

Hardware security

Jean-Jacques Quisquater

UCLouvain, Belgium

jjq@uclouvain.be

(jjq@mit.edu)

See you at LinkedIn

Thanks to David Samyde, Michaël Neve, Eric Peeters, François Koeune, and many other people

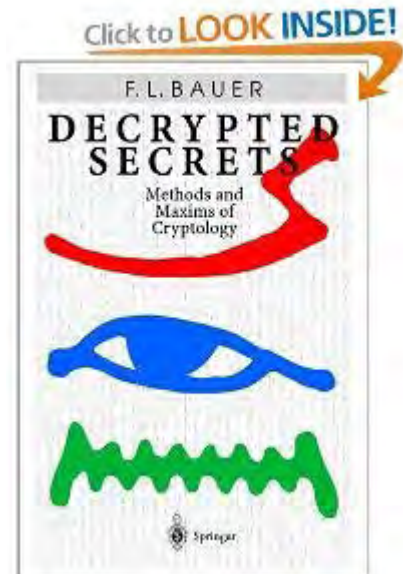
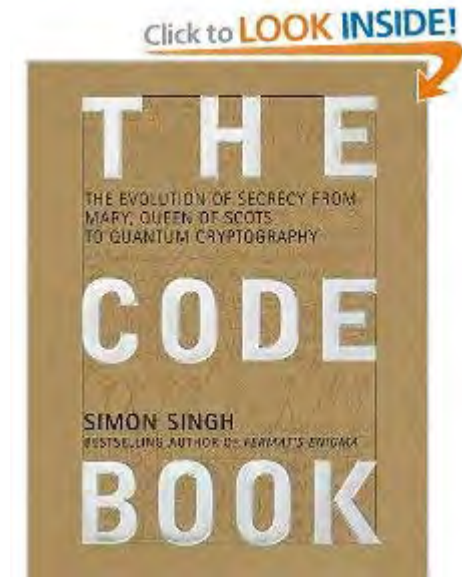
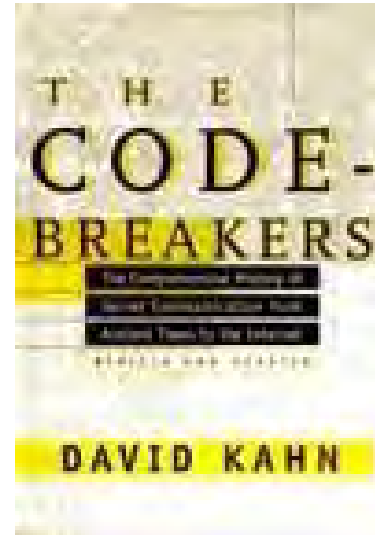
Jean-Jacques Quisquater

- Engineer in applied math (UCLouvain, Belgium)
- PhD in computer science (Orsay, LRI, Paris-Saclay, France)
- Philips Research (in Brussels): during 20 years, and next
- UCLouvain, Louvain-la-Neuve, professor (cryptography): 20 years
- 20 patents
- Introduction of strong crypto (DES, RSA) in smart cards
- ISO : first standard about digital signature
- First blockchain on the web: 1996
- Teaching at ENS-Ulm, Paris, about cryptography (1991-2002)
- Invited by Silvio Micali and Ron Rivest at CSAIL (and by Neil 😊)
- 250 papers in cryptography, security, ...

Some web sites (see also inside links) about the history of cryptography and related hardware

- Crypto museum:
 - <https://www.cryptomuseum.com/index.htm>
- Crypto mysteries:
 - <https://klausschmeh.net/>
- Varia:
 - <https://rijmenants.blogspot.com/>

Books for history



From other talks of this session

- **From: *The introduction***
 - *Side-channel attacks (timing, power, electromagnetic), hardware trojans, trusted execution environments, and the security implications of CPU architecture. How attackers reach below the software layer.*
 - ***operation gunman***
- **From : *Microarchitectural security***
 - *side-channels*

From other talks of this session

- *From: The introduction*
 - ***Side-channel attacks (timing, power, electromagnetic), hardware trojans, trusted execution environments, and the security implications of CPU architecture. How attackers reach below the software layer.***
 - ***operation gunman***
- *From : Microarchitectural security*
 - ***side-channels***

Introduction: what are we speaking about?

- Software ... hardware: and what about FPGA?
- USB key: software or hardware?
 - A recent example of attack: LEDGER cryptowallet
- What about homomorphic encryption?

Simple example: Changing a QR code

- Put a dangerous paper QR code on a legitimate one:
 - hardware security?

FPGA: Field-Programmable Gate Array

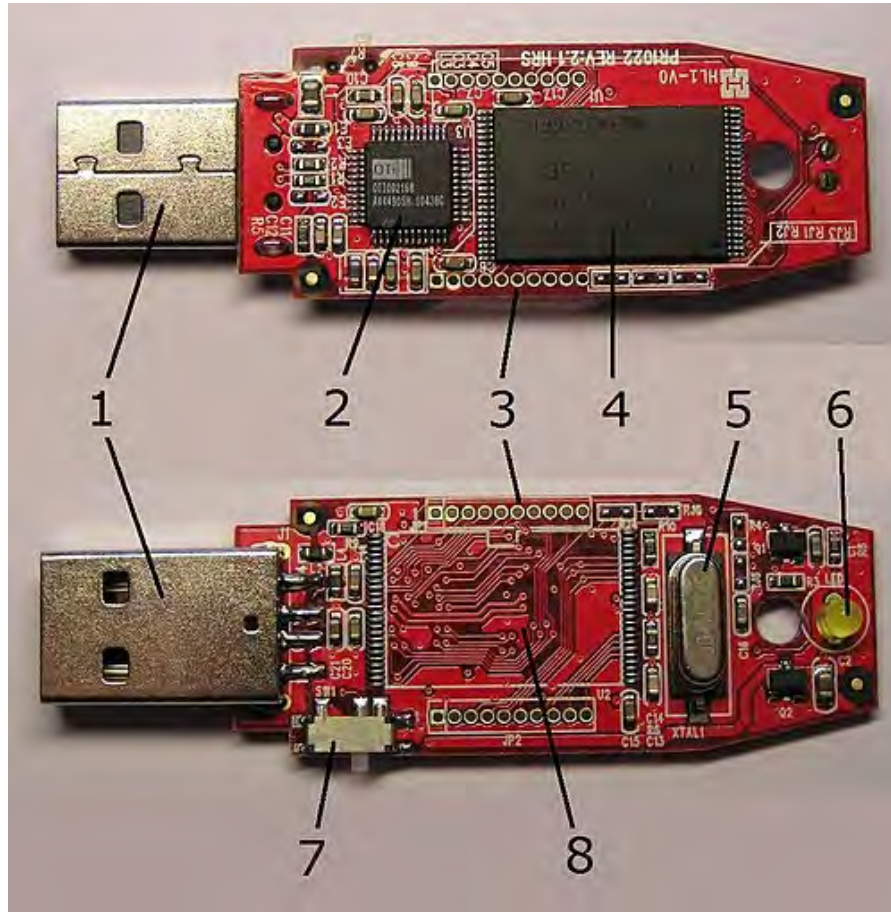
https://en.wikipedia.org/wiki/Field-programmable_gate_array

- A chip able to simulate other hardware, and software can use it
- Attacks for hardware are working



USB key: hardware + software

<https://en.wikipedia.org/wiki/BadUSB> (2014)



BadUSB is a computer security attack using USB devices that are programmed with malicious software. For example, USB flash drives can contain a programmable Intel 8051 microcontroller, which can be reprogrammed, turning a USB flash drive into a malicious device. This attack works by programming the fake USB flash drive to emulate a keyboard. Once it is plugged into a computer, it is automatically recognized and allowed to interact with the computer. It can then initiate a series of keystrokes which open a command window and issue commands to download malware.

- 2. Intel 8051
- 4. Flash memory

Cryptowallet LEDGER

[Products](#)[Ledger Wallet](#)[Learn](#)[For Business](#)[For Developers](#)[Support](#)EN

Your phone alone isn't secure

Only Ledger signers keep you safe. Don't be a victim of identity theft or wallet drains.

[Compare Ledger signers →](#)



Ledger Stax™

3.7" CURVED SCREEN

Premium from every angle, the elegant way to diversify your wealth and explore DeFi.

★★★★☆ 4.5/5

[Learn more →](#)



Ledger Flex™

2.8" GORILLA GLASS SCREEN

The new standard to buy, swap, stake and build your portfolio with ease.

★★★★☆ 4.3/5

[Learn more →](#)

NEW

Ledger Nano™ Gen5

2.8" LIGHTWEIGHT SCREEN

The fun, accessible way to manage your money, logins and digital life with clarity.

★★★★☆ 4/5

[Learn more →](#)



Ledger Nano™ Classics

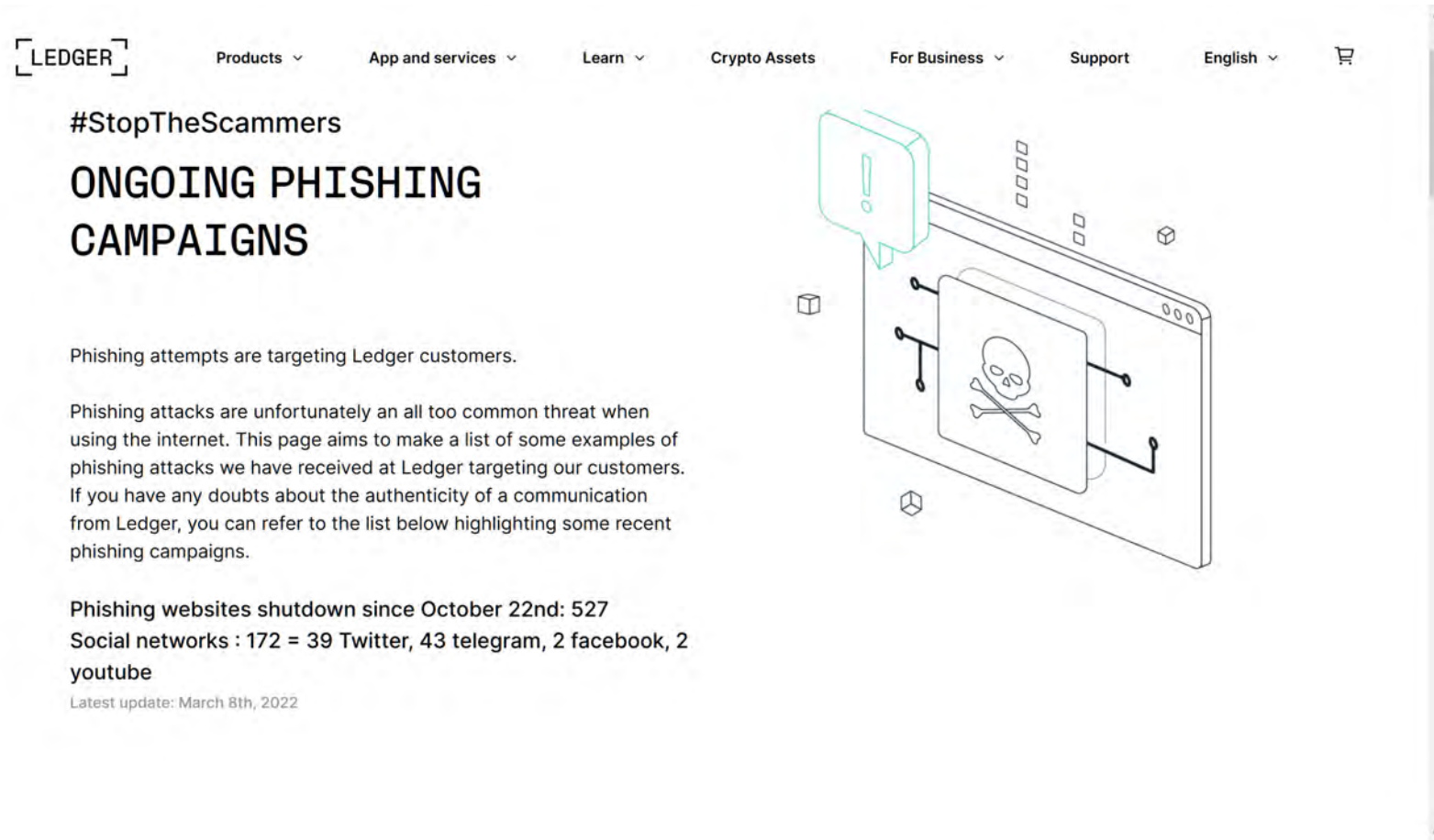
1.1" SCREEN

Reliable backup signers to swap, stake and HODL at home or on the go.

★★★★☆ 4.5/5

[Discover now →](#)

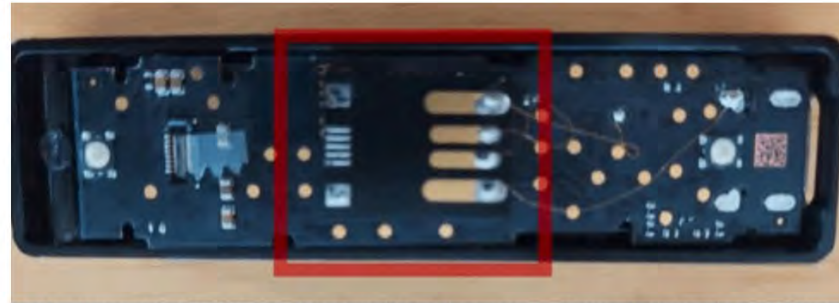
Phishing attack with another hardware ...



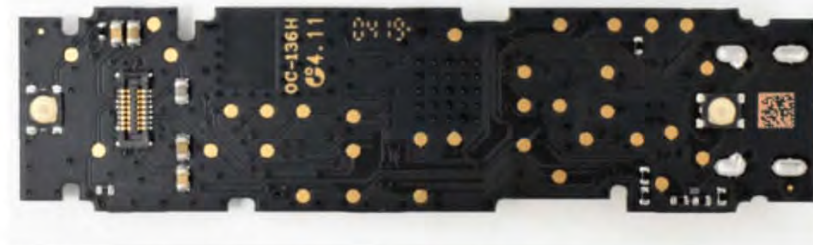
Modification of an authentic hardware

"This seems to be a simple flash drive strapped on to the Ledger with the purpose to be for some sort of malware delivery," Grover told BleepingComputer in a chat about the photos. "All of the components are on the other side, so I can't confirm if it is JUST a storage device, but.... judging by the very novice soldering work, it's probably just an off-the-shelf mini flash drive removed from its casing."

Grove also explained that "those four wires [highlighted in the photo] piggyback the same connections for the USB port of the Ledger."



Back of tampered Ledger hardware wallet, red square by Grove. Source: BleepingComputer.



Back of legitimate Ledger hardware wallet. Source: Ledger.

Previously, the attackers had [sent out phishing emails to victims](#), prompting them to type in their recovery seeds — the 12 or 24 words used to derive one's [private keys](#), giving anyone who possesses it complete control of the victim's funds. By tampering with the device, the attackers likely hoped to get their target to type their recovery words into the fake application, which would allow the bad actors to take control of the victim's funds.

OK versus fake!





hardware security - July 13, 2026, Jean-Jacques Quisquater -
Fab Futures - Cybersecurity - Class 2026

True or not?



Ledger secure signers > Secure your device

Check hardware integrity

🕒 Last updated: 13/05/2026

Every Ledger signer undergoes an automated Ledger Genuine Check during initial onboarding and every time it connects to My Ledger in the Ledger Wallet™ app.

During manufacturing, each genuine Ledger signer is provisioned with a secret key. When you connect your Ledger signer to our secure servers, it provides cryptographic proof of this key. Only a Ledger signer with a genuine secure element can complete this verification process, ensuring your hardware is not a counterfeit. Even perfect-looking packaging or branding can't fake it.

However, note that it cannot detect unauthorized physical modifications to the hardware—such as spying implants—if the original Secure Element remains intact.

Additionally, we recommend you to purchase directly from the official [Ledger Shop](#) or through our [authorized retail network](#). Purchasing from unlisted, unknown sellers introduces material security risks and is strongly discouraged.

⚠ Important notice

Please note that while you may open your Ledger signer to inspect its hardware integrity, any damage caused during the opening or inspection process will void the warranty. Additionally, handling an exposed circuit board without taking the proper precautions could result in permanent damage caused by electrostatic discharge (ESD). You can learn more about ESD and the proper precautions to take [here](#).



Ledger Stax™ Ledger Flex™ Ledger Nano™ Gen5 Ledger Nano X™ Ledger Nano S Plus™



Phishing contexts for Ledger

- Loss by Ledger of a large set of customer addresses (internal and via resellers),
- Pirates send emails with a fake link and some excuses to go there for the client,

Persistent Actor Targets Ledger Cryptocurrency Wallets

SHARE WITH YOUR NETWORK!



NOVEMBER 04, 2020 | THE PROOFPOINT THREAT RESEARCH TEAM

In July 2020, cryptocurrency wallet company Ledger revealed a [breach](#) of 9500 customers' names and contact information. In their announcement, they caution users to be aware of [credential phishing attempts](#) and state that they will "never ask [users] for the 24 words of [their] recovery phrase."

On October 25, 2020, Proofpoint researchers discovered several thousand messages claiming to be from Ledger with subjects like, "Your Ledger Live client may be compromised" and "Your Ledger assets may be at risk". The messages don't appear to be targeted at any specific industry or geography.

Lures

📧 Ledger <info@ledgersupport.io> ☆ To username@organizationname.tld ☆

Your Ledger Live client may be compromised

6:14 AM

[View in Browser](#)



Dear [redacted]

We regret to inform you that Ledger has experienced a security breach affecting approximately 85,000 of our customers and that the wallet associated with your e-mail address ([username@organizationname.tld](#)) is within those affected by the breach.



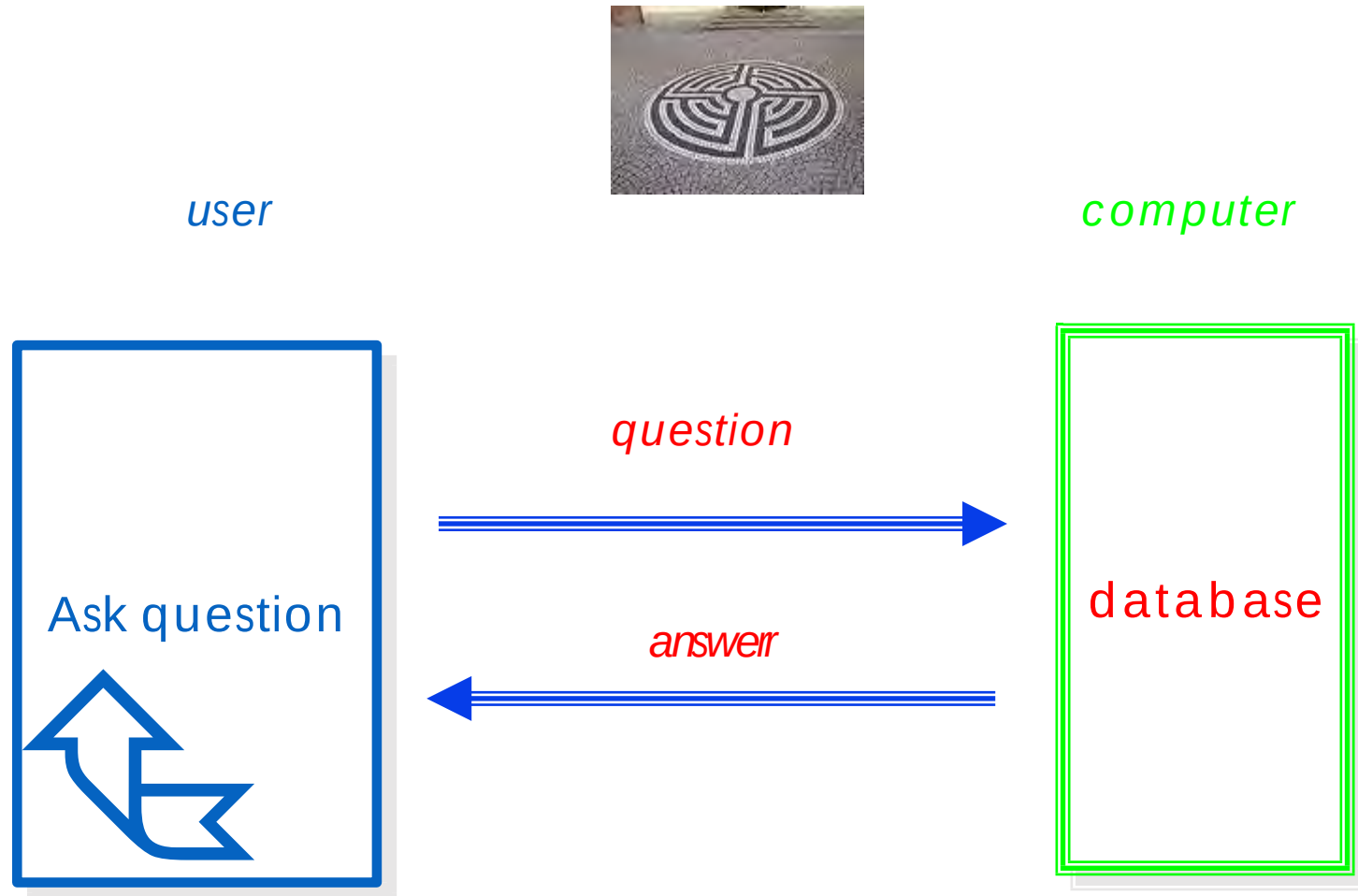
How can I help you today?



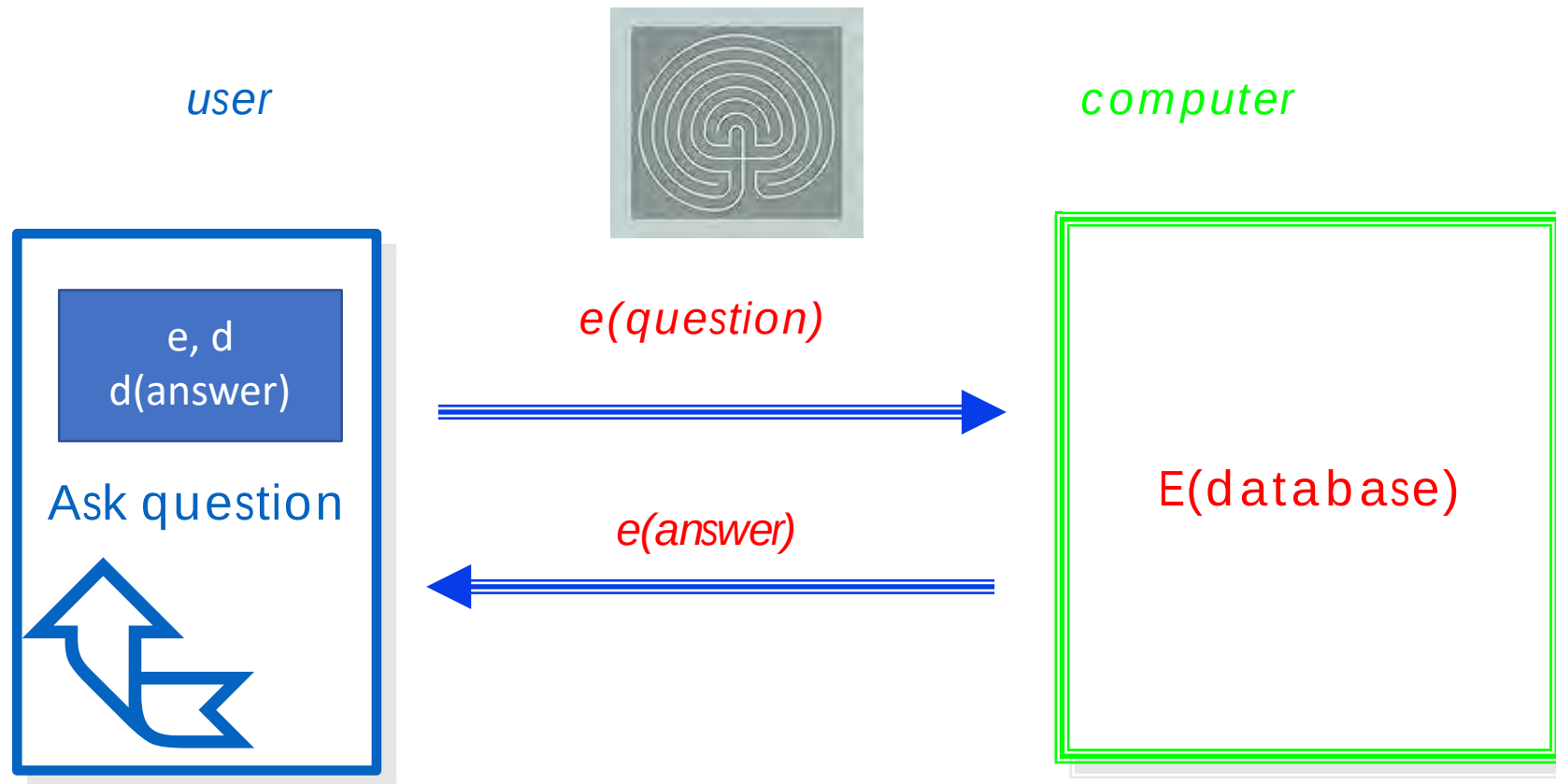
(Fully) Homomorphic encryption: then do we need hardware security?

- Good idea!
- Concept: Rivest, Adleman, Dertouzos (1978)
- But very expensive:
 - Long computations: need of coprocessors
 - Expansion of data (60x ?)
 - Long keys
- Companies: IBM, Microsoft, Google, ..., ZAMA, ...
- See zama:
 - <https://www.zama.org/introduction-to-homomorphic-encryption>
- Attacks exist.

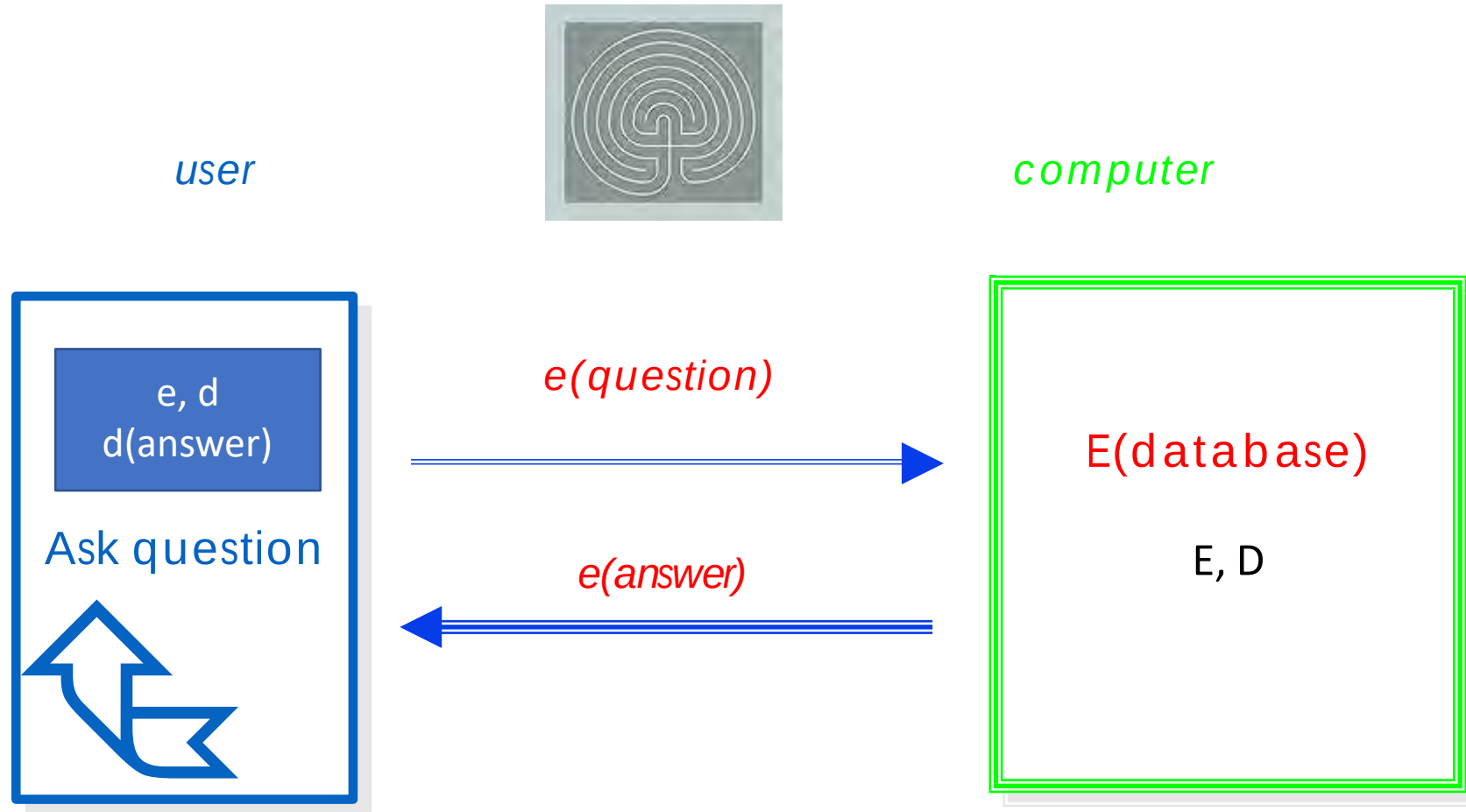
Databases and access to data



Databases and access to data II (homomorphic encryption: 2009, Gentry, Smart, Vercauteren, ...)



Final model (draft)



Old stories

Trojan horse

Kerckoffs principle

OTP

Early EMA

Operations GUNMAN and FAREWELL

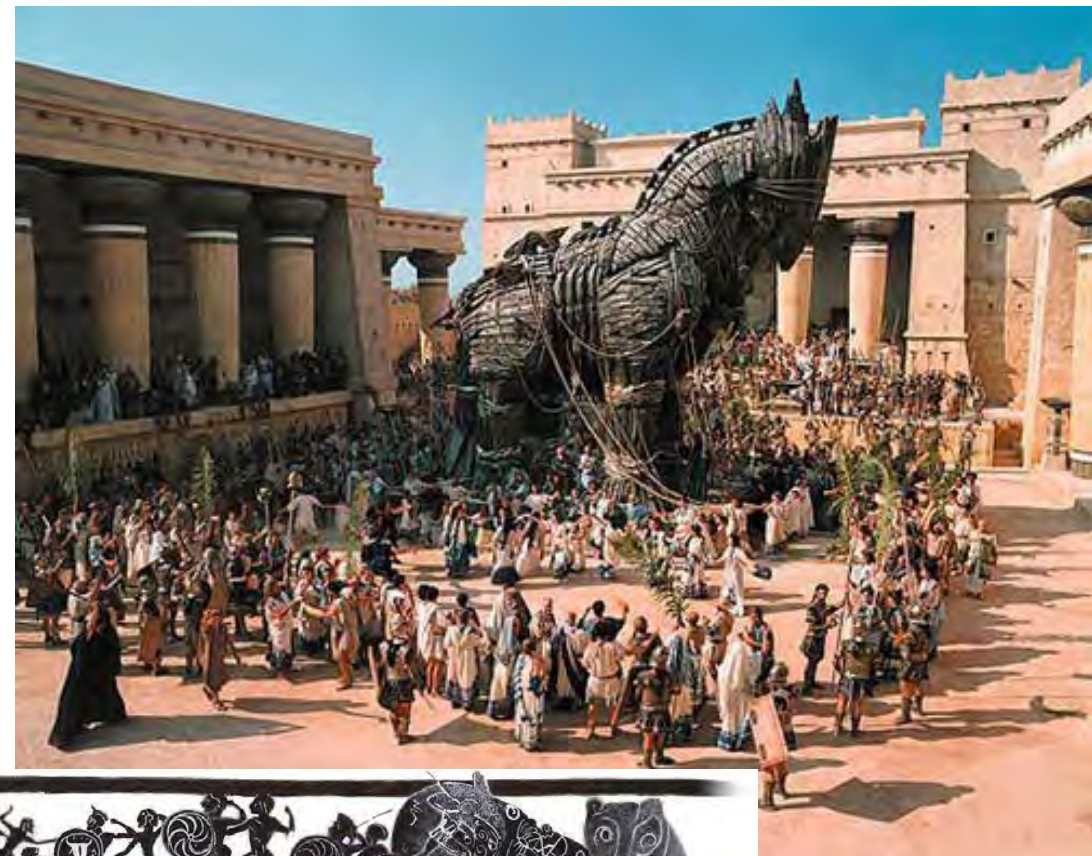
TEMPEST

And more ...

Trojan horse

circa 1260–1180 BC

- Strong myth
- constant problem (backdoor)





Codes, Ciphers, Cryptography, smart Cards : 4 historic keys for hardware security



hardware security - July 13, 2026, Jean-Jacques Quisquater - Fab
Futures - Cybersecurity - Class 2026



Codes, Ciphers, Cryptography, smart Cards : 4 historic keys for security



hardware security - July 13, 2026, Jean-Jacques Quisquater - Fab
Futures - Cybersecurity - Class 2026

JOURNAL

DEB

SCIENCES MILITAIRES.

Janvier 1883.

LA CRYPTOGRAPHIE MILITAIRE.

« La cryptographie est un auxiliaire
puissant de la tactique militaire. »
(Général L. B. de Villars, *Étude de la guerre*.)

I.

LA CRYPTOGRAPHIE DANS L'ARMÉE

A. Notions historiques.

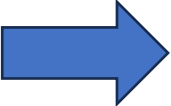
La Cryptographie ou l'Art de chiffrer est une science vieille
comme le monde ; confondue à son origine avec la télégraphie
militaire, elle a été cultivée, dès la plus haute antiquité, par les
Chinois, les Perses, les Carthaginois ; elle a été enseignée dans
les écoles tactiques de la Grèce, et tenue en haute estime par les
plus illustres généraux romains¹.

Depuis la modeste seyntale des Laécémoniens et les trucs
inventés ou rapportés par Énée le Tacticien, jusqu'au fameux

¹ C'est ce qu'on appelle : Stéganographie, chiffre ou écriture secrète : que ce soit à
dicté ou à l'écrit. Le dictionnaire de l'Académie donne le renseignement qui se rapporte à la
Cryptographie. Les anciens auteurs l'appellent plus ou moins correctement : *anagramma*,
anagrammatice, *anagrammatum*, *polygraphia*, *acrostichographia*, *cryptologia*, *atagoria*, *cryptomenyctice*,
hardward security, *hardward security*, *hardward security*, *hardward security*, *hardward security*,
glai : *cryptography*,
: Lettres militaires en code, *hardward security* : communication secrète dans ;

Auguste Kerckhoffs (journal La Cryptographie Militaire, 1883):
six design principles for military ciphers

Translated from French

- 
- The system must be practically, if not mathematically, indecipherable;
 - It must not be required to be secret, and it must be able to fall into the hands of the enemy without inconvenience;
 - Its key must be communicable and retainable without the help of written notes, and changeable or modifiable at the will of the correspondents;
 - It must be applicable to telegraphic correspondence;
 - It must be portable, and its usage and function must not require the concurrence of several people;
 - Finally, it is necessary, given the circumstances that command its application, that the system be easy to use, requiring neither mental strain nor the knowledge of a long series of rules to observe.

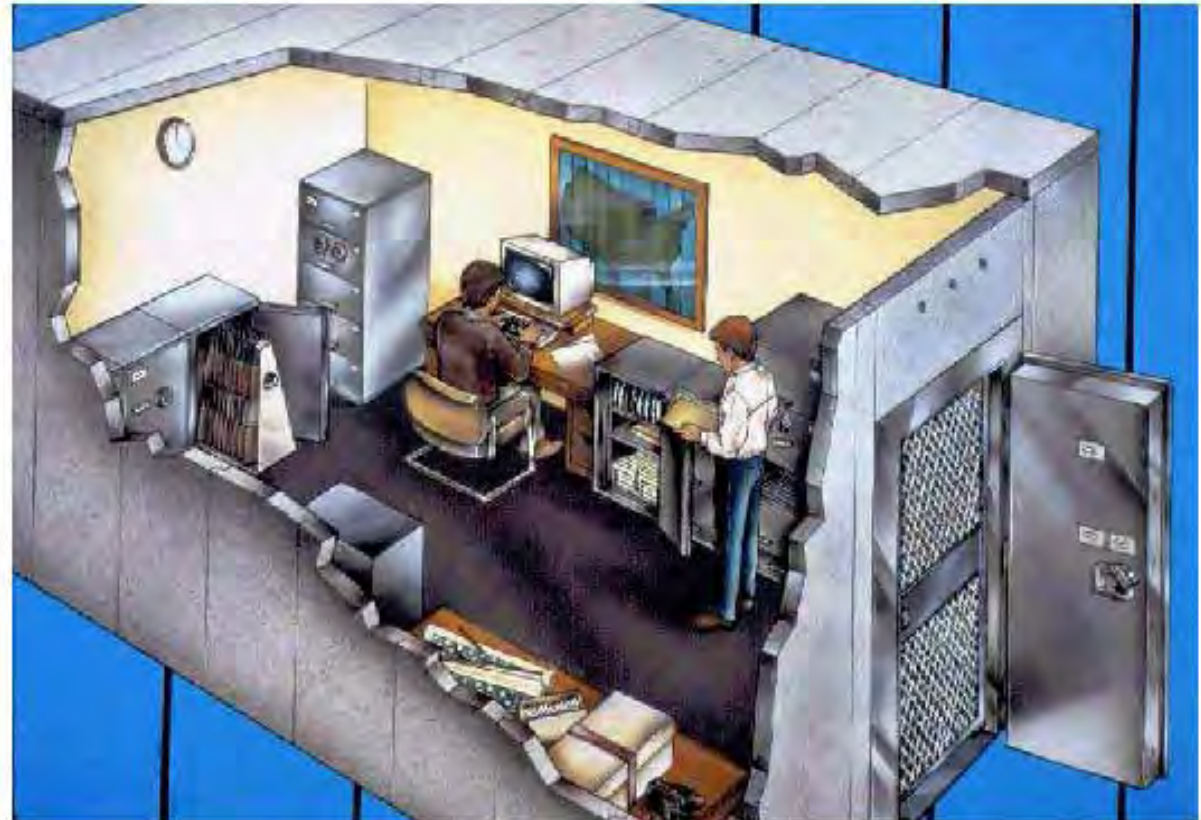
Early EMA

Electromagnetic attack

- **Late-1800s** Crosstalk is frequent problem in infantile telephone system.
- **1914-1915** Field telephone crosstalk in World War I exploited and jamming attempted, leading to lower signal British Fuller phone.
- **1918** Herbert Yardley and the Black Chamber discover radio transmitter emanations: *Yardley and his people found that various electronic devices used to handle classified information emanated information, and that these emanations could be exploited to reconstruct the classified materials.*
- **1940s** Receivers shielded for local oscillator radiation to prevent becoming beacons for enemy submarines in World War II.



Faraday cage (for TEMPEST)



Kleptography: Using Cryptography Against Cryptography

Adam Young* and Moti Yung**

Abstract. The notion of a Secretly Embedded Trapdoor with Universal Protection (SETUP) has been recently introduced. In this paper we extend the study of stealing information securely and subliminally from black-box cryptosystems. The SETUP mechanisms presented here, in contrast with previous ones, leak secret key information **without** using an explicit subliminal channel. This extends this area of threats, which we call “kleptography”.

We introduce new definitions of SETUP attacks (strong, regular, and weak SETUPS) and the notion of m out of n leakage bandwidth. We show a strong attack which is based on the discrete logarithm problem. We then show how to use this setup to compromise the Diffie-Hellman key exchange protocol. We also strengthen the previous SETUP against RSA. The strong attacks employ the discrete logarithm as a one-way function (assuring what is called “forward secrecy”), public-key cryptography, and a technique which we call probabilistic bias removal.

Key words: cryptanalytic attacks, kleptography, leakage bandwidth, Discrete Log, Diffie-Hellman, RSA, design and manufacturing of cryptographic devices and software, black-box devices, subliminal channels, information hiding, SETUP mechanisms, randomness, pseudorandomness.

1 Introduction

Numerous problems and subtleties exist when constructing a cryptosystem for use, since designing and manufacturing secure cryptosystems is a demanding task. Some of these problems are immediate and known, yet they require diligent engineering. Other issues are more involved or are yet unknown.

One area where problems have been recognized is in the information-hiding aspect of cryptosystems, and in particular the existence of “subliminal channels” in cryptosystems. Subliminal channels can be used to convey information in the output of a cryptosystem in a way that is different from the intended output. This notion was put forth by Simmons [Sim85, Sim94]. Other works on subliminal channels are [Des90] which showed an RSA channel and [KL95] which showed how to hide a shadow public key inside a key distribution method. The usage of subliminal channels expose information universally (to anyone).

* Dept. of Computer Science, Columbia University Email: ayoun@cs.columbia.edu.

** CertCo, NY, USA. Email: moti@cs.columbia.edu, moti@certco.com

Designing and implementing malicious hardware

Samuel T. King, Joseph Tucek, Anthony Cozzie, Chris Grier, Weihang Jiang, and Yuanyuan Zhou
University of Illinois at Urbana Champaign, Urbana, IL 61801

Abstract

Hidden malicious circuits provide an attacker with a stealthy attack vector. As they occupy a layer below the entire software stack, malicious circuits can bypass traditional defensive techniques. Yet current work on trojan circuits considers only simple attacks against the hardware itself, and straightforward defenses. More complex designs that attack the software are unexplored, as are the countermeasures an attacker may take to bypass proposed defenses.

We present the design and implementation of Illinois Malicious Processors (IMPs). There is a substantial design space in malicious circuitry; we show that an attacker, rather than designing one specific attack, can instead design hardware to support attacks. Such flexible hardware allows powerful, general purpose attacks, while remaining surprisingly low in the amount of additional hardware. We show two such hardware designs, and implement them in a real system. Further, we show three powerful attacks using this hardware, including a login backdoor that gives an attacker complete and high-level access to the machine. This login attack requires only 1341 additional gates: gates that can be used for other attacks as well. Malicious processors are more practical, more flexible, and harder to detect than an initial analysis would suggest.

1 Introduction

1.1 Motivation

Attackers may be able to insert covertly circuitry into integrated circuits (ICs) used in today's computer-based systems; a recent Department of Defense report [16] identifies several current trends that contribute to this threat. First, it has become economically infeasible to procure high performance ICs other than through commercial suppliers. Second, these commercial suppliers are increasingly moving the design, manufacturing,

and testing stages of IC production to a diverse set of countries, making securing the IC supply chain infeasible. Together, commercial-off-the-shelf (COTS) procurement and global production lead to an "enormous and increasing" opportunity for attack [16].

Maliciously modified devices are already a reality. In 2006, Apple shipped iPods infected with the RayMonE virus [4]. During the cold war, the CIA sabotaged oil pipeline control software, which was then allowed to be "stolen" by Russian spies [10]. Conversely, Russian agents intercepted and modified typewriters which were to be used at the US embassy in Moscow; the modifications allowed the Russians to copy any documents typed on said typewriters [16]. Recently, external hard drives sold by Seagate in Taiwan were shipped with a trojan installed that sent personal data to a remote attacker [1]. Although none of these attacks use malicious circuits, they clearly show the feasibility of covertly inserting malicious elements in the COTS supply chain.

Using modified hardware provides attackers with a fundamental advantage compared to software-based attacks. Due to the lower level of control offered, attackers can more easily avoid detection and prevention. The recent SubVirt project shows how to use virtual-machine monitors to gain control over the operating system (OS) [11]. This lower level of control makes defending against the attack far more difficult, as the attacker has control over all of the software stack above. There is no layer below the hardware, thus giving such an attack a fundamental advantage over the defense.

Although some initial work has been done on this problem in the security community, our understanding of malicious circuits is limited. IBM developed a "trojan circuit" to steal encryption keys [3]. By selectively disabling portions of an encryption circuit they cause the encryption key to be leaked. This is the best example of an attack implemented in hardware that we are aware of, yet it has several shortcomings. First, their attack operates on hardware-level abstractions directly. They leak encryption keys from an encryption circuit and they ig-

Bug Attacks

Eli Biham¹, Yaniv Carmeli¹, and Adi Shamir²

¹ Computer Science Department,
Technion - Israel Institute of Technology,
Haifa 32000, Israel
{biham,yanivca}@cs.technion.ac.il
<http://www.cs.technion.ac.il/~{biham,yanivca}>

² Computer Science Department,
The Weizmann Institute of Science,
Rehovot 76100, Israel
adi.shamir@weizmann.ac.il

Abstract. In this paper we present a new kind of cryptanalytic attack which utilizes bugs in the hardware implementation of computer instructions. The best known example of such a bug is the Intel division bug, which resulted in slightly inaccurate results for extremely rare inputs. Whereas in most applications such bugs can be viewed as a minor nuisance, we show that in the case of RSA (even when protected by OAEP), Pohlig-Hellman, elliptic curve cryptography, and several other schemes, such bugs can be a security disaster: Decrypting ciphertexts on *any* computer which multiplies *even one pair of numbers* incorrectly can lead to full leakage of the secret key, sometimes with a single well-chosen ciphertext.

Keywords: Bug attack, Fault attack, RSA, Pohlig-Hellman, ECC.

1 Introduction

With the increasing word size and sophisticated optimizations of multiplication units in modern microprocessors, it becomes increasingly likely that they contain some undetected bugs. This was demonstrated by the accidental discovery of the Pentium division bug in the mid 1990's, by the less famous Intel 80286 popf bug (that set and then cleared the interrupt-enable bit during execution of the very simple popf instruction, when no change in the bit was necessary), by the recent discovery of a bug in the Intel Core 2 memory management unit (which allow memory corruptions outside of the range of permitted writing for a process), etc.

In this paper we show that if some intelligence organization discovers (or secretly plants) even one pair of single-word integers a and b whose product is computed incorrectly (even in a single low order bit) by a popular microprocessor, then any key in any RSA-based security program running on any one of the millions of PC's that contain this microprocessor can be easily broken, unless appropriate countermeasures are taken. In some cases, the full key can be retrieved with a single chosen ciphertext, while in other cases (such as RSA protected by the popular OAEP technique), a larger number of ciphertexts is required. The attack

D. Wagner (Ed.): CRYPTO 2008, LNCS 5157, pp. 231–240, 2008.

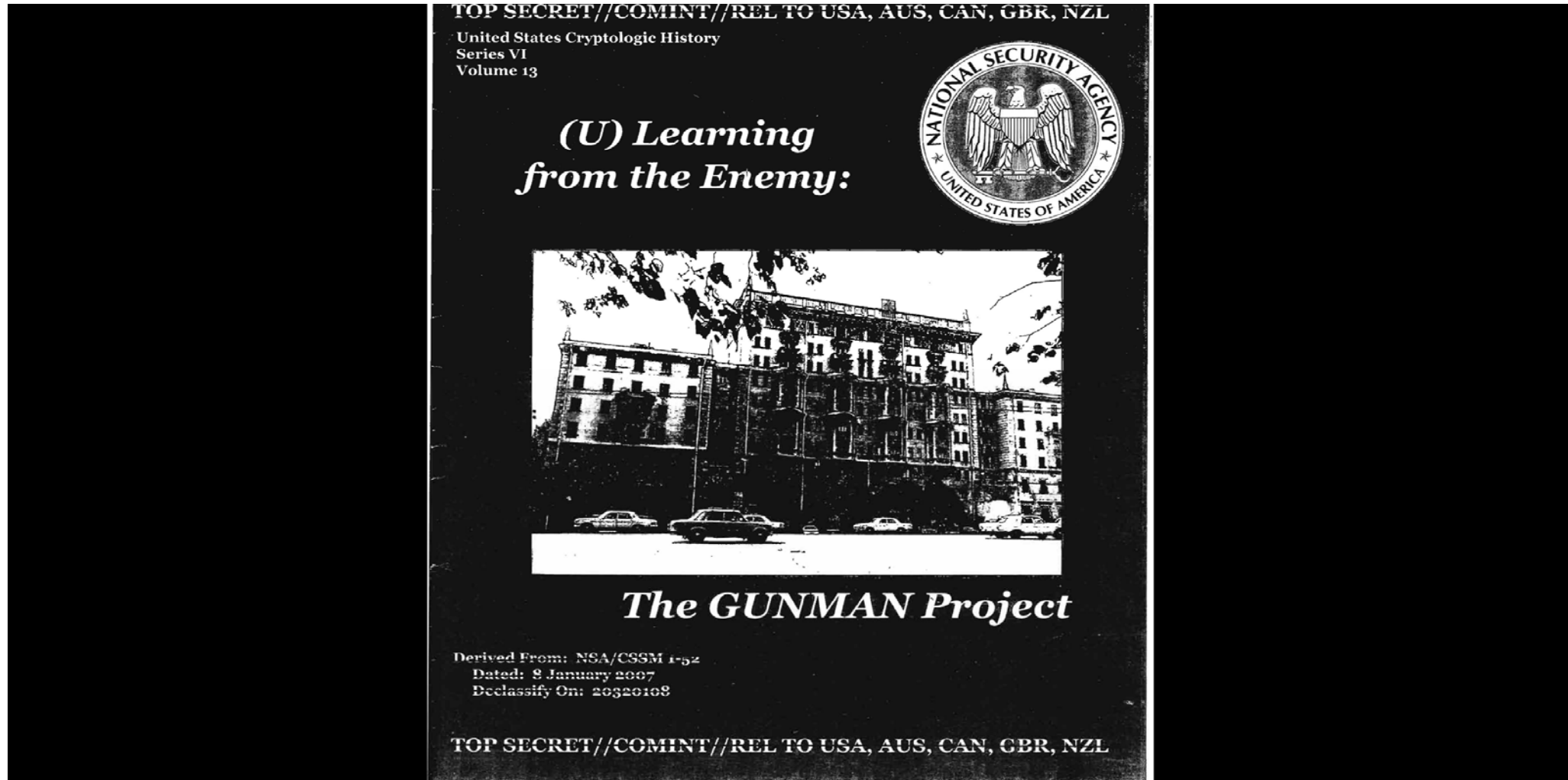
Design of cryptographic primitives and protocols: some historical steps

- Security by obscurity: hiding everything
- Principle of Kerckoffs (« only the key is secret ») - Shannon (« The enemy *knows* the system »)
- Resistance to linear and differential attacks
- **Side-channels attacks**
- **Fault attacks**
- New principle: « the enemy *generates* the key, the algorithm, the protocol and has *access* to the system (software, hardware, ...)»

Operation Farewell: not only a movie

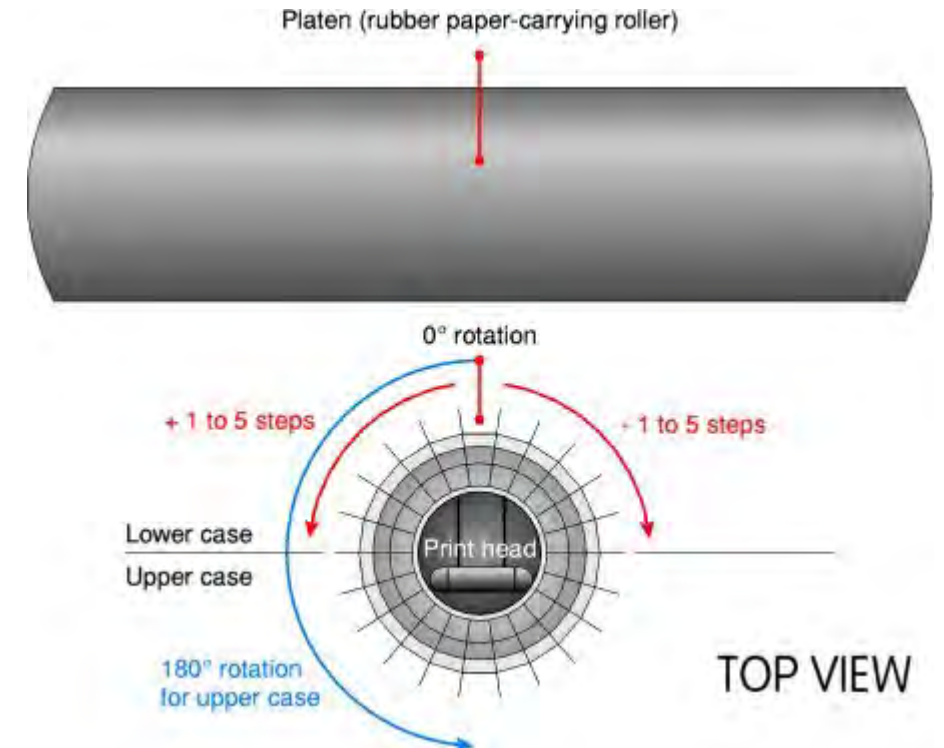
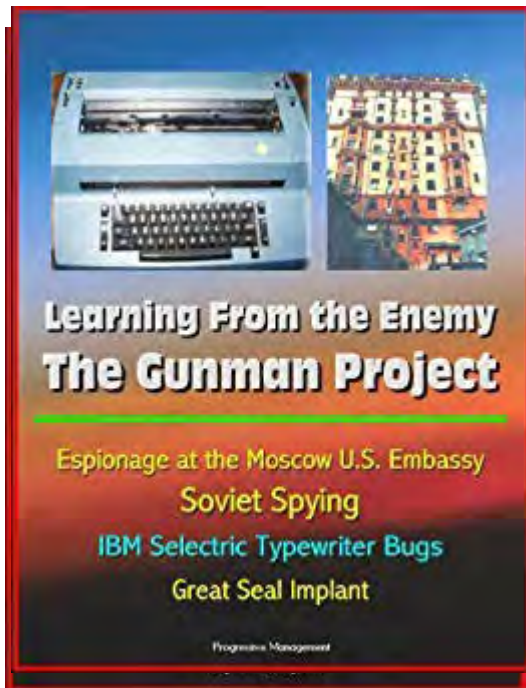


The GUNMAN project (US embassy in Moscow)

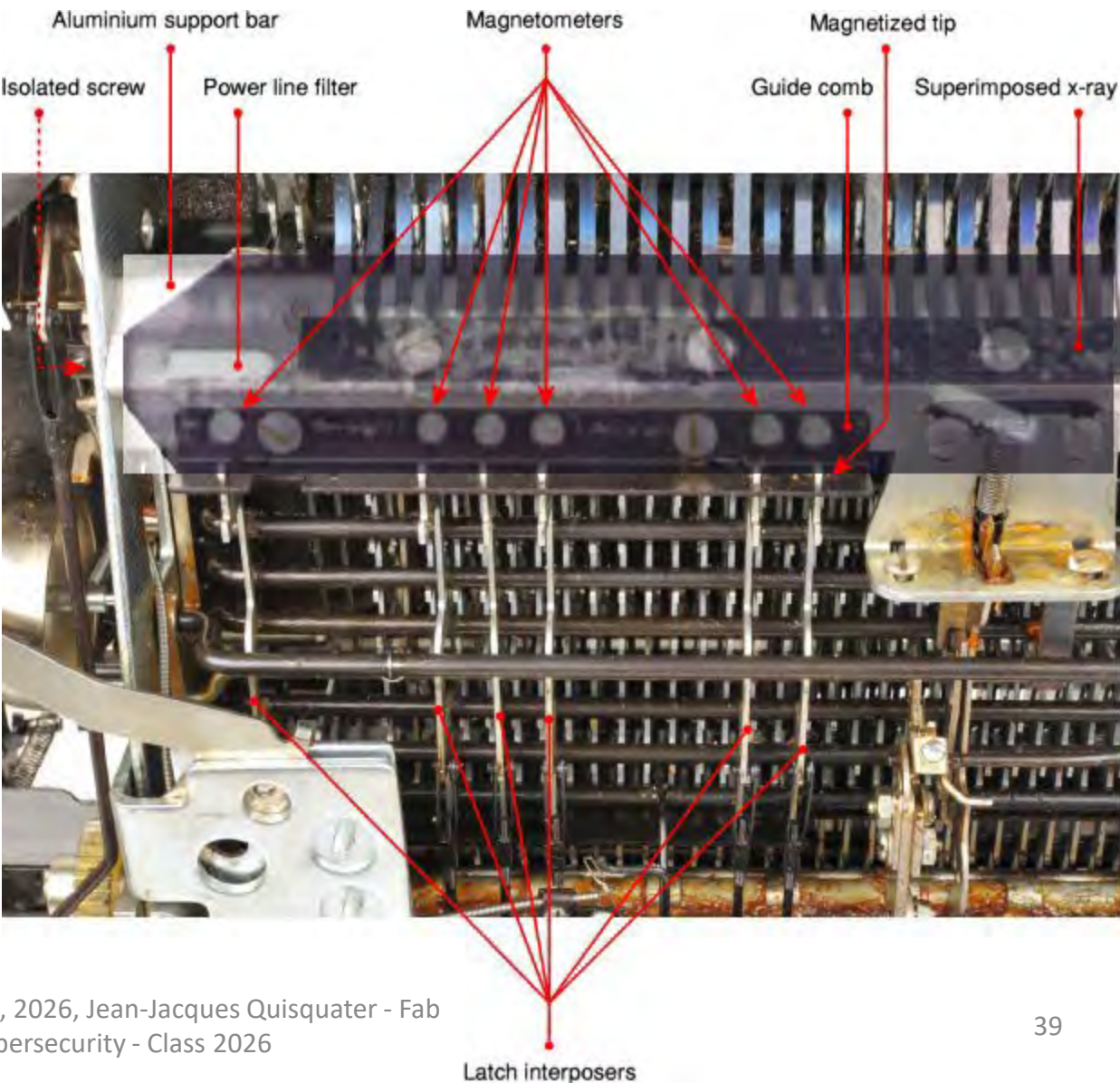
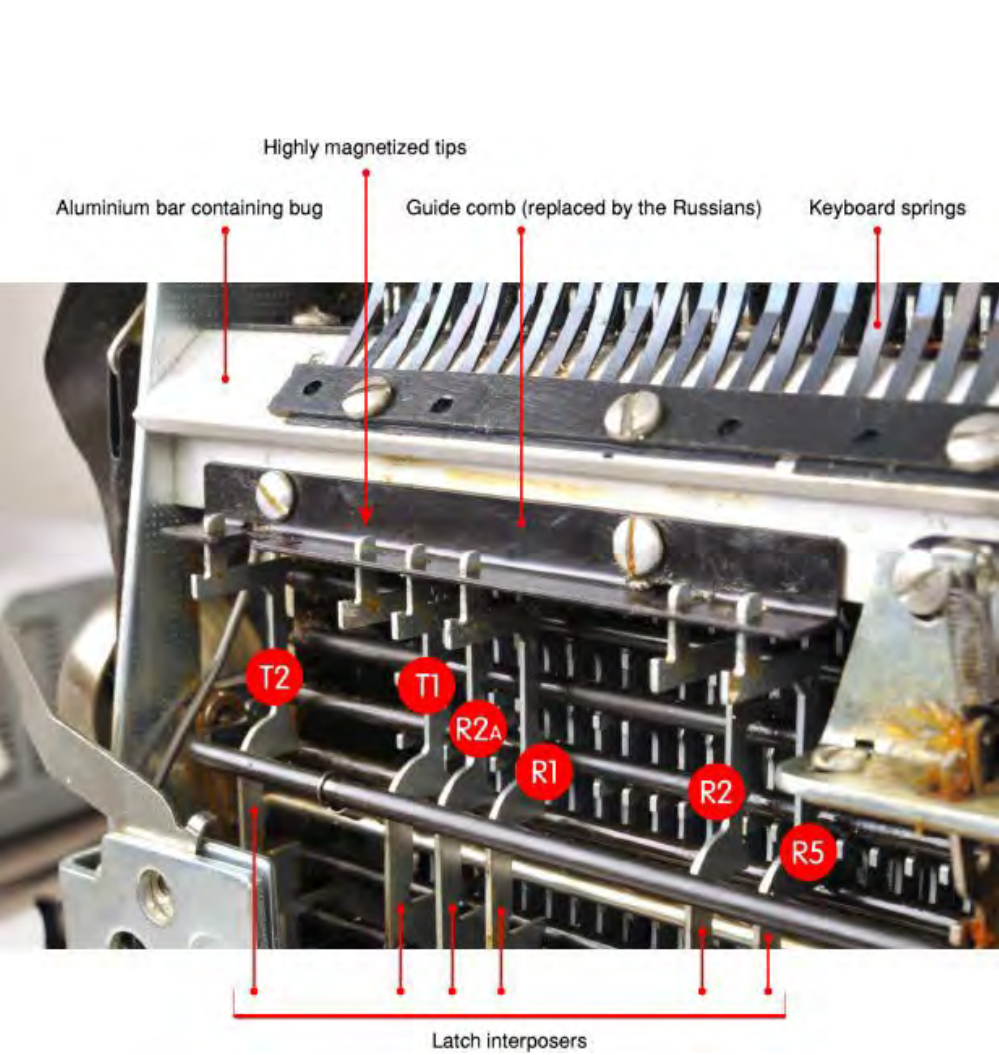


US embassy in Moscow (1984): IBM typewriter

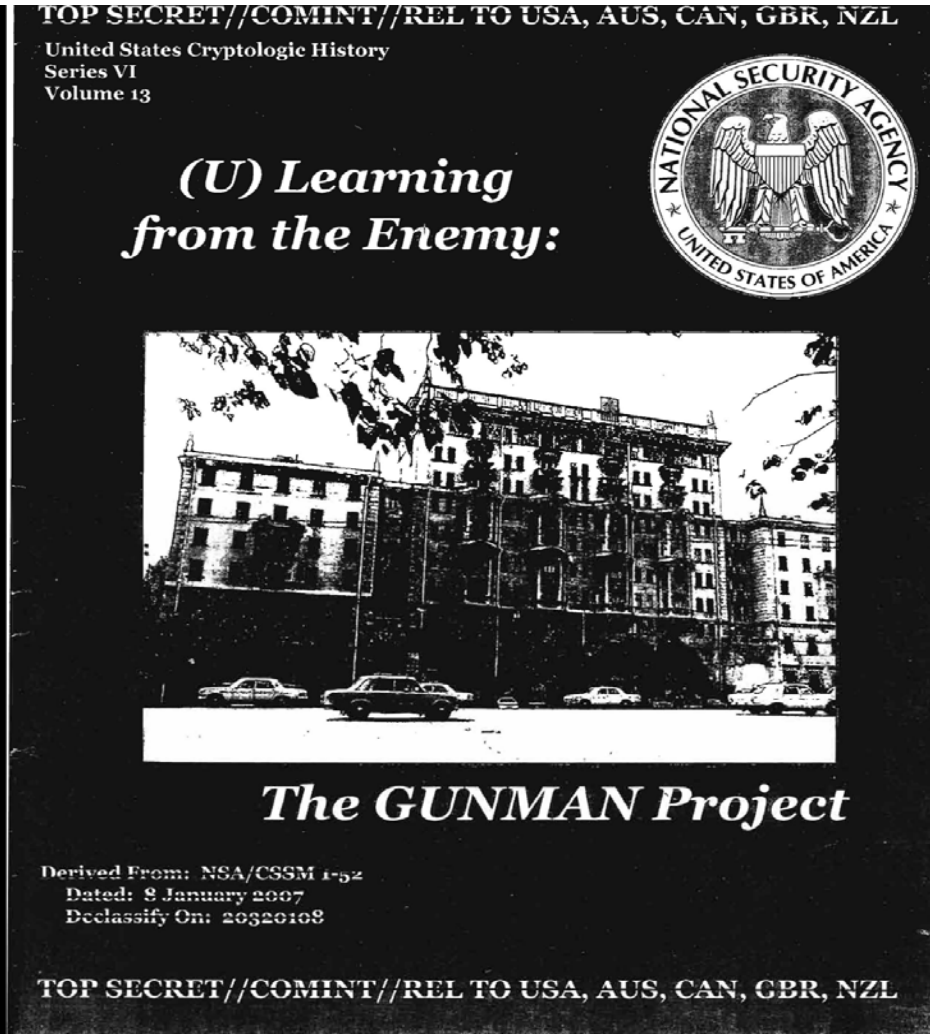
<https://www.cryptomuseum.com/covert/bugs/selectric/>



Modifications (France discovered and said it to USA)



NSA report (internal version) + book





CENTRAL
INTELLIGENCE
AGENCY

THE WORK OF A NATION.
THE CENTER OF INTELLIGENCE.

Report Information

Contact

Search CIA.gov...

SEARCH

عربي 中文 Français Русский Español More ▶

HOME

ABOUT CIA

CAREERS & INTERNSHIPS

OFFICES OF CIA

NEWS & INFORMATION

LIBRARY

KIDS' ZONE

Library



Library

Publications

Center for the Study of Intelligence

About CSI

CSI Publications

Books and Monographs

Studies in Intelligence

Index of Declassified Articles

How to Submit Articles

How to Obtain Publications

Studies Archive Indexes

CIA Museum

US Intelligence Sites

Home » Library » Center for the Study of Intelligence » CSI Publications » Studies in Intelligence » studies » 96unclass » **The Farewell Dossier**

The Farewell Dossier

Duping the Soviets

Gus W. Weiss

During the Cold War, and especially in the 1970s, Soviet intelligence carried out a substantial and successful clandestine effort to obtain technical and scientific knowledge from the West. This effort was suspected by a few US Government officials but not documented until 1981, when French intelligence obtained the services of Col. Vladimir I. Vetrov, "Farewell," who photographed and supplied 4,000 KGB documents on the program. In the summer of 1981, President Mitterrand told President Reagan of the source, and, when the material was supplied, it led to a potent counterintelligence response by CIA and the NATO intelligence services.

President Nixon and Secretary of State Kissinger conceived of détente as the search for ways of easing chronic strains in US-Soviet relations. They sought to engage the USSR in arrangements that would move the superpowers from confrontation to

We communists have to string along with the capitalists for a while. We need their credits, their agriculture, and their technology. But we are going to continue massive military programs and by the middle 1980s we will be in a position to return to a much more aggressive foreign policy designed to gain the upper hand in our relationship with the West. -- Leonid Brezhnev, remarks in 1971 to the Politburo at the beginning of détente.

CONNECT WITH CIA



TWITTER FEED

Tweets by @CIA



CIA
@CIA

This is an S-100 pressure suit for a U-2R plane. High-altitude pilots wear pressure suits as protection from cockpit depressurization.[cia.gov/about-cia/cia-...](https://www.cia.gov/about-cia/cia-...)

#HISTINT #Museum

Embed

View on Twitter

View @CIA Twitter Feed

Teletypes with a trick: embassy of France in Moscow

1) Les téléimprimeurs de l'Ambassade de France à Moscou

Cet épisode de la guerre froide en marge de l'affaire d'espionnage Farewell (surnom de la taupe du KGB qui s'était mise au service de la France) est peu connu. Pourtant il semble avoir eu des conséquences désastreuses sur la suite de celle-ci. C'est le Colonel Cattieu qui dirigeait à l'époque le Service central du chiffre et de la sécurité des télécommunications(SCCST) (l'ANSSI de l'époque) qui m'en a fait le récit. Il l'a relatée dans un bulletin de l'ARCSI consacré à Myosotis.

Comme beaucoup le savent ici, l'introduction de l'électricité dans les machines de traitement de l'écrit, parmi lesquels figurent les cryptographes, a généré de nouvelles vulnérabilités du fait notamment des parasites émis par ces machines. Ceux-ci peuvent dans certaines circonstances être compromettants. Lorsque ces phénomènes ont été découverts ils ont donné lieu à l'édition par l'OTAN de normes spécifiques hautement classifiées communément appelées normes « TEMPEST ». Mais dans l'affaire qui nous occupe il ne s'agissait pas de signaux parasites fortuits mais provoqués.

Téléimprimeur Sagem SPE 5

Tempest



Les téléscripteurs français (Quai d'Orsay) de l'ambassade à Moscou (1983)

- Grâce à *Jour*, probablement, les nouveaux téléscripteurs installés à l'ambassade de France à Moscou, entre octobre 1976 et février 1977, furent «écoutés» pendant six ans. L'ambassade de France à Moscou était depuis longtemps une cible favorite du KGB, et le livre raconte comment dans les années 60 de charmantes Mata Hari soviétiques entreprirent de séduire l'ambassadeur, Maurice Dejean, et l'attaché de l'air, le colonel Louis Guibaud. ...
- « Jour » est une recrue du KGB (actif entre 1945 et 1983), employé du chiffre au Quai d'Orsay, Paris, ...



With only a
simple add-on

capacitor



Tempest (codename)

From Wikipedia, the free encyclopedia

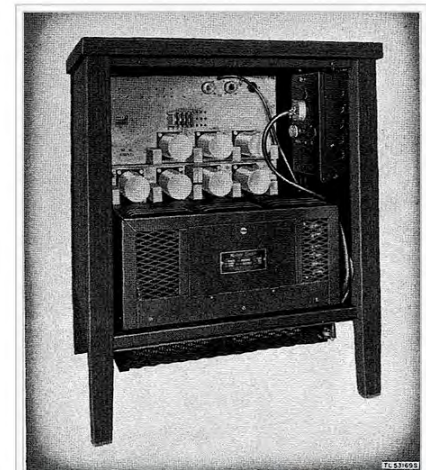
TEMPEST (Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions)^[1] is a U.S. [National Security Agency](#) specification and a [NATO](#) certification^{[2][3]} referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations.^[4] TEMPEST covers both methods to spy upon others and how to shield equipment against such spying. The protection efforts are also known as emission security (EMSEC), which is a subset of [communications security](#) (COMSEC).^[5]

The NSA methods for spying on computer emissions are classified, but some of the protection standards have been released by either the NSA or the Department of Defense.^[6] Protecting equipment from spying is done with distance, shielding, filtering, and masking.^[7] The TEMPEST standards mandate elements such as equipment distance from walls, amount of shielding in buildings and equipment, and distance separating wires carrying classified vs. unclassified materials,^[6] filters on cables, and even distance and shielding between wires or equipment and building pipes. Noise can also protect information by masking the actual data.^[7]

While much of TEMPEST is about [leaking electromagnetic emanations](#), it also encompasses sounds and mechanical vibrations.^[6] For example, it is possible to log a user's keystrokes using the [motion sensor](#) inside [smartphones](#).^[8] Compromising emissions are defined as unintentional [intelligence](#)-bearing signals which, if intercepted and analyzed ([side-channel attack](#)), may disclose the information transmitted, received, handled, or otherwise processed by any information-processing equipment.^[9]

Contents [hide]

- [History](#)
- [Shielding standards](#)
- [Certification](#)
- [RED/BLACK separation](#)
- [Correlated emanations](#)
- [Public research](#)
- [In popular culture](#)
- [See also](#)
- [References](#)
- [External links](#)



Bell 131B2 mixer, used to [XOR](#) teleprinter signals with one time tapes, was the first device from which classified plain text was extracted using radiated signals.

History [\[edit\]](#)

During World War II, [Bell Telephone](#) supplied the U.S. military with the **131-B2** mixer device that encrypted teleprinter signals by **XOR**'ing them with key material from **one-time tapes** (the **SIGTOT** system) or, earlier, a rotor-based key generator called **SIGCUM**. It used electromechanical relays in its operation. Later Bell informed the Signal Corps that they were able to detect electromagnetic spikes at a distance from the mixer and recover the plain text. Meeting skepticism over whether the phenomenon they discovered in the laboratory could really be dangerous, they demonstrated their ability to recover plain text from a Signal Corps' crypto center on Varick Street in Lower Manhattan. Now alarmed, the Signal Corps asked Bell to investigate further. Bell identified three problem areas: radiated signals, signals conducted on wires extending from the facility, and magnetic fields. As possible solutions, they suggested shielding, filtering and masking.



Rotor machines, like this **SIGCUM**, were an early source of compromising TEMPEST effects

Bell developed a modified mixer, the 131-A1 with shielding and filtering, but it proved difficult to maintain and too expensive to deploy. Instead, relevant commanders were warned of the problem and advised to control a 100-foot (30.48-meter)-diameter zone around their communications center to prevent covert interception, and things were left at that. Then in 1951, the CIA rediscovered the problem with the 131-B2 mixer and found they could recover plain text off the line carrying the encrypted signal from a quarter-mile away. Filters for signal and power lines were developed, and the recommended control-perimeter radius was extended to 200 feet, based more on what commanders could be expected to accomplish than any technical criteria.

A long process of evaluating systems and developing possible solutions followed. Other compromising effects were discovered, such as fluctuations in the power line as rotors stepped. The question of exploiting the noise of electromechanical encryption systems had been raised in the late 1940s, but was re-evaluated now as a possible threat. Acoustical emanations could reveal plain text, but only if the pick-up device was close to the source. Nevertheless, even mediocre microphones would do.

Soundproofing the room made the problem worse by removing reflections and providing a cleaner signal to the recorder.

In 1956, the [Naval Research Laboratory](#) developed a better mixer that operated at much lower voltages and currents and therefore radiated far less. It was incorporated in newer NSA encryption systems. However, many users needed the higher signal levels to drive teleprinters at greater distances or where multiple teleprinters were connected, so the newer encryption devices included the option to switch the signal back up to the higher strength. NSA began developing techniques and specifications for isolating sensitive-communications pathways through filtering, shielding, grounding, and physical separation: of those lines that carried sensitive plain text – from those intended to carry only non-sensitive data, the latter often extending outside of the secure environment. This separation effort became known as the **Red/Black Concept**. A 1958 joint policy called NAG-1 set radiation standards for equipment and installations based on a 50-foot (15.24-meter) limit of control. It also specified the classification levels of various aspects of the TEMPEST problem. The policy was adopted by Canada and the UK the next year. Six organizations, Navy, Army, Air Force, NSA, CIA, and the State Department were to provide the bulk of the effort for its implementation.



Relay logic, such as in this **Flexowriter** was another major early source of TEMPEST radiation.

Shielding standards [\[edit \]](#)

Many specifics of the TEMPEST standards are [classified](#), but some elements are public. Current United States and [NATO](#) Tempest standards define three levels of protection requirements:^[11]

- **NATO SDIP-27 Level A** (formerly AMSG 720B) and **USA NSTISSAM Level I**

"Compromising Emanations Laboratory Test Standard"

This is the strictest standard for devices that will be operated in *NATO Zone 0* environments, where it is assumed that an attacker has almost immediate access (e.g. neighbouring room, 1 m distance).

- **NATO SDIP-27 Level B** (formerly AMSG 788A) and **USA NSTISSAM Level II**

"Laboratory Test Standard for Protected Facility Equipment"

This is a slightly relaxed standard for devices that are operated in *NATO Zone 1* environments, where it is assumed that an attacker cannot get closer than about 20 m (or where building materials ensure an attenuation equivalent to the free-space attenuation of this distance).

- **NATO SDIP-27 Level C** (formerly AMSG 784) and **USA NSTISSAM Level III**

"Laboratory Test Standard for Tactical Mobile Equipment/Systems"

An even more relaxed standard for devices operated in *NATO Zone 2* environments, where attackers have to deal with the equivalent of 100 m of free-space attenuation (or equivalent attenuation through building materials).

Additional standards include:

- **NATO SDIP-29** (formerly AMSG 719G)

"Installation of Electrical Equipment for the Processing of Classified Information"

This standard defines installation requirements, for example in respect to grounding and cable distances.

- **AMSG 799B**

"NATO Zoning Procedures"

Defines an attenuation measurement procedure, according to which individual rooms within a security perimeter can be classified into Zone 0, Zone 1, Zone 2, or Zone 3, which then determines what shielding test standard is required for equipment that processes secret data in these rooms.

The NSA and Department of Defense have declassified some TEMPEST elements after [Freedom of Information Act](#) requests, but the documents black out many key values and descriptions. The declassified version of the [TEMPEST test standard](#) is heavily [redacted](#), with emanation limits and test procedures blacked out.^{[[citation needed](#)]} A redacted version of the introductory Tempest handbook NACSIM 5000 was publicly released in December 2000. Additionally, the current [NATO](#) standard SDIP-27 (before 2006 known as AMSG 720B, AMSG 788A, and AMSG 784) is still classified.

Public research [\[edit \]](#)

In 1985, [Wim van Eck](#) published the first unclassified technical analysis of the security risks of emanations from [computer monitors](#). This paper caused some consternation in the security community, which had previously believed that such monitoring was a highly sophisticated attack available only to [governments](#); van Eck successfully eavesdropped on a real system, at a range of hundreds of [metres](#), using just \$15 worth of equipment plus a [television](#) set.

As a consequence of this research, such emanations are sometimes called "van Eck radiation", and the eavesdropping technique [van Eck phreaking](#), although government researchers were already aware of the danger, as [Bell Labs](#) noted this vulnerability to secure [teleprinter](#) communications during [World War II](#) and was able to produce 75% of the plaintext being processed in a secure facility from a distance of 80 feet. (24 metres)^[18] Additionally the NSA published *Tempest Fundamentals*, *NSA-82-89*, *NACSIM 5000*, *National Security Agency* (Classified) on February 1, 1982. In addition, the van Eck technique was successfully demonstrated to non-TEMPEST personnel in [Korea](#) during the [Korean War](#) in the 1950s.^[citation needed]

[Markus Kuhn](#) has discovered several low-cost techniques for reducing the chances that emanations from computer displays can be monitored remotely.^[19] With [CRT](#) displays and [analog](#) video cables, filtering out [high-frequency](#) components from [fonts](#) before rendering them on a computer screen will attenuate the energy at which text characters are broadcast.^{[20][21]} With modern [flat panel displays](#), the high-speed digital [serial interface \(DVI\)](#) cables from the [graphics controller](#) are a main source of compromising emanations. Adding random [noise](#) to the [least significant bits](#) of pixel values may render the emanations from flat-panel displays unintelligible to eavesdroppers but is not a secure method. Since DVI uses a [certain bit code scheme](#) that tries to transport a balanced signal of 0 bits and 1 bits, there may not be much difference between two pixel colors that differ very much in their color or intensity. The emanations can differ drastically even if only the last bit of a pixel's color is changed. The signal received by the eavesdropper also depends on the frequency where the emanations are detected. The signal can be received on many frequencies at once and each frequency's signal differs in [contrast](#) and [brightness](#) related to a certain color on the screen. Usually, the technique of smothering the RED signal with noise is not effective unless the power of the noise is sufficient to drive the eavesdropper's receiver into [saturation](#) thus overwhelming the receiver input.

[LED](#) indicators on computer equipment can be a source of compromising optical emanations.^[22] One such technique involves the monitoring of the lights on a [dial-up modem](#). Almost all modems flash an LED to show activity, and it is common for the flashes to be directly taken from the data line. As such, a fast optical system can easily see the changes in the flickers from the data being transmitted down the wire.

Recent research^[23] has shown it is possible to detect the radiation corresponding to a keypress event from not only [wireless](#) (radio) keyboards, but also from traditional wired keyboards, and even from laptop keyboards. From the 1970s onward, Soviet bugging of US Embassy [IBM Selectric](#) typewriters allowed the keypress-derived mechanical motion of bails, with attached magnets, to be detected by implanted magnetometers, and converted via hidden electronics to a digital radio frequency signal. Each eight character transmission provided Soviet access to sensitive documents, as they were being typed, at US facilities in Moscow and Leningrad.^[24]

In 2014, researchers introduced "AirHopper", a bifurcated attack pattern showing the feasibility of data exfiltration from an isolated computer to a nearby mobile phone, using FM frequency signals.^{[25][26]}

In 2015, "BitWhisper", a Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations was introduced. "BitWhisper" supports bidirectional communication and requires no additional dedicated peripheral hardware.^{[27][28]}

[Main page](#)
[Contents](#)
[Featured content](#)
[Current events](#)
[Random article](#)
[Donate to Wikipedia](#)
[Wikipedia store](#)

Interaction

[Help](#)
[About Wikipedia](#)
[Community portal](#)
[Recent changes](#)
[Contact page](#)

Tools

[What links here](#)
[Related changes](#)
[Upload file](#)
[Special pages](#)
[Permanent link](#)
[Page information](#)
[Wikidata item](#)
[Cite this page](#)

Print/export

[Download as PDF](#)
[Printable version](#)

Languages



[Deutsch](#)
[Español](#)
[Magyar](#)

Van Eck phreaking

From Wikipedia, the free encyclopedia

Van Eck phreaking (also known as **Van Eck Radiation**) is a form of eavesdropping in which special equipment is used to pick up [side-band electromagnetic emissions](#) from electronic devices that correlate to hidden signals or data for the purpose of recreating these signals or data in order to spy on the electronic device. Side-band electromagnetic radiation emissions are present in (and with the proper equipment, can be captured from) keyboards, computer displays, printers, and other electronic devices.

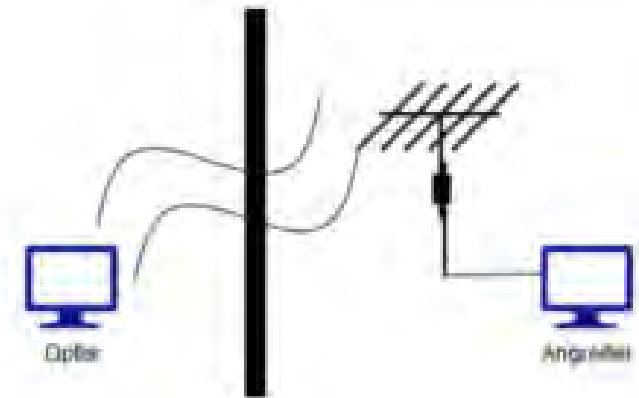
In 1985, **Wim van Eck** published the first unclassified technical analysis of the security risks of emanations from [computer monitors](#). This paper caused some consternation in the security community, which had previously believed that such monitoring was a highly sophisticated attack available only to [governments](#); van Eck successfully eavesdropped on a real system, at a range of hundreds of [metres](#), using just \$15 worth of equipment plus a [television](#) set.

As a consequence of this research, such emanations are sometimes called "van Eck radiation", and the eavesdropping technique van Eck phreaking. Government researchers were already aware of the danger, as [Bell Labs](#) had noted this vulnerability to secure [teleprinter](#) communications during [World War II](#) and was able to produce 75% of the plaintext being processed in a secure facility from a distance of 80 feet (24 metres).^[1] Additionally the NSA published *Tempest Fundamentals*, *NSA-82-89*, *NACSIM 5000*, *National Security Agency* (Classified) on February 1, 1982. In addition, the van Eck technique was successfully demonstrated to non-TEMPEST personnel in [Korea](#) during the [Korean War](#) in the 1950s.

While [Phreaking](#) is the process of exploiting [telephone networks](#), it is used here because of its connection to eavesdropping. Van Eck phreaking of CRT displays is the process of [eavesdropping](#) on the contents of a [CRT](#) by detecting its [electromagnetic emissic](#)

Contents [hide]

- 1 [Basic principle](#)
 - 1.1 [CRTs](#)
 - 1.2 [LCDs](#)
 - 1.3 [Communicating using Van Eck phreaking](#)
 - 1.4 [Tailored access batteries](#)
- 2 [Potential risks](#)
- 3 [Further research](#)
- 4 [See also](#)
- 5 [References](#)
- 6 [External links](#)



Side-channel attacks (physical) (+ covert channel)

- See also other talk
- Old stories
- Remote attacks:
 - Timing (first attack by Kocher)
- Local attacks
 - Passive:
 - Plain or differential
 - Timing:
 - Power:
 - Electromagnetic (EMA)
 - Other:
 - Active:
 - fault attacks

SPA

Help

About Wikipedia

Community portal

Recent changes

Contact page

Tools

What links here

Related changes

Upload file

Special pages

Permanent link

Page information

Wikidata item

Cite this page

Print/export

Download as PDF

Printable version

Languages

Français

한국어

Lietuvių

日本語

Русский

中文

Edit links

In **cryptography**, **power analysis** is a form of **side channel attack** in which the attacker studies the power consumption of a cryptographic hardware device (such as a **smart card**, **tamper-resistant "black box"**, or **integrated circuit**). The attack can non-invasively extract cryptographic keys and other secret information from the device.

Simple power analysis (SPA) involves visually interpreting power *traces*, or graphs of electrical activity over time.

Differential power analysis (DPA) is a more advanced form of power analysis, which can allow an attacker to compute the intermediate values within cryptographic computations through statistical analysis of data collected from multiple cryptographic operations. SPA and DPA were introduced to the open cryptology community in 1998 by **Paul Kocher**, **Joshua Jaffe** and **Benjamin Jun**.^[1]

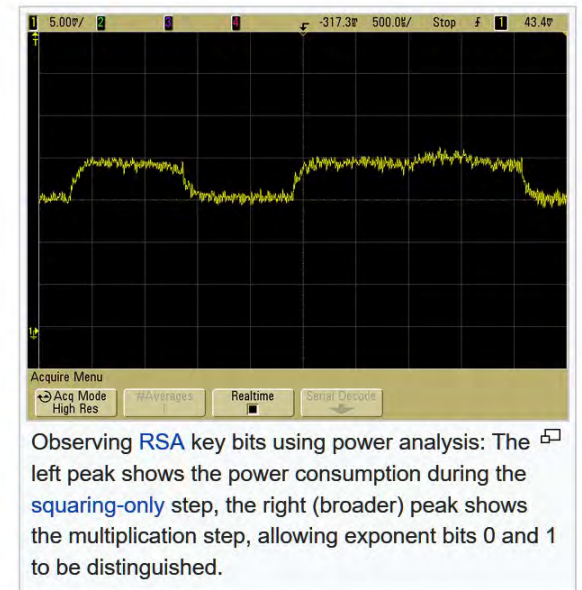
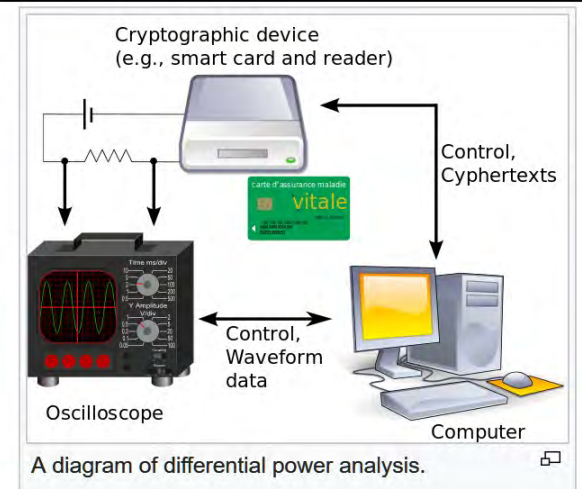
Contents [hide]

- 1 Simple power analysis
- 2 Differential power analysis
- 3 High-order differential power analysis
- 4 Power analysis and algorithmic security
- 5 Standards and practical security concerns
- 6 Preventing simple and differential power analysis attacks
- 7 Patents
- 8 References

Simple power analysis [edit]

Simple power analysis (SPA) is a **side-channel attack** which involves visual examination of graphs of the **current** used by a device over time. Variations in power consumption occur as the device performs different operations. For example, different instructions performed by a microprocessor will have differing power consumption profiles. As a result, in a power trace from a smart card using **DES** encryption, the sixteen rounds can be seen clearly. Similarly, squaring and multiplication operations in RSA implementations can often be distinguished, enabling an adversary to compute the secret key. Even if the magnitude of the variations in power consumption are small, standard digital **oscilloscopes** can easily show the data-induced variations. Frequency filters and averaging functions (such as those built into oscilloscopes) are often used to filter out high-frequency components.

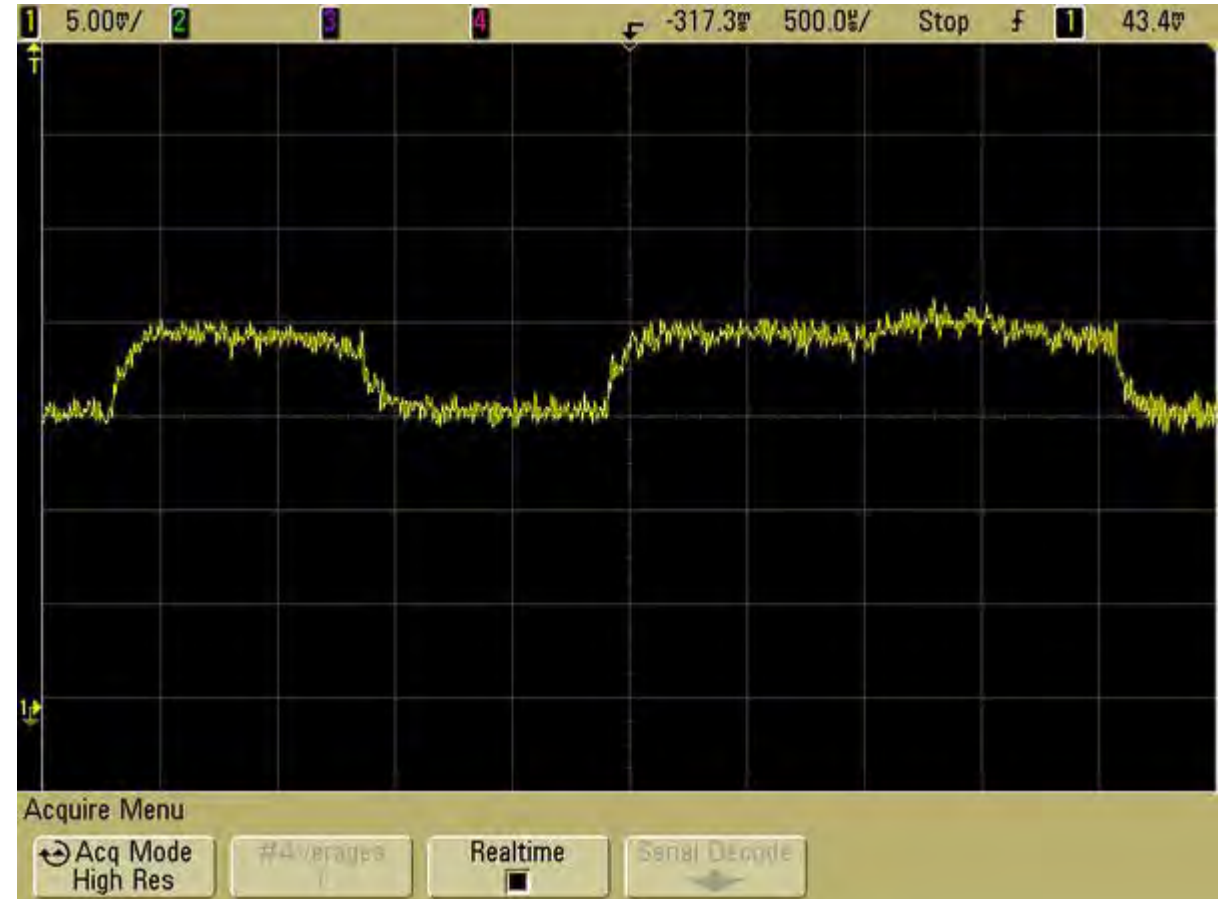
Differential power analysis [edit]



Attacks: plain or differential?

- Plain:
- Differential: use of correlated inputs taking into account the circuit

Set-up and output

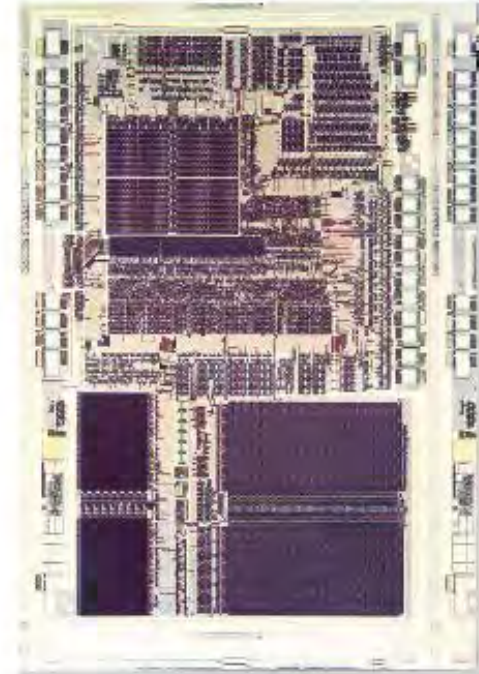
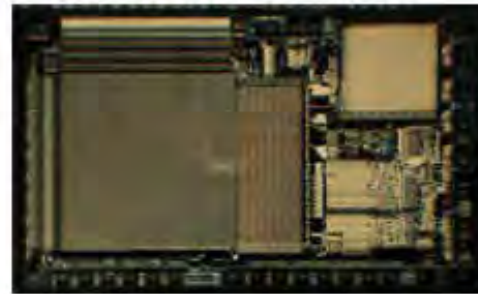
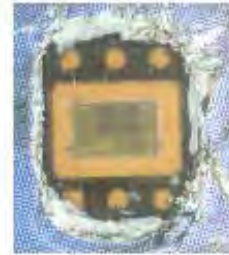


Smart cards and chips

(some attacks were well known long time ago)

- SPA (single power analysis)
- DPA (differential power analysis)
- Timing attacks
- EMA (electromagnetic analysis)
- DEMA

Smart cards (old)



Short Story of Smart Cards

- René Barjavel (1966) « La nuit des temps » (Gondas)
- several inventors in USA (IBM - 1968), Japan, Germany, France
- Roland Moreno (F) pushed the right version (1974)
- Michel Ugon and Louis Guillou were the technical inventors (~ 1977)
- **SPOM**: single chip (security): 1981: first crypto algo and protocol (secret key): tests in France
- first **DES**: 1985 (TRASEC, Belgium, TB100 -> Proton)
- first **RSA**: CORSAIR(Philips): 1989 (coprocessor)
- first **RISC 32 bits**: 1997 (CASCADE-> GemExpresso)
- first **JAVA** smart card: 1997 (Schlumberger-software)
- ...



Ring by Moreno (1974)



The chip (a complete computer)

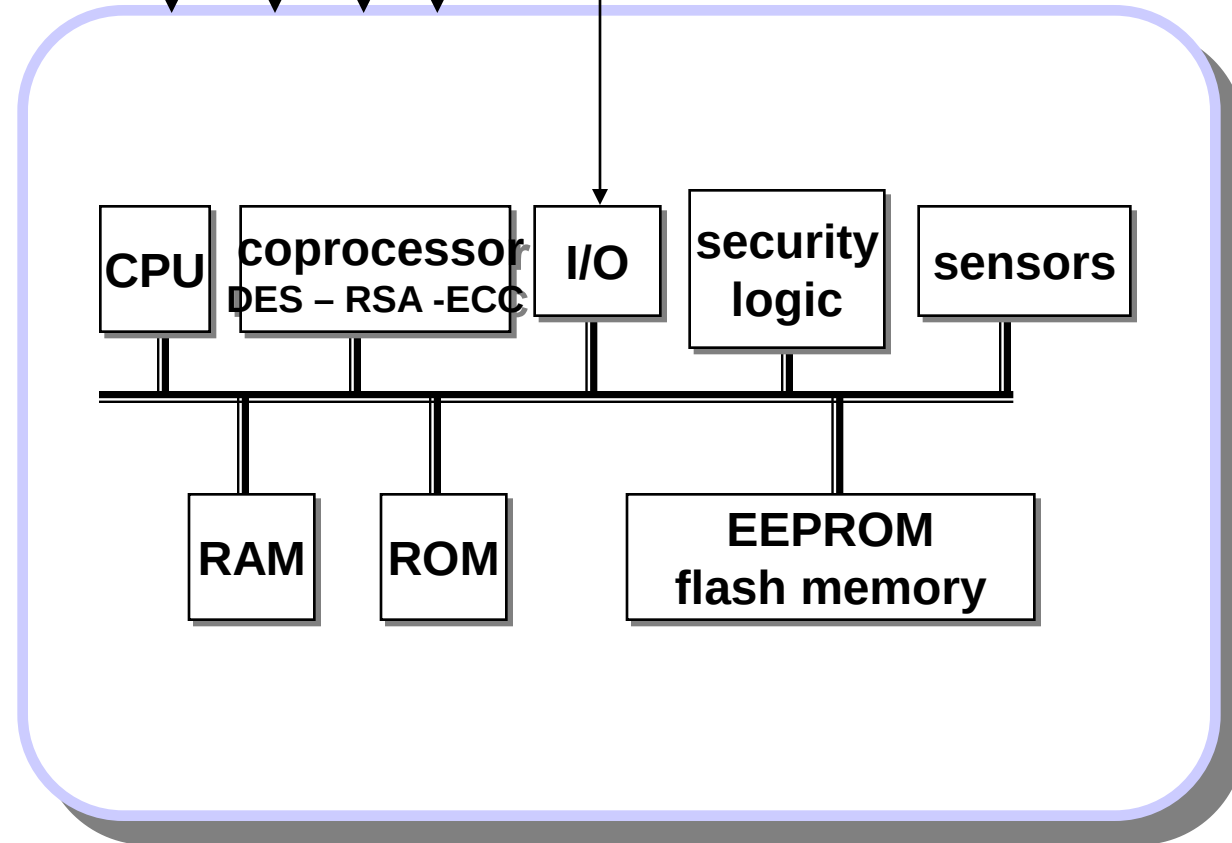
- CPU
- security logic and sensors
- ROM: OS - including self-test procedures
- RAM (mainly static)
- (E)EPROM and/or flash memory
 - cryptographic keys
 - PIN
 - biometric profiles
 - applications
- serial I/O
- internal bus(es)
- accelerators for cryptoalgorithms DES, RSA ... (coprocessors)



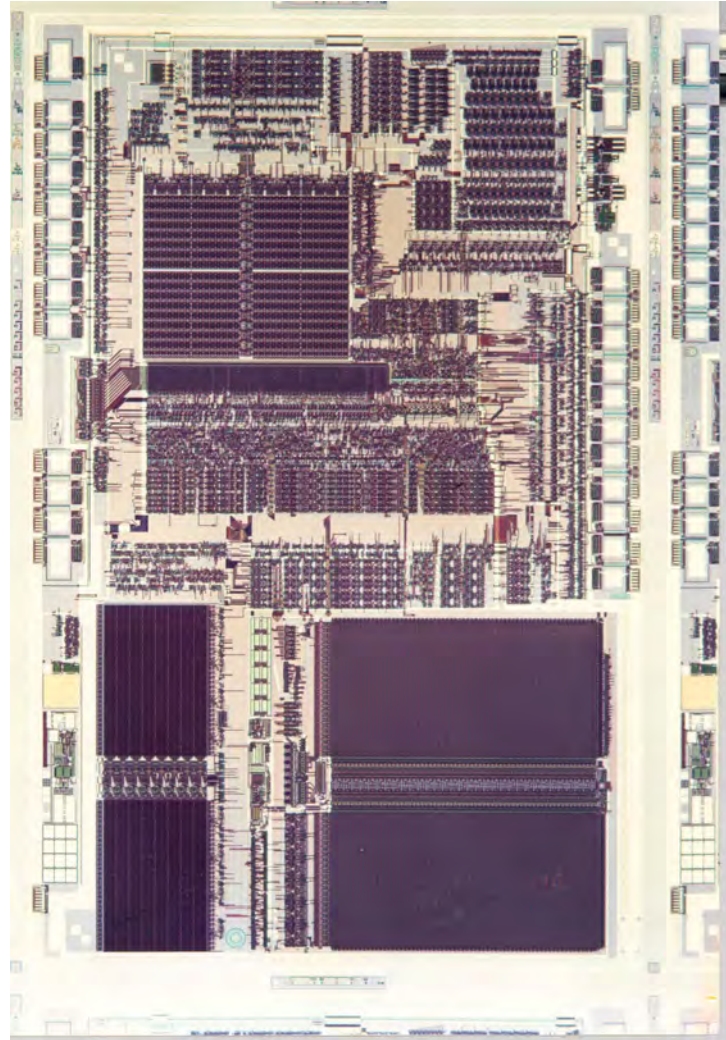
Reset Ground Volt Clock

The chip (IC)

firewall



A complete computer on one chip



Security of smart cards

- The design of first smart cards: only classical design for security (like OS)
- Cryptography
- Secure protocols
- From 1996 smart card as a secure hardware (complete and correct model)



Technical design of smart cards

- Objectives: efficient, not expensive, secure device
 - Identification
 - Authentication
 - Storing money, rights ...
 - Enciphering ...: SECURE COMPUTATION WITH SECRETS
- Methodology
 - Design having in mind the hard possible attacks (including future)
 - New designs, new implementations, verification
- Goals:
 - No correlation between the output (in the general sense) and the internal secrets (keys)



Commercial problem

- What if the attacks (analysis) are « better » than the product?
- Management of the whole system (not only a smart card)
 - Early replacement of smart cards
 - Tracing
 - Flexible security
 - Possible for many applications including banking applications (more difficult for pay-TV-like applications)



Taxonomy of Attackers (from IBM)

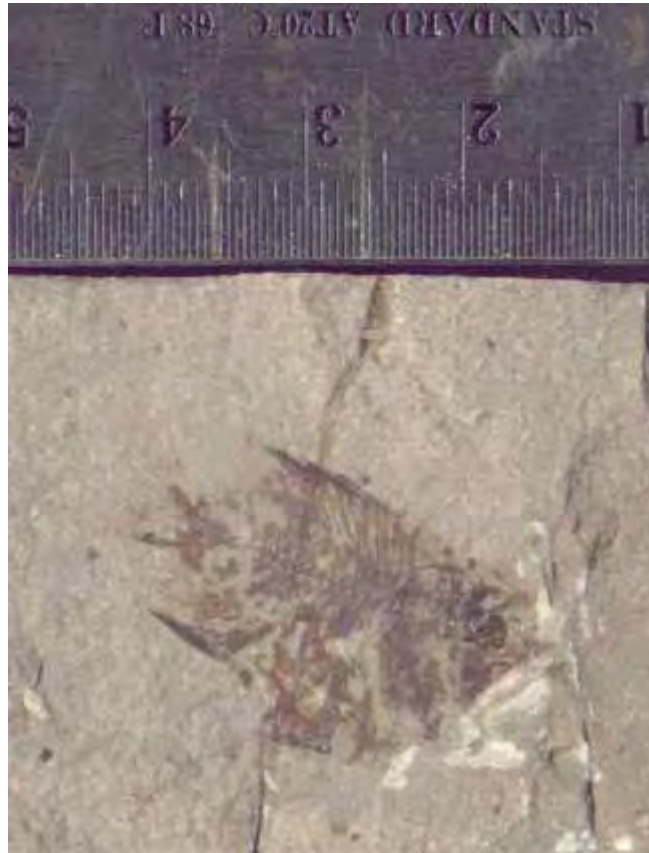
- *Class I* – Clever outsiders - Insufficient knowledge of system, not highly sophisticated equipment, look for existing weaknesses.
- *Class II* – Knowledgeable Insiders - Have potential access to most parts of systems, and highly sophisticated tools.
- *Class III* – Funded Organizations – Governments, terrorists, Mafia have teams of experts, big budgets, most advanced tools.



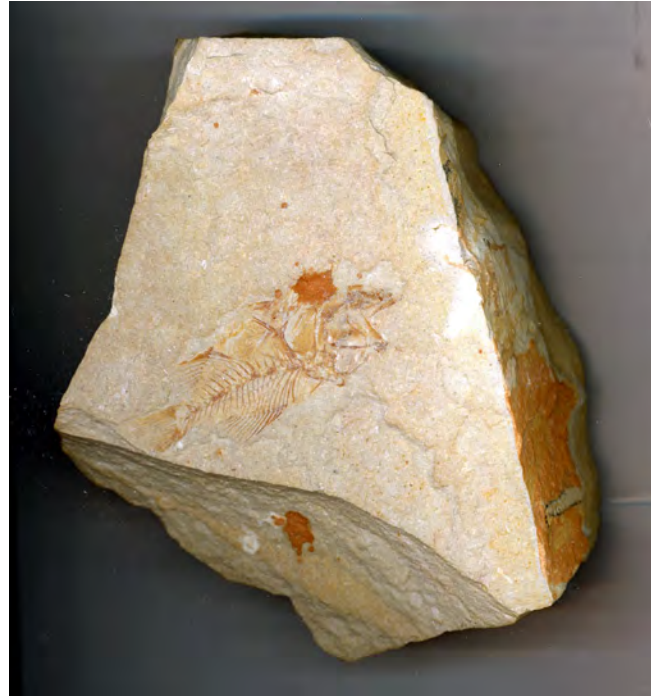
Class I: Hidden Key in Stone



Class I (photo)



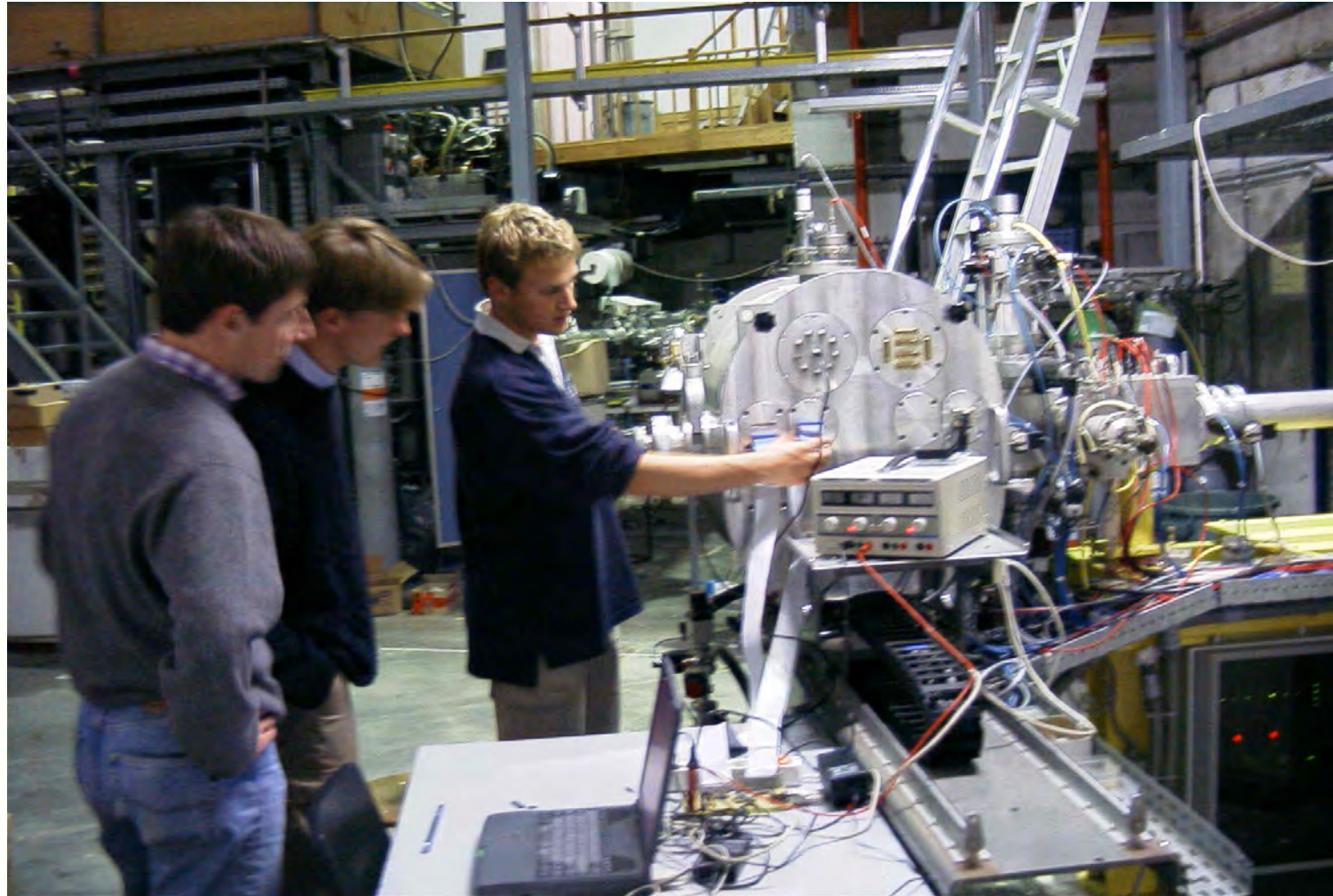
Class I: scanner (+ photoshop)



Class I (photoshop - end)



Class II? Free slot of a cyclotron

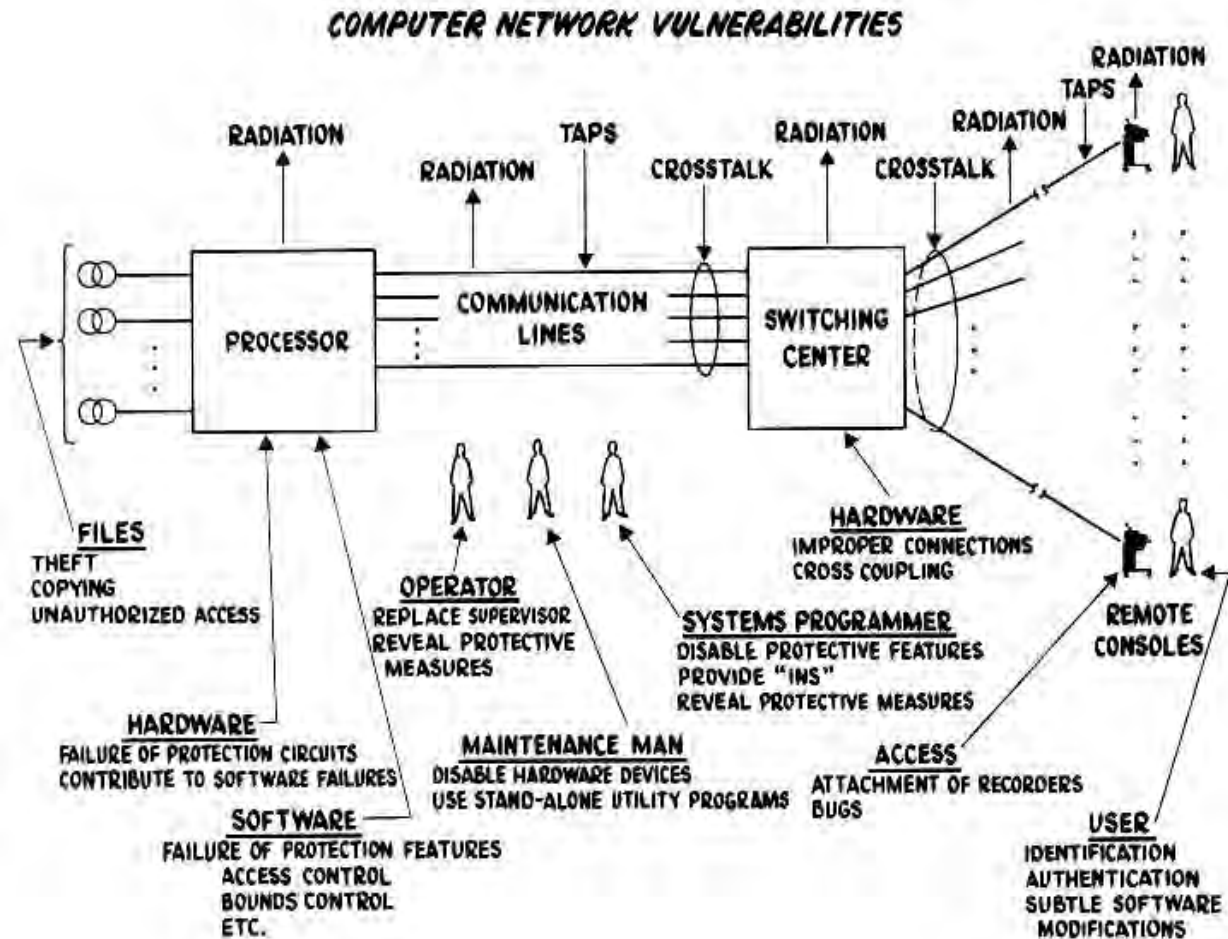


Side Story of Side Channel Analysis

- 1986: PIN code of smart card broken by timing attack ...
- 1992: TNO discovers a relation between smart card power consumption and program code
- 1992: Philips did the same ...
- 1994: TNO develops software to visualise program structure
- 1995: BellCore invents the “MicroWave Attack”, and Differential Fault Analysis (DFA)
- 1995: Paul Kocher invents timing attack
- 1997: Paul Kocher invents Differential Power Analysis (DPA)
- 1998: TNO implements DPA
- 1998: Gemplus invents Voltage Manipulation (VM)
- 1999: TNO implements VM for Single Fault Injection (SFI)
- 2000: Q.-Samyde implements Electromagnetic Analysis (EMA)



Security: Baran (1964, Rand)



EMA analysis (story)

- Old printer (1976) « playing »,
- A Saturday (1978) working with a CRT and a FM receiver,
- **Date:** Wed, 18 Aug 1999 19:15:09 +0300 (EEST)
From: Berke Durak <durakb@crit2.univ-montp2.fr>
To: cypherpunks@toad.com
Subject: *Controlled CPU TEMPEST emanations Hello, After having implemented and successfully tested Ross Anderson's idea to use the video output to synthesize a mediumwave AM signal, I wondered if a similar effect could be obtained by using only the CPU, since it was easy to correlate CPU activity with radio noise. I've just written a quick C program that tries to force activity on the memory bus in a repetitive pattern, with adjustable frequency. After having fiddled with the timings for about one hour, I managed to broadcast a test tune using my Pentium 120 running Linux, giving extremely clear reception on FM band at about 87.5 Mhz (I have in no way calculated or predicted this frequency).*
- Next question: Is it possible to implement a Java applet for Java smart card transmitting subliliinal information (covert channel) using EM effects? Answer ...

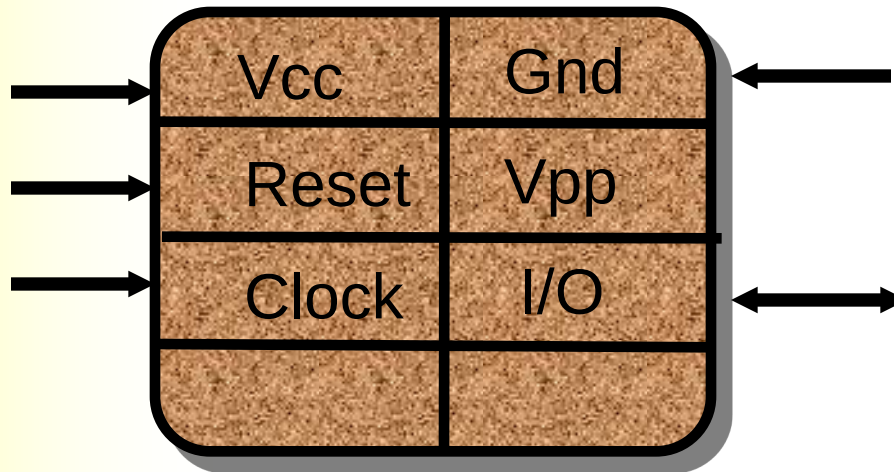


Principles of leakage

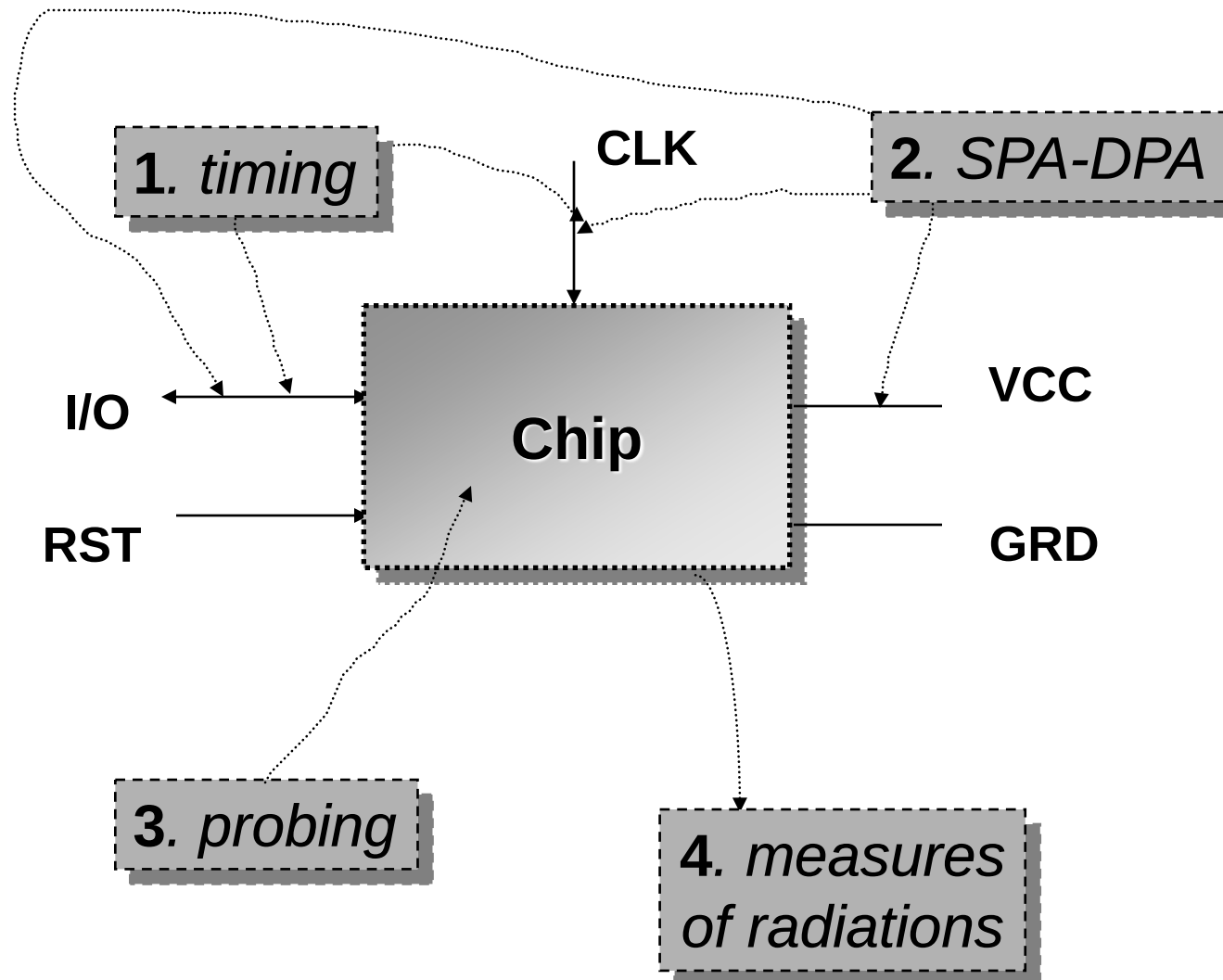
A smart card is a computer without peripherals, it needs external power, reset, clock and a communication connection.

Information sources:

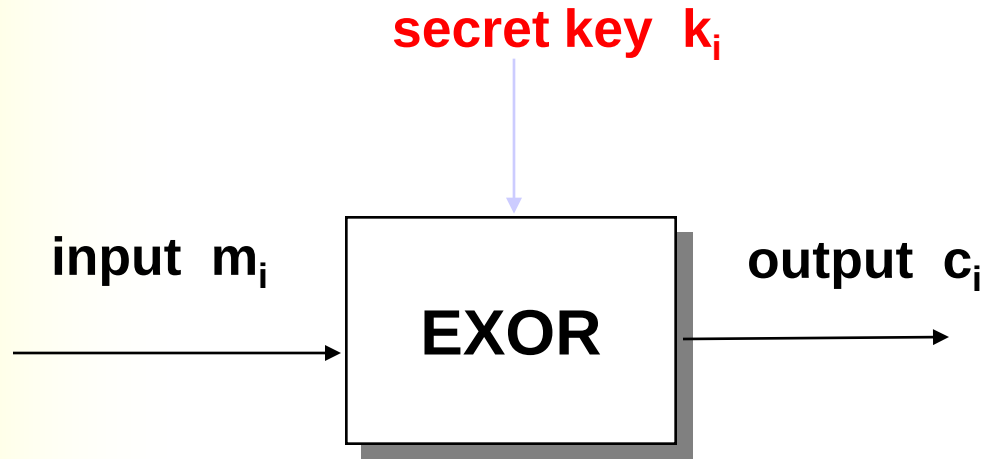
- time
- data flow
- power consumption
- electromagnetic emission
- temperature
- etc.



Generic model of card for passive attacks



Analysis of a simple model (Vernam)



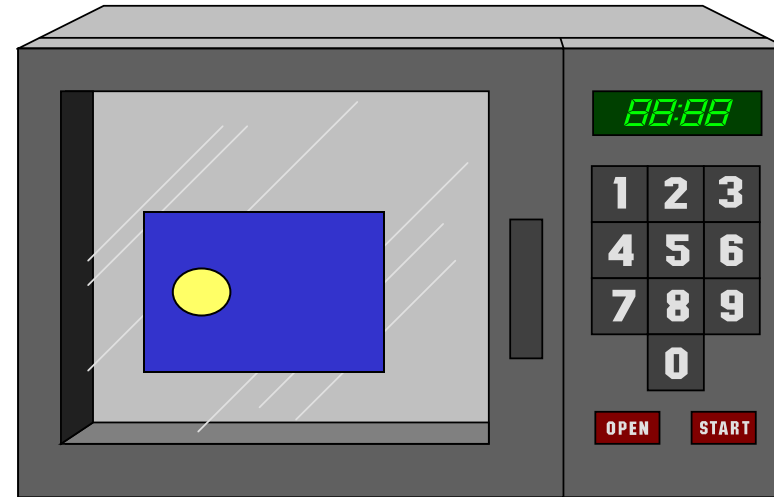
m_i	k_i	c_i
0	0	0
0	1	1
1	0	1
1	1	0

m_i	k_i	c_i
0	0	0
0	1	1
1	0	1
1	1	0

if for some reason the two zeroes are not the same (SPA ...)
this perfect system is completely broken.



Fault attacks



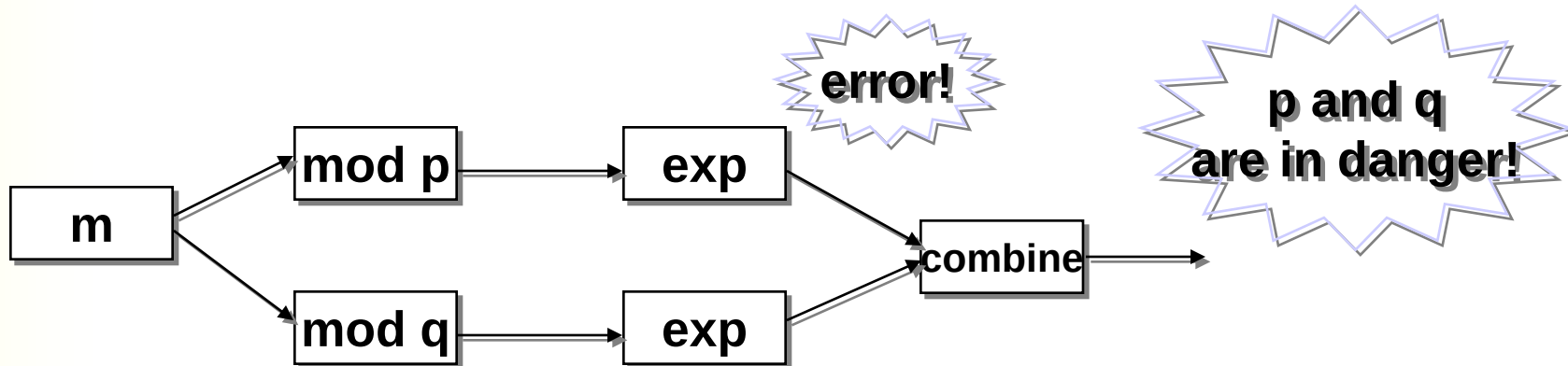
Key=1010110...



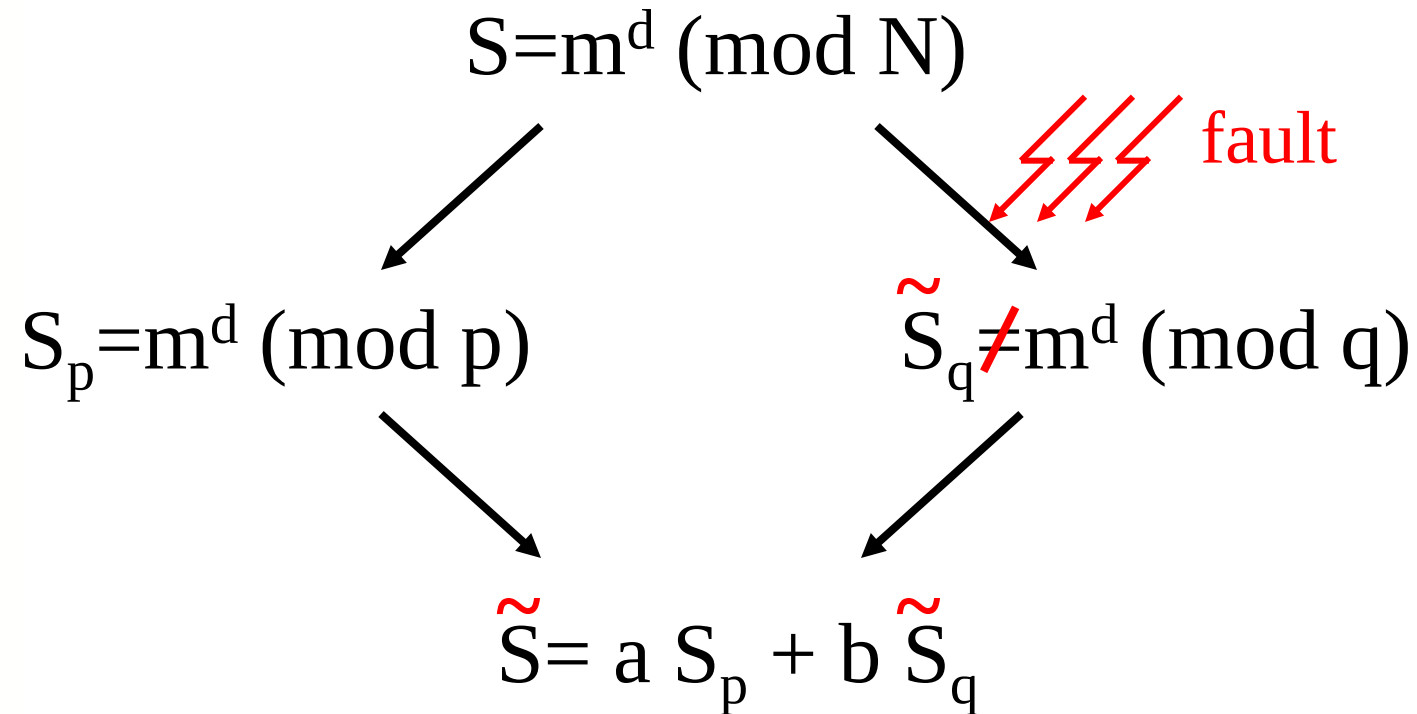
Implementation problems (Joye, Lenstra, Q.)

- optimisation: minimisation of the number of multiplications and square

- Chinese Remainder Theorem



Fault attacks on CRT (RSA)



where:

$$a = 1 \pmod{p}$$

$$a = 0 \pmod{q}$$

$$b = 0 \pmod{p}$$

$$b = 1 \pmod{q}$$



Without fault

- $S = a S_p + b S_q$ where: $a \equiv 1 \pmod{p}$, $a \equiv 0 \pmod{q}$
 $b \equiv 0 \pmod{p}$, $b \equiv 1 \pmod{q}$
- thus,
$$\begin{aligned} S^e \pmod{p} &= S_p^e \pmod{p} \\ &= m^{de} \pmod{p} \\ &= m \pmod{p} \end{aligned}$$
- same $\pmod{q}$



With fault

- $\tilde{S} = a S_p + b \tilde{S}_q$ where: $a \equiv 1 \pmod{p}$, $a \equiv 0 \pmod{q}$
 $b \equiv 0 \pmod{p}$, $b \equiv 1 \pmod{q}$
- thus,
$$\begin{aligned} \tilde{S}^e \pmod{p} &= S_p^e \pmod{p} \\ &= m^{de} \pmod{p} \\ &= m \pmod{p} \end{aligned}$$
- ~~same (mod q)~~
 $\tilde{S}^e \not\equiv m \pmod{q}$



- In other words, we have that

$$\tilde{S}^e - m = 0 \pmod{p}$$

$$\tilde{S}^e - m \neq 0 \pmod{q}$$

- or

$$p \mid (\tilde{S}^e - m)$$

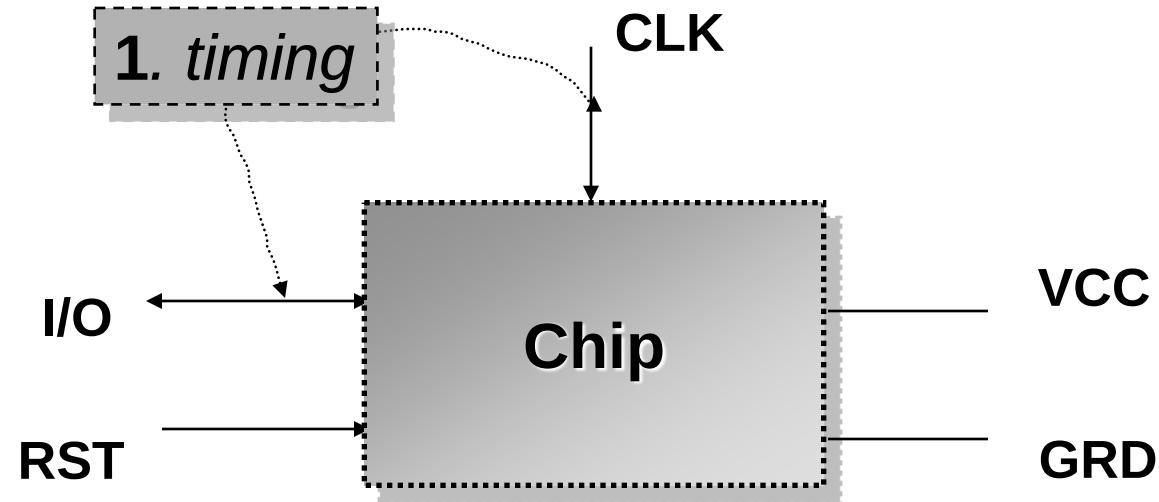
$$q \nmid (\tilde{S}^e - m)$$

- as $N = p q$, we get

$$\gcd((\tilde{S}^e - m), N) = p$$



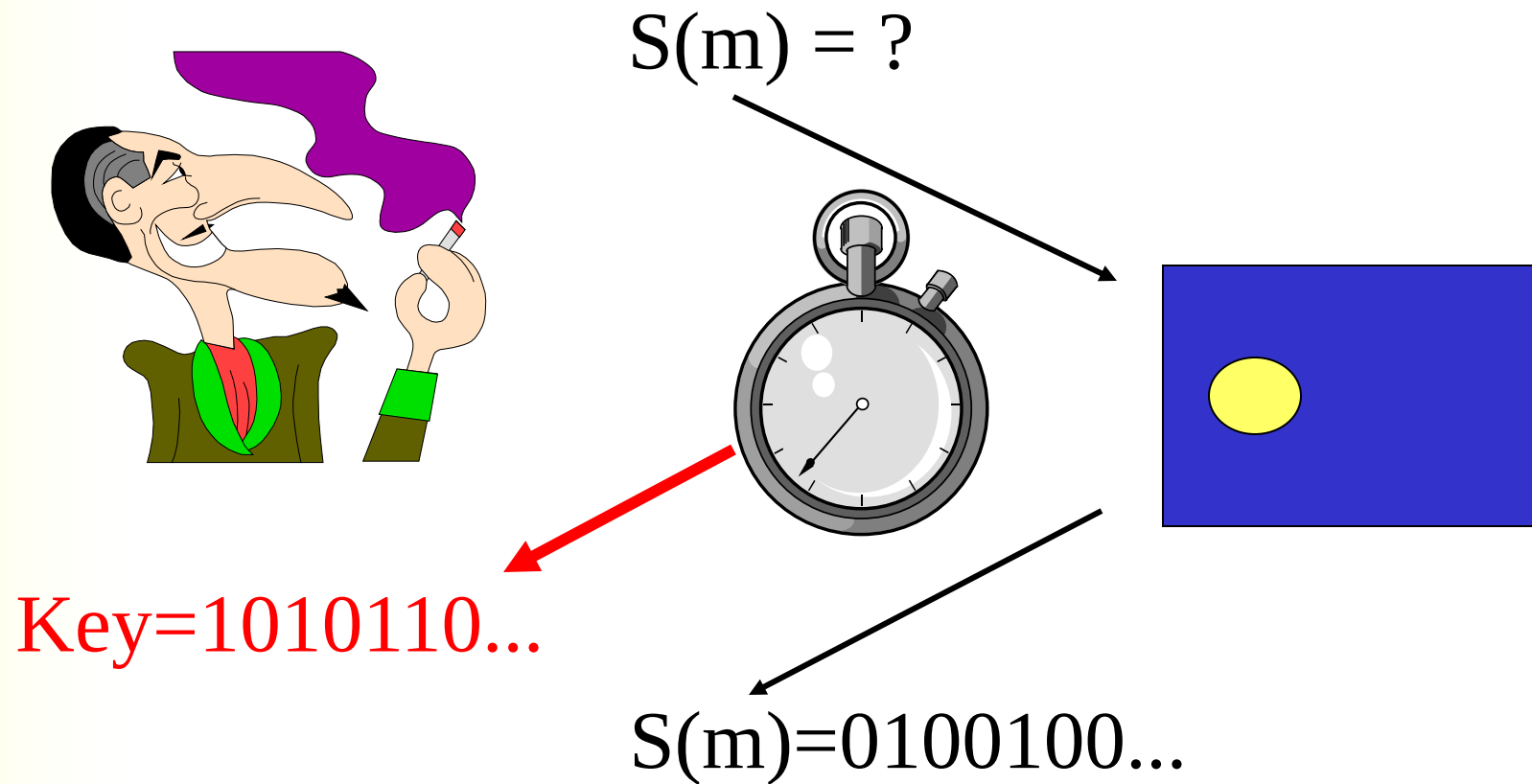
Timing attacks



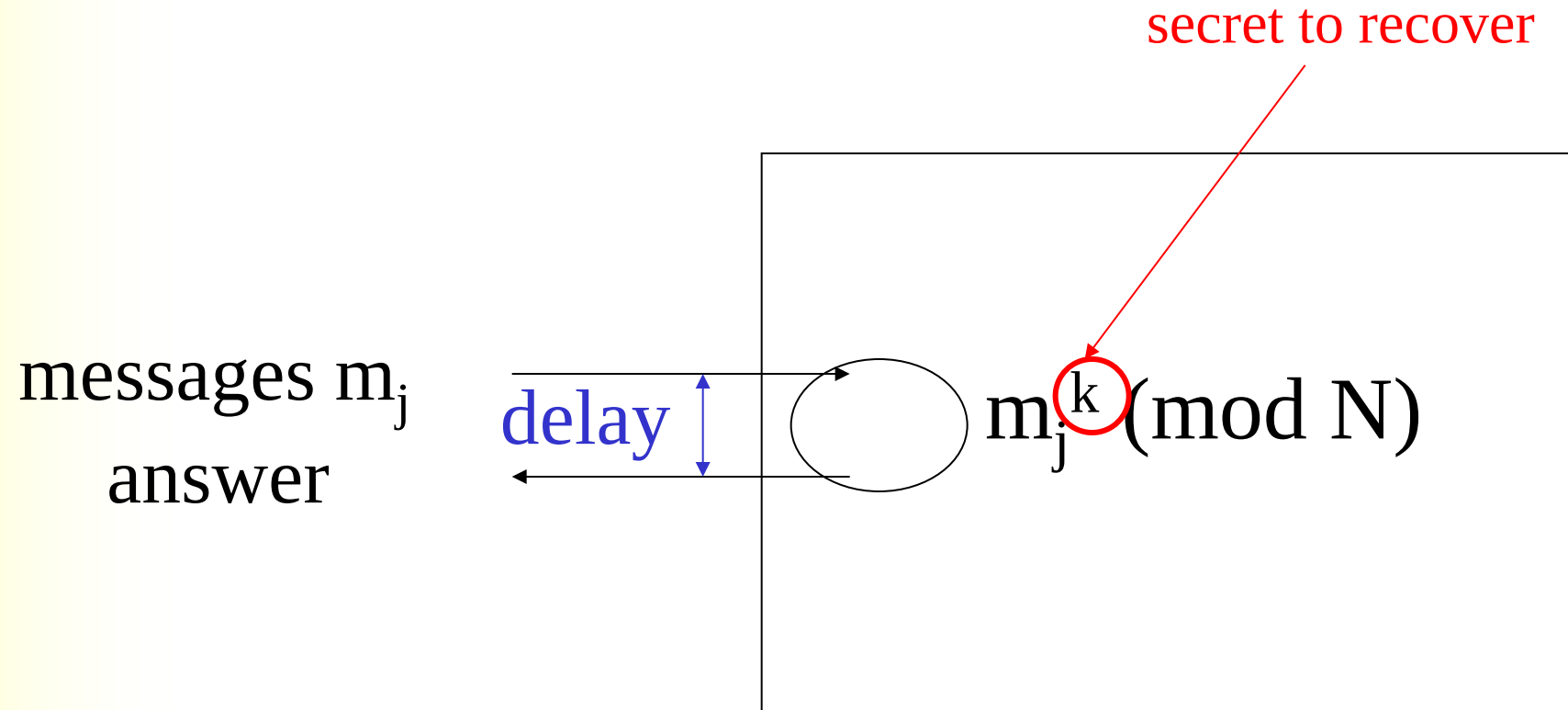
- the measure of the timing and the (some) knowledge of the implementation of the used cryptographic algorithm together a lot of well chosen inputs-outputs with some statistical treatment give the secret key in use (works well for RSA-like algorithms)
- countermeasure: I/O not related to the key at all (constant run-time for instance).



Timing attack



Scenario



Square and Multiply

To compute $m^k \pmod{N}$

```
x = 1
for i=1 to t do
    x = x2 (mod N)
    if (kj=1) then x = x.m (mod N)
od
```

Modular multiplications
(slow)



Montgomery Multiplication

- Efficient algorithm for modular multiplication
- Running time:



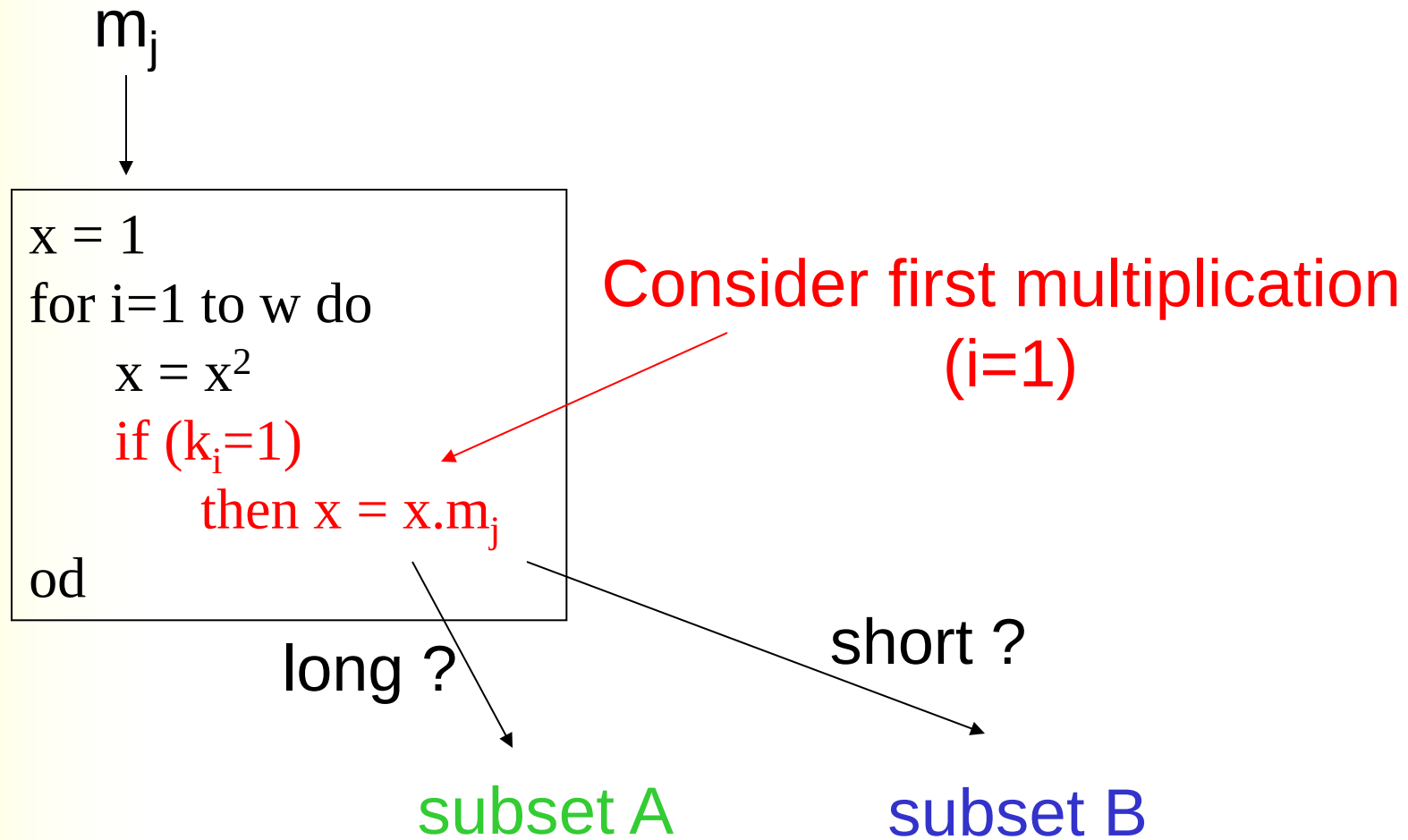
constant-time optional Extra Reduction

→ For a given multiplication,

- some messages will take time $c_0 + c_{ER}$
- others will take time c_0



Attacking the Multiply



Is that division meaningful?

```
x = 1
for i=1 to w do
    x = x2
    if (ki=1)
        then x = x.m
od
```

- YES, if the multiplication is actually executed at step 1
- NO, otherwise

→ by comparing **A** and **B**, we can deduce the bit value

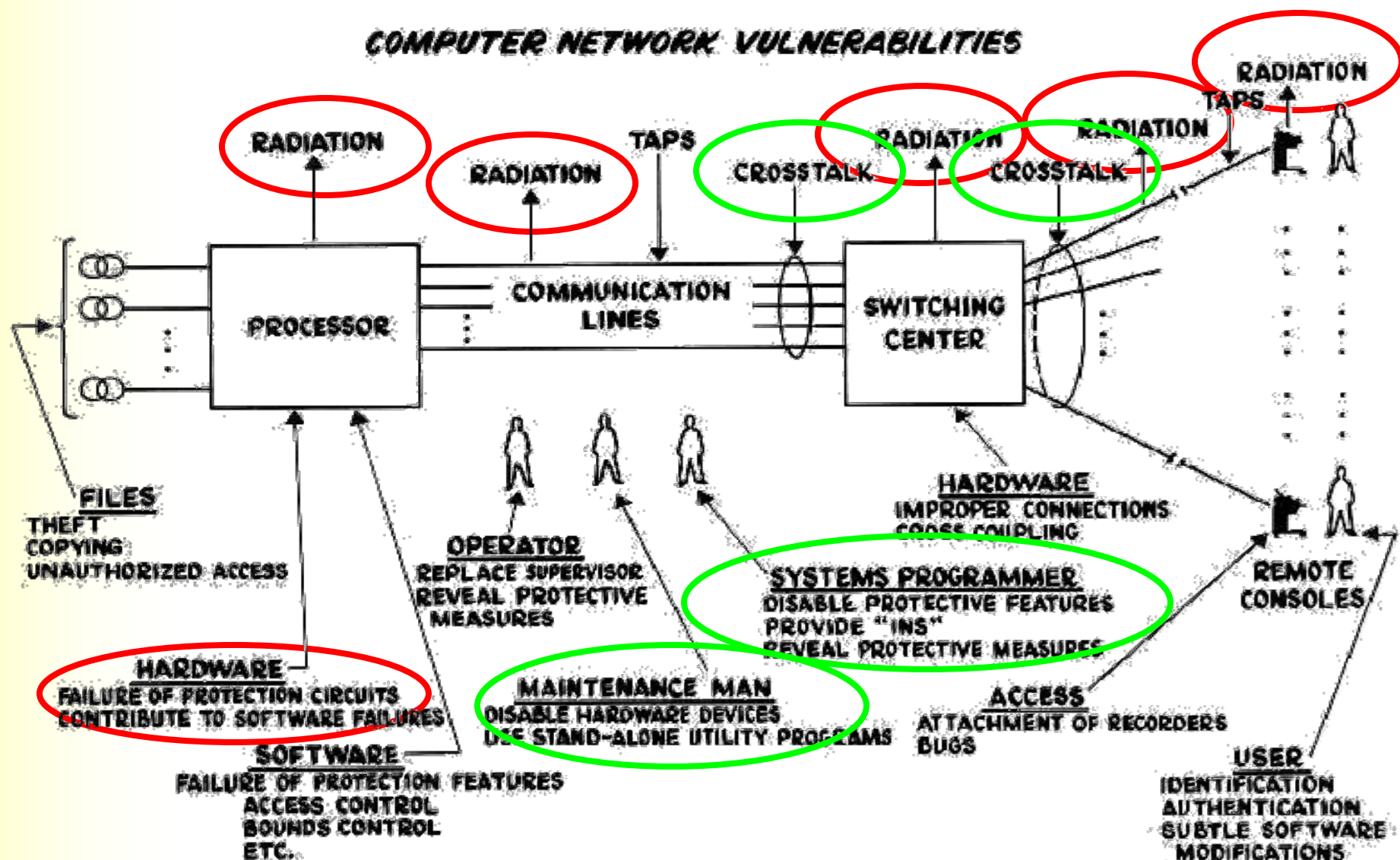


First Practical Results

key size	Result			
	without error corr.		with error corr.	
	size	speed	size	speed
64	1500-6500	>20 bits/s	1500-4500	>20 bits/s
128	12000-20000	2 bits/s	6000-10000	4 bits/s
256	70000-80000	1 bit/4s	15000-50000	1 bit/2s
512	±350000	1 bit/65s	100000-200000	1 bit/(15-30)s



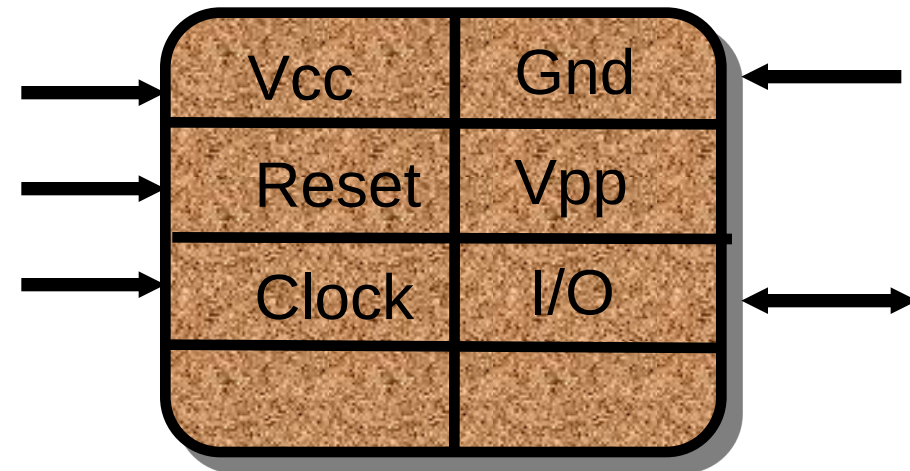
Further work



Potential leakages ?

Information sources:

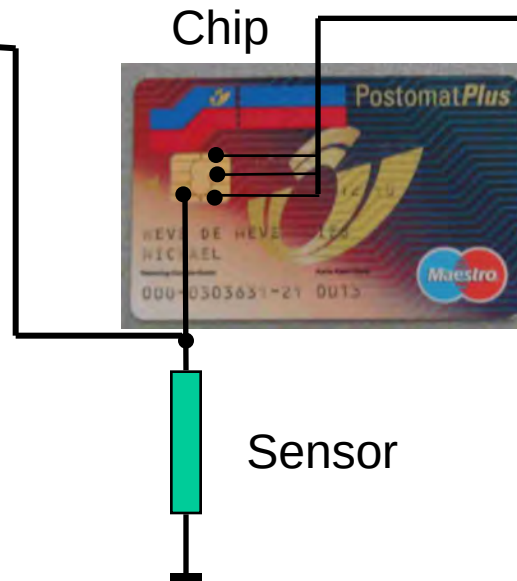
- time
- data flow
- power consumption
- electromagnetic emission
- temperature
- etc.



Power analysis configuration



Digital Oscilloscope



Chip

Sensor

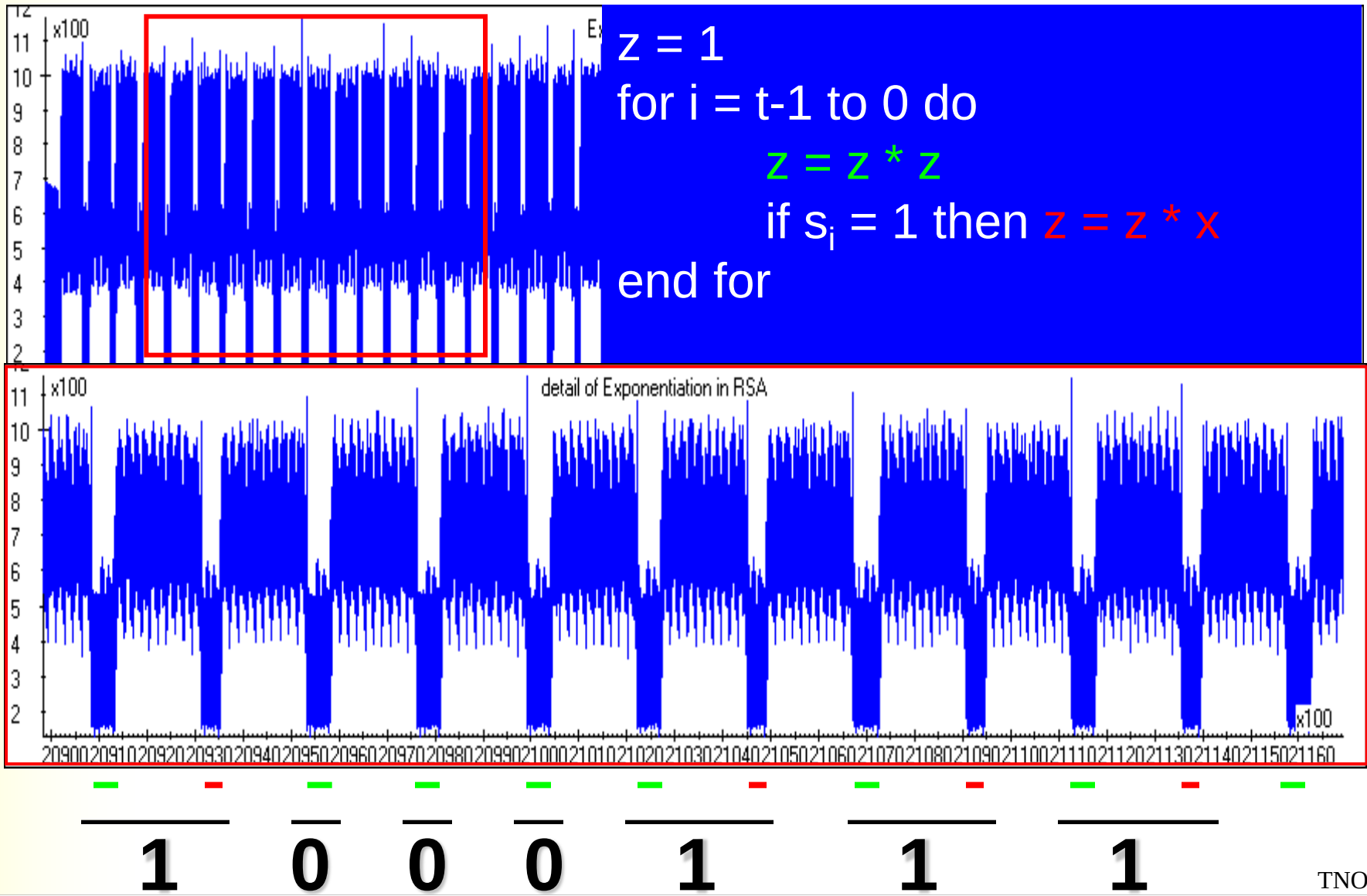


Pattern Generator

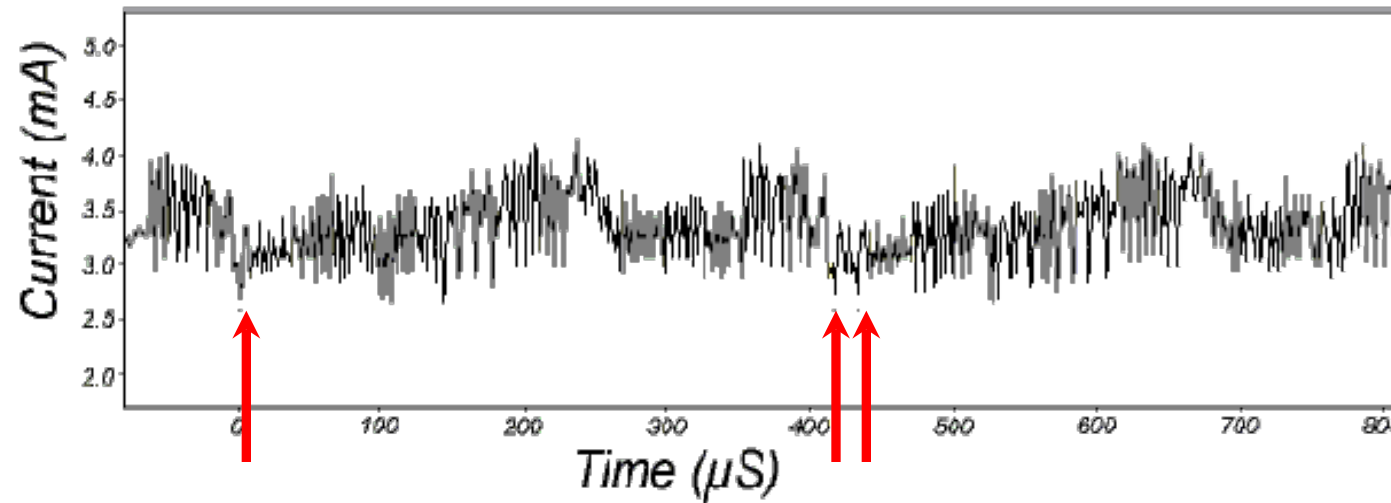
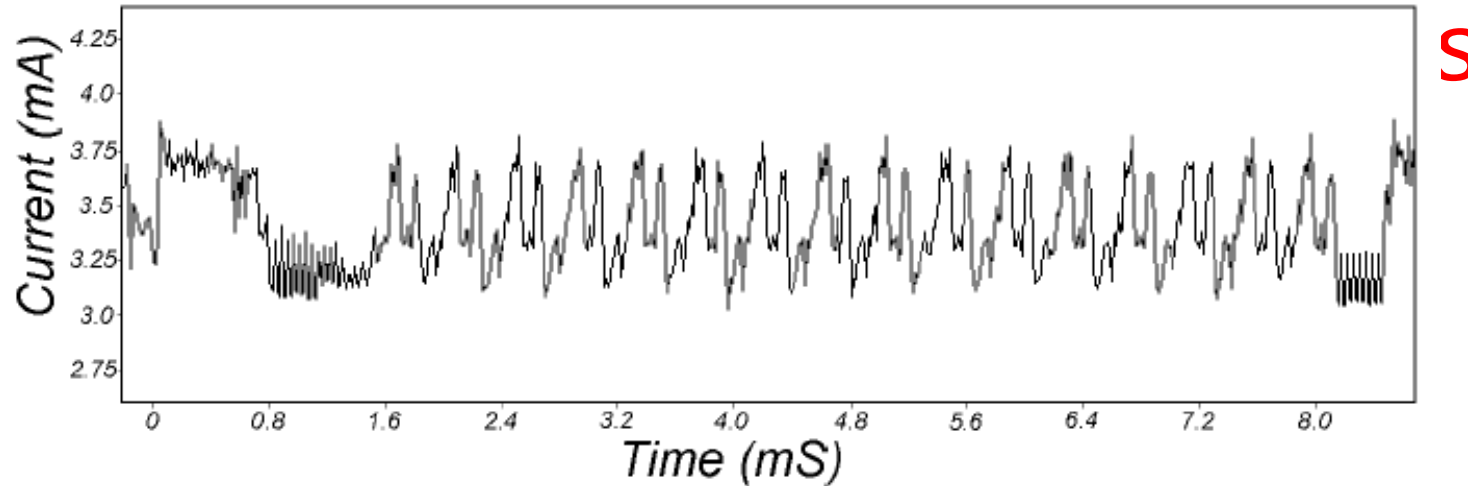




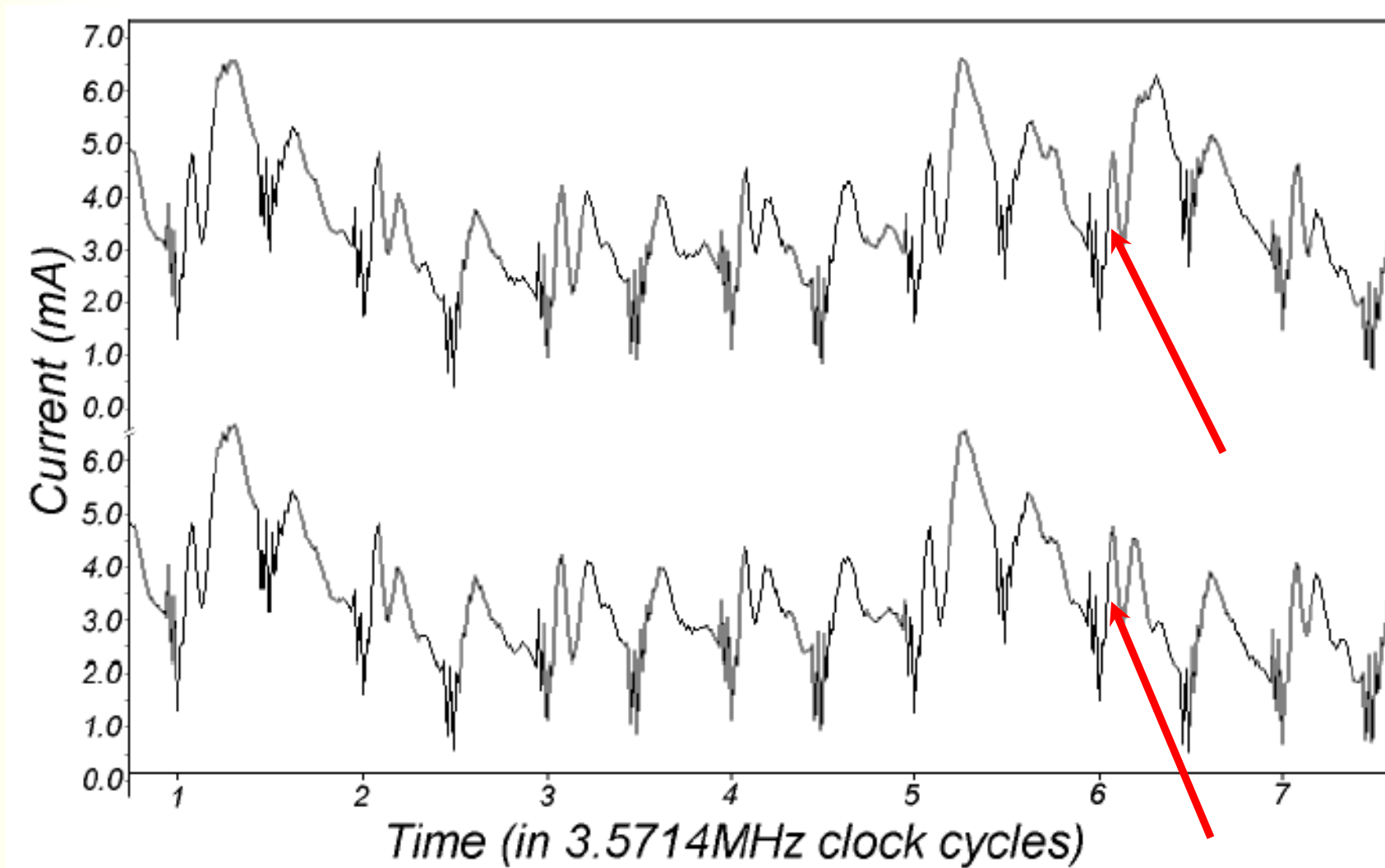
SPA on RSA



Simple Power Analysis



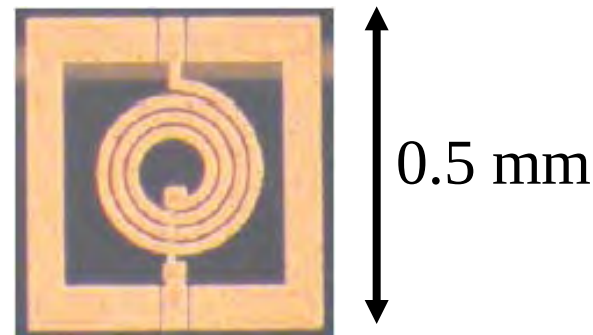
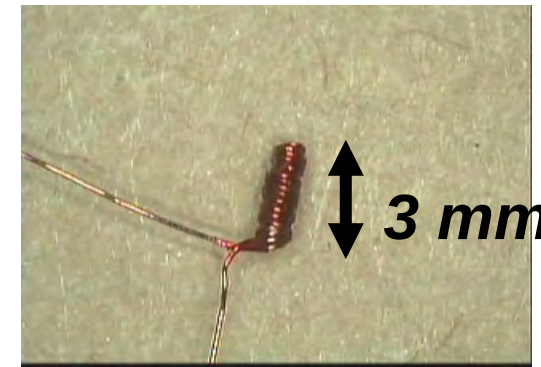
Individual clock cycles



Cryptography Research[©]

ElectroMagnetic Analysis

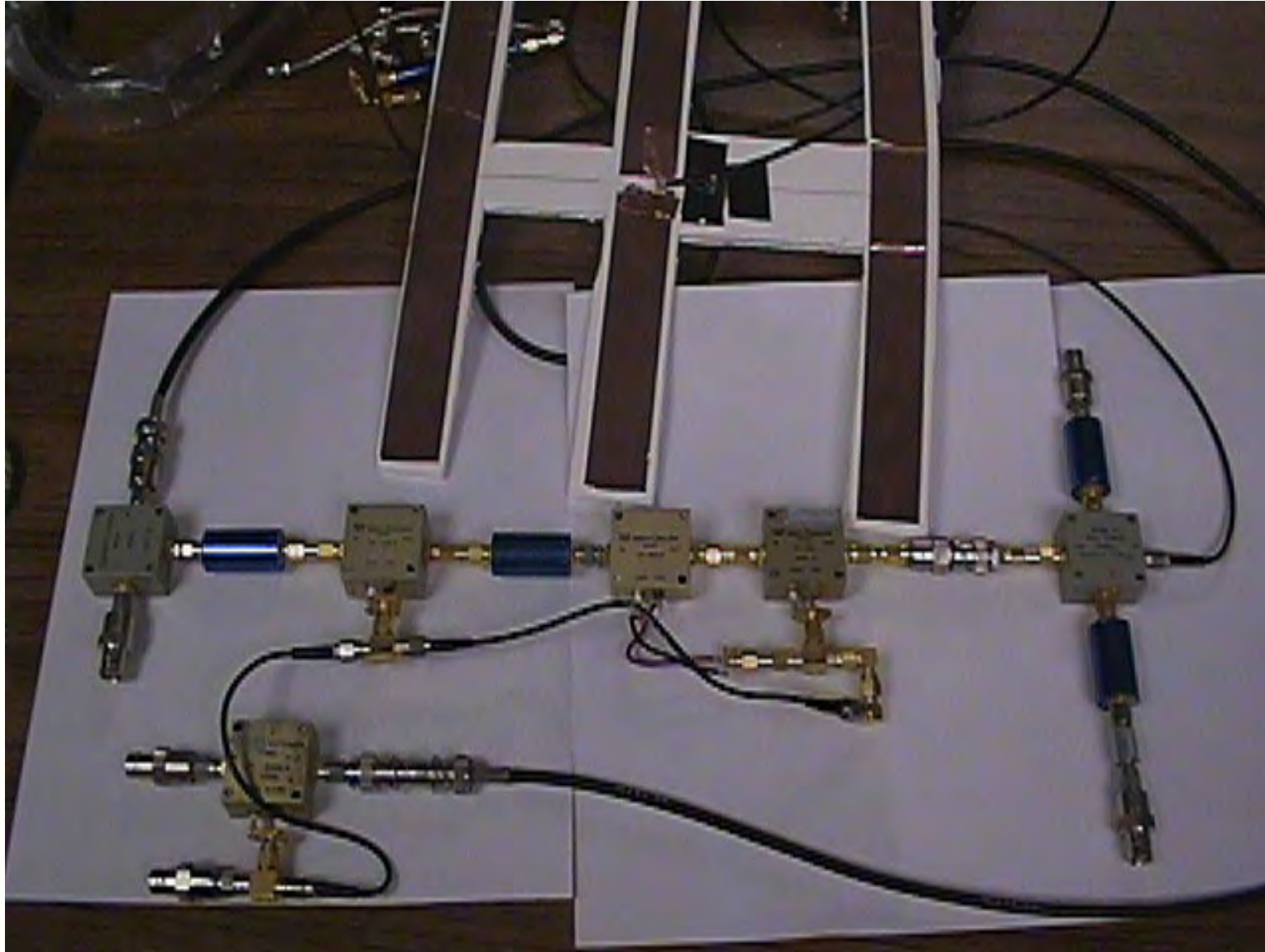
- Similar processing as PA, sensing and leakage are different.
- Use a different probe (that not interferes with the chip):
 - Hand-made (Gemplus)
 - RF receiver (IBM)
 - Flat inductor and MEMS (UCL)



ICOM wideband radio receiver with IF output



MAKE YOUR OWN

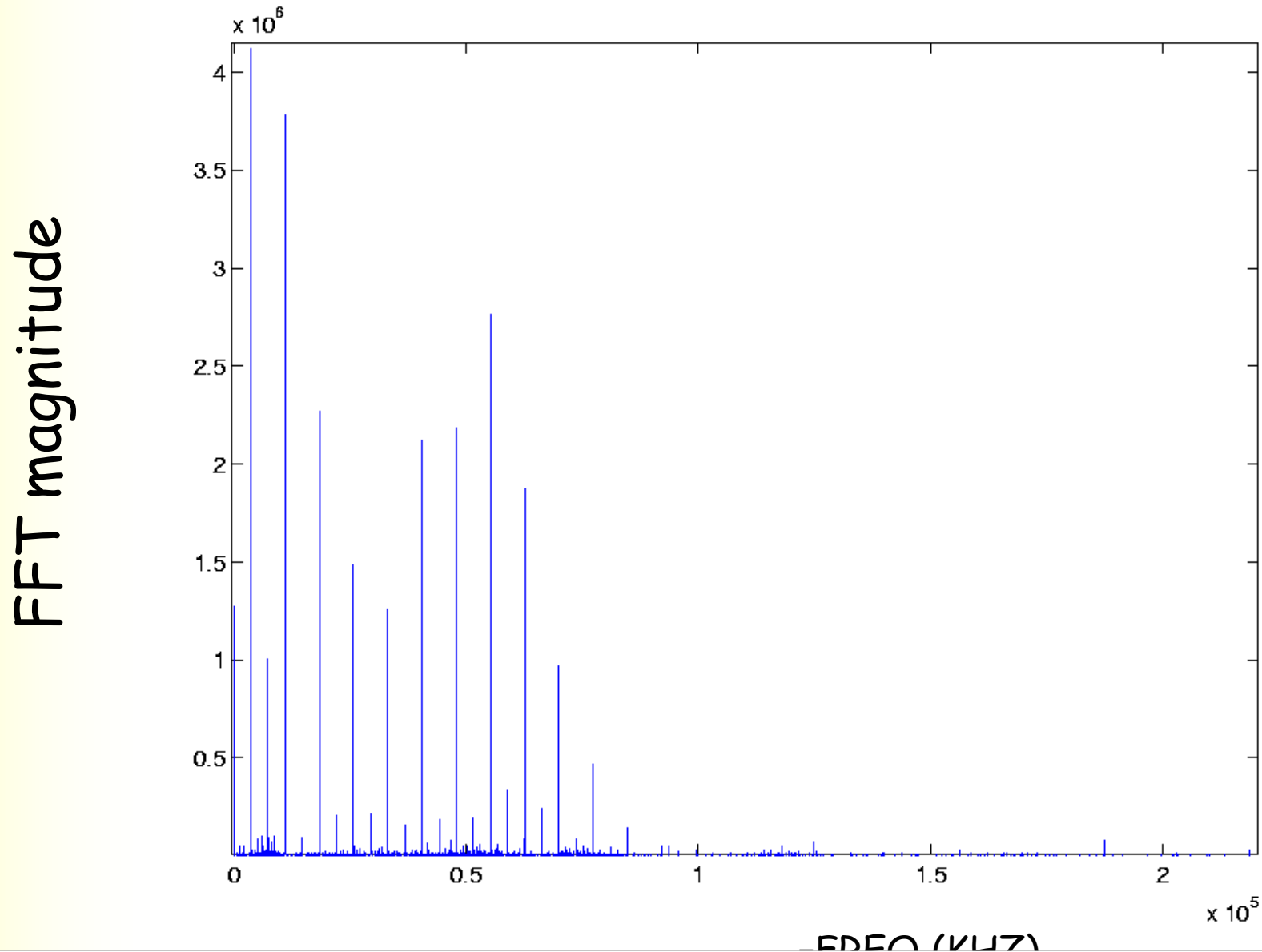


EM Emanations Background

- Origin/Types of EM Emanations
 - Direct emanations from intended currents.
 - Maxwell's equations, Ampere's and Faraday's laws.
 - Unintentional emanations from coupling effects.
 - Depend on physical factors, e.g., circuit geometry.
 - Most couplings ignored by circuit designers.
 - Manifest as modulation of carriers (e.g. clock harmonics) present/generated/introduced in device.
 - AM or Angle (FM/Phase) Modulation.
 - Compromising signals available via demodulation.
- Propagation of EM
 - Radiation, Conduction, Combination of both.
 - E.g., Faint EM signals riding on power line.

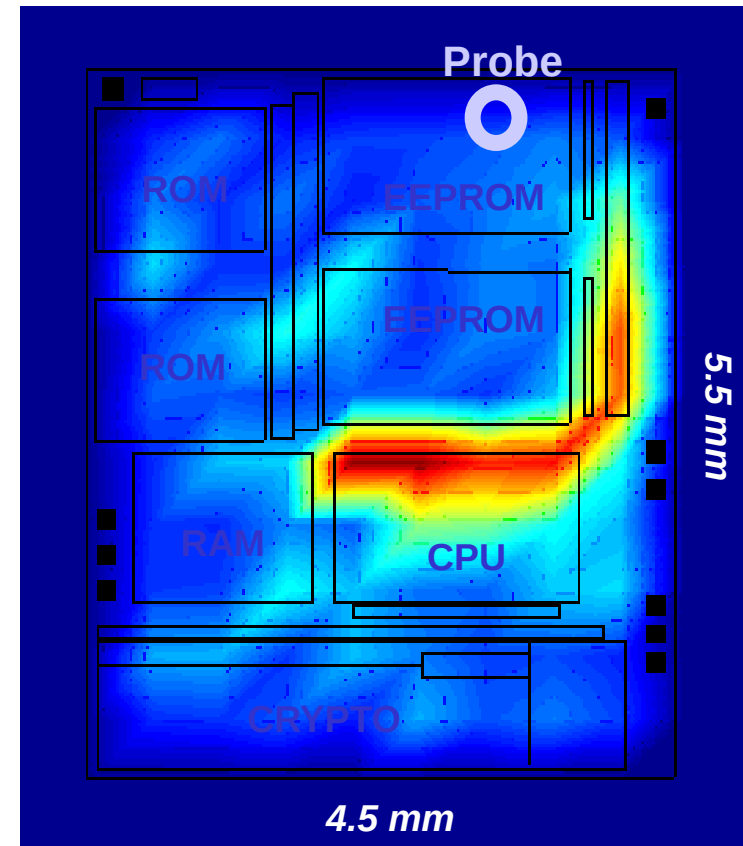
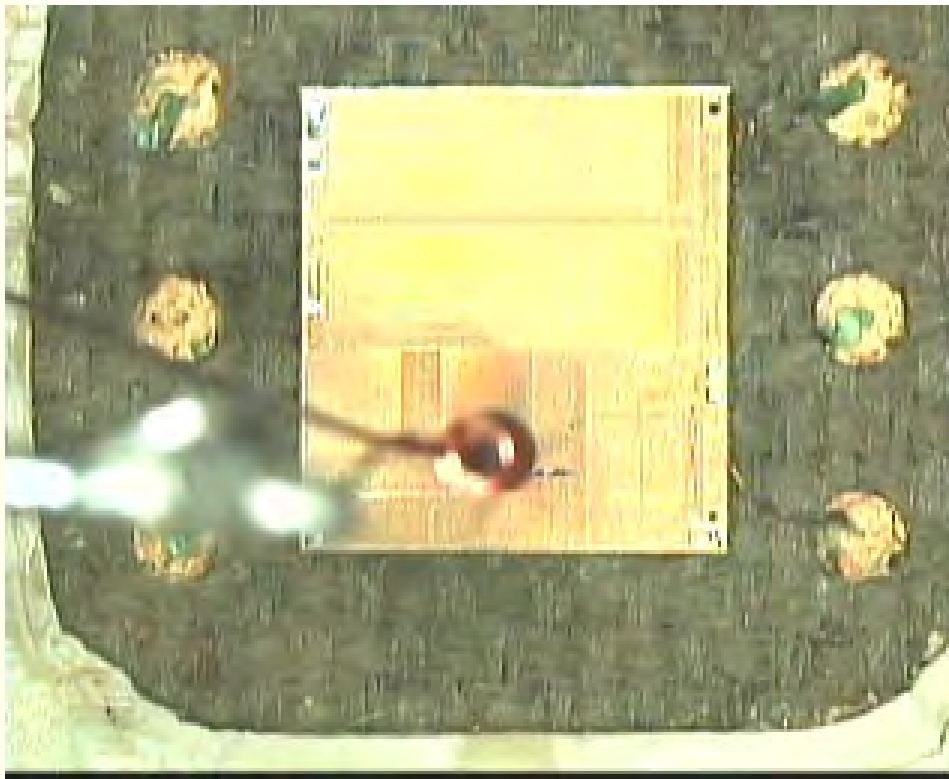


FFT OF RAW SIGNAL FROM EXPERIMENT 1 (0-250MHZ)



Spatial positioning

- Horizontal cartography (XY plane)
 - to pinpoint instruction related areas
 - better if automated

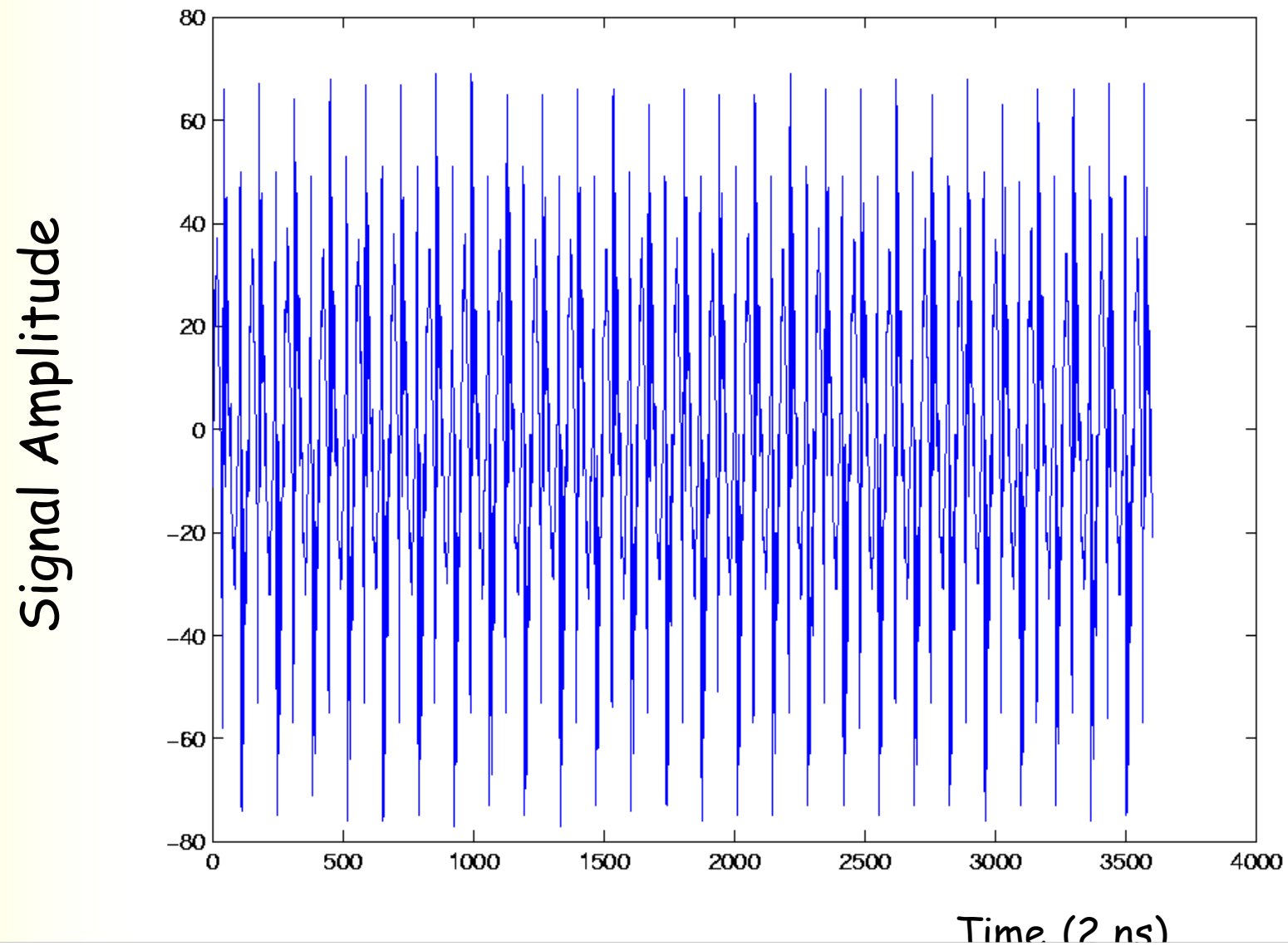


EXAMPLE 1

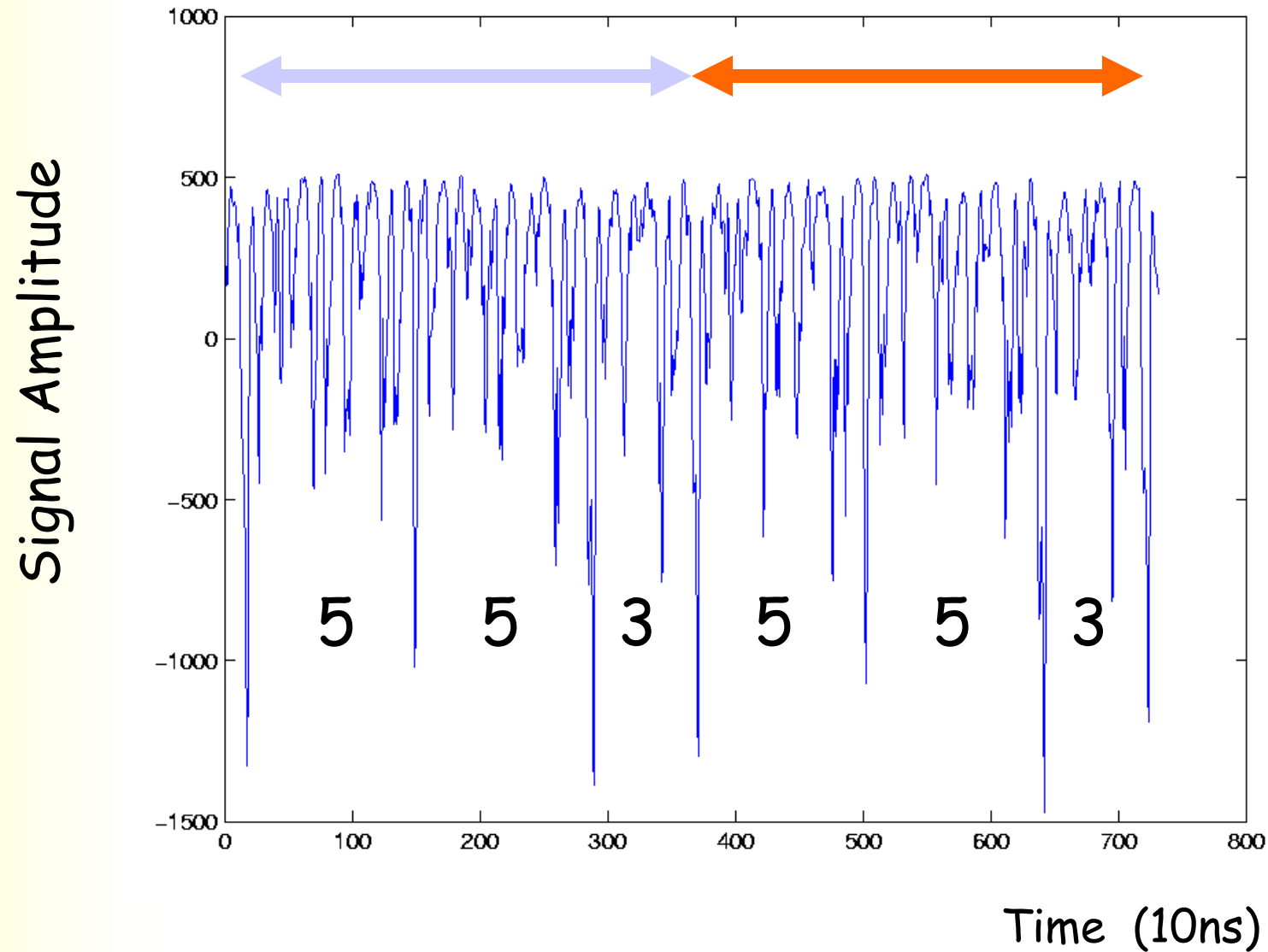
- 6805-based smart-card using external 3.68Mhz clock.
- 3 instruction, 13 cycle loop:
 - Access RAM containing a value B (5 cycles)
 - Check for external condition (5 cycles)
 - Jump back to start of loop (3 cycles)



Raw signal from near-field sensor during 2 iterations of loop (26 cycles)



AM Demodulated signal (150Mhz carrier, 50Mhz band) showing 2 iterations of Loop



EM vs. Power

- More noisy measurements, but sharper peaks. Better SNR => fewer samples
- Some bad instructions can leak information in EM that allow to defeat PA counter-measures
- Basic probe for PA is a resistor (but could be a little more developed), EM: inductive (shape, diam, impedance adaptation issue, ...)

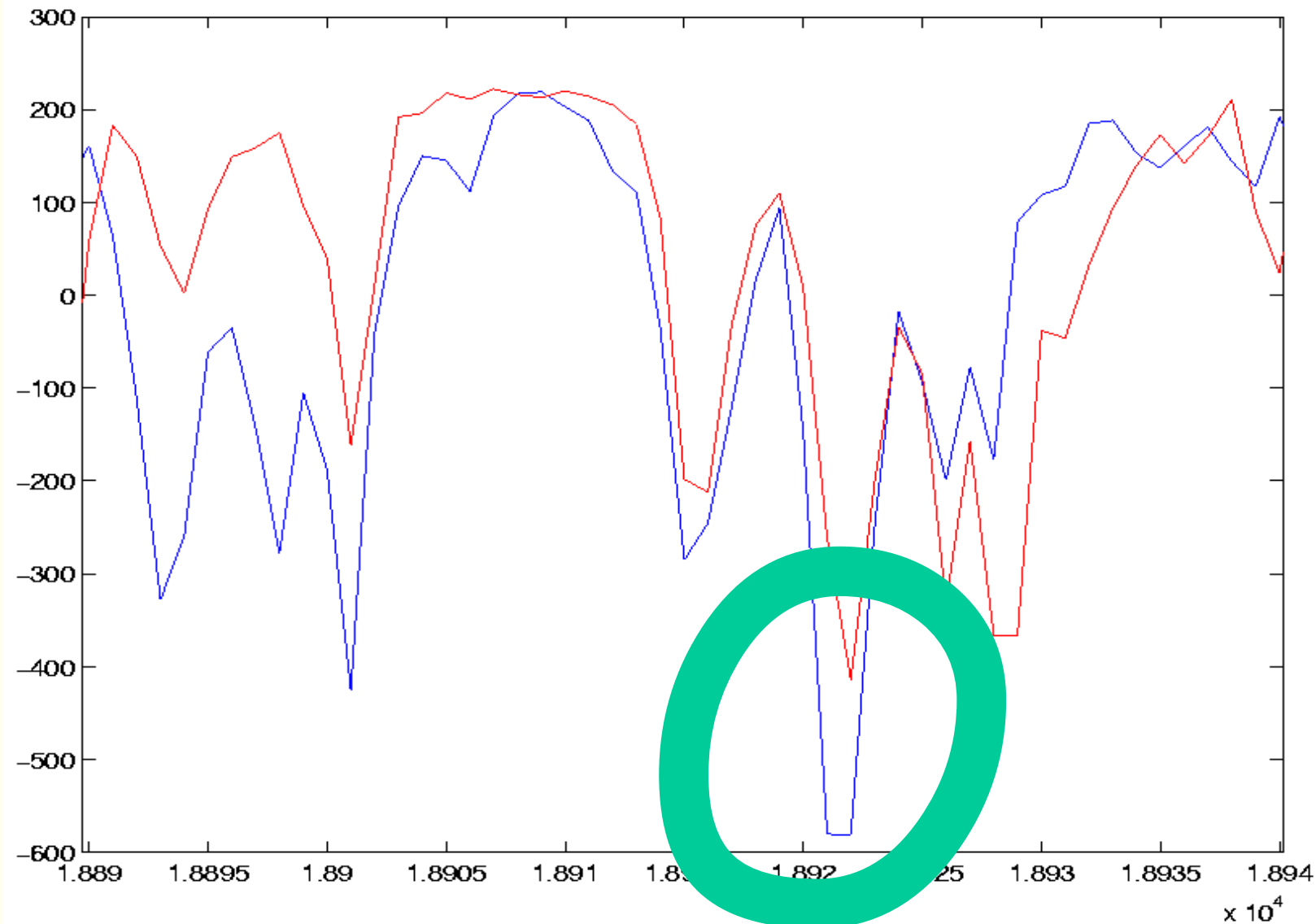


Bad Instructions

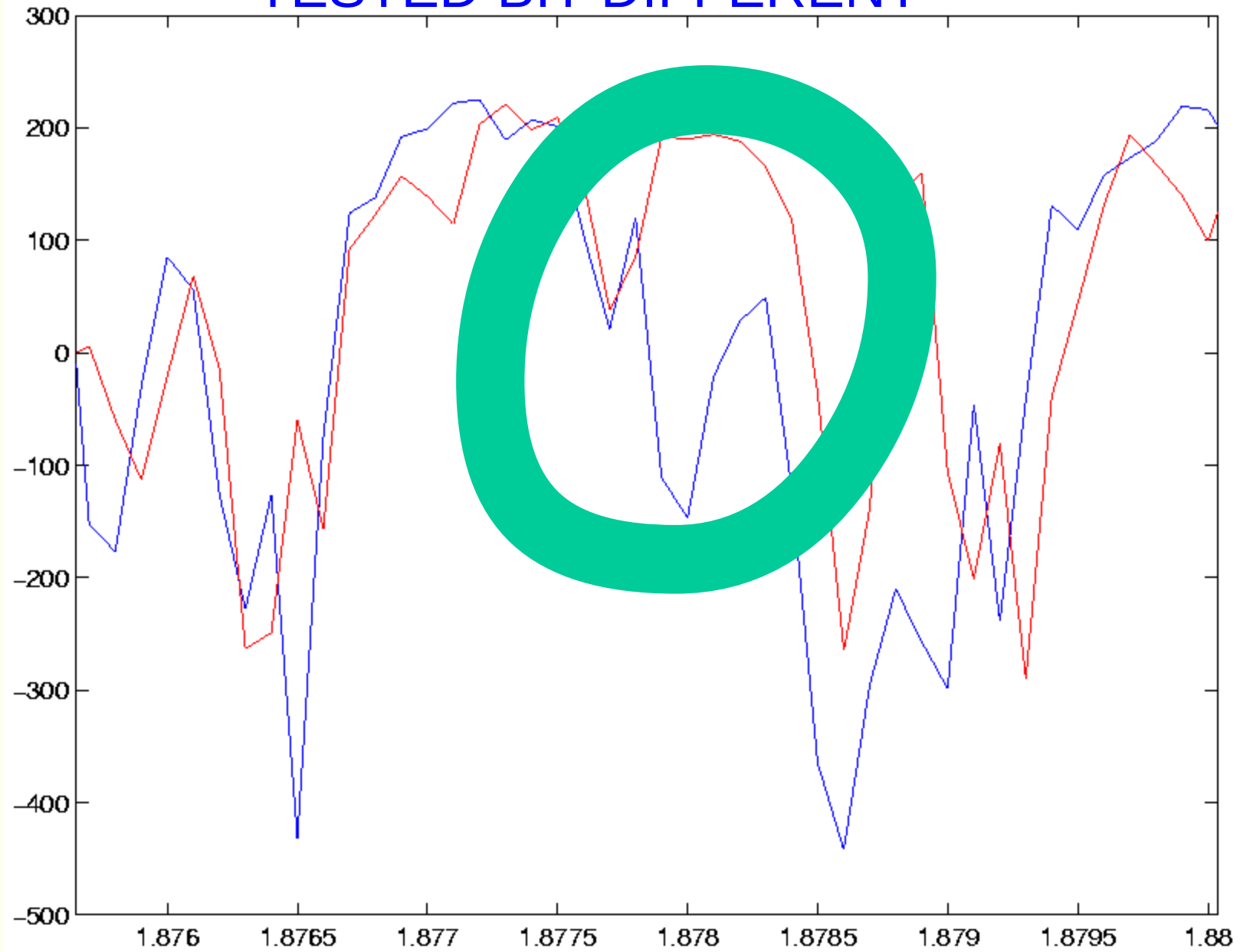
- Instructions where some EM leakage >> Power leakage.
- Typically CPU intensive rather than bus intensive.
- All architectures have BAD Instructions.
- Example: Bit-test on several 6805 based systems leaks tested bit.



TESTED BIT = 0 IN BOTH TRACES



TESTED BIT DIFFERENT



IBM©



Side Channel Conclusion

- Direct and serious threat to the security of crypto systems
- Applicable to all algorithms
- (mostly) a non-destructive class of attacks
- Can be developed in order of weeks, repeated in order of hours
- Can be prevented or discouraged by (combinations of) countermeasures



Fault Analysis



Faults insertion

- Aim: Cryptanalysis of an algorithm using fault(s)
 - Glitch attack clock
 - Local ionisation (Rads 2003)
 - UV light applied to a certain location
 - X-rays
 - Local heating
 - Optical attack (Ches 2002)
 - Eddy Currents (ESmart 2002)



Semi-Invasive attacks

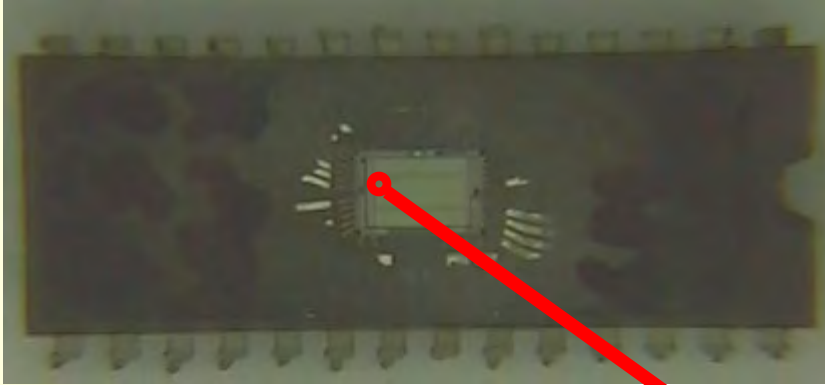
- Depackaging is required (access chip surface)



- No internal connections are required
- No expensive FIB or Laser cutter techniques
- No microprobing

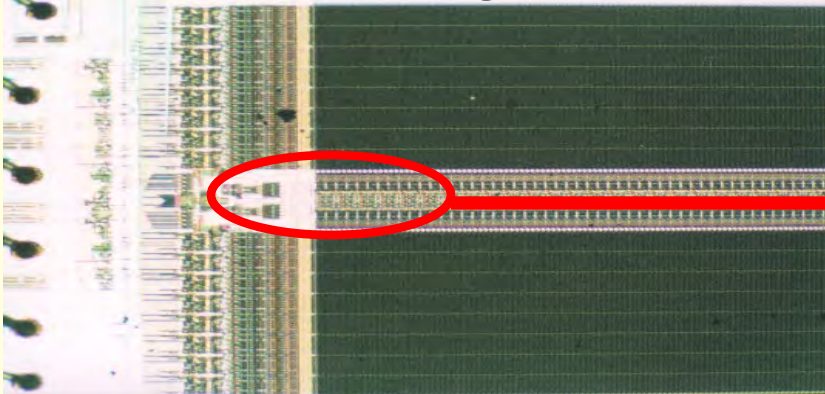


A static RAM

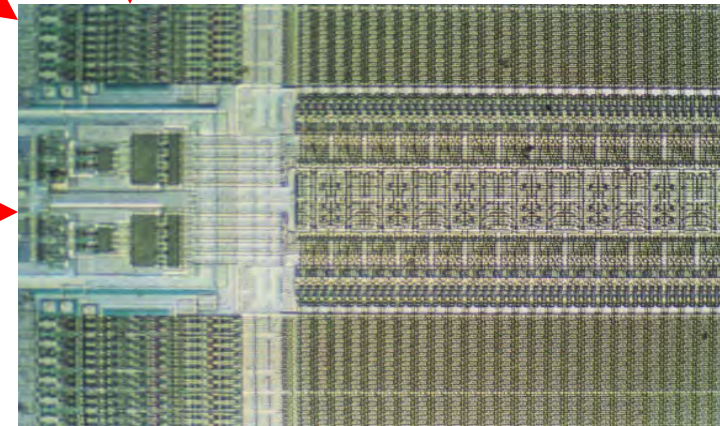


Depackaged RAM

Zoom on the regular structure



Regular structure

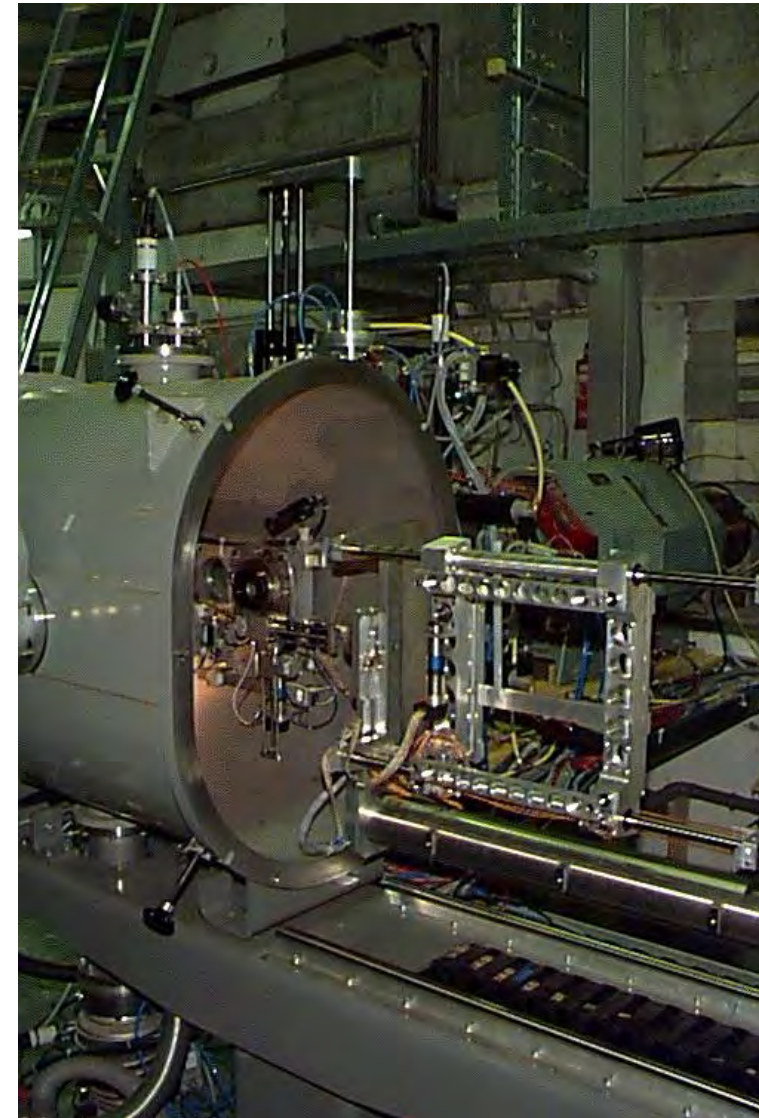


Resistance of memories to Heavy Ions

CYClotron of LOuvain-la-NEuve

HIF → Heavy ions beam
simulates the impact of cosmic
rays on chips

- Very high cost attack
- Insert and analyse induction of faults in different memory technologies
- Fault analyses in smart cards





Countermeasures

- Scramble the memory structure
- CRC
- Dedicated sensors
- Opaque passivation layer or top-layer shielding
- Self-timed circuit & Dual-rail logic
- Software countermeasures



Countermeasures

- Software
 - Check each bit before to set/reset it
 - Test integrity of all (Data, Crypto, ...)
- Hardware :
 - Scramble the memory structure
 - Implement CRC (well chosen)
 - Build new architecture for error detection/corrections
 - Asynchronous processors
 - Dedicated sensors and avoid static sensors

If there is a CRC check, there's a transistor to give a right or wrong value...

It could then be possible to lock the value (FPGA,...).



Countermeasures

- A lot: New hardware design, new technology, ...
- Randomize carefully!
- No difference between square and multiply (add and doubling for RSA): subtle solutions,
- ➡ • Verify the result before outputs,
- ...
- Very mathematical, very cryptographic,
- Another story



General conclusion

Side channels:

- is a direct and serious threat to the security of crypto systems
- is applicable to all algorithms
- is (mostly) a non-destructive class of attacks
- can be developed in order of weeks, repeated in order of hours
- can be prevented or discouraged by (combinations of) countermeasures



Timing attacks – fault attacks ...

Your wallet in Van Allen belt (December 1996)

<https://catless.ncl.ac.uk/Risks/18.64.html#subj12>

- One crucial question is the effectiveness of such attacks by malicious
- hackers. In fact, this problem was very well studied in the contexts of
- nuclear physics and of space applications (what about the behavior of
- semiconductors in such hard environments?). In that area, there is the
- concept of SEE (Single Event Effect) and it is what we are trying to study!
- A SEE is an event induced by radiation, temperature, microwave, ..., having
- some effect one time on a device. There are many studies about that. What
- we need to know are the SEEs
- --- relatively well focused (one or few bits are flipped),
- --- and/or at a given moment,
- --- and/or for a very short time.

Main conference about cryptographic hardware: CHES

The screenshot shows the CHES website header with the logo and navigation links: Home, CHES 2026, CHES 2027, About CHES, and Contact. Below the header is a section titled "Former CHES" displaying a grid of 25 conference thumbnails. Each thumbnail includes the year, the CHES logo, and the host location.

CHES 2025	CHES 2024	CHES 2023	CHES 2022	CHES 2021
Kuala Lumpur	Halifax	Prague	Leuven	virtual
CHES 2020	CHES 2019	CHES 2018	CHES 2017	CHES 2016
virtual	Atlanta	Amsterdam	Taipei	Santa Barbara
CHES 2015	CHES 2014	CHES 2013	CHES 2012	CHES 2011
Saint Malo	Busan	Santa Barbara	Leuven	Nara
CHES 2010	CHES 2009	CHES 2008	CHES 2007	CHES 2006
Santa Barbara	Lausanne	Washington	Vienna	Yokohama
CHES 2005	CHES 2004	CHES 2003	CHES 2002	CHES 2001
Edinburgh	Boston	Cologne	San Francisco	Paris
CHES 2000	CHES 1999			
Worcester	Worcester			

Active side-channel attacks: fault injection

- Joye, M., Lenstra, A. & Quisquater, J.-J. (1999). Chinese remaindering based cryptosystems in the presence of faults. Journal of Cryptology, 12(4), 241-245.
- Against RSA:
 - One faulty signature is enough to recover the secret ket if the public key is known
 - 2 faulty signatures is enough to recover the secret key if you don't know the public key ...

RSA:

Chinese Remaindering Based Cryptosystems in the Presence of Faults

Marc Joye

UCL Crypto Group, Dép. de Mathématique, Université de Louvain
Chemin du Cyclotron, 2, B-1348 Louvain-la-Neuve, Belgium
mjoye@geocities.com

Arjen K. Lenstra

Citibank, N.A.
4 Sylvan Way, Parsippany, NJ 07054, U.S.A.
arjen.lenstra@citicorp.com

Jean-Jacques Quisquater

UCL Crypto Group, Lab. de Microélectronique, Université de Louvain
Place du Levant, 3, B-1348 Louvain-la-Neuve, Belgium
jjq@dice.ucl.ac.be

Abstract. We present some observations on public-key cryptosystems that use the Chinese remaindering algorithm. Our results imply that careless implementations of such systems could be vulnerable. Only one faulty signature, in some explained context, is enough to recover the secret key.

Active side-channel attacks: fault injection

CHES 2023
Test of Time Award

A Differential Fault Attack Technique Against SPN Structures and the AES

G. Piret*, J.-J. Quisquater

CHES 2003 Workshop

Cologne, Germany

- Used today in standard test for chips
- Abstract
- In this paper we describe a differential fault attack technique working against Substitution-Permutation Networks, and requiring very few faulty ciphertexts. The fault model used is realistic, as we consider random faults affecting bytes (faults affecting one only bit are much harder to induce). We implemented our attack on a PC for both the AES and Khazad. We are able to break the AES-128 with **only 2 faulty ciphertexts**, assuming the fault occurs between the antepenultimate and the penultimate MixColumn.

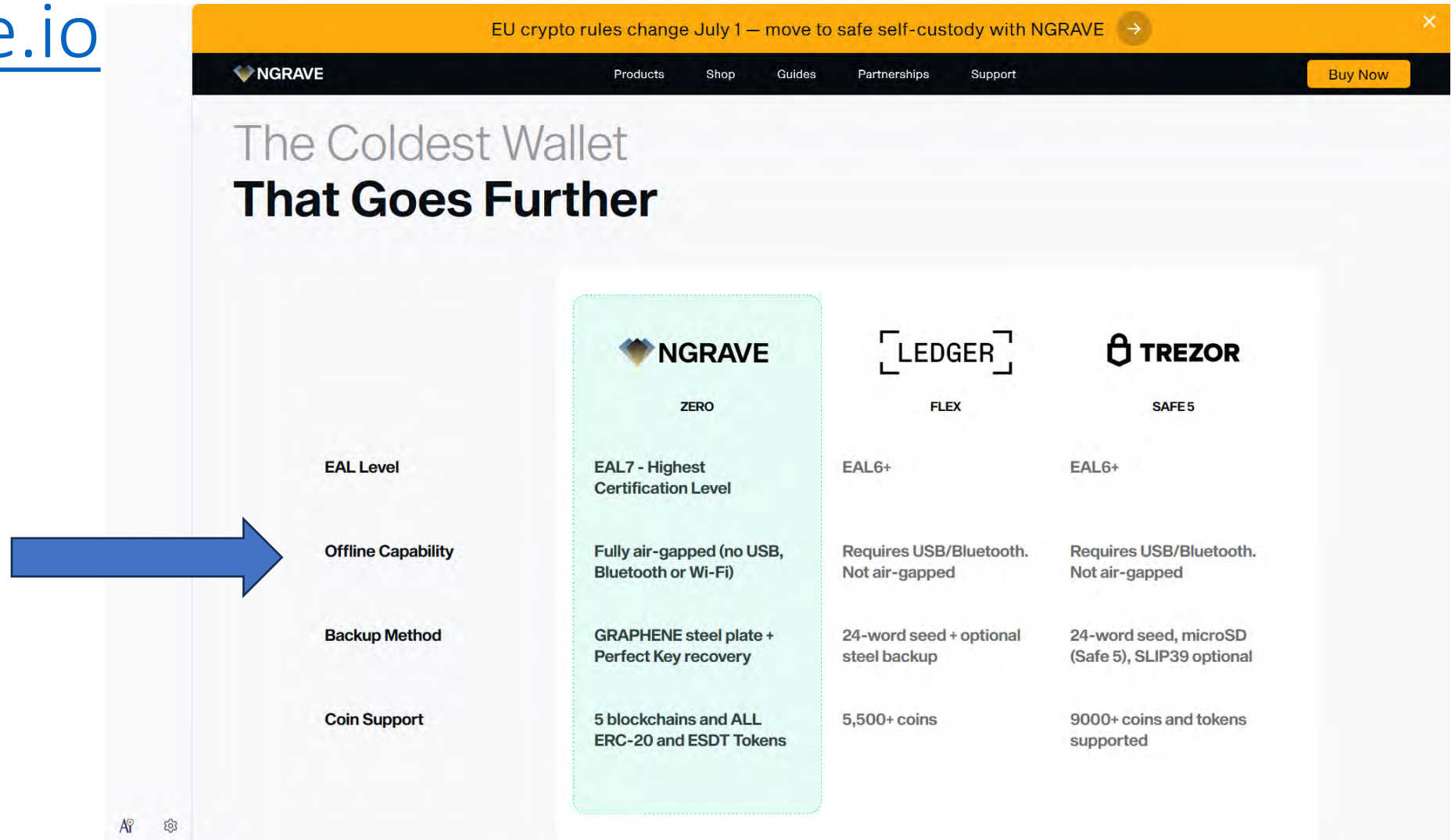


Air-gapped protection

- Device physically not connected to outside (difficult because need of some power and outputs)
- Example: computer outputs only printer paper (or QR code) and inputs only by scanning
- Example for cryptowallet: nGRAVE

Wallet nGRAVE: input-output by QR code

<https://ngrave.io>



The screenshot shows the nGRAVE website with a comparison table of three hardware wallets: nGRAVE ZERO, Ledger Flex, and Trezor Safe 5. A large blue arrow points from the left towards the comparison table.

	NGRAVE ZERO	LEDGER FLEX	TREZOR SAFE 5
EAL Level	EAL7 - Highest Certification Level	EAL6+	EAL6+
Offline Capability	Fully air-gapped (no USB, Bluetooth or Wi-Fi)	Requires USB/Bluetooth. Not air-gapped	Requires USB/Bluetooth. Not air-gapped
Backup Method	GRAPHENE steel plate + Perfect Key recovery	24-word seed + optional steel backup	24-word seed, microSD (Safe 5), SLIP39 optional
Coin Support	5 blockchains and ALL ERC-20 and ESDT Tokens	5,500+ coins	9000+ coins and tokens supported

Postquantum cryptography and attacks in the context of hardware

- Need of research (a lot)
- Side-channel attacks and fault attacks are well working ...

Conclusion

- Security is never complete
- No winner.