Les attaques par canaux cachés (ou auxiliaires ?)

Jean-Jacques Quisquater

UCLouvain, Belgique

Académie Royale de Belgique

jjq@uclouvain.be

Avertissements

- Toutes informations données ici, ainsi que oralement, sont publiques mais, pas toujours, bien publiées.

- Vu la durée et le public, il n’est pas du tout dans nos intentions d’être exhaustif, ni à jour. Pour donner un panorama complet, il faudrait au moins 3 heures.

- Certaines explications sont volontairement approximatives pour être compris du plus grand nombre.

- Nous avons voulu aussi traiter l’histoire de techniques qui sont souvent ignorées et même tronquées. Les spécialistes n’apprendront seulement, peut-être, que cela.

Présentation

- Ces attaques sont bien connues des militaires depuis longtemps et ce fut alors classifié. On parlait d'émissions compromettantes. Dans les années 80, elles furent pratiquement découvertes dans plusieurs laboratoires industriels en Europe sans être publiées et, je suis témoin, même censurées sans aucune action. Puis, en 1996, Paul Kocher publia sa première attaque en mesurant le temps d'exécution de divers algorithmes cryptographiques, à distance !, et il nous montrait qu'on pouvait ainsi récupérer la clé secrète. Ce fut alors le début d'une révolution, qui continue.
- Nous parlerons en termes pratiques et illustrés de ces différentes attaques :
- • les attaques passives où on "écoute" seulement les fuites de ces canaux cachés (son, temps, ondes électromagnétiques, etc) d'ordinateurs, serveurs, microprocesseurs et ces attaques ne peuvent donc pas être détectées : dans certains cas cela peut se faire à grande distance (sur internet)
- • les attaques actives avec diverses méthodes d'injection (lumière, chaleur, laser, faisceau de cyclotron, ondes électromagnétiques, utilisation des protocoles, etc) pour engendrer des fautes transitoires ou permanentes qui perturbent les résultats des calculs. Le but le plus souvent est de capter les informations indirectes qui donneront, après transformations et calculs, la clé secrète convoitée. Ici, il faudra avoir accès ou être proche de l'objet attaqué mais c'est bien sûr possible pour beaucoup d'objets dans la nature (carte à puce, IoT, etc).
- Il existe de nombreuses contremesures à ces attaques, bien appliquées dans le domaine des cartes à puce. Dans le cas de la consommation électrique (attaques dites SPA et DPA), les contremesures ont été vigoureusement brevetées et ont donné lieu à une lutte juridique intense entre les inventeurs (ils furent les gagnants) et les principales firmes de carte à puce. Plusieurs conférences internationales, CARDIS, CHES, et autres, reprennent ces recherches actuelles et sont fort suivies.
- Les attaques les plus subtiles (Spectre, Meltdown), liées aux caches ou à la prédiction d'instructions, ont été contenues en imposant une nouvelle conception des processeurs à Intel, AMD, IBM, etc.
- Ces attaques ne sont pas confinées au matériel mais bien aussi, et surtout dans les cas pratiques, au logiciel. Un logiciel qui utilise une clé secrète en un temps non constant est un logiciel dangereux et il y en a beaucoup. Un autre vecteur d'attaque est un programme espion qui parvient à partager un processeur avec un programme cible.

CRYPTO 2000 : UCSB rump session

CRYPTO 2000

August 20–24, 2000
Santa Barbara, California, USA

Rump Session Program

This is a list of talks given at the rump session. We will include here any information regarding the paper provided by the authors, such as abstract, pointers or preprints. Authors are encouraged to send information. The papers are ordered as per the program.

Title: AES update
Presenter: Morris Dworkin
Contact Email: dworkin@nist.gov

Title: Assassinating SASAS
Authors: Alex Biryukov and Adi Shamir
Contact Email: shamir@wisdom.weizmann.ac.il
Abstract

Title: A simple algebraic representation of Rijndael
Authors: Niels Ferguson, Richard Schroeppel and Doug Whiting
Contact Email: niels@ferguson.net

Title: Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms
Authors: Kazumaro Aoki, Tetsuya Ichikawa, Masayuki Kanda, Mitsuru Matsui, Shiho Moriai, Junko Nakajima, Toshio Tokita
Contact Email: shiho@isl.ntt.co.jp
Note: This appears in SAC 2000
Abstract

Title: Improved impossible differentials on Twofish
Authors: Eli Biham and Vladimir Furman
Contact Email: vfurman@cs.technion.ac.il

Title: The left super-summit-set attack on Ko-Lee-Cheon-Han-Kang-Park key agreement protocol in B_45
Authors: Jim Hughes
Contact Email: jim@network.com

Title: ECSTR (XTR): Elliptic curve singular trace representation
Authors: Alfred Menezes and Scott Vanstone
Contact Email: vanstone@certicom.com

Title: Search on Encrypted Data
Contact Email: kurosawa@crypt.ss.titech.ac.jp
Abstract.ps

Title: TWEEDLE, a sound variation of TWINKLE
Authors: Jean-Jacques Quisquater
Contact Email: jjq@dice.ucl.ac.be

Title: Sharing block ciphers
Authors: Ernie Brickell, Giovanni Di Crescenzo and Yair Frankel
Contact Email: giovanni@research.telcordia.com

Title: A new application of EPR for quantum key distribution
Authors: Jaroslav Hruby
Contact Email: hruby@gcucmp.cz

Title: Correlation Cryptanalysis of SSC2
Authors: Greg Rose and Phil Hawkes
Contact Email: ggr@qualcomm.com
Abstract

Title: Simple electro-magnetic analysis for smartcards: New results
Authors: Jean-Jacques Quisquater and David Samyde
Contact Email: jjq@dice.ucl.ac.be

Title: Root Finding Interpolation Attack
Authors: Kaoru Kurosawa, Tetsu Iwata and Viet Duong Quang
Contact Emails: kurosawa@crypt.ss.titech.ac.jp, tez@crypt.ss.titech.ac.jp , viet@crypt.ss.titech.ac
Note: This appears in SAC 2000.
Abstract.ps

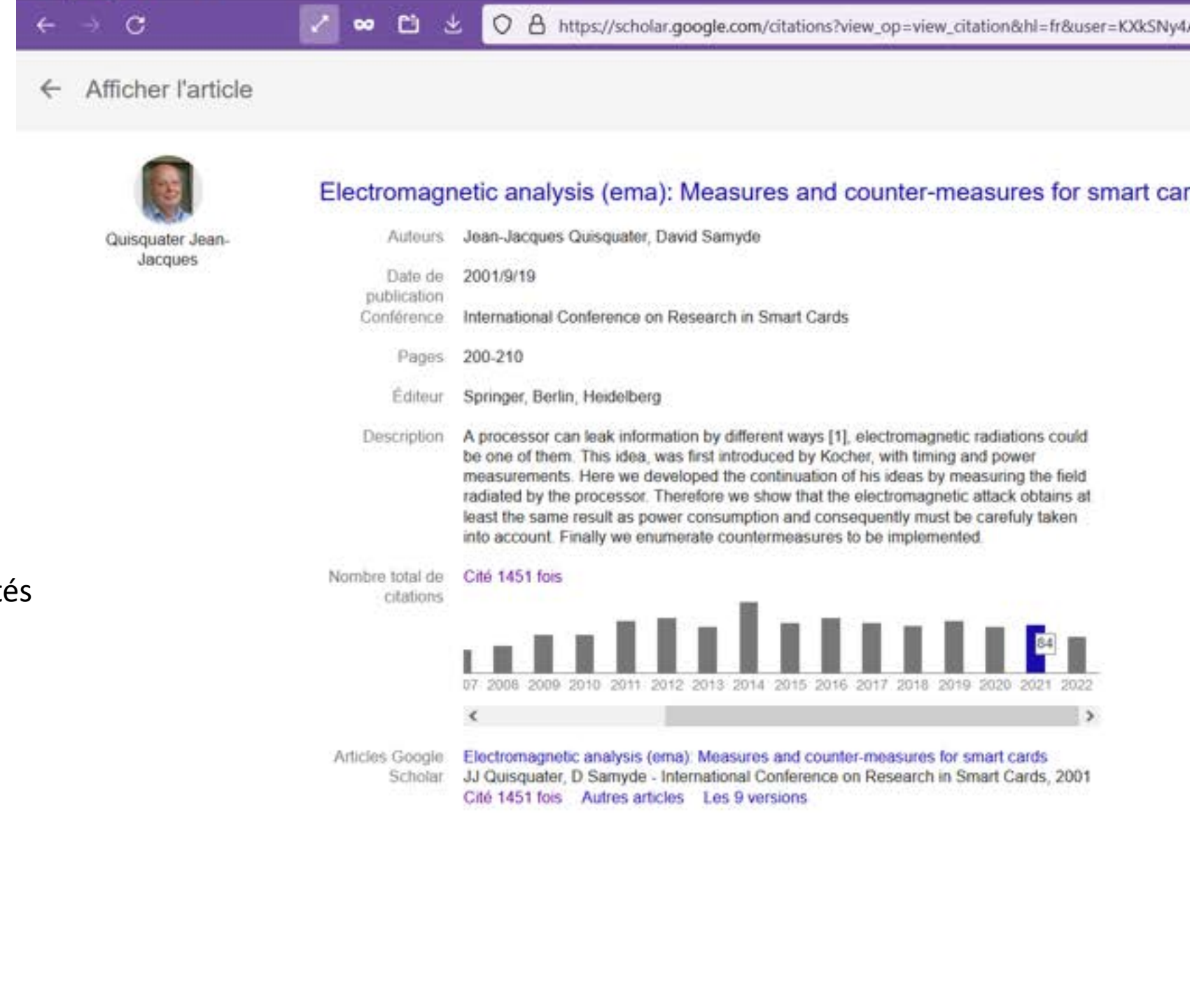
Title: Timing attacks: state of the art
Authors: Werner Schindler, Francois Koeune and Jean-Jacques Quisquater
Contact Email: werner.schindler@bsi.bund.de

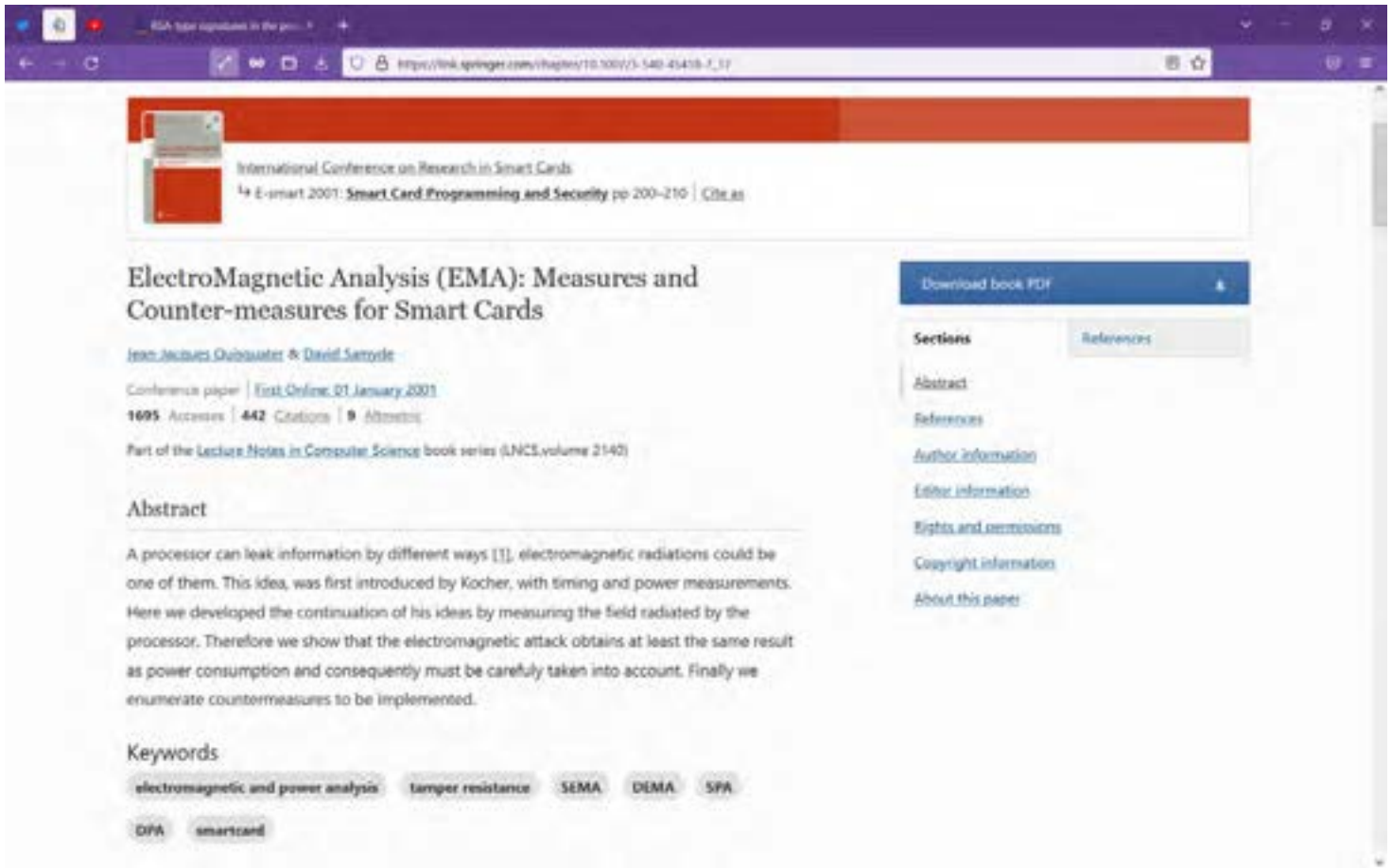
Title: A Non Euclidean Ring Data Scrambler (NERDS) - a public key cryptosystem
Authors: Emiliano Kargieman, Ariel Pacetti and Ariel Waissbein
Contact Email: wata@core-sdi.com
Abstract

Title: Timing Analysis in Exponentiation for RSA
Authors: B. Canvel and C.T.J. Dodson
Contact Email: dodson@umist.ac.uk
Abstract

David Samyde

- A proposé cet exposé à Gérard,
- A contribué à UCL Crypto Group
- A contribué dans différentes sociétés de certification
- A travaillé chez Intel.





International Conference on Research in Smart Cards
E-smart 2001: Smart Card Programming and Security pp 200–210 | Cite as

ElectroMagnetic Analysis (EMA): Measures and Counter-measures for Smart Cards

Jean-Jacques Quisquater & David Samyde

Conference paper | First Online: 01 January 2001

Part of the Lecture Notes in Computer Science book series (LNCS,volume 2140)

Abstract

A processor can leak information by different ways [1], electromagnetic radiations could be one of them. This idea, was first introduced by Kocher, with timing and power measurements. Here we developed the continuation of his ideas by measuring the field radiated by the processor. Therefore we show that the electromagnetic attack obtains at least the same result as power consumption and consequently must be carefuly taken into account. Finally we enumerate countermeasures to be implemented.

Keywords

electromagnetic and power analysis | tamper resistance | SEMA | DEMA | SPA | DPA | smartcard

Download book PDF

Sections | References

Timing attack: 1996

Annual International Cryptology Conference

CRYPTO 1996: **Advances in Cryptology — CRYPTO '96** pp 104–113 | Cite as

Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems

Paul C. Kocher

Conference paper | First Online: 01 January 2001

Part of the Lecture Notes in Computer Science book series (LNCS,volume 1109)

Sections | References

- Abstract
- References
- Author information
- Editor information
- Rights and permissions
- Copyright information
- About this paper

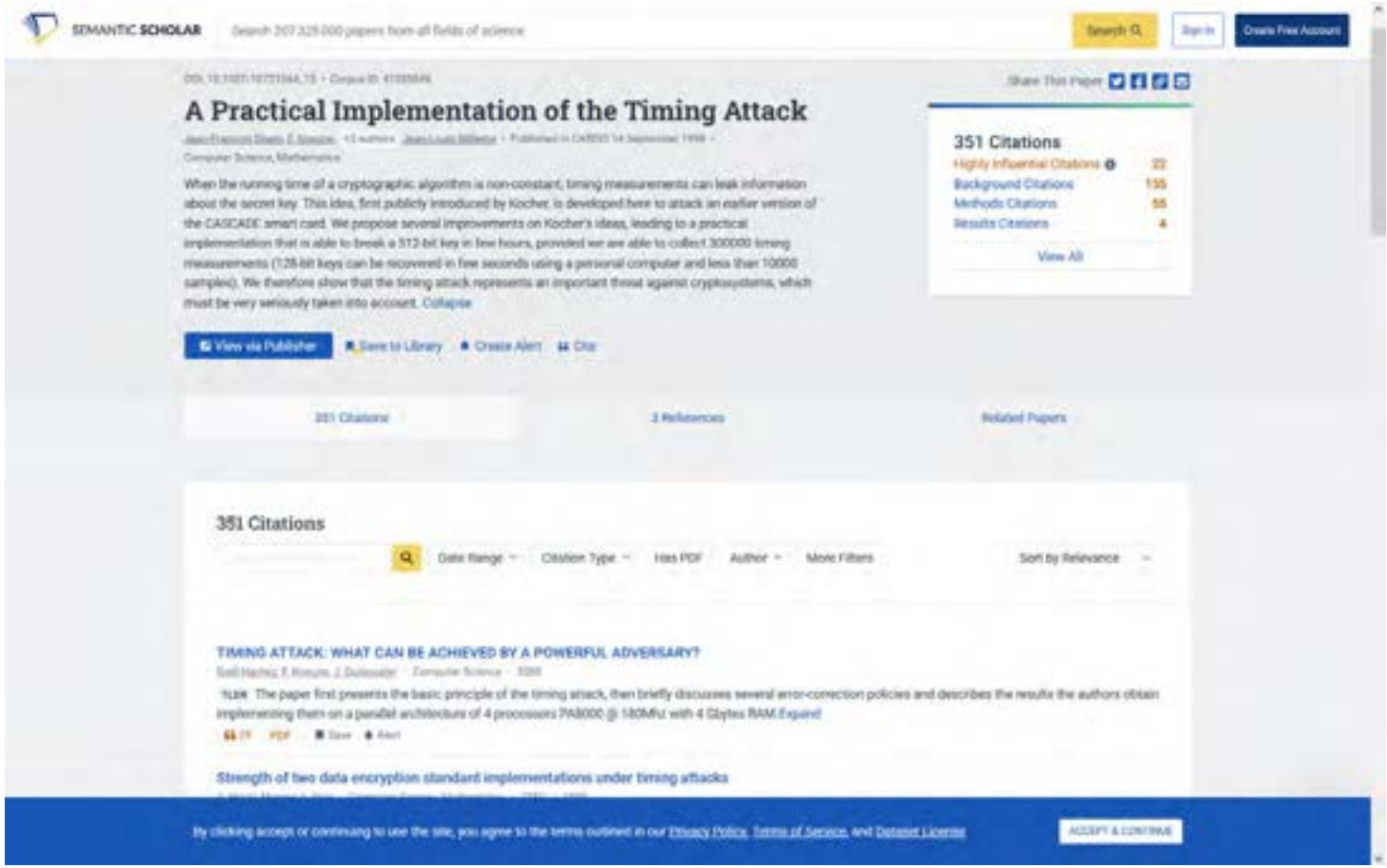
Abstract

By carefully measuring the amount of time required to perform private key operations, attackers may be able to find fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems. Against a vulnerable system, the attack is computationally inexpensive and often requires only known ciphertext. Actual systems are potentially at risk, including cryptographic tokens, network-based cryptosystems, and other applications where attackers can make reasonably accurate timing measurements. Techniques for preventing the attack for RSA and Diffie-Hellman are presented. Some cryptosystems will need to be revised to protect against the attack, and new protocols and algorithms may need to incorporate measures to prevent timing attacks.

Keywords

timing attack | cryptanalysis | RSA | Diffie-Hellman | DSS

Timing attack : CARDIS 1998 : LLN : Première démo publique



Tout d’abord 3 démos

- Mesure température,
- Mesure consommation du chargement d’une page web,
- Caméra infrarouge et rémanence du clavier.

Rémanence de chaleur (d’un clavier)

Thermanator: Thermal Residue-Based Post Factum Attacks On Keyboard Password Entry

Tyler Kaczmarek
UC Irvine
tkaczmar@uci.edu

Ercan Ozturk
UC Irvine
ercano@uci.edu

Gene Tsudik
UC Irvine
gene.tsudik@uci.edu

ABSTRACT

As a warm-blooded mammalian species, we humans routinely leave thermal residues on various objects with which we come in contact. This includes common input devices, such as keyboards, that are used for entering (among other things) secret information, such as passwords and PINs. Although thermal residue dissipates over time, there is always a certain time window during which thermal energy readings can be harvested from input devices to recover recently entered, and potentially sensitive, information.

To-date, there has been no systematic investigation of thermal profiles of keyboards, and thus no efforts have been made to secure them. This serves as our main motivation for constructing a means for password harvesting from keyboard thermal emanations. Specifically, we introduce Thermanator, a new post factum insider attack based on heat transfer caused by a user typing a password on a typical external keyboard. We conduct and describe a user study that collected thermal residues from 30 users entering 10 unique passwords (both weak and strong) on 4 popular commodity keyboards. Results show that entire sets of key-presses can be recovered by non-expert users as late as 30 **seconds** after initial password entry, while partial sets can be recovered as late as 1 **minute** after entry. Furthermore, we find that Hunt-and-Peck typists are particularly vulnerable. We also discuss some Thermanator mitigation strategies.

The main take-away of this work is three-fold: (1) using external keyboards to enter (already much-maligned) passwords is even less secure than previously recognized, (2) post factum (planned or impromptu) thermal imaging attacks are realistic, and finally (3) perhaps it is time to either stop using keyboards for password entry, or abandon passwords altogether.

1 INTRODUCTION

Insider attacks are very common, estimated to account for ≈ 28% of all electronic crimes in industry [13]. This includes some high-profile attacks, such as the 2014 Sony hack [20]. At the same time, it is well known that security of a system is based on its weakest link. Furthermore, it is often assumed that involvement of a fallible (or simply gullible) human user corresponds to this weakest link, e.g., as in Shoulder-Surfing and Lunch-Time attacks. However, other insider attacks that focus on stealing passwords by compromising the user environment, e.g., Acoustic Emanations [3, 8, 28] or Keyboard Vibrations [17], show that the weakest link is a consequence of a law of Physics. However, such insider attacks must occur instantaneously, in real time, in order to succeed. In other words, to exploit them, the adversary must be able to record the environment as the user is entering a password. Real-time adversarial presence (whether in person or via a nearby compromised recording device) raises the bar for the attack. This prompts the question:

Are there any observable physical effects of password entry that linger and can therefore be collected **afterwards**?

1.1 Heat Transfer & Thermal Emanations

Any time two objects with unequal temperatures come in contact with each other, an exchange of heat occurs. This is unavoidable. Being warm-blooded, human beings naturally prefer environments that are colder than their internal temperature. Because of this heat disparity, it is inevitable that we leave thermal residue on numerous objects that we routinely touch, especially, with with bare fingers. Furthermore, it takes time for these heated objects to cool off and lose heat energy imparted by human contact. It is both not surprising and worrisome that this includes our interactions with keyboards that are used for entering sensitive private information, such as passwords.

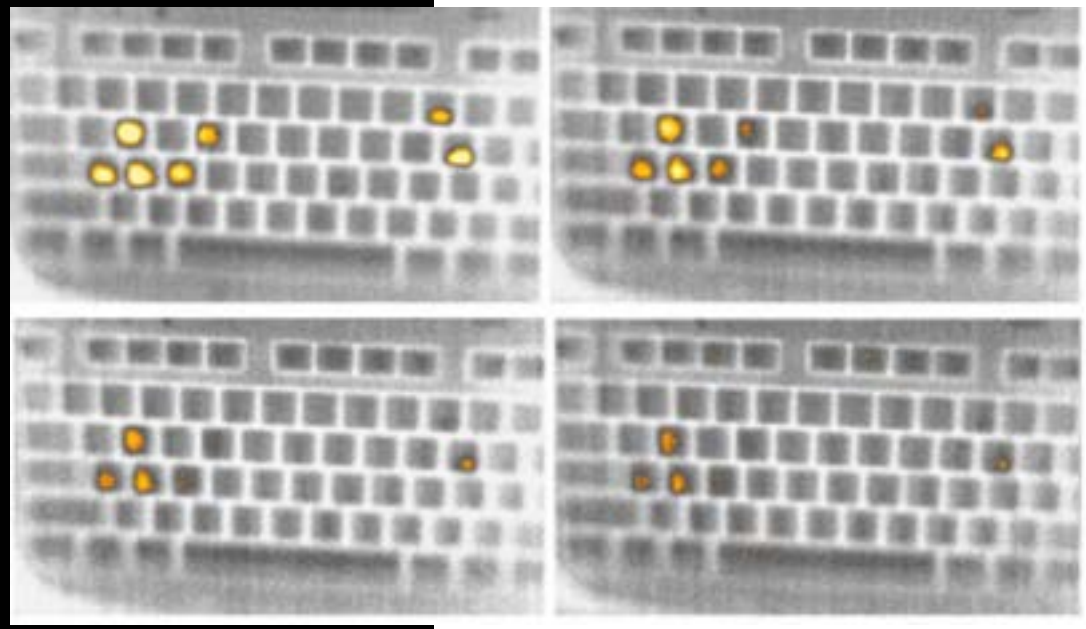
Based on this observation, we consider a mostly unexplored attack space where heat transfer and subsequent thermal residue can be exploited by a clever adversary to steal passwords from a keyboard some time after it was used for password entry. The main distinctive benefit of this attack type is that adversary's real time presence is not required. Instead, a successful attack can occur with after-the-fact adversarial presence: as our results show, many seconds later.

While there has been some prior work on using thermal emanations to crack PINs, mobile phone screen-locks and opening combinations of vaults/safes [1, 2, 14, 26], this work represents the first comprehensive investigation of human-based thermal residues and emanations of external computer keyboards.

1.2 Expected Contributions

In this paper, we propose and evaluate a particular human-based side-channel attack class, called Thermanator. This attack class is based on exploiting thermal residues left behind by a user (victim) who enters a password using a typical external keyboard. Shortly after password entry, the victim either steps away inadvertently, or is drawn away (perhaps as a result of being prompted by the adversary) from the personal workplace. Then, the adversary captures thermal images of the victim keyboard. We examine the efficacy of Thermanator Attacks for a moderately sophisticated adversary equipped with a mid-range thermal imaging camera. The goal of the attack is to learn information about the victim password.

To confirm viability of Thermanator Attacks, we conducted a rigorous two-stage user study. The first stage collected password entry data from 31 subjects using 4 common keyboards. In the second stage, 8 non-expert subjects acted as adversaries and attempted to derive the set of pressed keys from the thermal imaging data collected in the first stage. Our results show that even novice adversaries can use thermal residues to reliably determine the entire



Attaques basées sur le comportement humain

Table 1: Feature Comparison of Common Human-Based Attack Types.

Attack Type:	Attack Goal:	Adversary Timeliness	Careless Victim?	Equipment Needed:	Prior Profiling Required?
Lunch-Time	Hijack Log-in Session	15 min (default)	YES	None	NO
Shoulder-Surfing	Password	Real-Time	YES	Pair of Eyes or Video Camera	NO
Acoustic Emanations	Password	Real-Time	NO	Audio Recorder	YES
Keyboard Vibrations	Password	Real-Time	NO	Accelerometer	YES
Thermanator	Password	up to 1 min	NO	Thermal Camera	NO

Corneal reflections

OPEN ACCESS Freely available online

PLOS ONE

Identifiable Images of Bystanders Extracted from Corneal Reflections

Rob Jenkins[1]*, Christie Kerr[2]

1 Department of Psychology, University of York, York, North Yorkshire, United Kingdom, **2** School of Psychology, University of Glasgow, Glasgow, Lanarkshire, United Kingdom

Abstract

Criminal investigations often use photographic evidence to identify suspects. Here we combined robust face perception and high-resolution photography to mine face photographs for hidden information. By zooming in on high-resolution face photographs, we were able to recover images of unseen bystanders from reflections in the subjects' eyes. To establish whether these bystanders could be identified from the reflection images, we presented them as stimuli in a face matching task (Experiment 1). Accuracy in the face matching task was well above chance (50%), despite the unpromising source of the stimuli. Participants who were *unfamiliar* with the bystanders' faces (n = 16) performed at 71% accuracy [$t(15) = 7.64$, $p < .0001$, $d = 1.91$], and participants who were *familiar* with the faces (n = 16) performed at 84% accuracy [$t(15) = 11.15$, $p < .0001$, $d = 2.79$]. In a test of spontaneous recognition (Experiment 2), observers could reliably name a familiar face from an eye reflection image. For crimes in which the victims are photographed (e.g., hostage taking, child sex abuse), reflections in the eyes of the photographic subject could help to identify perpetrators.

Citation: Jenkins R, Kerr C (2013) Identifiable Images of Bystanders Extracted from Corneal Reflections. PLoS ONE 8(12): e83325. doi:10.1371/journal.pone.0083325

Editor: Matthew Longo, Birkbeck, University of London, United Kingdom

Received June 17, 2013; **Accepted** November 2, 2013; **Published** December 26, 2013

Funding: This research was funded by the Economic and Social Research Council, UK. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Competing Interests: The authors have declared that no competing interests exist.

* E-mail: rob.jenkins@york.ac.uk

Zoom …

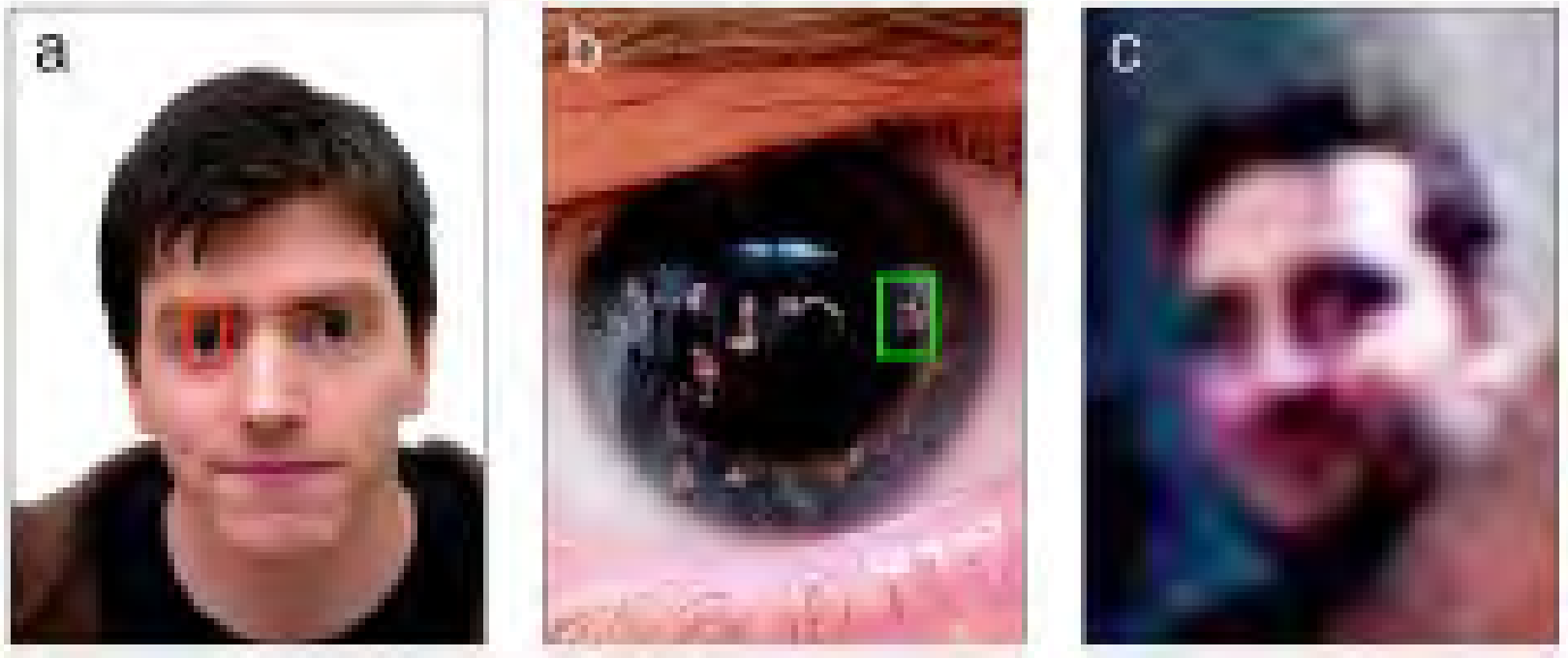
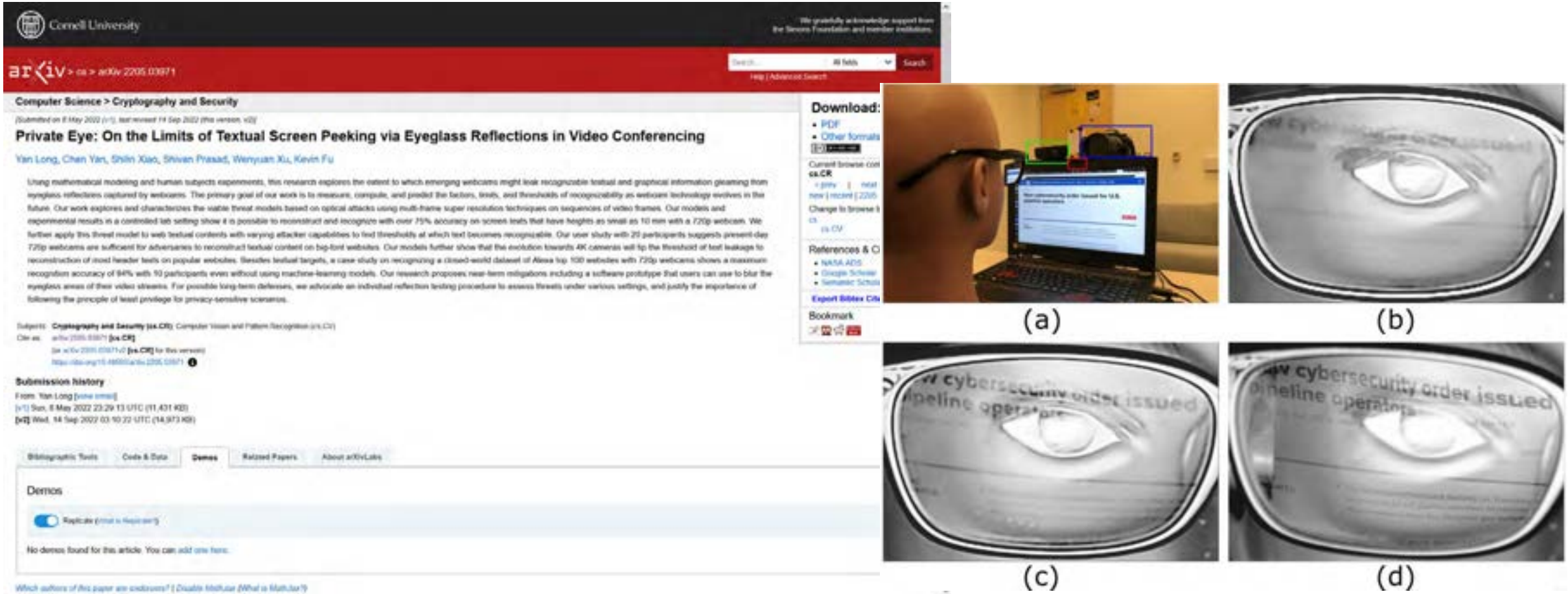


Image processing

Réflexions sur les lunettes



Consommation de chargement de pages web

Current Events: Identifying Webpages by Tapping the Electrical Outlet

Shane S. Clark[1] Hossen Mustafa[2] Benjamin Ransford[3]
Jacob Sorber[4] Kevin Fu[5] and Wenyuan Xu**[2,6]

[1]University of Massachusetts Amherst [2]University of South Carolina
[3]University of Washington [4]Clemson University [5]University of Michigan
[6]Zhejiang University

Abstract. Computers plugged into power outlets leak identifiable information by drawing variable amounts of power when performing different tasks. This work examines the extent to which this side channel leaks private information about web browsing to an observer taking measurements at the power outlet. Using direct measurements of AC power consumption with an instrumented outlet, we construct a classifier that correctly identifies unlabeled power traces of webpage activity from a set of 51 candidates with 99% precision and 99% recall. The classifier rejects samples of 441 pages outside the corpus with a false-positive rate of less than 2%. It is also robust to a number of variations in webpage loading conditions, including encryption. When trained on power traces from two computers loading the same webpage, the classifier correctly labels further traces of that webpage from either computer. We identify several reasons for this consistently recognizable power consumption, including system calls, and propose countermeasures to limit the leakage of private information. Characterizing the AC power side channel may help lead to practical countermeasures that protect user privacy from an untrustworthy power infrastructure.

1 Introduction

Computer users commonly assume that software mechanisms, such as in-browser encryption, protect their private information. Research on side channels has challenged this assumption by showing that computer components such as the CPU [18] and the keyboard [32] can leak private information. Along the same lines, this paper examines the feasibility of inferring private information from a general-purpose computer's AC power consumption, despite significant additive noise from the power grid [6].

Past work has exploited AC power side channels for information leakage, but at the level of an entire household [24] or a device with a constrained state space [8, 6]. For example, a television that is dedicated to displaying videos produces relatively consistent power consumption over multiple plays of the same video. Given a small number of candidate videos, it is possible to identify which of them is playing [8]. A general-purpose computer, on the other hand, exhibits a tremendous state space because of its practically unconstrained operation. Executing the same computing task at

** Corresponding faculty author

Published in Proceedings of European Symposium on Research in Computer Security, 2013

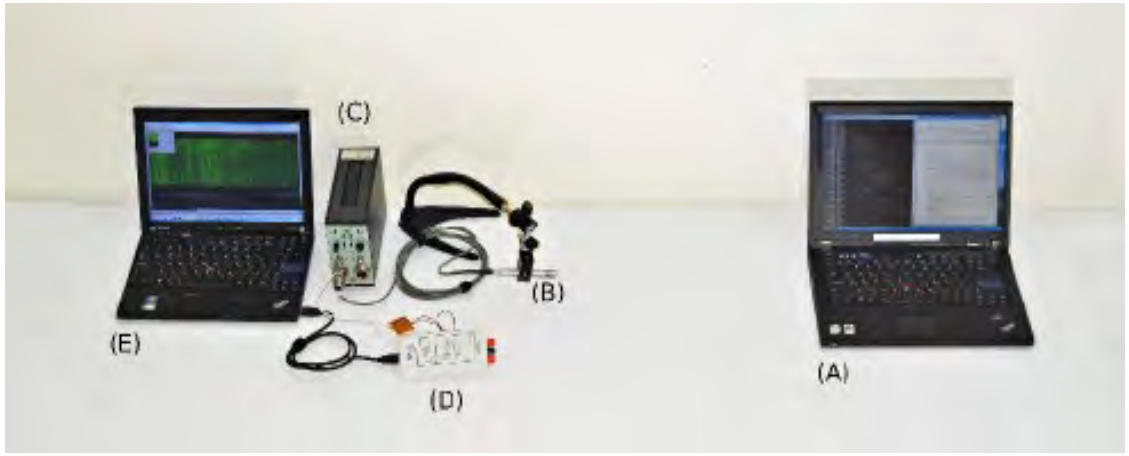
The graduate acoustic attack: “The sound of silence” °

Jean-Jacques Quisquater (UCL-Crypto)

Moti Yung (Google, Columbia)

° Thanks to Garfunkel and Simon

Tuesday August 19, 2014, 2pm, CRYPTO-UCSB:
3 set-ups of acoustic attacks against a long RSA key (Genkin-Shamir-Tromer)



Acoustic attack: the model

Your COMPUTER with RSA key to be attacked

→At some distance vibrating OBJECT (MICROPHONE) connected to another computer

→signal and cryptographic processing

→RSA key in the hand of enemy

We want more: attacking from outside such an computer put in a sound-proof room …

- We want to expand our knowledge of **Acoustical Intelligence** (**ACOUSTINT**, sometimes **ACINT**): it is an intelligence gathering discipline that collects and processes acoustic phenomena.
- Here is a possible set-up for the computer (and the user ☺) …

Acoustic attack: new model

Your COMPUTER with RSA key to be attacked

→At some distance some vibrating OBJECT (which one?)

→Full-proof-sound room and window

→signal and cryptographic processing

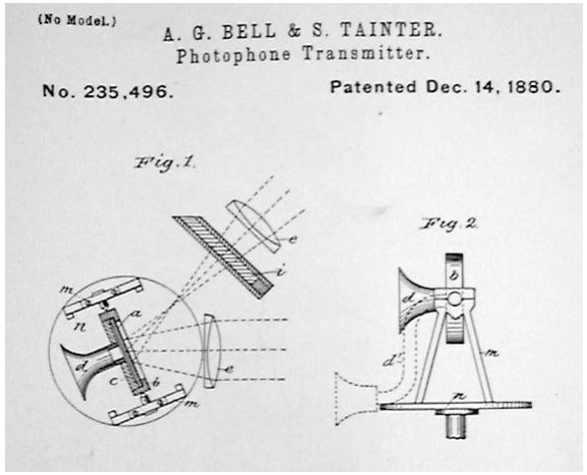
→RSA key in the hand of enemy

Is it possible?

By the way how old are acoustic attacks?

A Century Old Invention: the photophone.

April 26th, 1880 – **Alexander Graham Bell** & **Sumner Tainter** announce their invention - the Photophone. Sound is transmitted on reflected light-rays a **distance of 213 meters**. They also claim, "it can transmit songs with great purity of tone." This is the forerunner of CDs, DVDs, fiber optic telephone transmission, and **remote eavesdropping**.

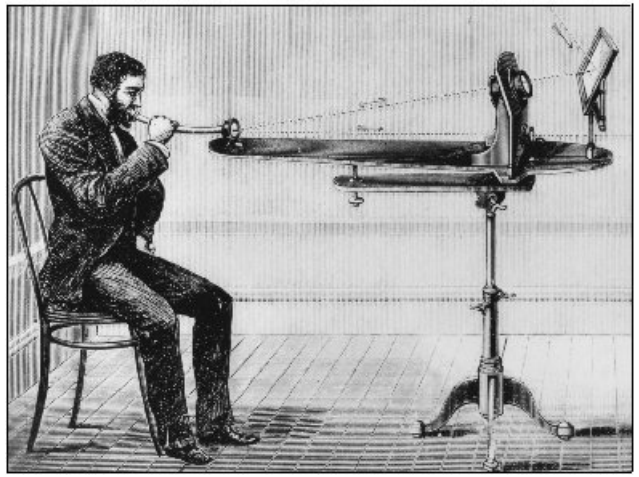

(No Model.)

A. G. BELL & S. TAINTER.
Photophone Transmitter.

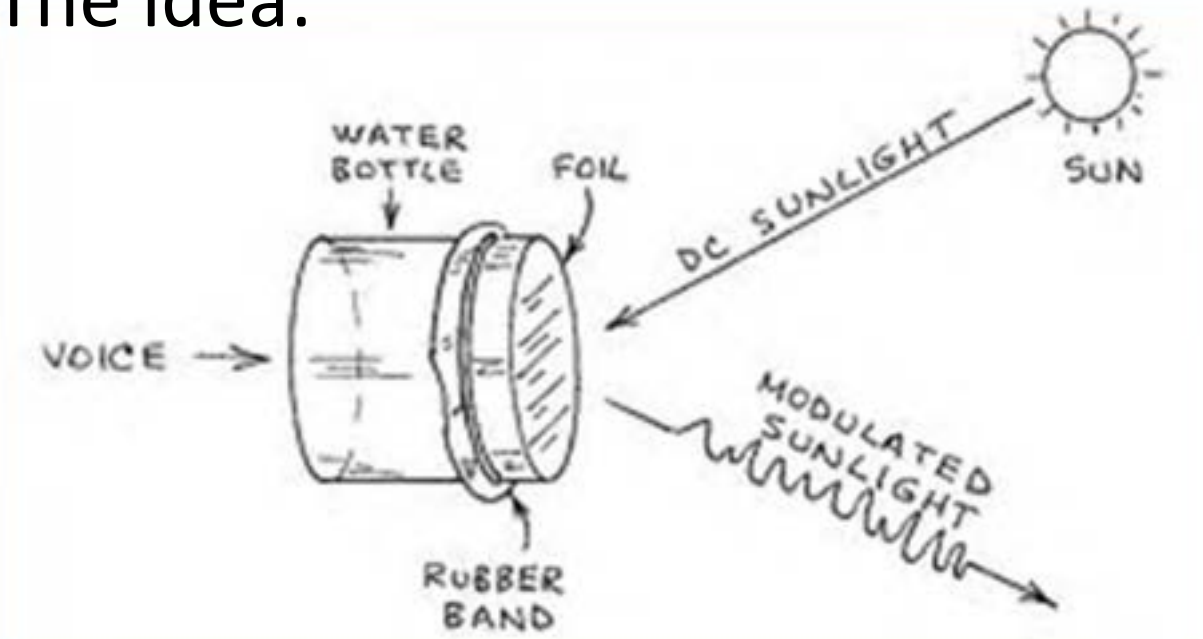
No. 235,496. Patented Dec. 14, 1880.

Fig. 1.

Fig. 2.

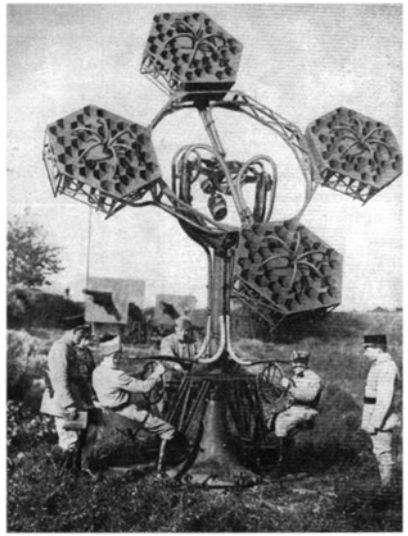


The idea:



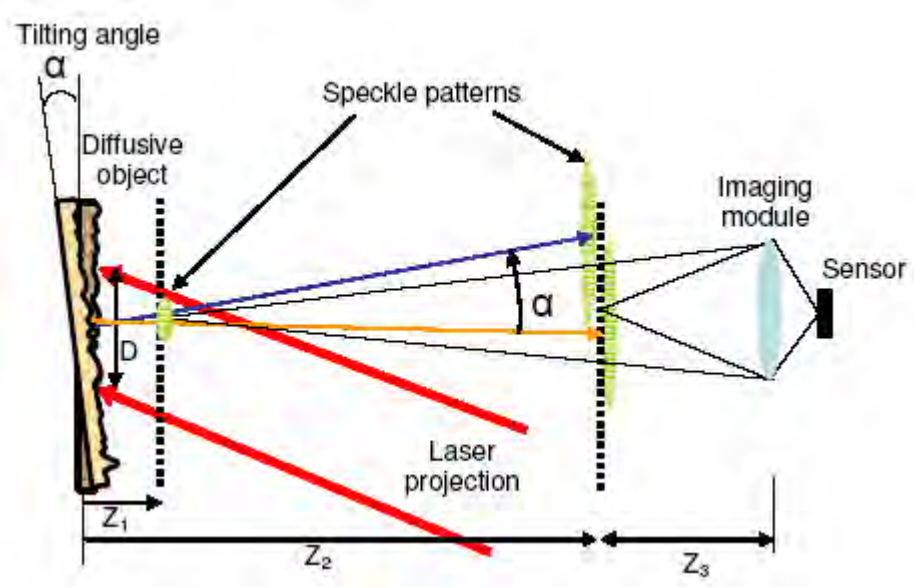
Other old projects (acoustic locators)

Professor Mayer's topophone [1880]



More about active acoustic attacks:
1. replacing sun by remote laser in the photophone

- *Simultaneous remote extraction of multiple speech sources and heart beats from secondary speckles pattern,* by Zeev Zalevsky, Yevgeny Beiderman, Israel Margalit, Shimshon Gingold, Mina Teicher, Vicente Mico, and Javier Garcia (Bar-Ilan University and Universitat de València): *Optics Express*, Vol. 17, Issue 24, pp. 21566-21580 (2009).



The configuration includes projection of laser beam and observation of the movement of the secondary **speckle pattern** that are created on top of the target (diffusive object). The speckles are self interference random patterns and have the remarkable quality that each individual speckle serves as a reference point from which one may **track the changes** in the phase of the light that is being scattered from the surface. The sensor is a fast expensive camera (7800 fps) used in defocused mode.

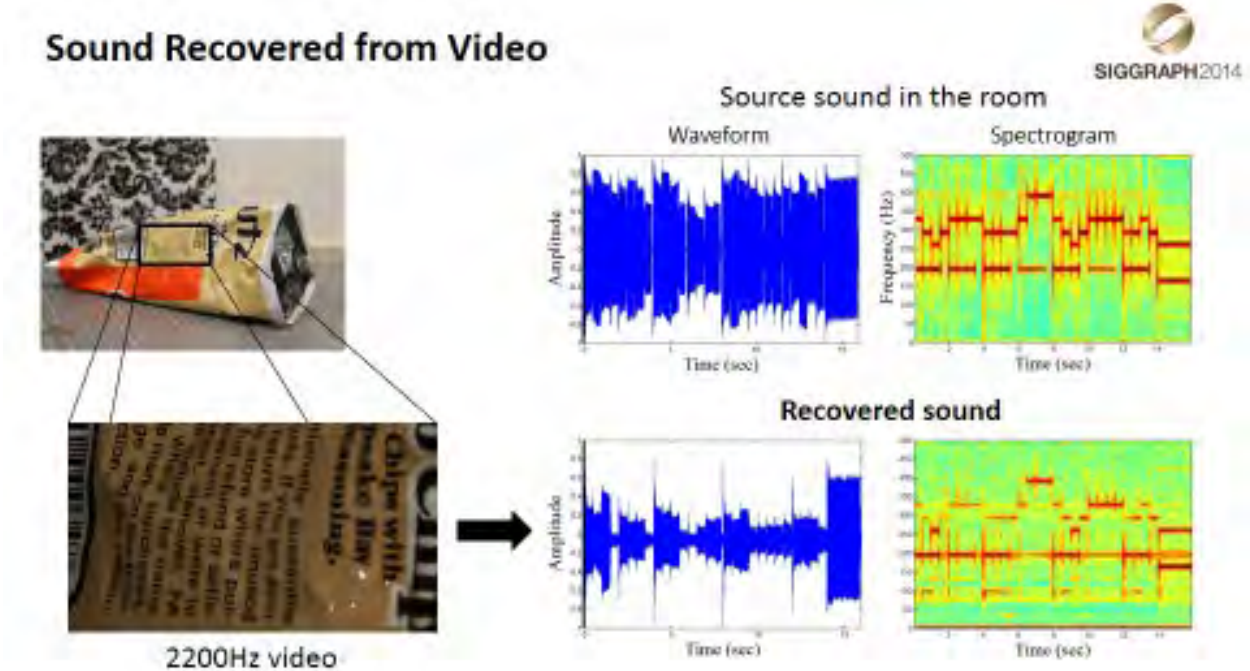
Then taping a cellular phone or
listening from the back of the neck!
Possible range is 100 meters or more using a telescope.

(a).

(a).

2. A new passive acoustic attacks:
the visual microphone (SIGGRAPH 2014, last week) by
Abe Davis, Michael Rubinstein, Neal Wadhwa, Gautham Mysore,
Frédo Durand, William T. Freeman

- Replacing the sensor (classical microphone) by any familiar vibrating object close to the sound then using a remote camescope: they then amplify a lot these vibrations from the object using an algorithm (Eulerian Video Magnification). Then they recover the sound.



Final model and set-up

- RSA "sound" from a computer to be attacked,
- corresponding vibrations of a familiar object close to the computer,
- (mirror and) sound-proof window and room,
- external camescope (using a trick: the rolling shutter) with zoom for the attack,
- translation of the images into "sound" using Eulerian Video Magnification,
- if necessary "deblurring" of the sound thanks to the equivalent method for images (using several sources), see http://users.soe.ucsc.edu/~milanfar/ (March 2014 in recent news)
- then using the ideas from the CRYPTO 2014 paper.

More: The gyrophone (usenix 2014, next Friday)

An old story from 1956 ("Spycatchers", by Peter Wright):

- British intelligence wanted to read Egyptian diplomatic traffic encrypted by Hagelin machine from their embassy in London to the foreign office in Cairo
- The secret key was set each morning by moving the rotors to a new initial setting.
- The British MI5 made sure that a nearby basement telephone was always connected
- All they had to do each morning was to count the number of clicks heard over the phone during the key setup on the adjacent Hagelin machine.

Militaires : TEMPEST

Tempest (codename)

From Wikipedia, the free encyclopedia

TEMPEST is a U.S. National Security Agency specification and a NATO certification[1][2] referring to spying on information systems through leaking emanations, including unintentional radio or electrical signals, sounds, and vibrations.[3][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.[8] 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]

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.

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 ft (30 m) -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 (60 m), based more on what commanders could be expected to accomplish than any technical criteria.

Machine à voter : 1985 …

Premières attaques civiles

- TNO (Pays-Bas)
- IBM
- Sandia (livre de Gus Simmons)
- Philips

Attaques passives (écoutes)
(Applications aux cartes à puce)

New system uses low-power Wi-Fi signal to track moving humans — even behind walls

'Wi-Vi' is based on a concept similar to radar and sonar imaging.

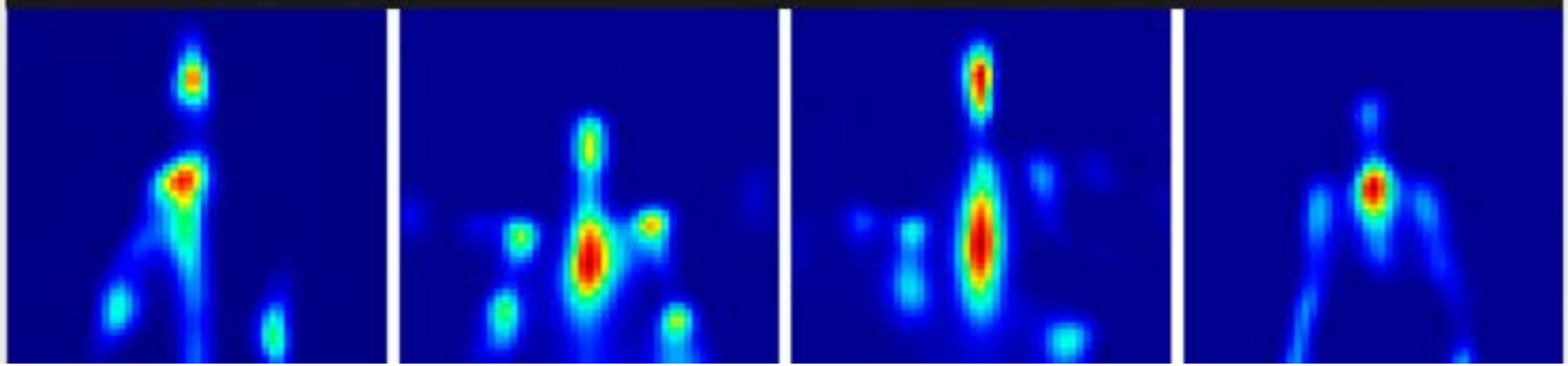
Helen Knight, MIT News correspondent
June 28, 2013

Illustration: Christine Daniloff/MIT

HOUSEHOLD RADAR CAN SEE THROUGH WALLS AND KNOWS HOW YOU'RE FEELING

Modern wireless tech isn't just for communications. It can also sense a person's breathing and heart rate, even gauge emotions

BY EADEL ADIB | 30 MAY 2019 | 10 MIN READ



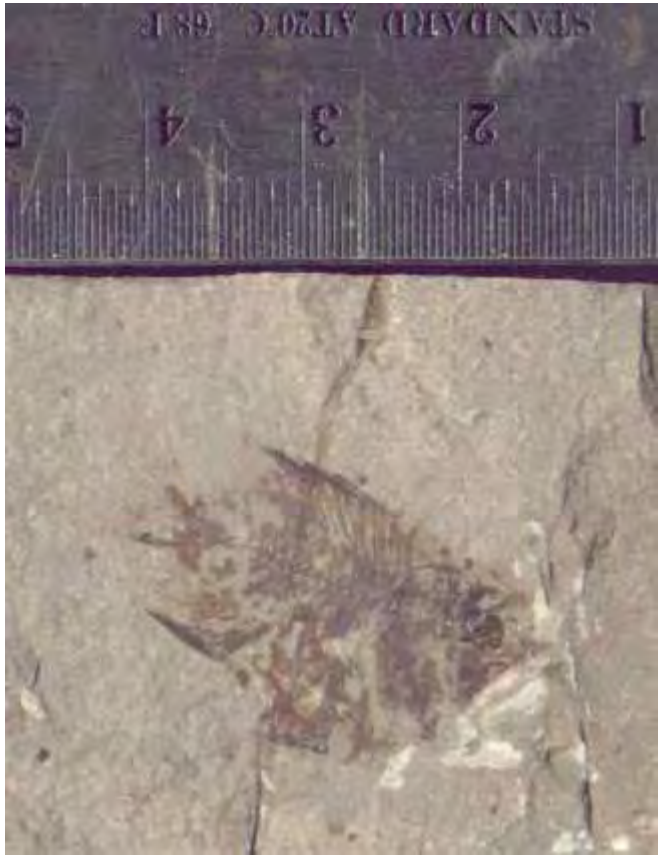
Taxonomy of Attackers (from IBM)

- *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

Fossile de poisson

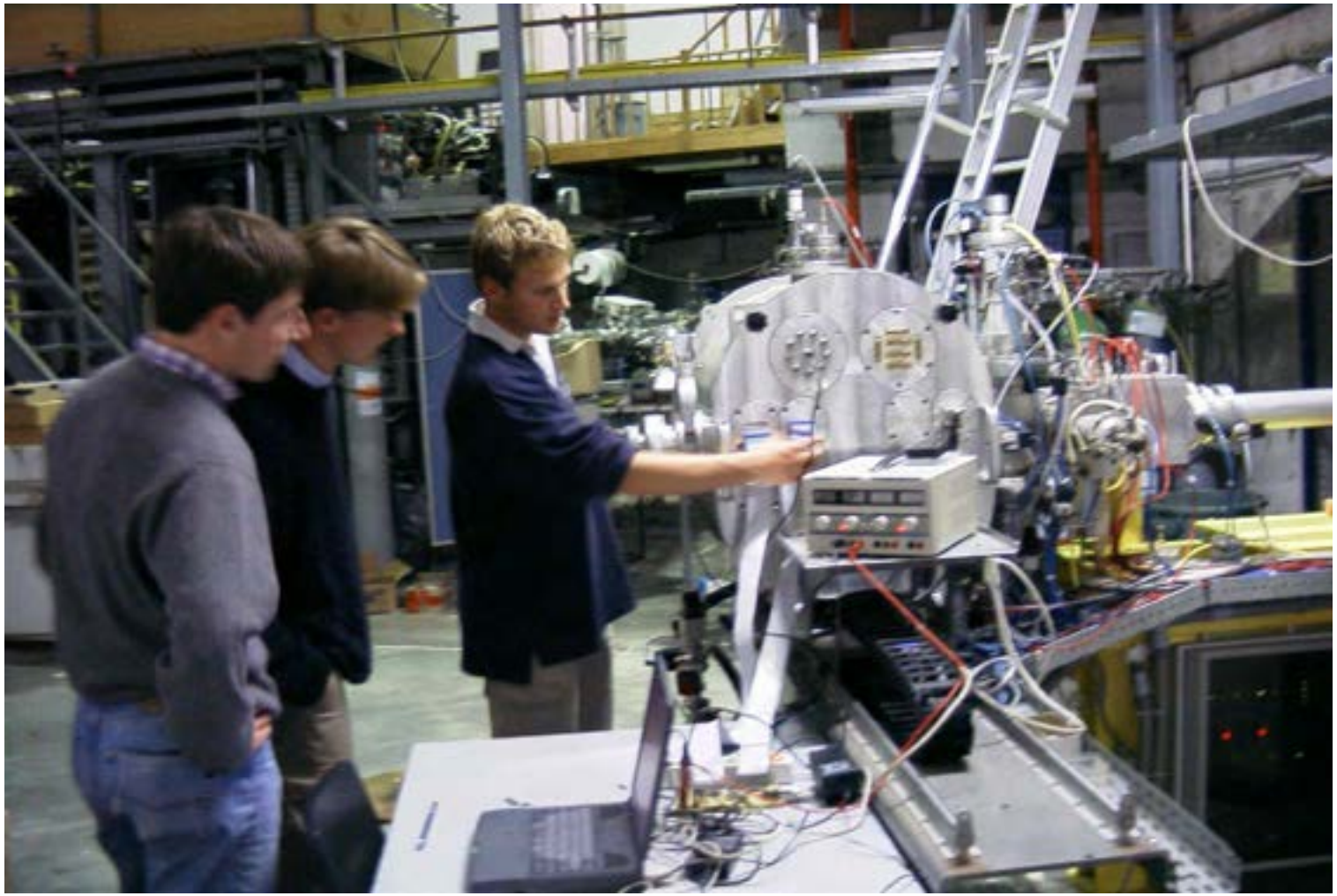
Class I (photo)



Class I: scanner (+ photoshop)

Class I (photoshop - end)

Class II? Free slot

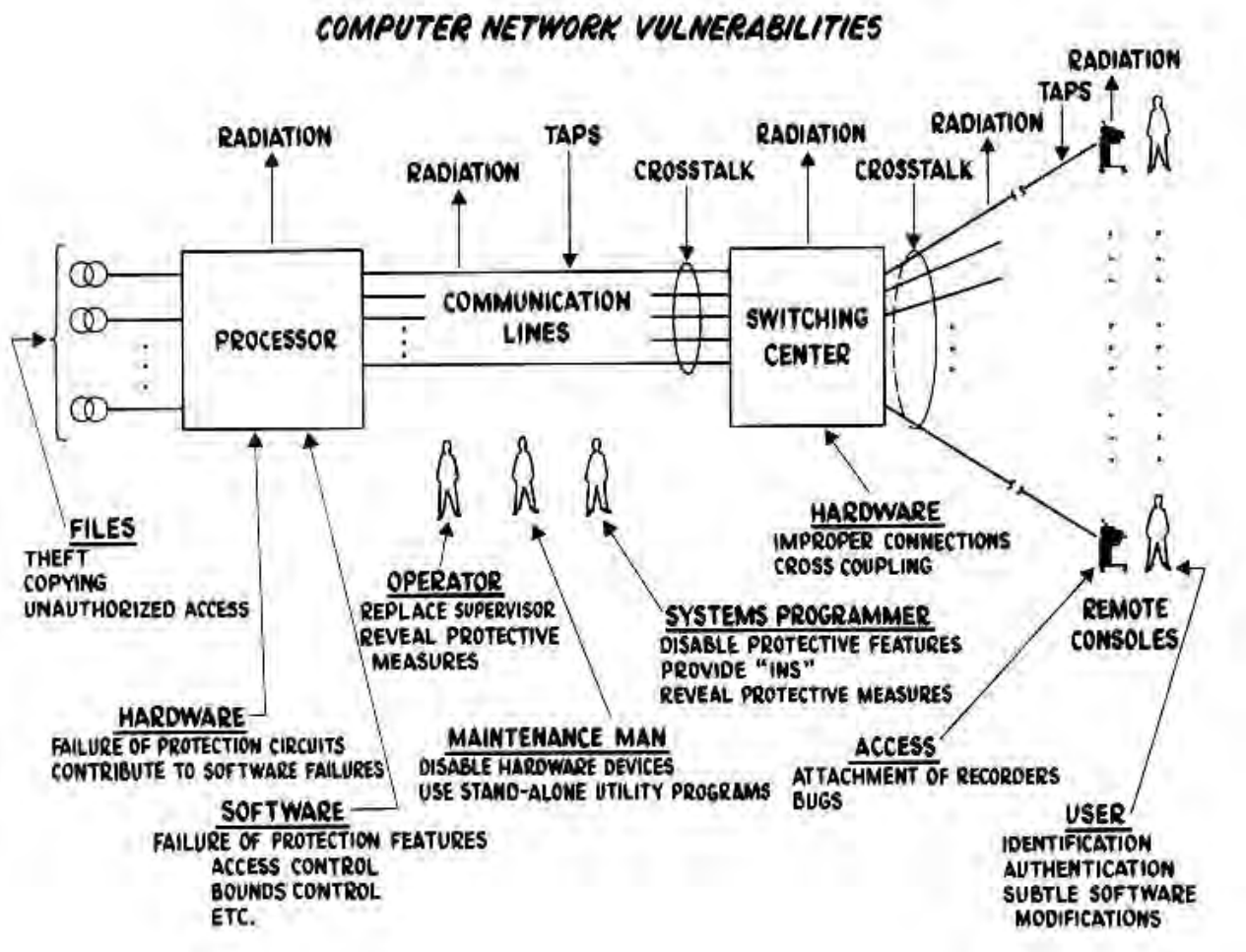


Attaque transitoire
De RAM par
un faisceau de
cyclotron

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)



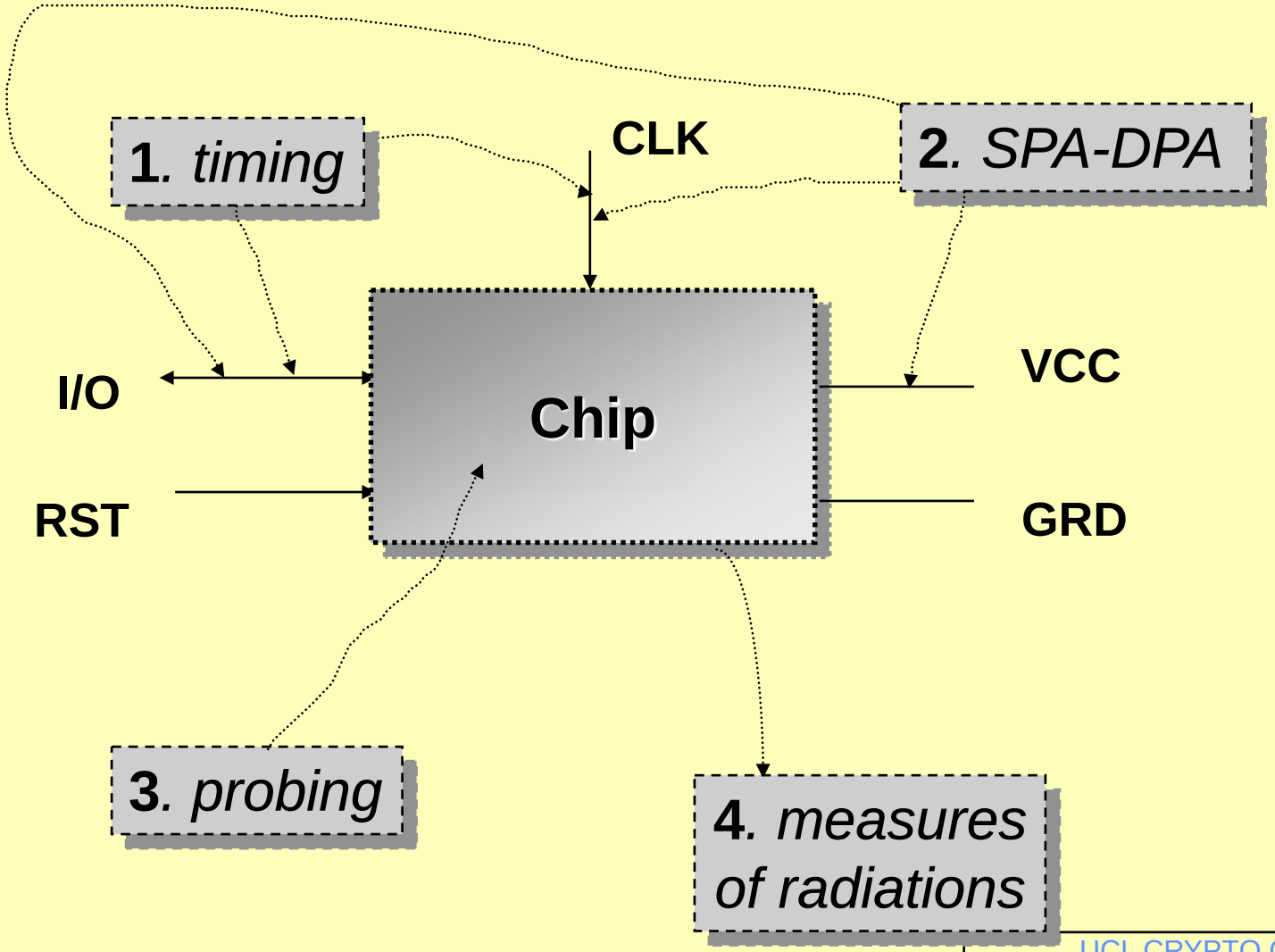
EMA analysis (my story)

- Old printer (1976) « playing »,
- A Saturday (1978) working with a CRT and a FM receiver,

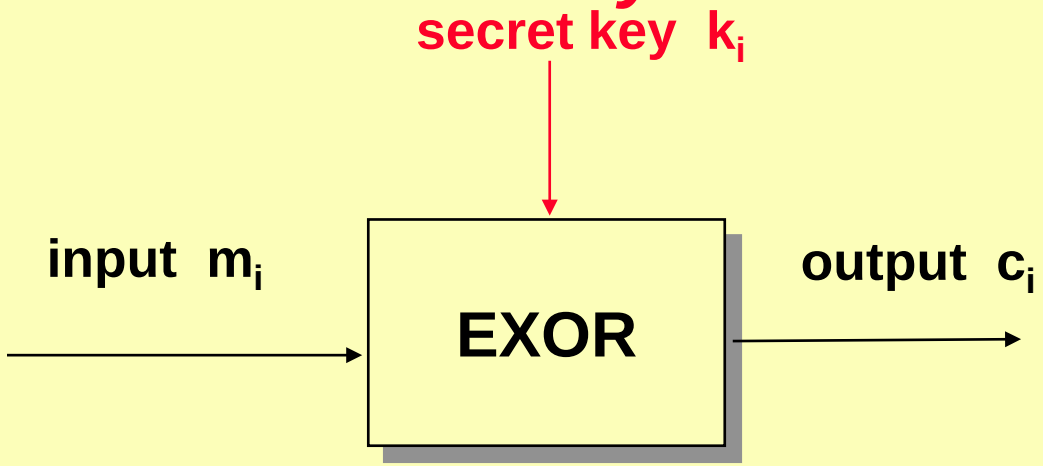
- **Date**: Wed, 18 Aug 1999 19:15:09 +0300 (EEST)
  From: Berke Durak <durakb@crit2.univ-montp2.fr>
  To: cypherpunks@toad.com
  Subject: *Controlled CPU TEMPEST emanations Hello, After having implemented and successfully tested Ross Anderson's idea to use the video output to synthesize a mediumwave 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 …

Generic model of card for passive attacks



Analysis of a simple model (Vernam)

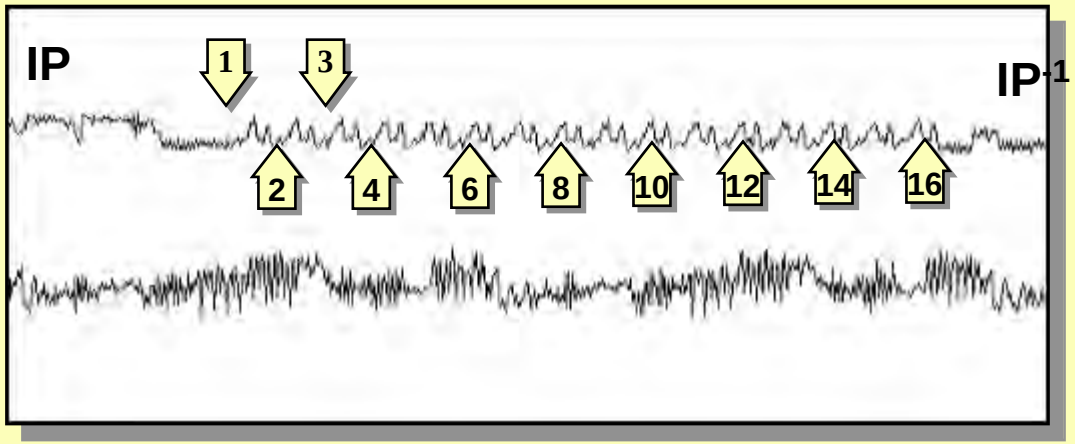


mi	ki	ci
0	0	0
0	1	1
1	0	1
1	1	0

mi	ki	ci
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.

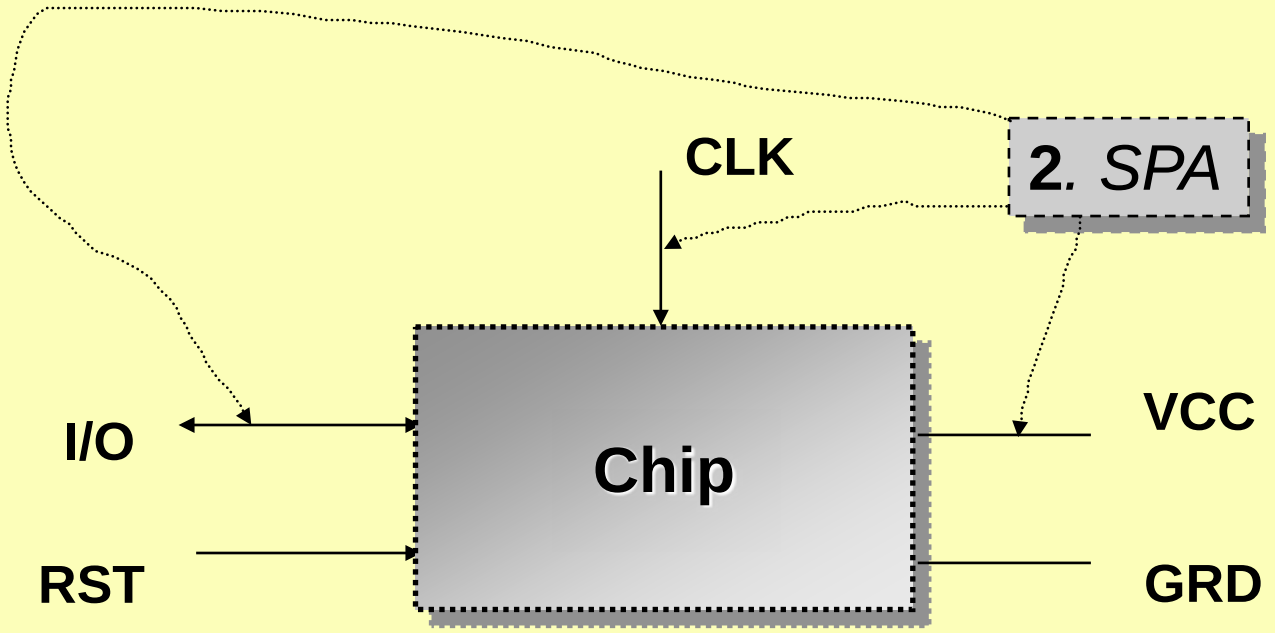
Simple Power analysis (example)



These traces (power consumption of a typical smart card) are coming from the original paper by Cryptography Research (Paul Kocher)

- the upper one describes the full execution of the 16 rounds of DES and the permutations;
- the lower one describes the rounds 2 and 3 of DES.

Simple Power analysis (countermeasures)



- adding (pseudo) random behavior to the cryptographic algorithms
- hypothesis: some instructions are leaking less information (addition, EXOR, ...)

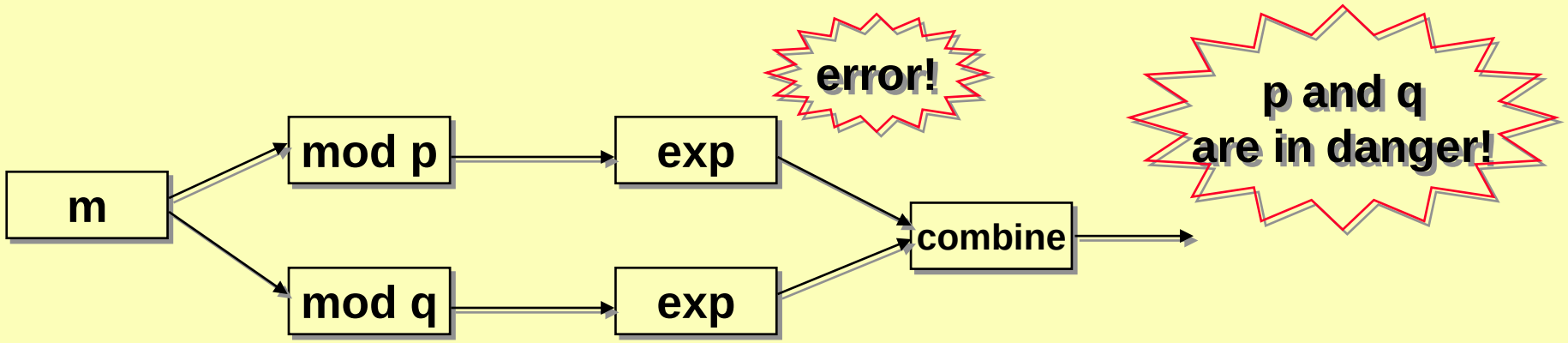
Glitch attack (Lenstra, Joye, Q)

- The first version was called the Bellcore attack
- Context: smart card answers to a request of a RSA signature: one interaction, public key is known
- During a computation of the smart card a special event occurs (error, bug, clock, current, radiation, laser, …)
- See paper by R. Anderson and M. Kuhn
- This event gives an error: this error is not detected and the computation continues …
- The worse case is when the computation uses the secret key in a specific way (example: RSA with CRT)
- The results is outputted
- Simple computation allows an opponent to recover the secret key!
- Countermeasure: verification of output before …

Implementation problems

- optimisation: minimisation of the number of multiplications and square

- Chinese Remainder Theorem



Timing Attack

J.-F. Dhem, F. Koeune, P.-A. Leroux
P. Mestré, J.-J. Quisquater and J.-L. Willems

UCL Crypto Group

Scenario

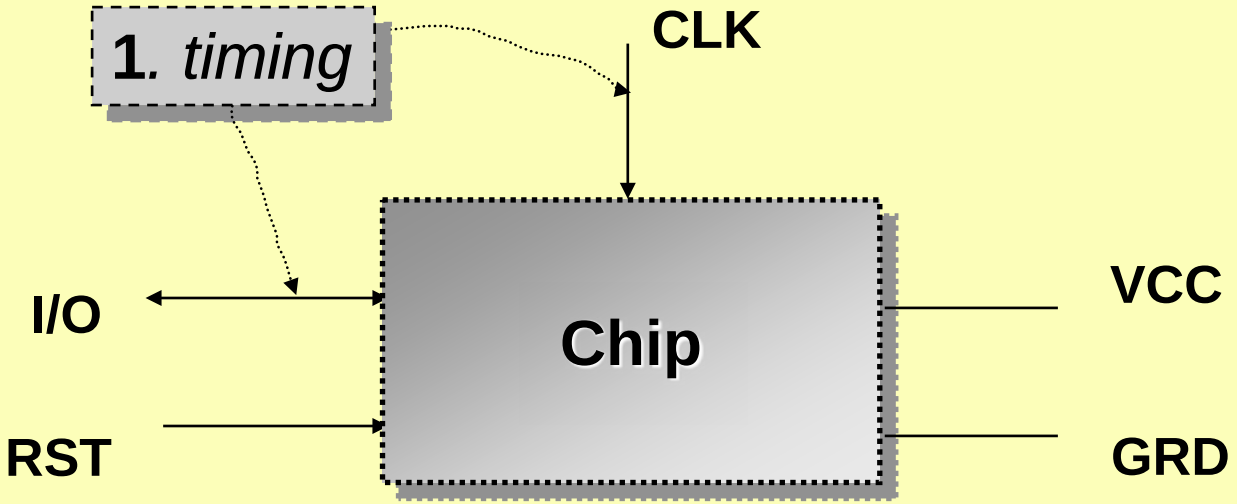
- An attacker is observing many RSA signatures

$$m_j^k \pmod N$$

and to collect messages m_j and the corresponding timings

- His goal : recover the secret parameter **k**

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).

Square and Multiply

To compute $m^k \pmod N$,

```
x = 1
for i=1 to t do
    x = x^2 (mod N)
    if (k_j=1) then x = x.m  (mod N)
od
```

the two multiplications are performed using the Montgomery multiplication algorithm

Montgomery Multiplication

- Allows to compute A.B (mod N) very efficiently
- The whole multiplication will require at most one modular reduction, at the end of the process

Attacking the Multiply

```
x = 1
for i=1 to n do
      x = x^2
      if (k_i=1)
            then x = x.m
od
```

At step i,

- **if k_i=0, nothing**
- **if k_i=1, a multiplication, which will be longer for some messages than for others**

Knowing $k_1..k_{i-1}$, we are able to divide the sample into two subsets A and B

Attacking the Multiply

We are thus able to build two subsets which will behave differently *if the multiplication is executed*

In practice

Begin by attacking bit 1 (=consider the first multiplication, that *would* occur if bit 1 was set)

- **for every message of the sample : if the message induces a reduction, put it in subset A, otherwise put it in subset B**
- **if the mean time for A is significantly greater than that for B, then conclude a multiplication has actually occured at that point (k_1=1), else conclude k_1=0**

Once we know bit 1, attack bit 2.

Problem

- What does significantly mean ?
- When can we say that two subsets are different ?

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

Optimized TA

Schindler (2000])

- **Formal treatment of the TA problem**
- **Characterization of the "additional reduction phenomenon"**
- **Optimal decision strategy**

Optimized strategy

- **Decision strategy proved (well, almost) to be a Bayes strategy (i.e. optimal)**
- **Characterization of error probability**
  → *Theoretical estimation of sample size*
- **Characterization of error-detection**

Drawbacks

- **More detailed knowledge of implementation necessary (e.g. time taken by additional reduction)**

can be approximated

- **Must know hamming weight of secret key**

can be guessed

(no need for more messages)

In practice

1. **By statistical treatment, guess (even roughly) unknown implementation characteristics**

2. **For each "likely" value of hamming weight, apply attack (using same sample)**

3. **Correct key (or small subset) will show up**

Current Results (02/2001)

Key size	Classical	Optimized
128	5 000 – 8 000	1 000 – 2 000
512	150 000 – 200 000	8000

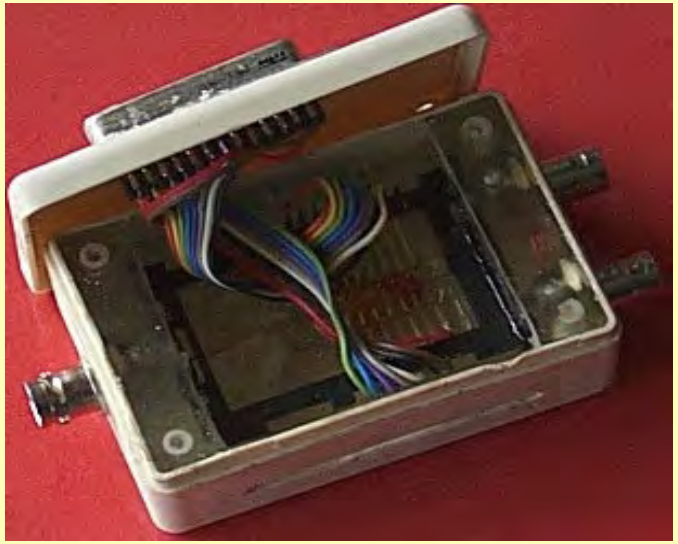
- Practice in accordance with theory
- Slight improvement should still come…

Countermeasures

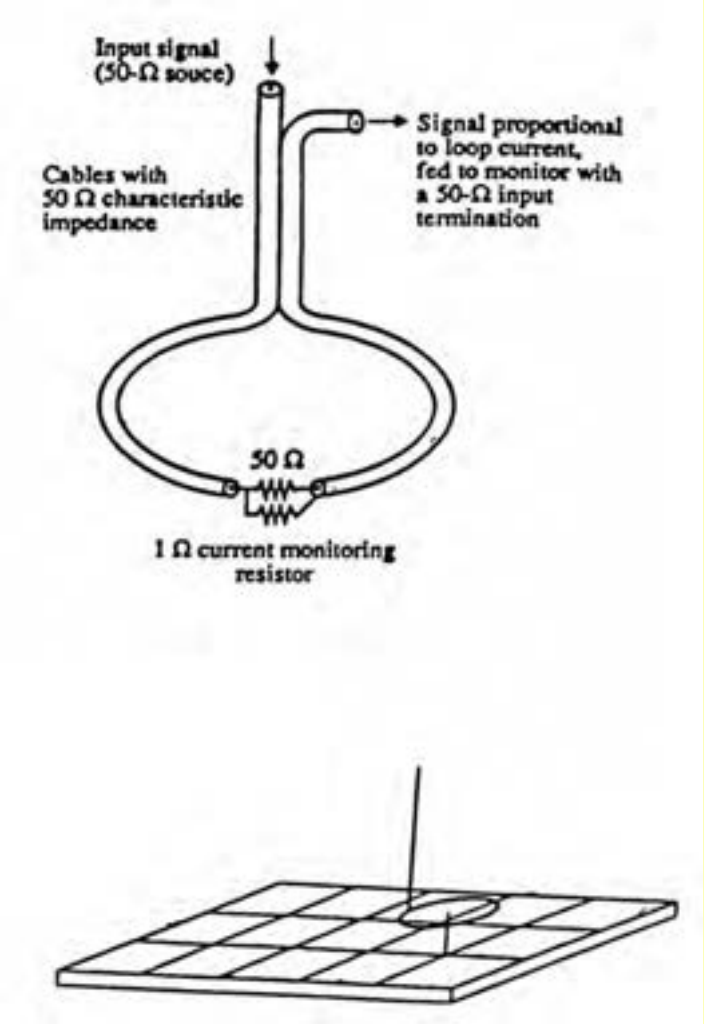
- hide timing variation (e.g. always perform a reduction)
- [Kocher96] : hide parameters (blinding)
- [Dhem98] : method to chain modular multiplication requiring only one reduction, after the last multiplication

ElectroMagnetic Analysis

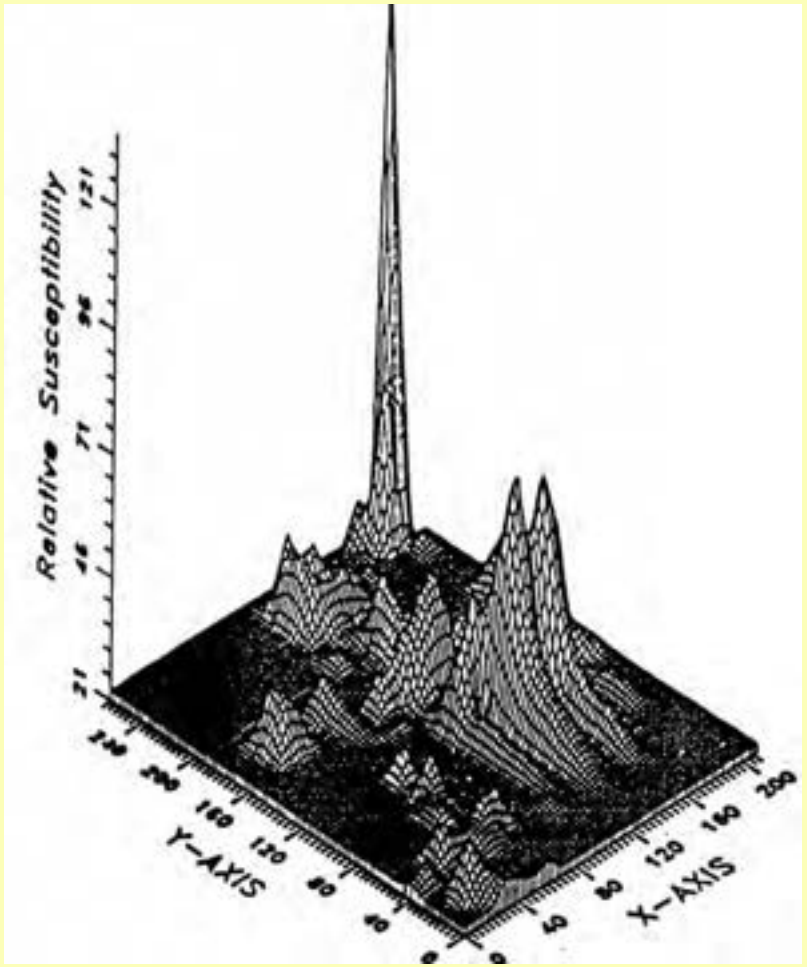
- Power, time and another side-channel : EM
- Use of an antenna for measuring the field from the smart card.



6809 at 66,3 MHz

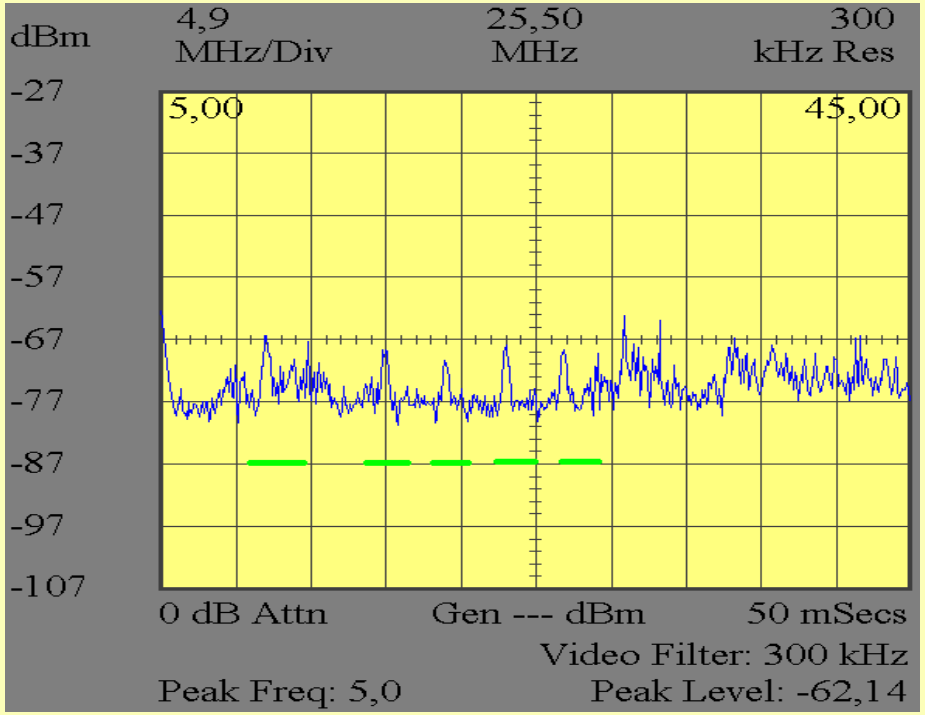


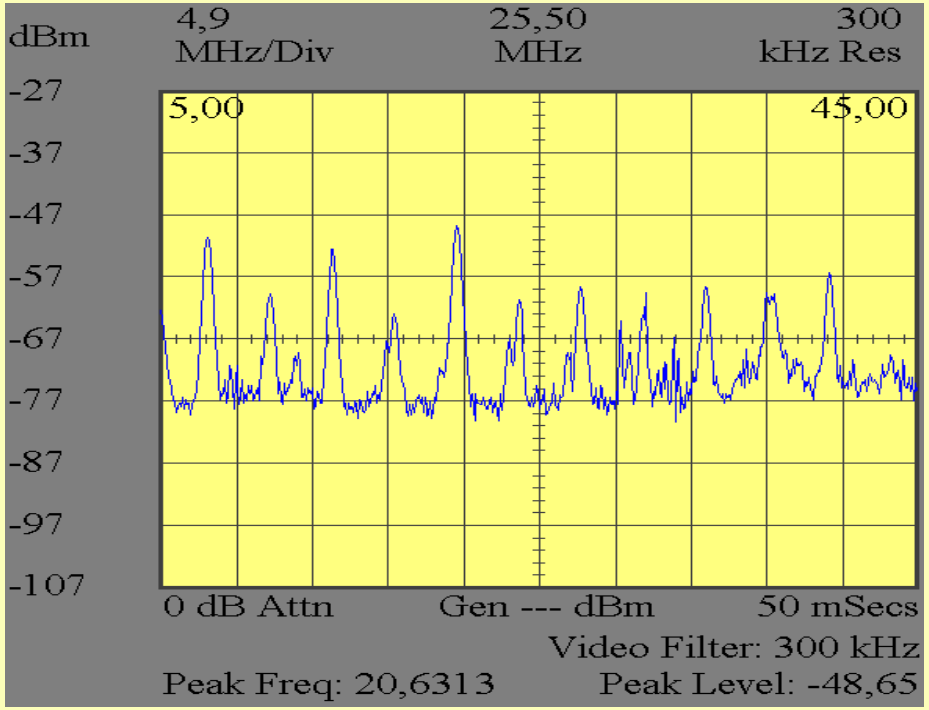
6809 : local measures



Smart card at RESET (EMA)

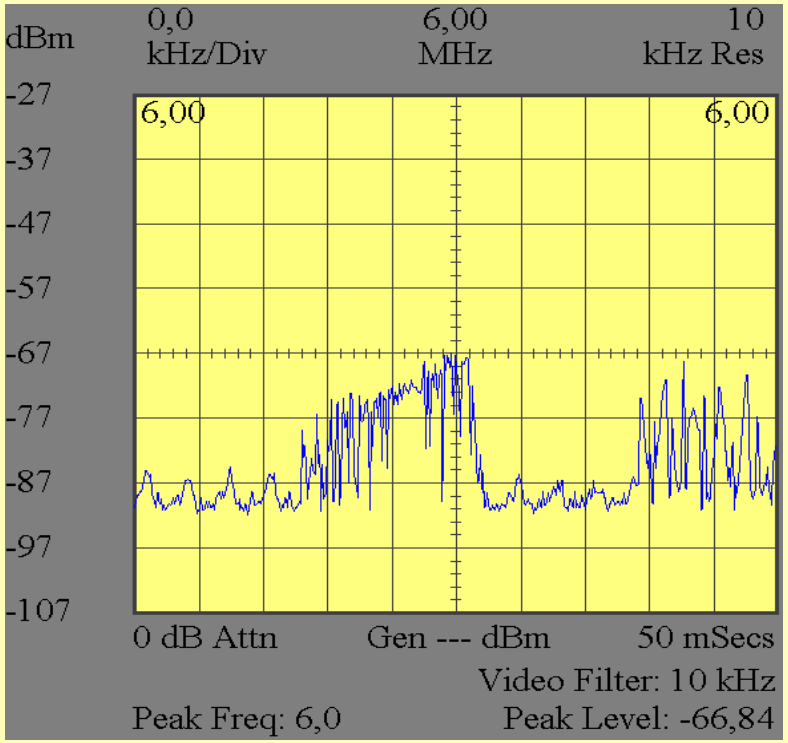
- **EMA from 0 to 70 MHz.**



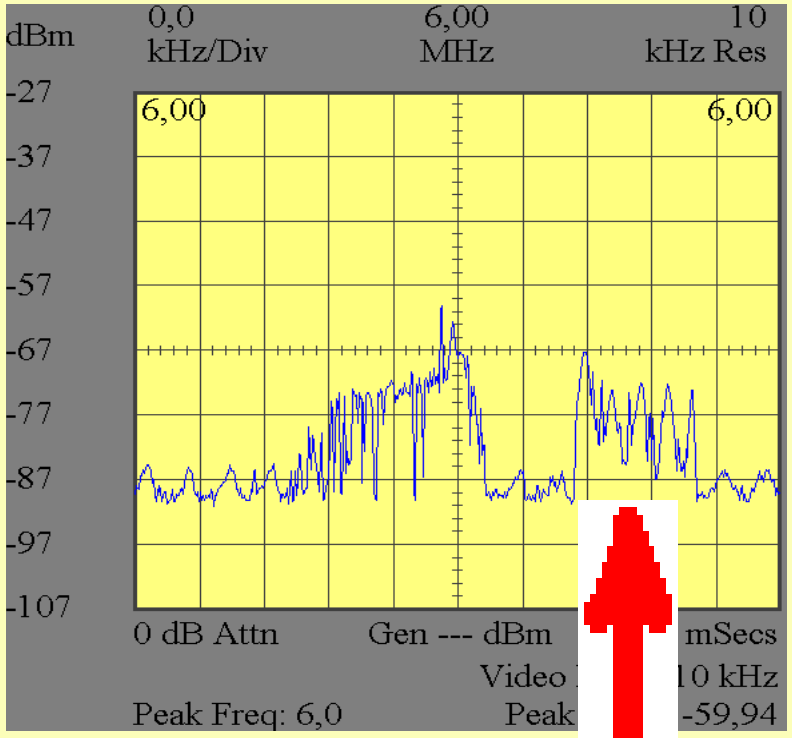


at 6 MHz

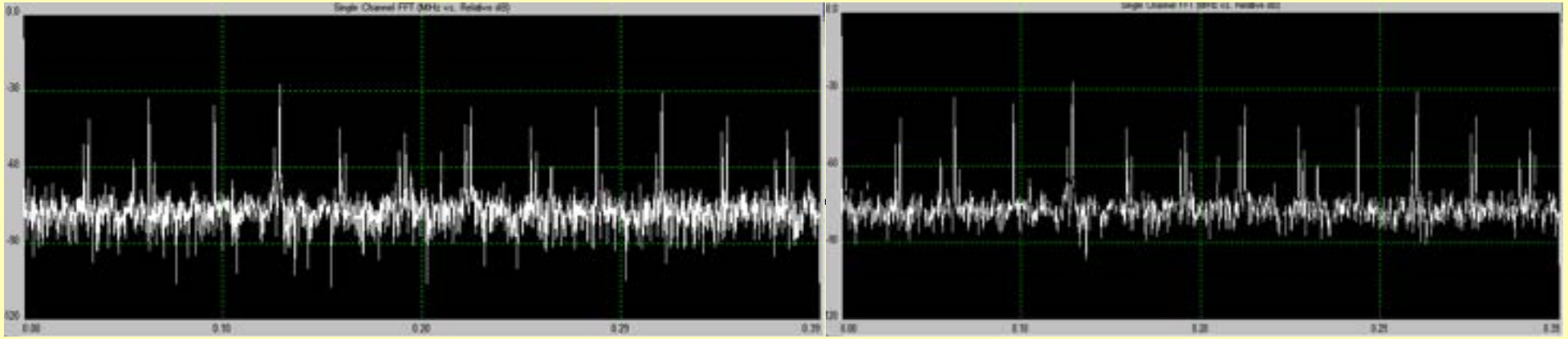
- before DES

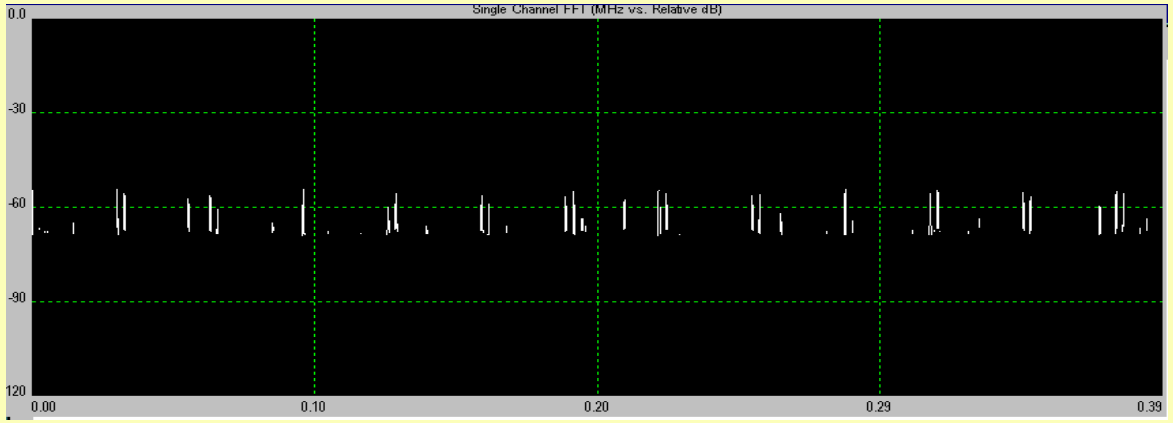


after DES

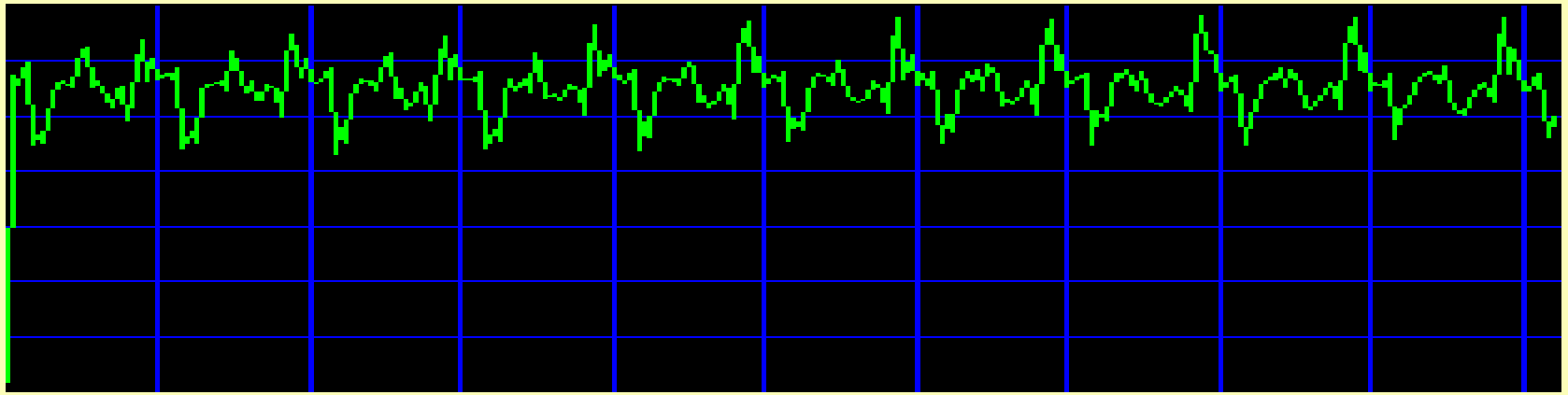


❒ Extracting infos: before and after computations



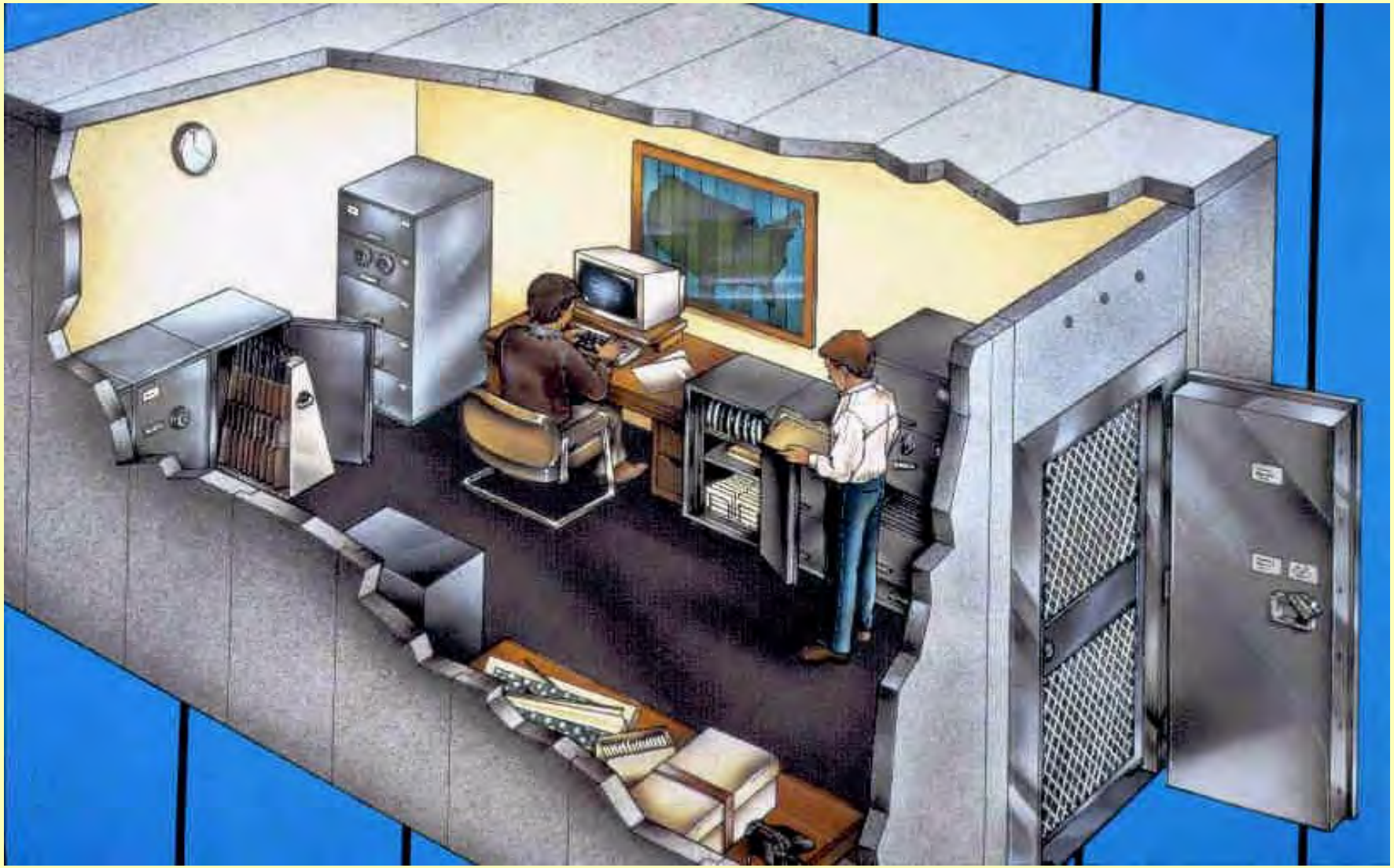


EMA for DES



Solutions?

- New designs of chips (clock, SOI, …)
- New implementations of cryptographic algos
- Faraday cages
- Flexible implementations (software, hardware, never do the same thing!)



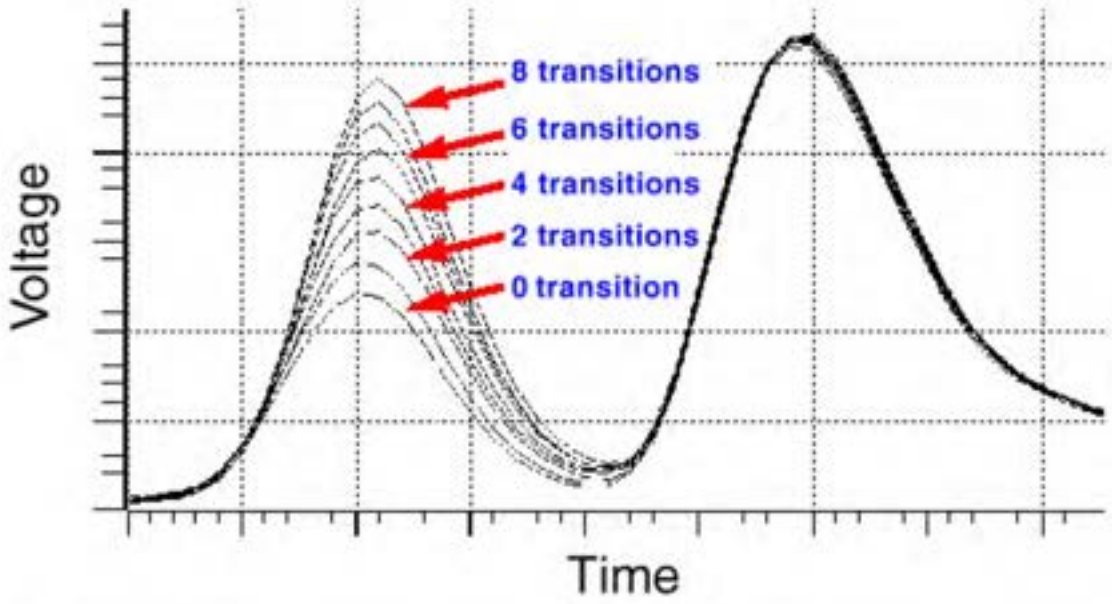
Anecdotes : PIN à distance

- Carte à puce

Attaques actives

Differential Power Analysis

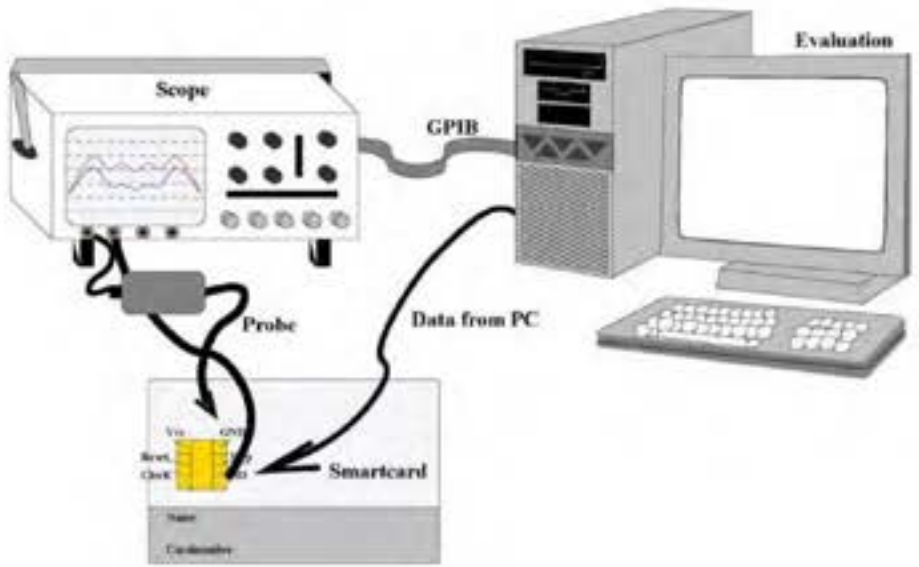
- Data-dependent leakage variations



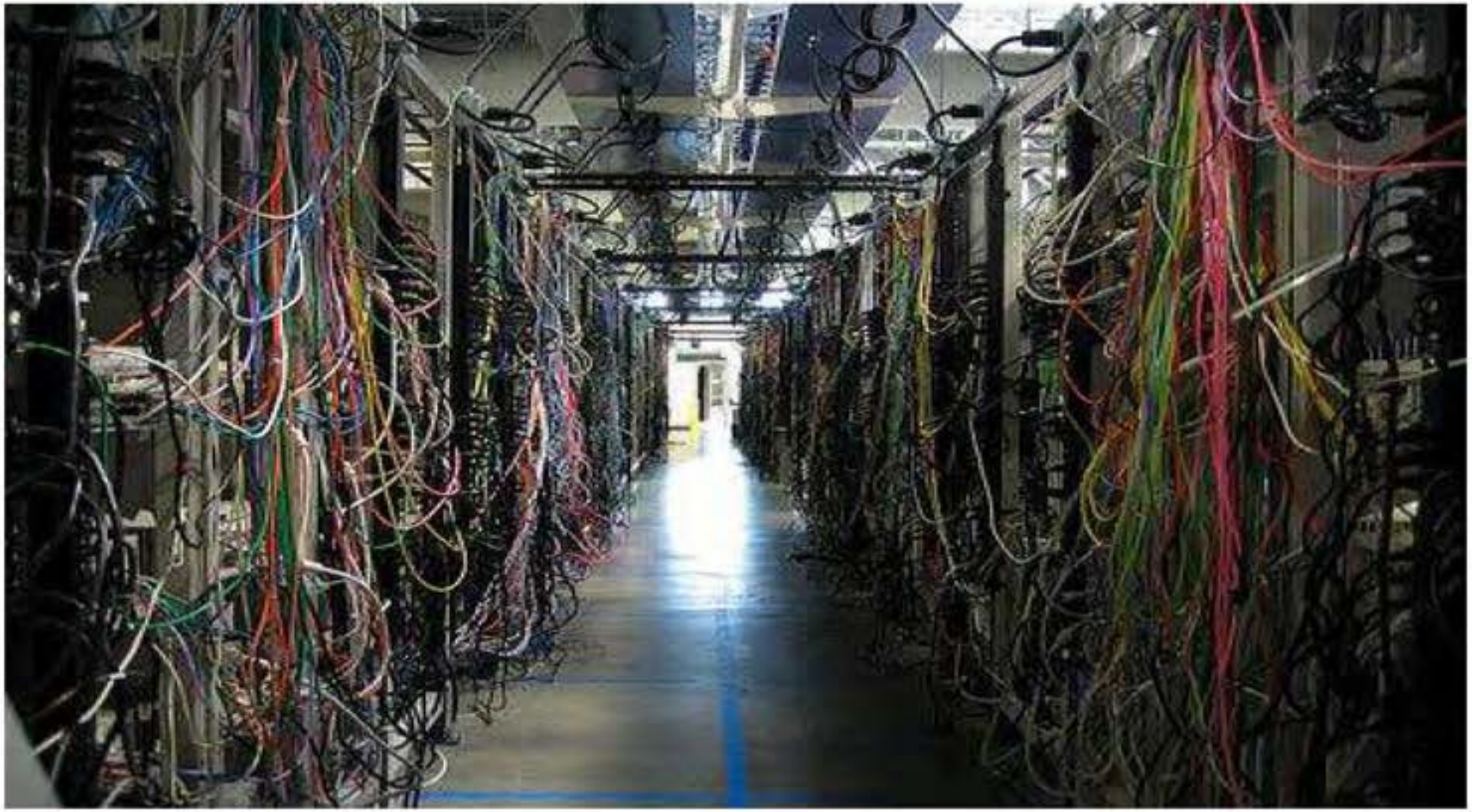
e.g. CMOS => Power consumptions dependent on the number of bit switches

Measurements setups

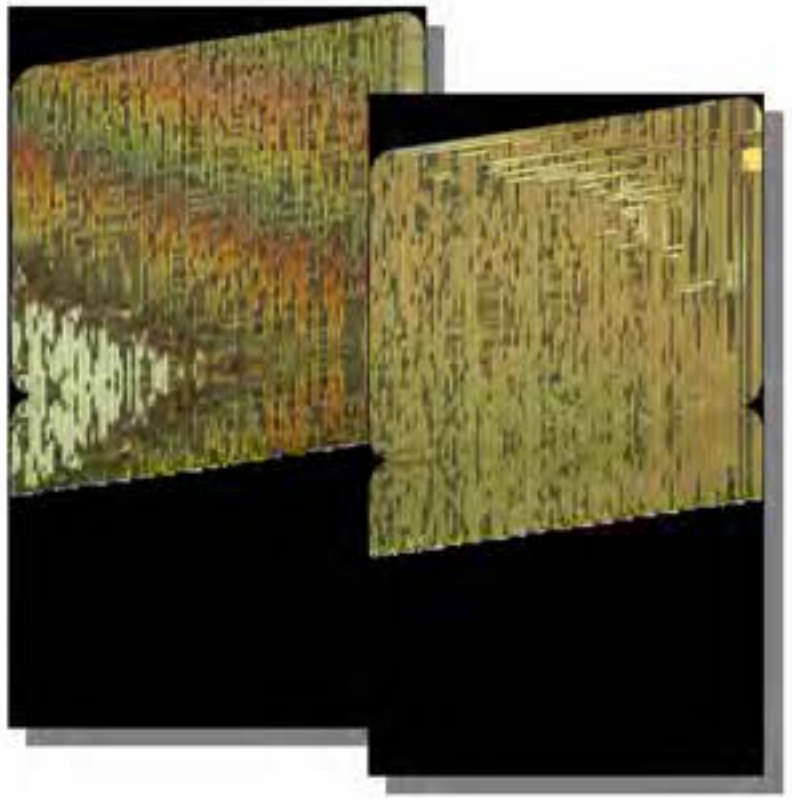
- Target cryptographic device: smart cards, FPGAs, …
- Measurement circuit: small resistor inserted between ground pin and actual ground, small antenna, …
- Acquisition device: 1 Gsample/sec oscilloscope



Spaghetti for digital circuits …



Spaghetti circuits



The Sorcerer's Apprentice Guide to Fault Attacks

HAGAI BAR-EL, HAMID CHOUKRI, DAVID NACCACHE, MICHAEL TUNSTALL, AND CLAIRE WHELAN

Invited Paper

The effect of faults on electronic systems has been studied since the 1970s when it was noticed that radioactive particles caused errors in chips. This led to further research on the effect of charged particles on silicon, motivated by the aerospace industry, which was becoming concerned about the effect of faults in airborne electronic systems. Since then various mechanisms for fault creation and propagation have been discovered and researched. This paper covers the various methods that can be used to induce faults in semiconductors and exploit such errors maliciously. Several examples of attacks stemming from the exploiting of faults are explained. Finally a series of countermeasures to thwart these attacks are described.

Keywords*—*Fault attacks, glitch attacks, side-channel attacks, smart cards.

I. Introduction

One of the first examples of faults being injected into a chip was accidental. It was noticed that radioactive particles produced by elements naturally present in packaging material [1] caused faults in chips. Specifically, uranium-235, uranium-238, and thorium-230 residues present in the packaging decay to lead-206 while releasing α particles. These particles create a charge in sensitive chip areas, causing bits to flip. While these elements were only present in two or three parts per million, this concentration was sufficient to affect chip behavior. Subsequent research included studying and simulating the effects of cosmic rays on semiconductors [2]. Cosmic rays are very weak at ground level due to the earth's atmosphere, but their effect becomes more pronounced in the upper atmosphere and outer space. This problem is further compounded by the fact that the more RAM a computer has, the higher the chance of a fault occurring. This has provoked a great deal of research by organizations such as NASA and Boeing. Most of the work on fault resistance was motivated by this vulnerability to charged particles. Considerable engineering endeavors were devoted to the "hardening" of electronic devices designed to operate in harsh environments. This has mainly been done using simulators to model circuits and study the effect of randomly induced faults. Various fault induction methods have since been discovered but all have in common similar effects on chips. One such example is the use of a laser to imitate the effect of charged particles [3]. The different faults that can be produced have been characterized to enable the design of suitable protections. The first attack that used a fault to derive secret information [4] targeted the RSA public-key cryptosystem. Basically, by introducing a fault into one of the primes, the modulus can be exposed and as a result compromise the RSA system. This led to similar attacks on other cryptographic algorithms. The countermeasures that can be used to thwart fault attacks had already been largely defined and successfully deployed.

This survey is organized as follows. In Section II the various methods of fault injection and their effects are described. We then turn to theoretical (Section III) and practical (Section IV) attacks. Finally, countermeasures are described in Section V.

II. Methods of Fault Injection

The most common fault injection techniques are as follows.

1) *Variations in supply voltage* during execution may cause a processor to misinterpret or skip instructions. This method is widely researched and practiced behind closed doors by the smart-card industry but does not often appear in the open literature.
2) *Variations in the external clock* may cause data misread (the circuit tries to read a value from the data bus before the memory had time to latch out the asked value) or an instruction miss (the circuit starts executing instruction

Manuscript received August 4, 2004; revised December 20, 2004. The work of C. Whelan is supported by the Irish Research Council (IRCSET).

H. Bar-El is with Discretix Technologies Ltd., Ruhovot 76374, Israel (e-mail: hagai.bar-el@discretix.com).

H. Choukri is with IXL Laboratory, Bordeaux 1 University, Talence Cedex F-33405, France (e-mail: h.choukri@voila.fr).

D. Naccache and M. Tunstall are with the Information Security Group, Royal Holloway, University of London, Egham TW20 0EX, U.K. (e-mail: david.naccache@rhul.ac.uk; m.j.tunstall@rhul.co.uk).

C. Whelan is with the School of Computing, Dublin City University, Dublin 9, Ireland (e-mail: cwhelan@computing.dcu.ie).

Digital Object Identifier 10.1109/JPROC.2005.862424

IMA International Conference on Cryptography and Coding

Cryptography and Coding 1997: **Crytography and Coding** pp 155–160 | Cite as

RSA-type signatures in the presence of transient faults

Marc Joye, Jean-Jacques Quisquater, Feng Bao & Robert H. Deng

Conference paper | First Online: 01 January 2005

Part of the Lecture Notes in Computer Science book series (LNCS,volume 1355)

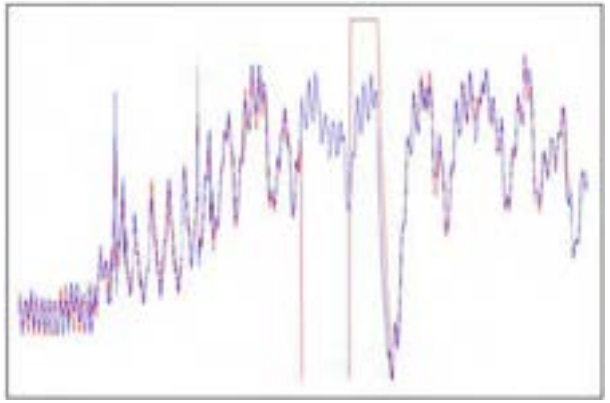
Abstract

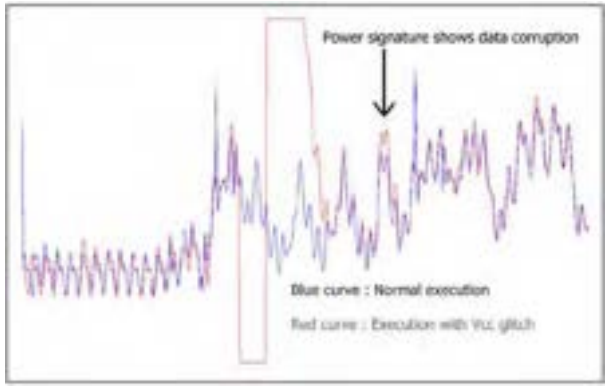
In this paper, we show that the presence of transient faults can leak some secret information. We prove that only one faulty RSA-signature is needed to recover one bit of the secret key. Thereafter, we extend this result to Lucas-based and elliptic curve systems.

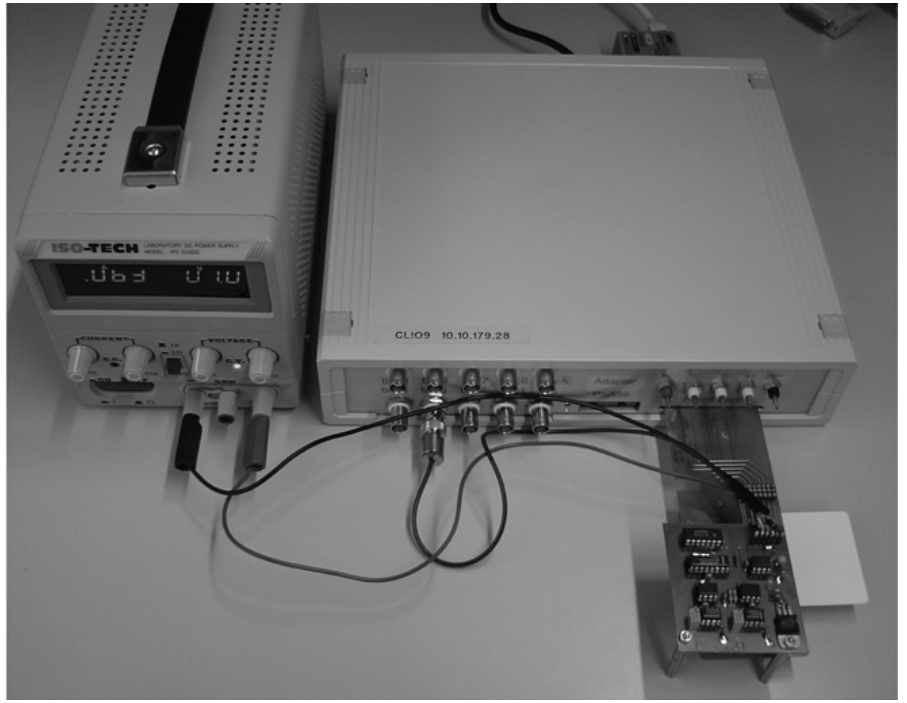
Keywords

RSA **Lucas sequences** **elliptic curves** **transient faults**

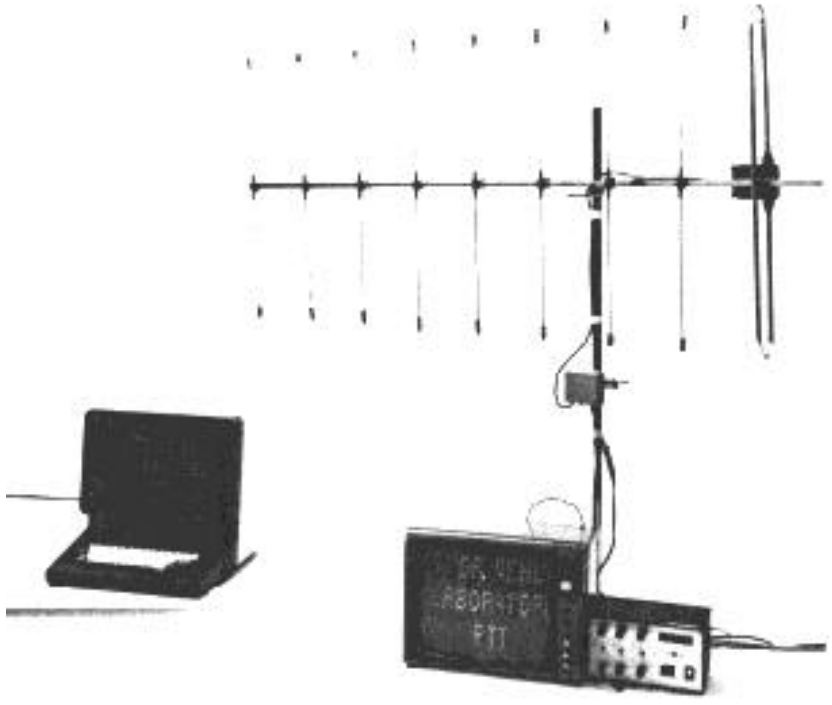
Glitch




Power signature shows data corruption
Blue curve : Normal execution


ISO-TECH
CLIO9 10.10.179.28

Retour dans le passé : 1985 : effet van Eck



Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?

Wim van Eck
PTT Dr. Neher Laboratories, St. Paulusstraat 4, 2264 XZ Leidschendam, The Netherlands

This paper describes the results of research into the possibility of "eavesdropping' on video display units, by picking up and decoding the electromagnetic interference produced by this type of equipment. During the research project, which started in January, 1983, it became more and more clear that this type of information theft can be committed very easily using a normal TV receiver.

Keywords: Electromagnetic radiation, eavesdropping, data security, privacy, Electromagnetic compatibility.

1. Introduction

It is well known that electronic equipment produces electromagnetic fields which may cause interference to radio and television reception. The phenomena underlying this have been thoroughly studied over the past few decades. These studies have resulted in internationally agreed methods for measuring the interference produced by equipment. These are needed because the maximum interference levels which equipment may generate have been laid down by law in most countries.

However, interference is not the only problem caused by electromagnetic radiation. It is possible in some cases to obtain information on the signals used inside the equipment when the radiation is picked up and the received signals are decoded. Especially in the case of digital equipment this possibility constitutes a problem, because remote reconstruction of signals inside the equipment may enable reconstruction of the data the equipment is processing

This problem is not a new one; defence specialists have been aware of it for over twenty years. Information on the way in which this kind of "eavesdropping" can be prevented is not freely available. Equipment designed to protect military information will probably be three or four times more expensive than the equipment likely to be used for processing of non-military information

Un dernier pour la route

https://www.cs.tau.ac.il/~tromer/synesthesia/synesthesia.pdf

Synesthesia: Detecting Screen Content via Remote Acoustic Side Channels*

Daniel Genkin
University of Michigan
genkin@umich.edu

Mihir Pattani
University of Pennsylvania
mihirsa@seas.upenn.edu

Roei Schuster
Tel Aviv University, Cornell Tech
rs864@cornell.edu

Eran Tromer
Tel Aviv University, Columbia University
tromer@cs.tau.ac.il

May 8, 2019 (initial publication September 11, 2018)

Abstract

We show that subtle acoustic noises emanating from within computer screens can be used to detect the content displayed on the screens. This sound can be picked up by ordinary microphones built into webcams or screens, and is inadvertently transmitted to other parties, e.g., during a videoconference call or archived recordings. It can also be recorded by a smartphone or "smart speaker" placed on a desk next to the screen, or from as far as 10 meters away using a parabolic microphone.

Empirically demonstrating various attack scenarios, we show how this channel can be used for real-time detection of on-screen text, or users' input into on-screen virtual keyboards. We also demonstrate how an attacker can analyze the audio received during video call (e.g., on Google Hangout) to infer whether the other side is browsing the web in lieu of watching the video call, and which web site is displayed on their screen.

Fuite acoustique des écrans LCD (alimentation C)