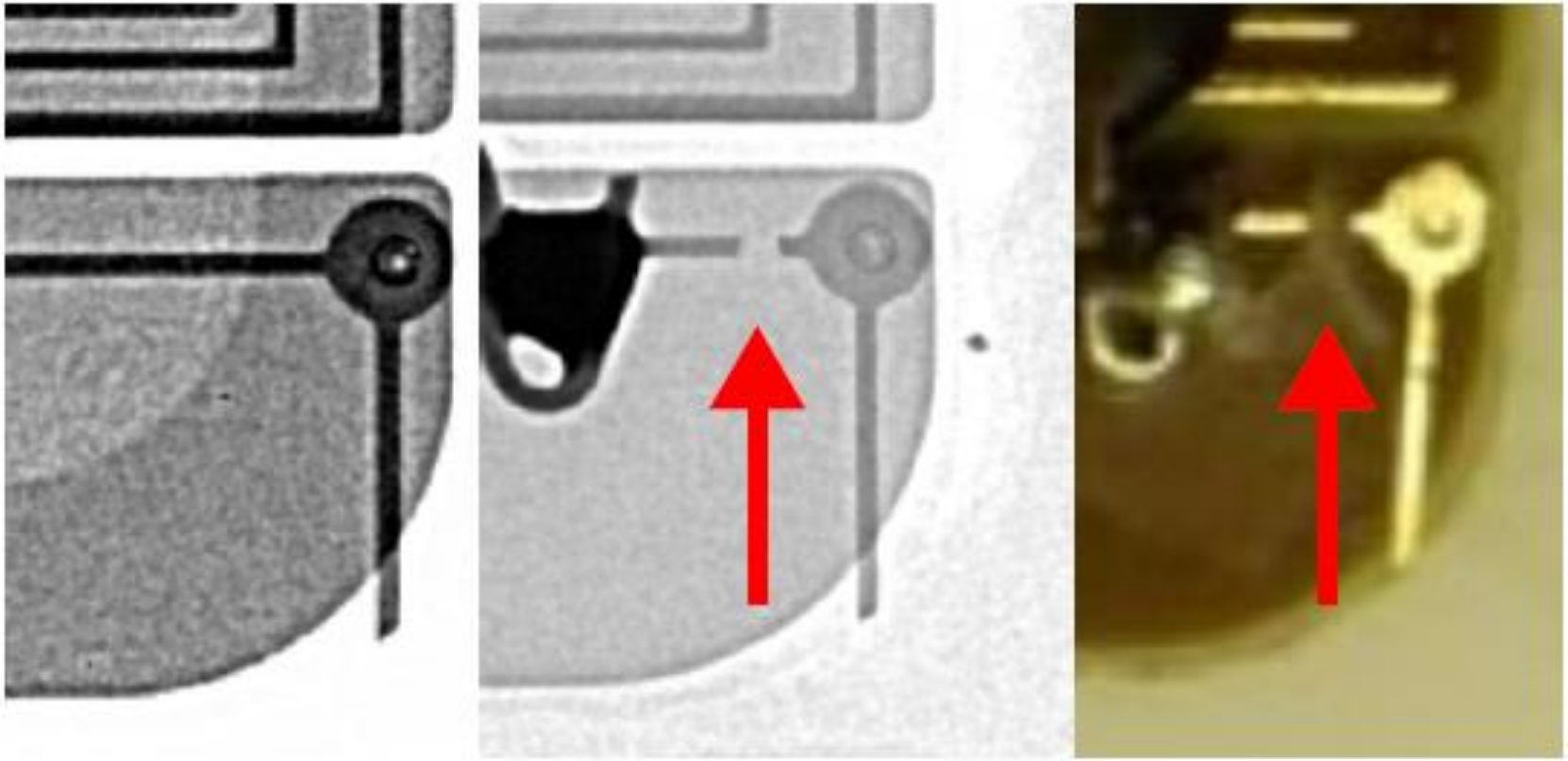



no visible signal activity here!

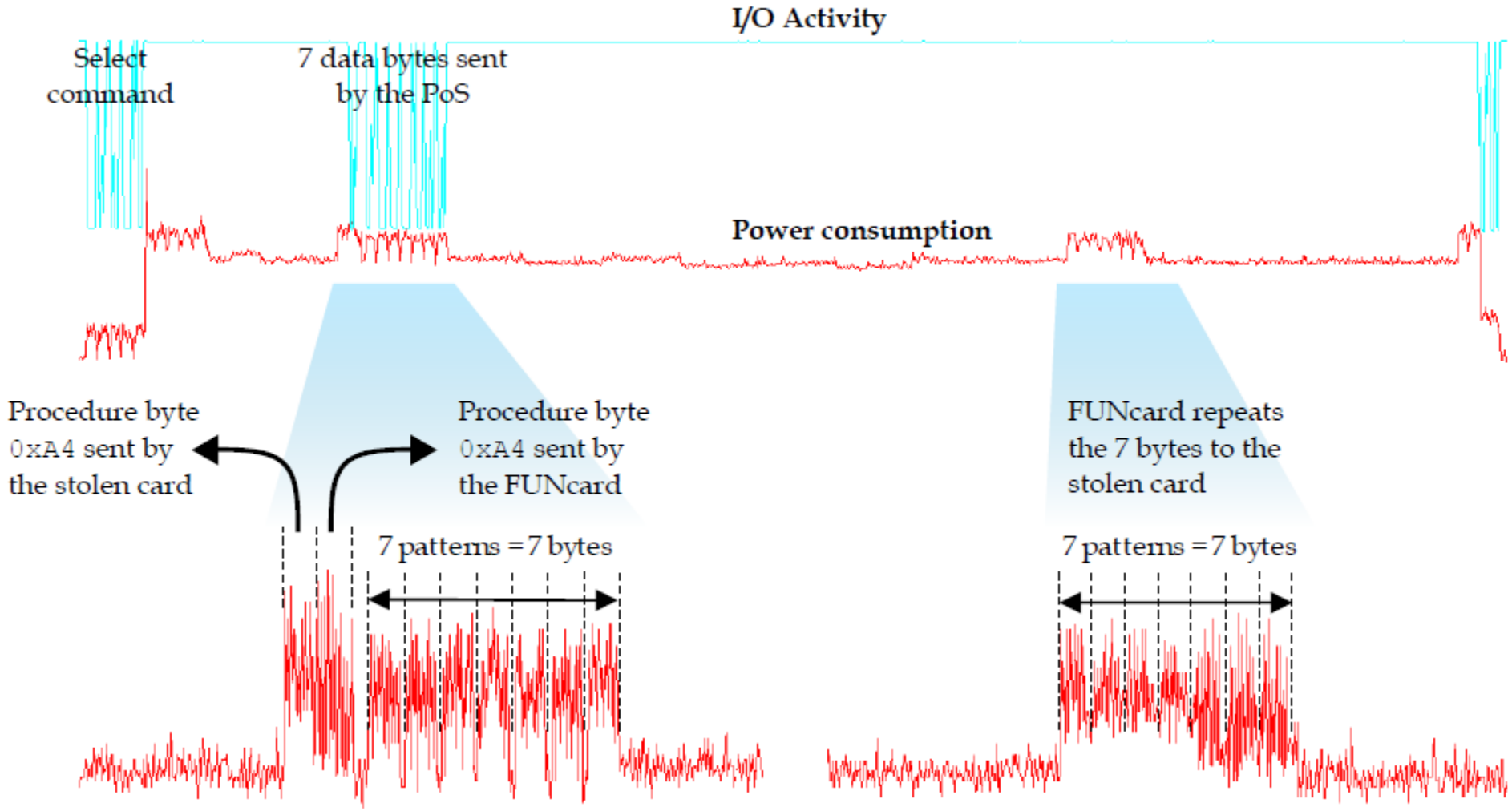
# Back to X-Ray: Solution to Riddle!

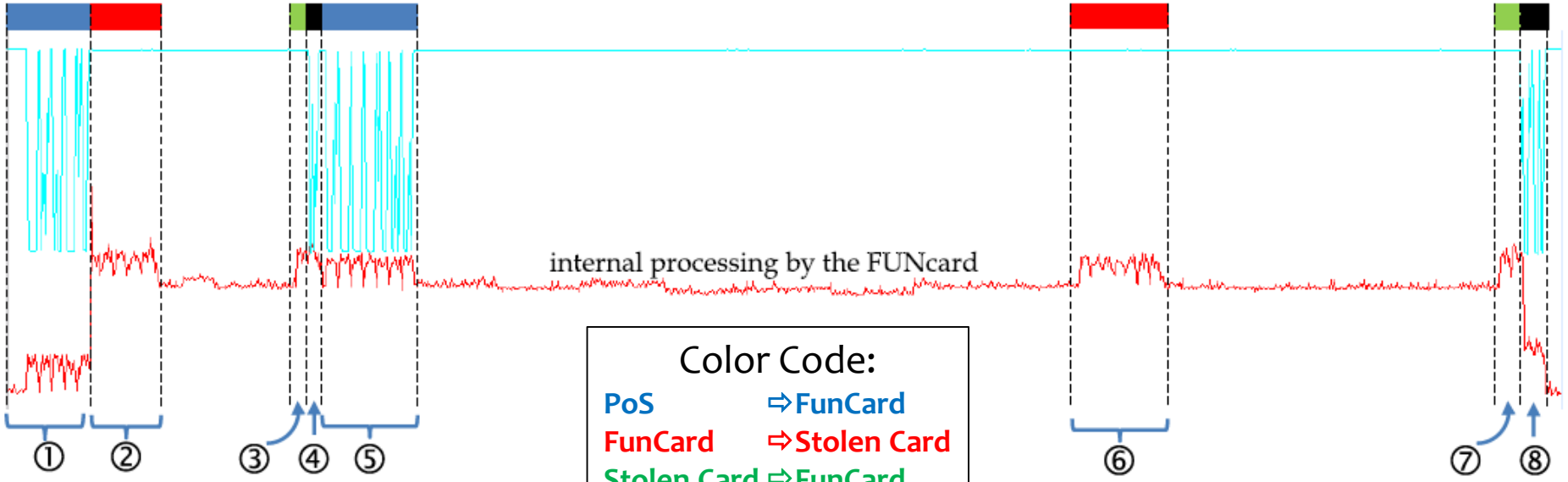


# Anti-Forensic Protection by Fraudster



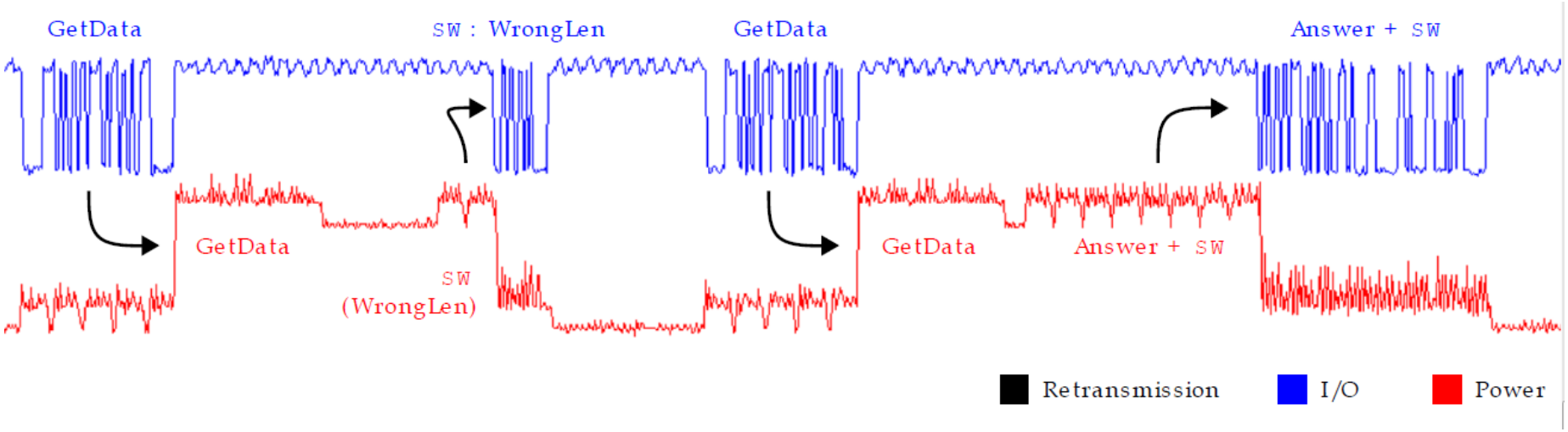
# Using Power Consumption Analysis





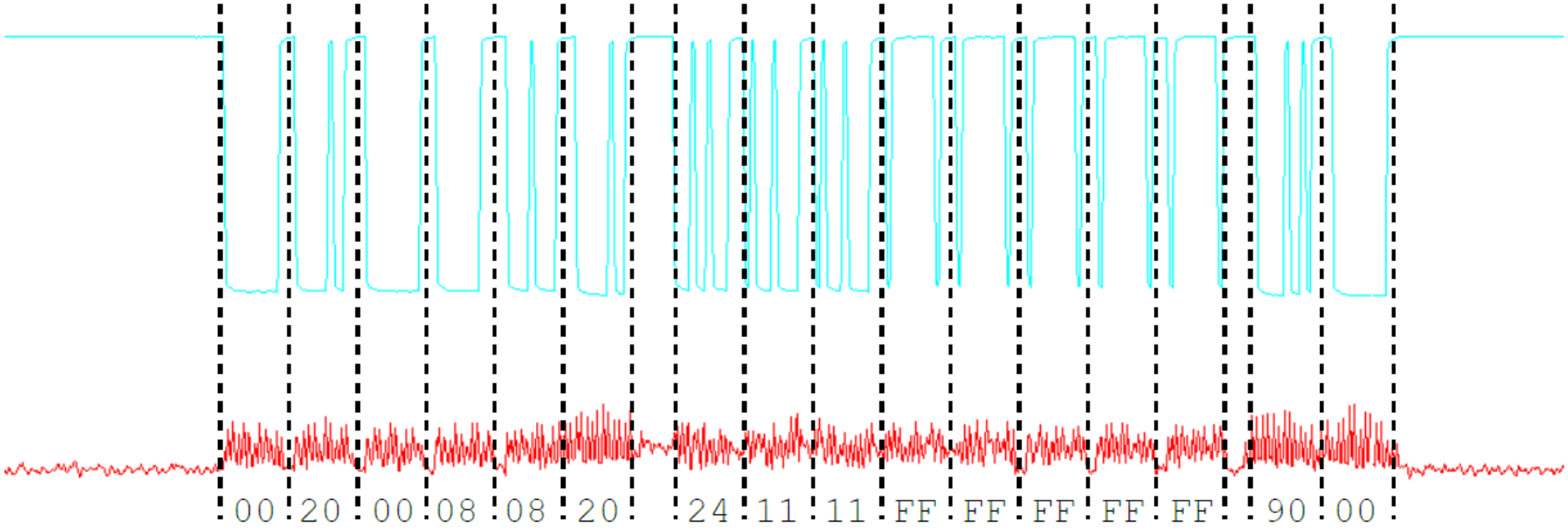

① PoS sends the ISO command 00 A4 04 00 07
② Command echoed to the stolen card by the FunCard
③ Stolen card sends the procedure byte A4 to the FunCard
④ FunCard retransmits the procedure byte to the PoS
⑤ PoS sends data to FunCard
⑥ FunCard echoes data to stolen card
⑦ Stolen card sends SW to FunCard
⑧ FunCard transmits SW to PoS

# Power Consuption During GetData




Confirms the modus operandi

# VerifyPIN Power Trace Analysis




Power trace of the forgery during VerifyPIN command.

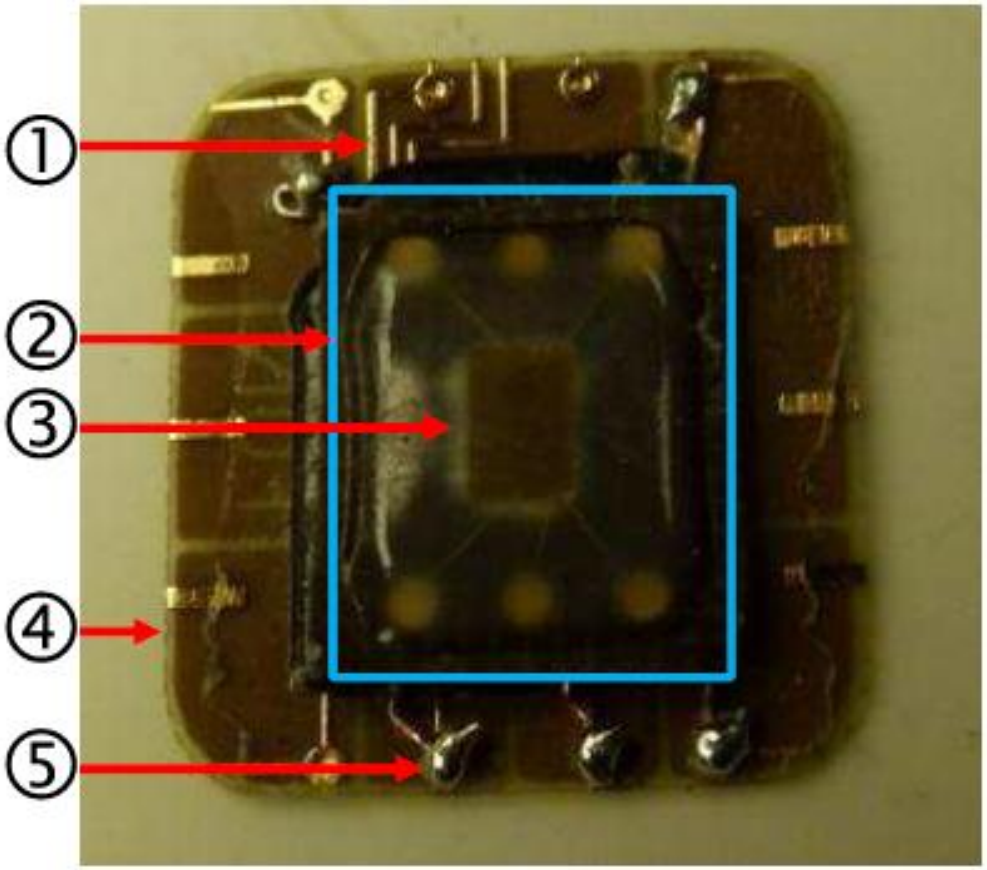
Note the absence of retransmission on the power trace before the sending of the SW

# Having Finished All Experiments

We can ask the judge's authorization to perform invasive analysis.

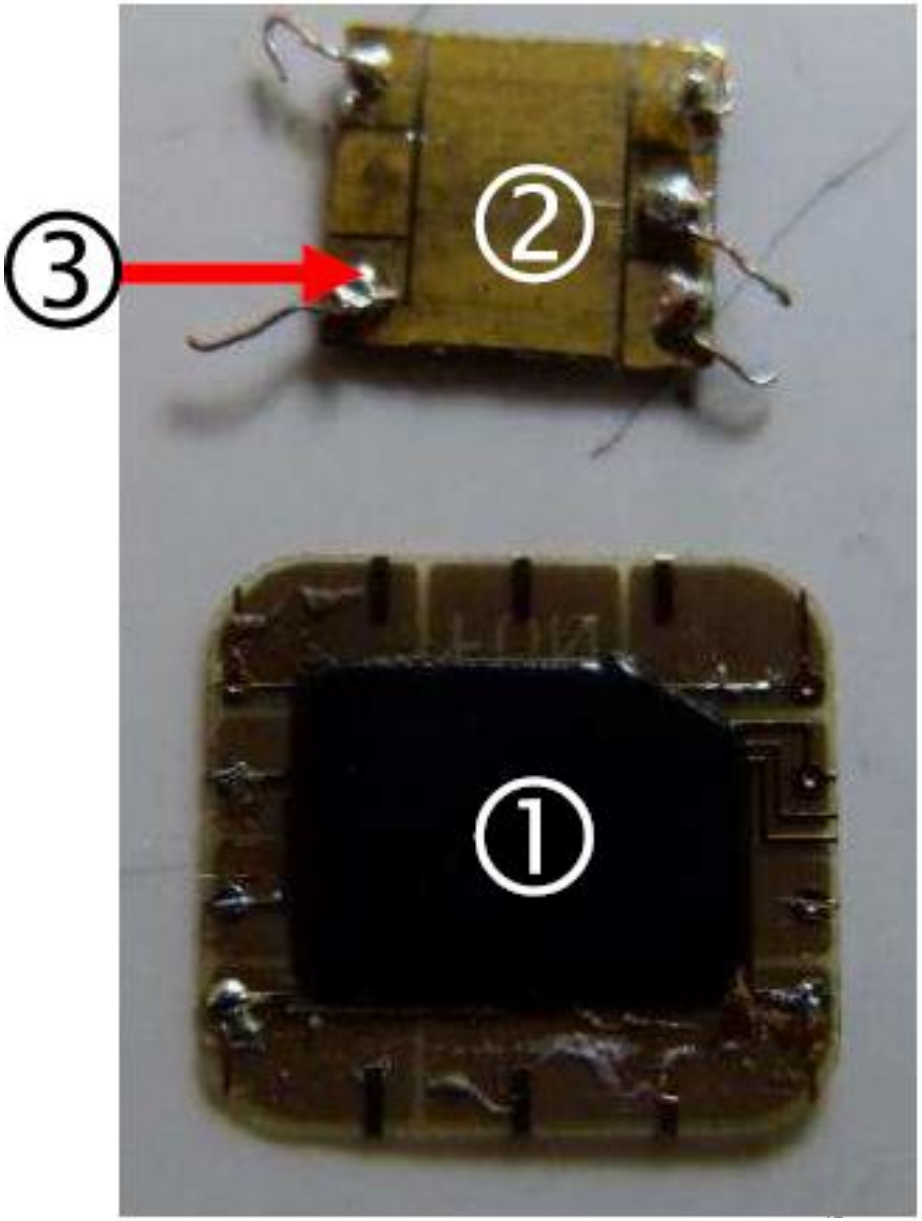
Authorization granted.

# Invasive Analysis



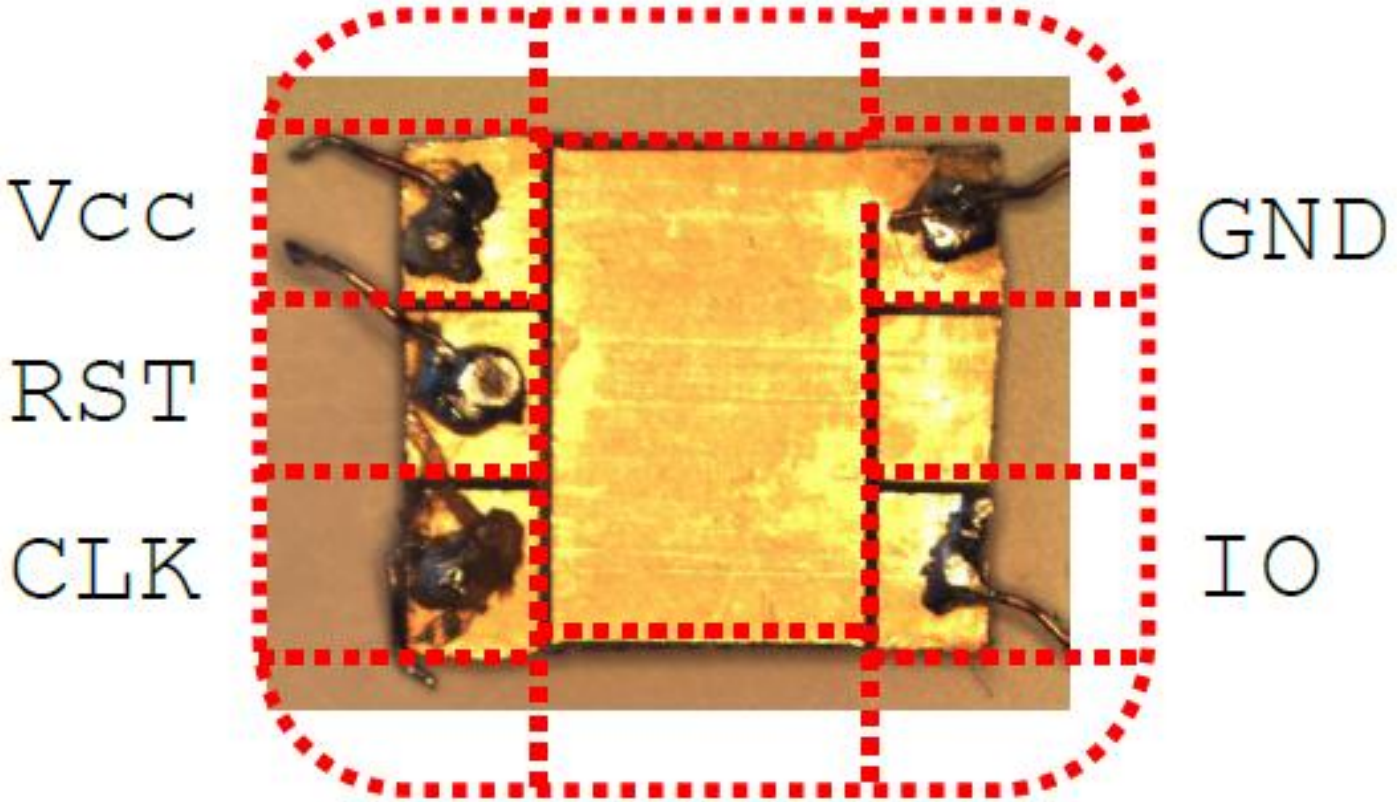

① Connection grid
② Stolen card module (outlined in blue)
③ Stolen card's chip
④ FunCard module
⑤ Welding of connection wires

# Invasive Analysis



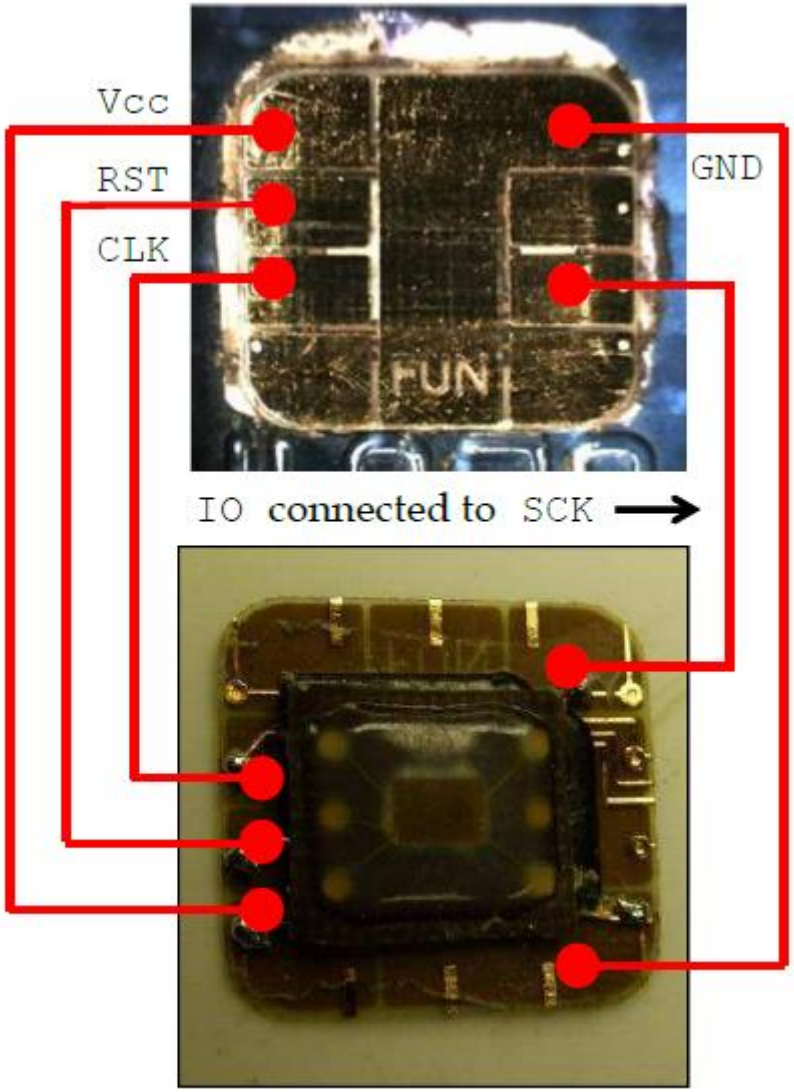

① FunCard module
② Genuine stolen card
③ Welded wire

# Original EMV Chip Clipped by Fraudster




Cut-out pattern over laid

# Wiring Diagram of the Forgery



# Economical Damage

Cost of device replacement in the field

Cost of fraud (stolen money)

Damage to reputation

plus:

Forensic analysis cost. Here: 3 months of full time work.

# In Conclusion

Attackers of modern embedded IoT devices

- Use advanced tools
- Are very skilled engineers
- Are well aware of academic publications
- Use s/w and h/w anti-forensic countermeasures

If you do not design your IoT device with that in mind and if stakes are high enough, **the device will be broken.**