Next Talk: Fault Attacks

➔ on PCs?! ➔

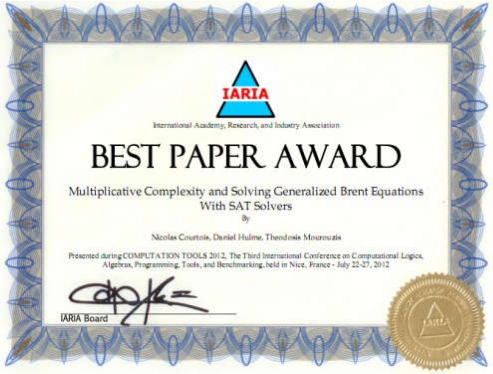
➔ and without root privileges?! ➔

”On Feasibility and Performance of RowHammer Attack”

Nicolas T. Courtois
Varnavas Papaioannou
University College London, UK

Dr. Nicolas T. Courtois blog.bettercrypto.com

1. cryptologist and codebreaker



IARIA

International Academy, Research, and Industry Association

BEST PAPER AWARD

Multiplicative Complexity and Solving Generalized Brent Equations With SAT Solvers

By

Nicolas Courtois, Daniel Hulme, Theodosis Mourouzis

Presented during COMPUTATION TOOLS 2012, The Third International Conference on Computational Logics, Algebras, Programming, Tools, and Benchmarking, held in Nice, France - July 22-27, 2012

IARIA Board

NewScientist

The global science and technology weekly | 7 June 2003

NEW! US JOBS SECTION

MEGAWATER

The biggest engineering folly of all time?

JOHN BARROW

How our world could be just a computer simulation

CIPHER CRISIS

UNIVERSITY CIPHER CHAMPION

March 2013

Cyber Security Challenge UK

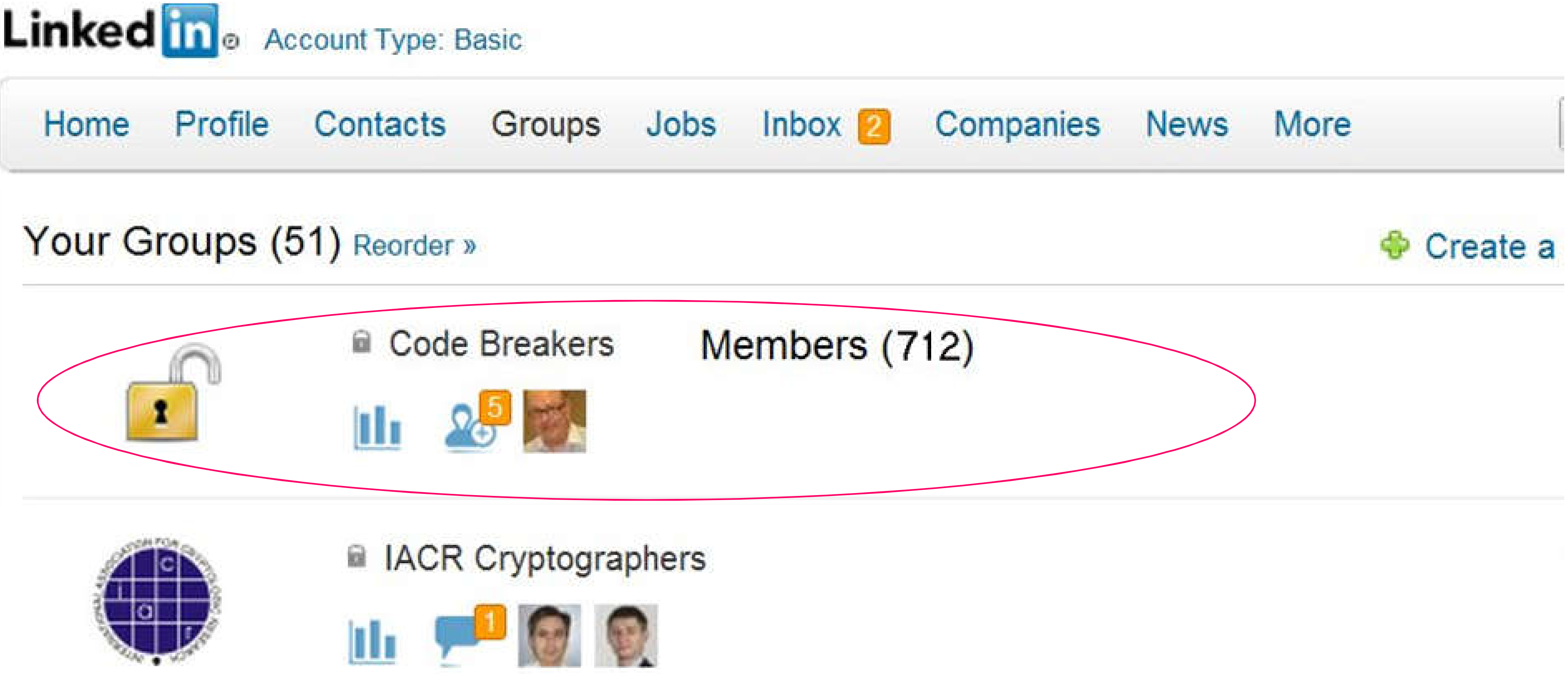
2. payment and smart cards (e.g. bank cards, Oyster cards etc…)

Oyster cracker vows to clone cards

Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

LinkedIn



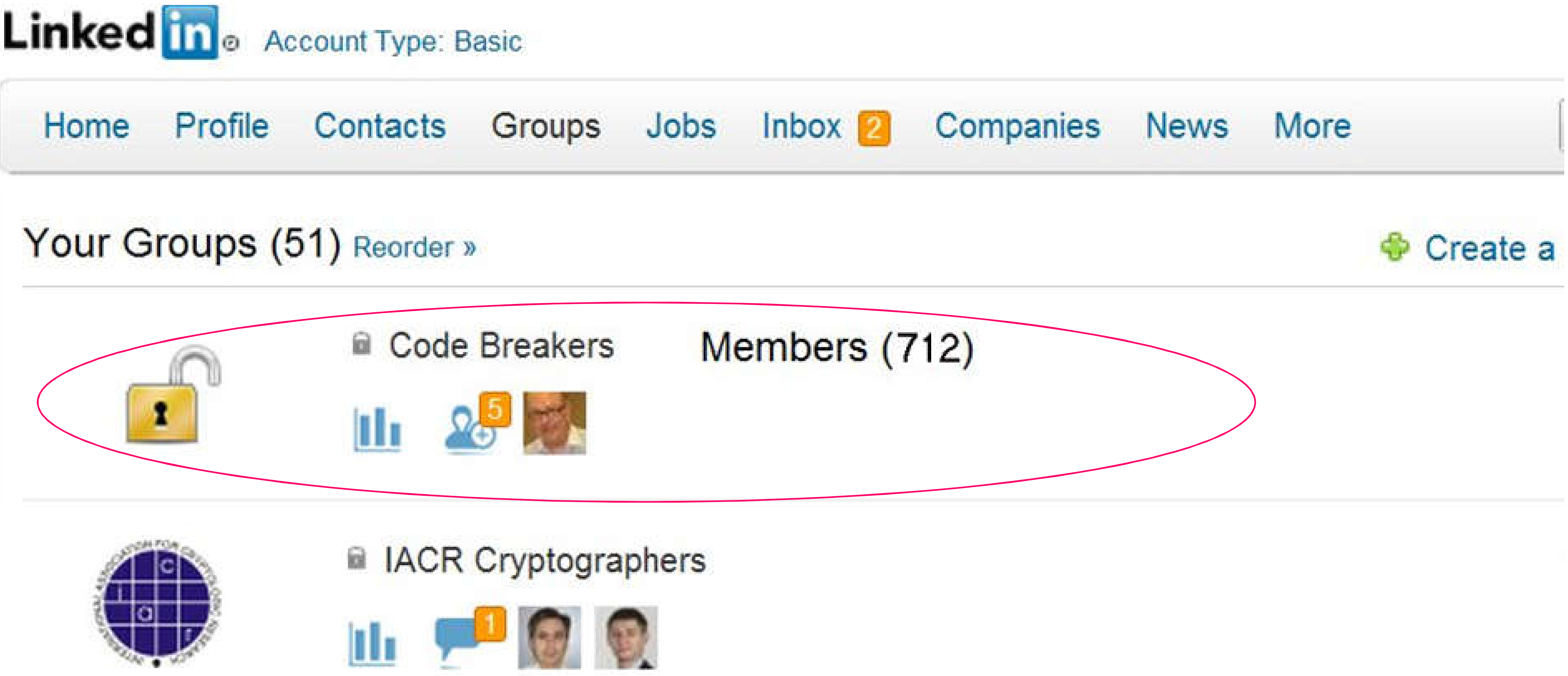
Account Type: Basic

Your Groups (51) Reorder »

Code Breakers Members (712)

IACR Cryptographers

LinkedIn



Account Type: Basic

Your Groups (51)

Code Breakers Members (712)

IACR Cryptographers

This Talk:

- Fault Attacks on PCs

This Talk:

- Fault Attacks on PCs
  - – [NEW: high performance, avoid root privileges]

boring? technical?

This Talk:

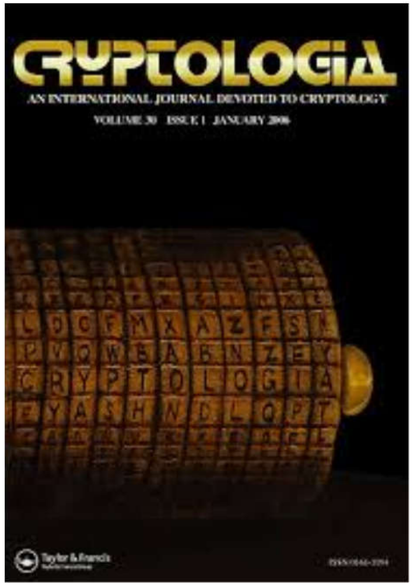
- Earlier historical context: smart cards
- Fault Attacks on PCs

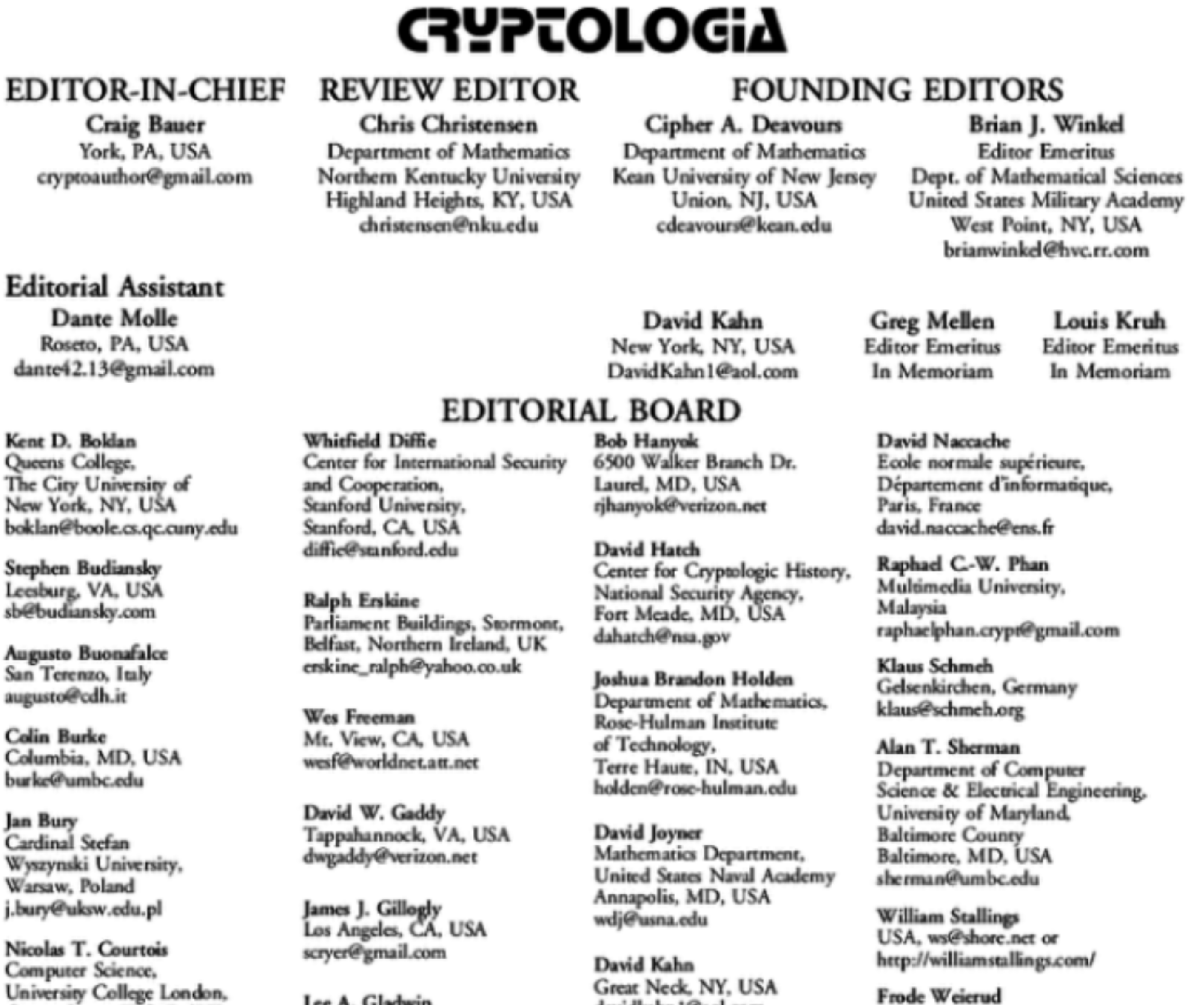
This Talk:

- Even Earlier: Cold War crypto, DC history etc.
- Earlier historical context: smart cards
- Fault Attacks on PCs

secure against fault attacks!

Crypto History


CRYPTOLOGIA
AN INTERNATIONAL JOURNAL DEVOTED TO CRYPTOLOGY
VOLUME 30 ISSUE 1 JANUARY 2006
Taylor & Francis



CRYPTOLOGIA

EDITOR-IN-CHIEF

Craig Bauer
York, PA, USA
cryptoauthor@gmail.com

REVIEW EDITOR

Chris Christensen
Department of Mathematics
Northern Kentucky University
Highland Heights, KY, USA
christensen@nku.edu

FOUNDING EDITORS

Cipher A. Deavours
Department of Mathematics
Kean University of New Jersey
Union, NJ, USA
cdeavours@kean.edu

Brian J. Winkel
Editor Emeritus
Dept. of Mathematical Sciences
United States Military Academy
West Point, NY, USA
brianwinkel@hvc.rr.com

David Kahn
New York, NY, USA
DavidKahn1@aol.com

Greg Mellen
Editor Emeritus
In Memoriam

Louis Kruh
Editor Emeritus
In Memoriam

Editorial Assistant

Dante Molle
Roseto, PA, USA
dante42.13@gmail.com

EDITORIAL BOARD

Kent D. Boklan
Queens College,
The City University of
New York, NY, USA
boklan@boole.cs.qc.cuny.edu

Stephen Budiansky
Leesburg, VA, USA
sb@budiansky.com

Augusto Buonafalce
San Terenzo, Italy
augusto@cdh.it

Colin Burke
Columbia, MD, USA
burke@umbc.edu

Jan Bury
Cardinal Stefan
Wyszynski University,
Warsaw, Poland
j.bury@uksw.edu.pl

Nicolas T. Courtois
Computer Science,
University College London,

Whitfield Diffie
Center for International Security
and Cooperation,
Stanford University,
Stanford, CA, USA
diffie@stanford.edu

Ralph Erskine
Parliament Buildings, Stormont,
Belfast, Northern Ireland, UK
erskine_ralph@yahoo.co.uk

Wes Freeman
Mt. View, CA, USA
wesf@worldnet.att.net

David W. Gaddy
Tappahannock, VA, USA
dwgaddy@verizon.net

James J. Gillogly
Los Angeles, CA, USA
scryer@gmail.com

Lee A. Gladwin

Bob Hanyok
6500 Walker Branch Dr.
Laurel, MD, USA
rjhanyok@verizon.net

David Hatch
Center for Cryptologic History,
National Security Agency,
Fort Meade, MD, USA
dahatch@nsa.gov

Joshua Brandon Holden
Department of Mathematics,
Rose-Hulman Institute
of Technology,
Terre Haute, IN, USA
holden@rose-hulman.edu

David Joyner
Mathematics Department,
United States Naval Academy
Annapolis, MD, USA
wdj@usna.edu

David Kahn
Great Neck, NY, USA

David Naccache
Ecole normale supérieure,
Département d'informatique,
Paris, France
david.naccache@ens.fr

Raphael C.-W. Phan
Multimedia University,
Malaysia
raphaelphan.crypt@gmail.com

Klaus Schmeh
Gelsenkirchen, Germany
klaus@schmeh.org

Alan T. Sherman
Department of Computer
Science & Electrical Engineering,
University of Maryland,
Baltimore County
Baltimore, MD, USA
sherman@umbc.edu

William Stallings
USA, ws@shore.net or
http://williamstallings.com/

Frode Weierud

[Crypto] Fault Attacks [in Cybersecurity]

- Powerful
- Difficult to make [technical difficulty + countermeasures + good security engineering]

Defense in Depth!

Computer systems have multiple layers, e.g.

- HW components
- Chipset/MB
- Kernel Ring 0
- OS
- UAC
- HTTP sandboxing
- Java script

Defense in Depth

Computer systems have multiple layers, e.g.

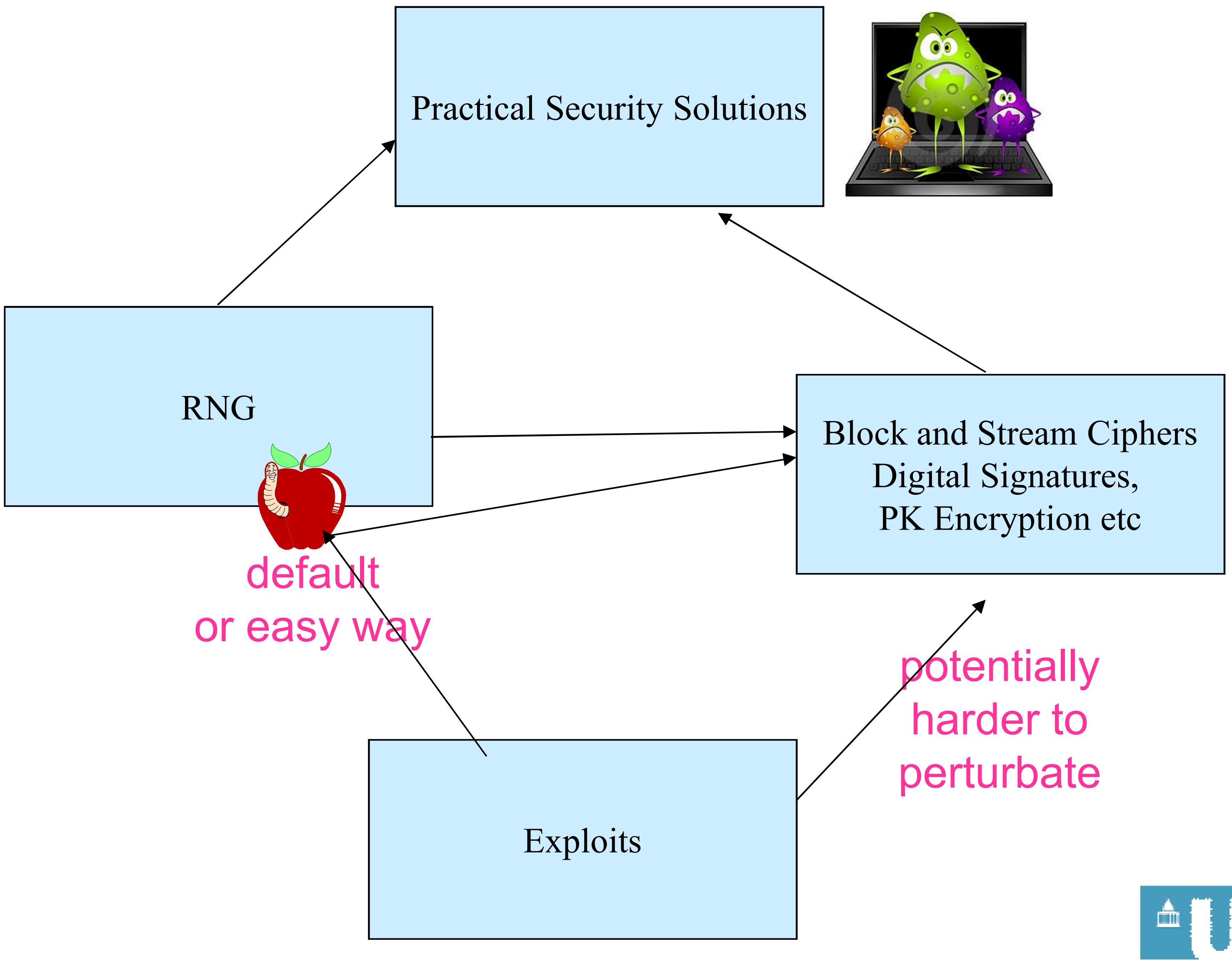
- HW components
- Chipset/MB
- Kernel Ring 0
- OS
- UAC
- HTTP sandboxing
- Java script

Powerful!

Who Wins?

Attackers or Defenders?

Fault Attacks in Cybersecurity



Practical Security Solutions

RNG

Block and Stream Ciphers
Digital Signatures,
PK Encryption etc

default
or easy way

potentially
harder to
perturbate

Exploits

DFA =

(Differential Fault Analysis)

DFA Attacks…

(Differential Fault Analysis)

1. Provoke faults in the device,
2. Deduce the key by detailed mathematical analysis.

DFA Requirements

One needs to be able to run the same crypto algorithm many times with the same inputs.

The inputs do NOT need to be known.

- they usually are, but today we will realistic example when they aren't (!) and yet the key is found.

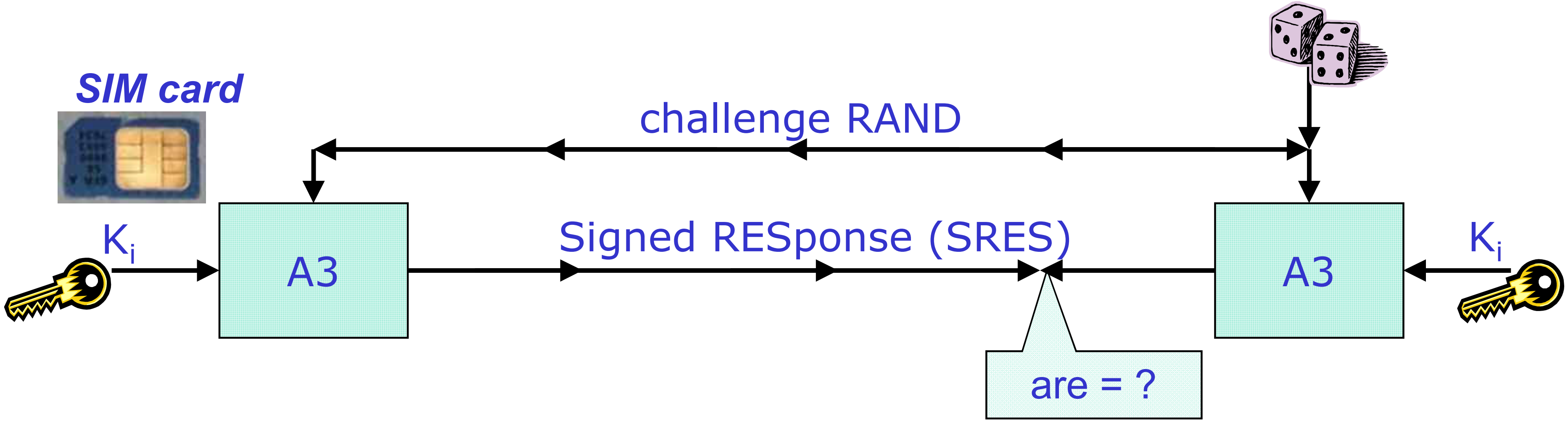
DFA requires

⇒ a DETERMINISTIC crypto process with a known output

(from which the attacker wants to extract the secret key)

Examples when this happens:

GSM SIM card Authentication



- RUN GSM ALGORITHM

Example: A0 88 00 00 10 XX ……………..XX

CLA

INS

both 0

16 bytes random nonce

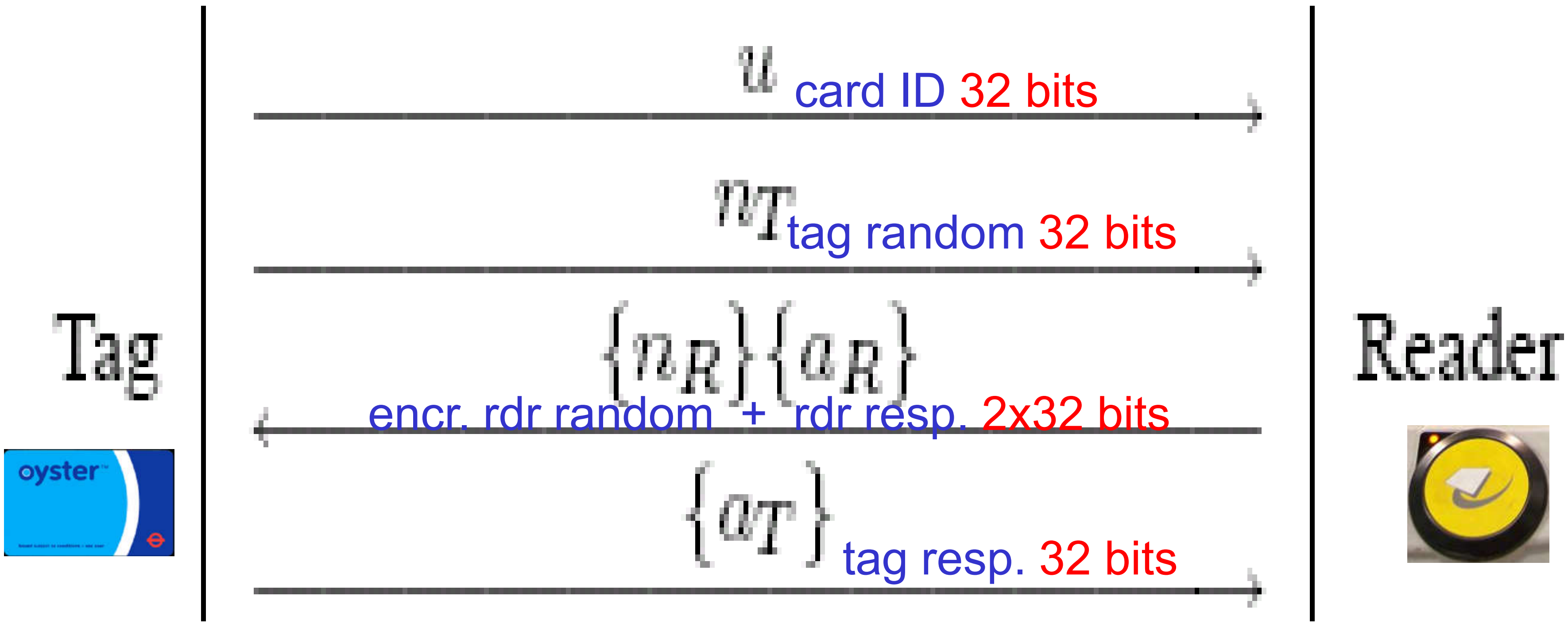
no L_e, no data in reply expected, result will be visible in the status bytes = 0x9F Le

In Contrast – 3G USIM Cards

No DFA attack, 2 reasons:

- the base station is authenticated first!
- the SQN should be checked for freshness.
  - so the card should never accept to do the same crypto computation twice

In Contrast – MiFare Classic



Tag

Reader

u card ID 32 bits

n_T tag random 32 bits

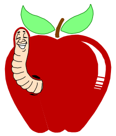
$\{n_R\}\{a_R\}$ encr. rdr random + rdr resp. 2x32 bits

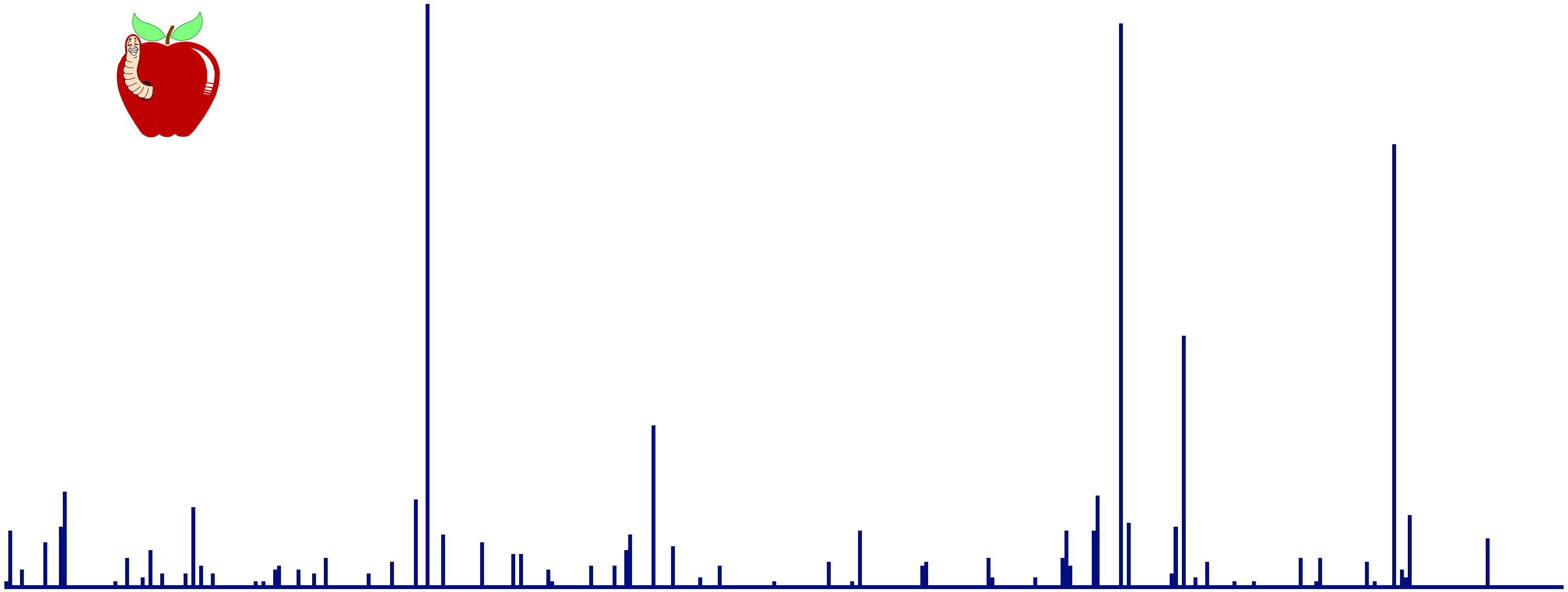
$\{a_T\}$ tag resp. 32 bits

The reader is authenticated first !

No DFA attack unless card random repeats

Example: London Oyster Card From 2006

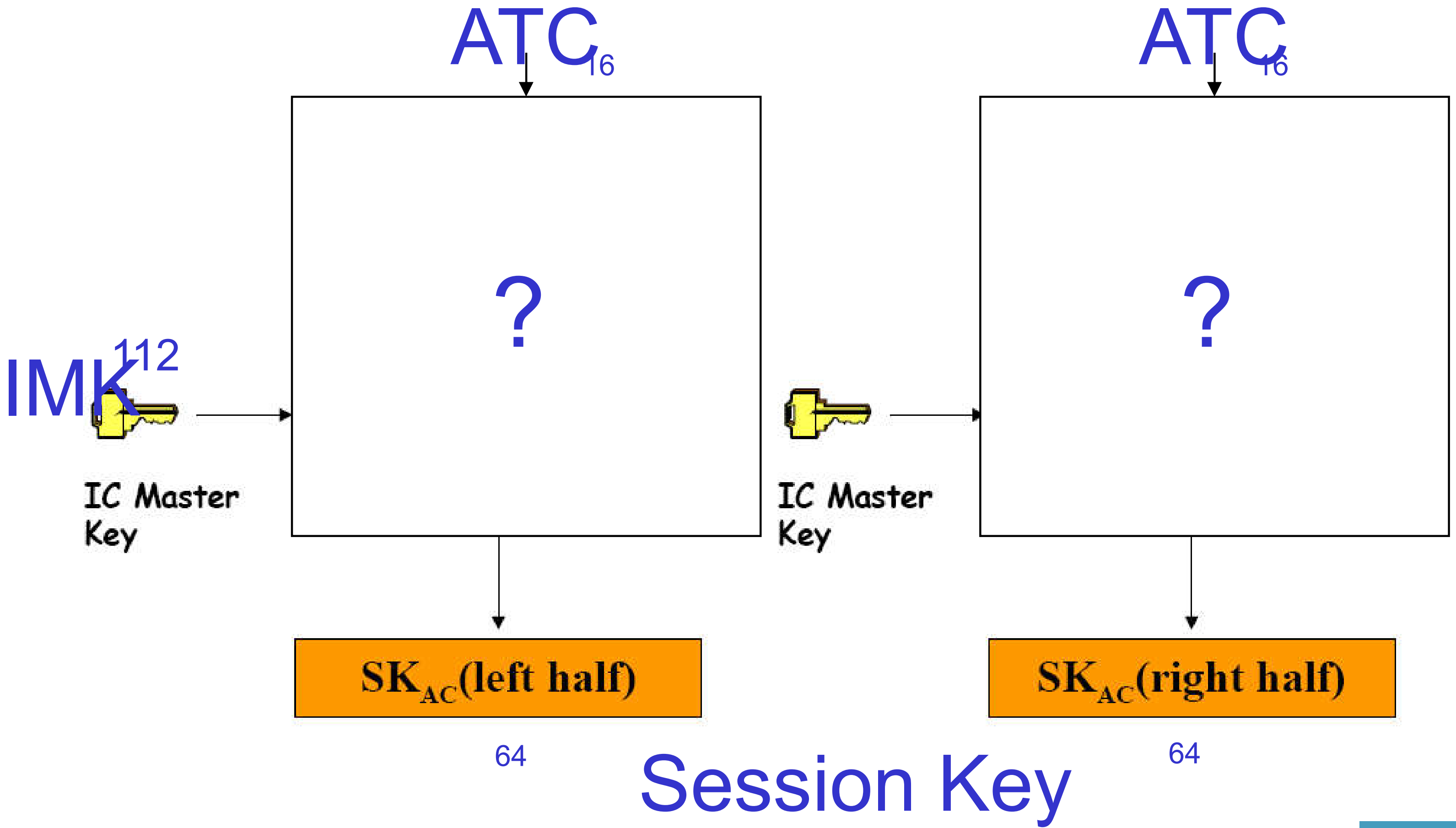




- Min-entropy = 2.8 bits.
- Courtois Dark Side Attack time $2^{2.8}$ x 10 s = 3 minutes per key extracted from the card [theoretical speed].

In Contrast – Bank Cards

Assuming ATC is always incremented => Session Key depends on ATC => Impossible to get the same cryptogram twice => DFA is impossible!



Conjecture/Claim: [Courtois@eSmart 2010]

Fault attacks are feasible in practice

only when

the industry uses

BAD PROTOCOLS ?

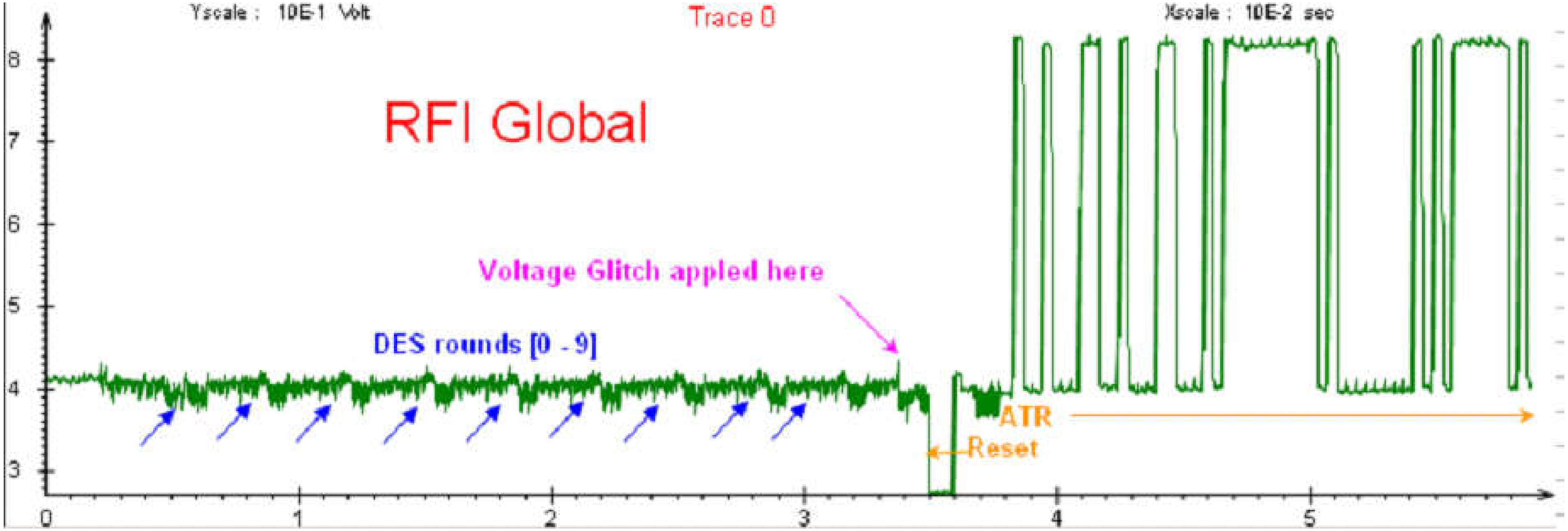
commercial security=>bad security?

Fault Attacks in Practice on [Unnamed] Smart Cards

[Courtois Jackson Ware,
eSmart conference, France, 2010]

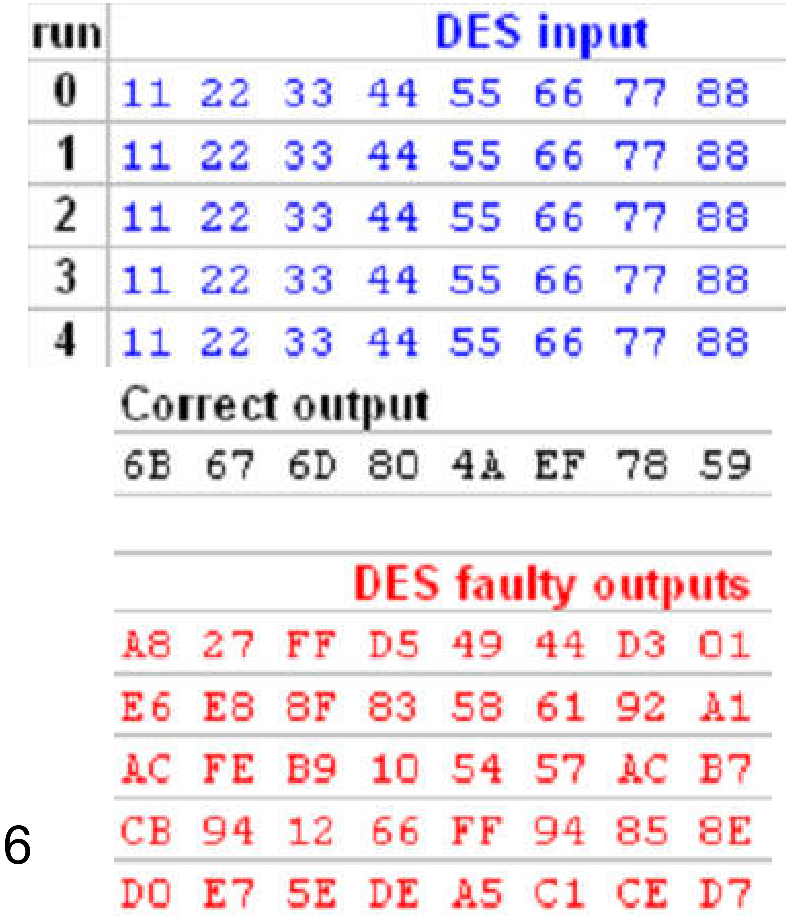
Lab Work

- Voltage glitch applied close to the final round.
- Triggers ATR - defensive behaviour, attack detected.



Glitches in 8th Round

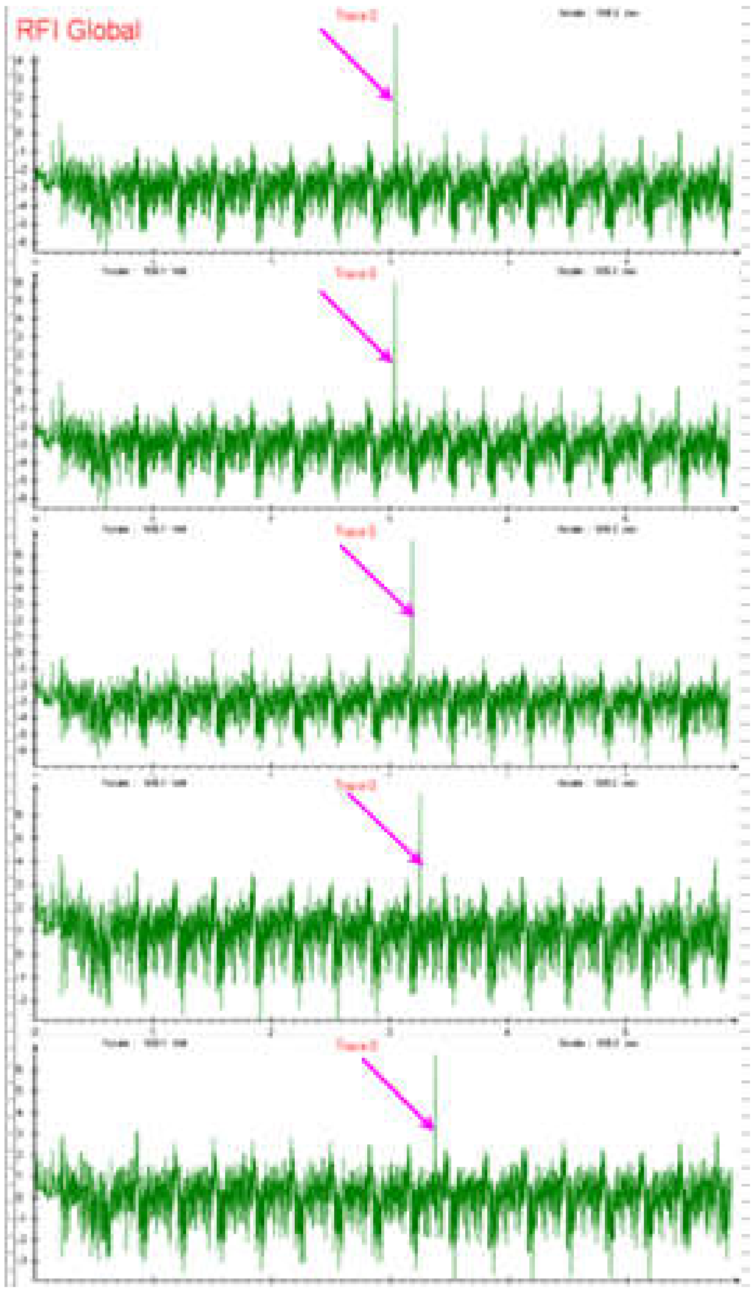
Done 5 consecutive faults
with precise timing
and consistent perturbation type:



run	DES input
0	11 22 33 44 55 66 77 88
1	11 22 33 44 55 66 77 88
2	11 22 33 44 55 66 77 88
3	11 22 33 44 55 66 77 88
4	11 22 33 44 55 66 77 88

Correct output
6B 67 6D 80 4A EF 78 59

DES faulty outputs
A8 27 FF D5 49 44 D3 01
E6 E8 8F 83 58 61 92 A1
AC FE B9 10 54 57 AC B7
CB 94 12 66 FF 94 85 8E
D0 E7 5E DE A5 C1 CE D7

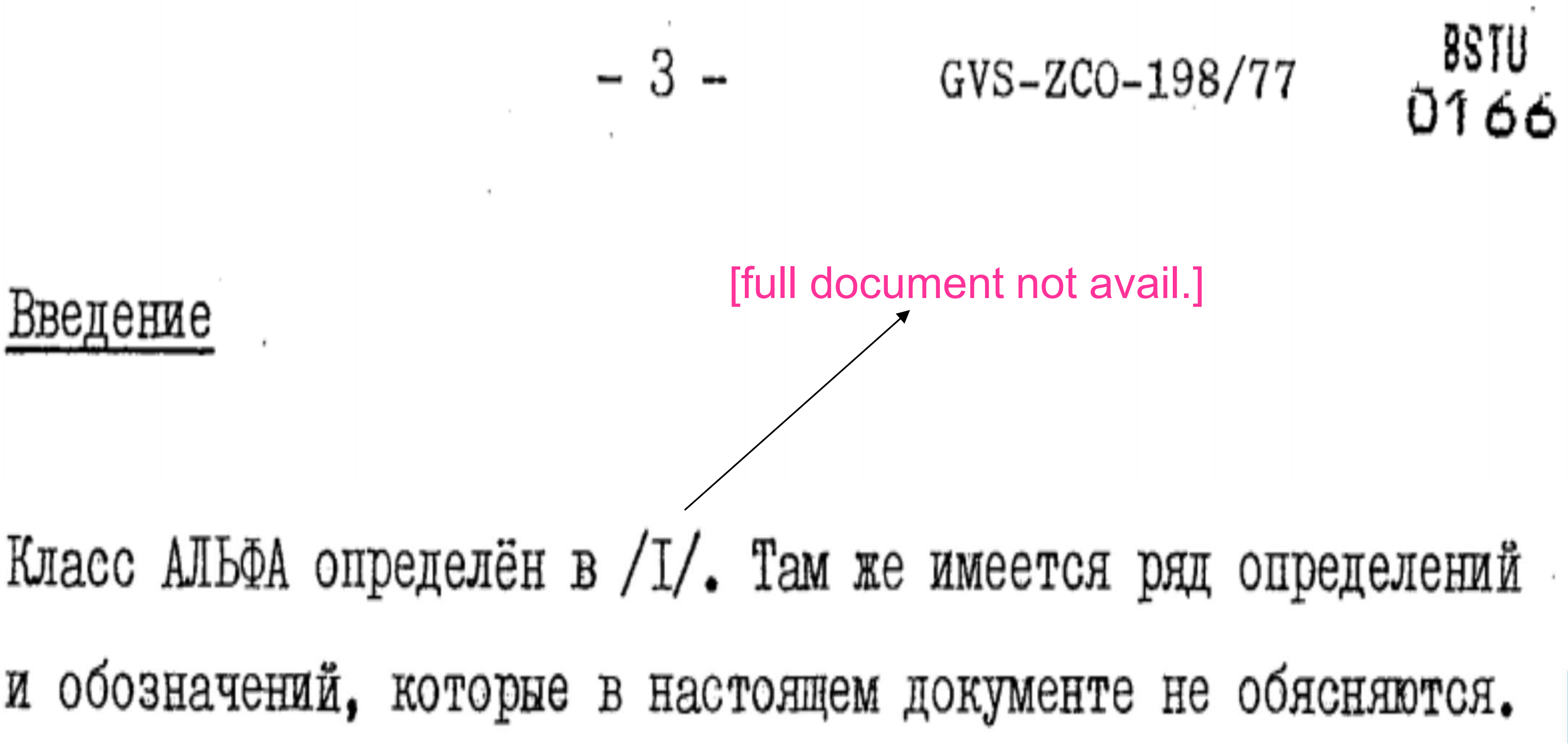


Cold War

Differential Cryptanalysis and Fault Attacks

Eastern German Block Cipher Class Alpha = c.1970

obscure origins…



- 3 -

GVS-ZCO-198/77

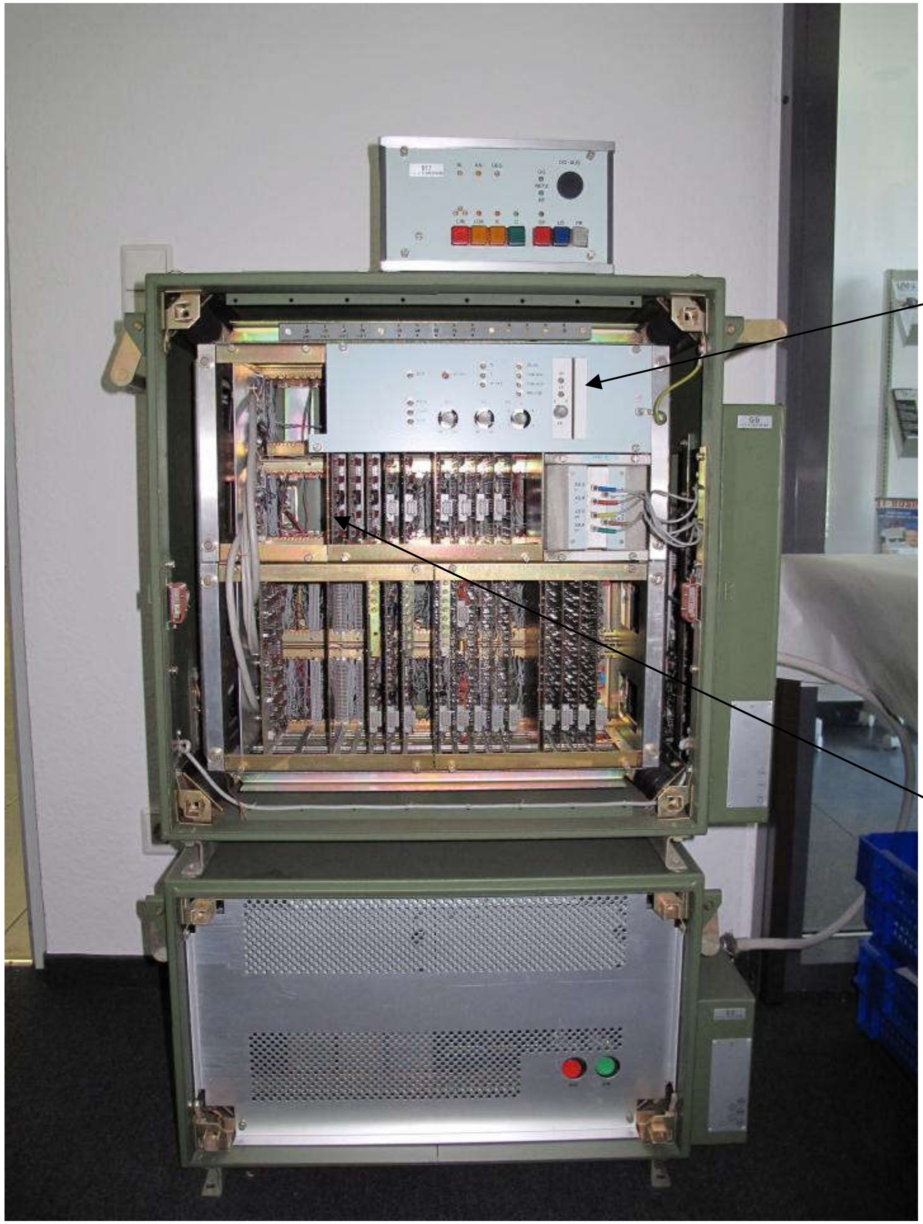
BSTU
01 66

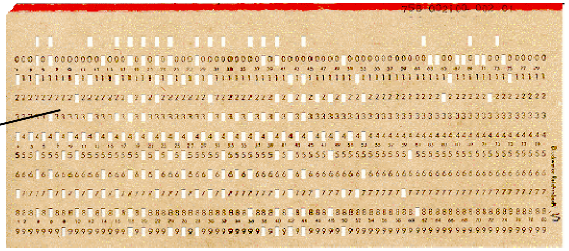
Введение

[full document not avail.]

Класс АЛЬФА определён в /I/. Там же имеется ряд определений и обозначений, которые в настоящем документе не обясняются.

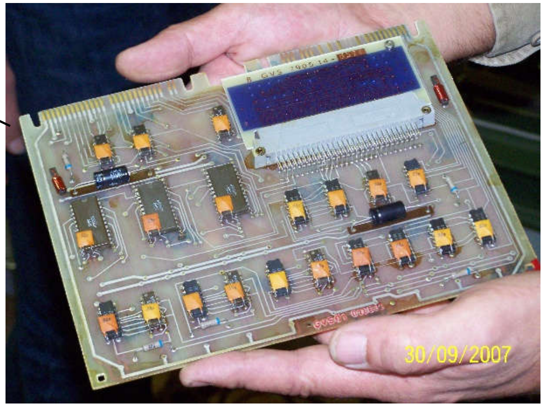
East German SKS V/1 and T-310





240 bits

“quasi-absolute security”
[1973-1990]



long-term secret
90 bits only!

T-310 is SECURE against Fault Attacks

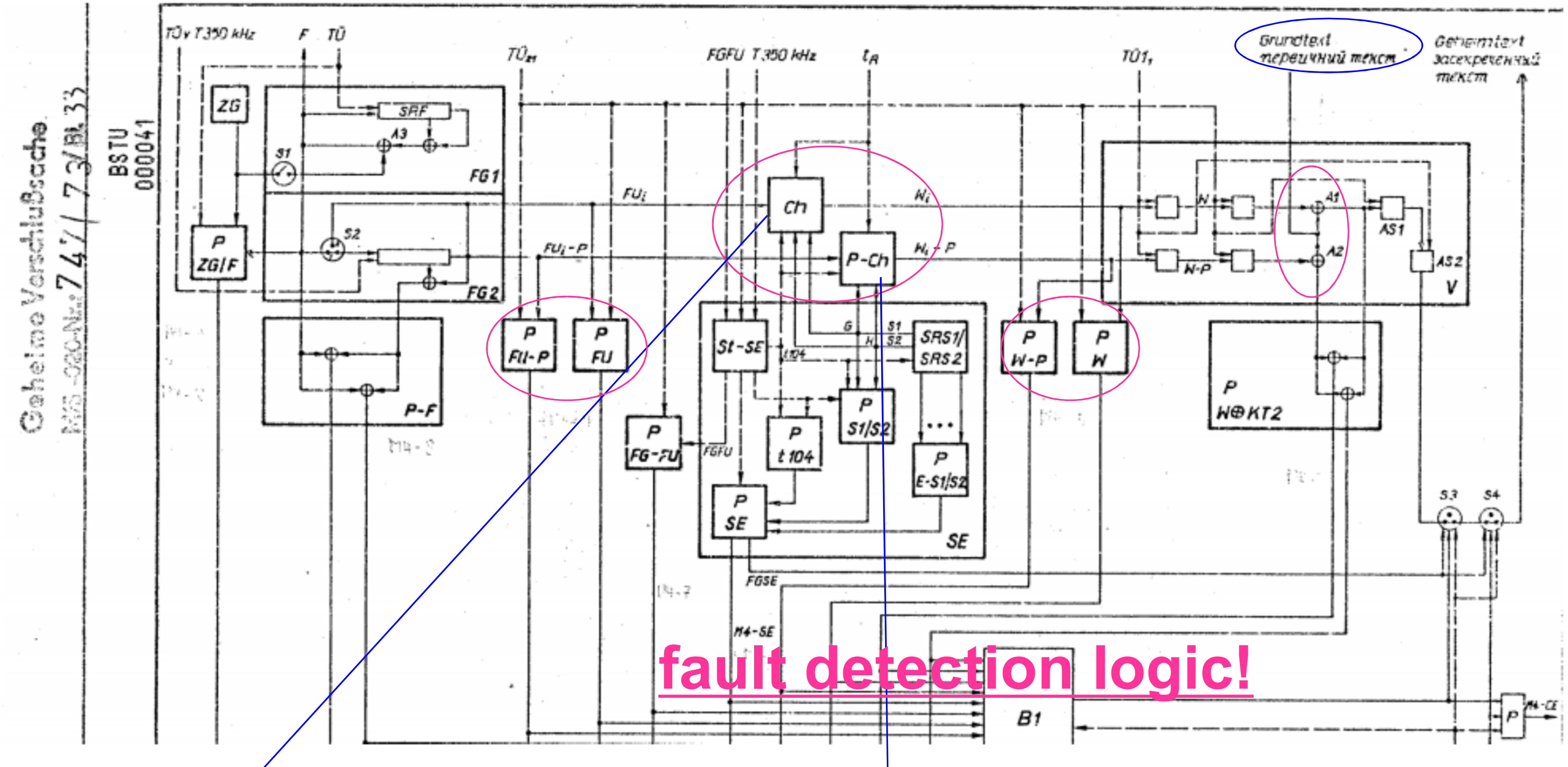
On two accounts:

⇒ has a physical RNG=>IV =>cannot do encryption twice

⇒ everything is DUPLICATED

Security Against Fault Attacks:

=> obligatory in Eastern Bloc Cryptography in 1973!



fault detection logic!

w_i CH - Zwischenwurmreihe mit den Elementen $w_{i,k}^{CH}$.

w_i PCH - Prüfzwischenwurmreihe mit den Elementen $w_{i,k}^{PCH}$ (k=1bis104) (Fg Überwachung).

Differential Cryptanalysis = DC

Wikipedia DC entry says:

In 1994 […] IBM [...] Coppersmith published a paper stating that DC was known to IBM as early as 1974.

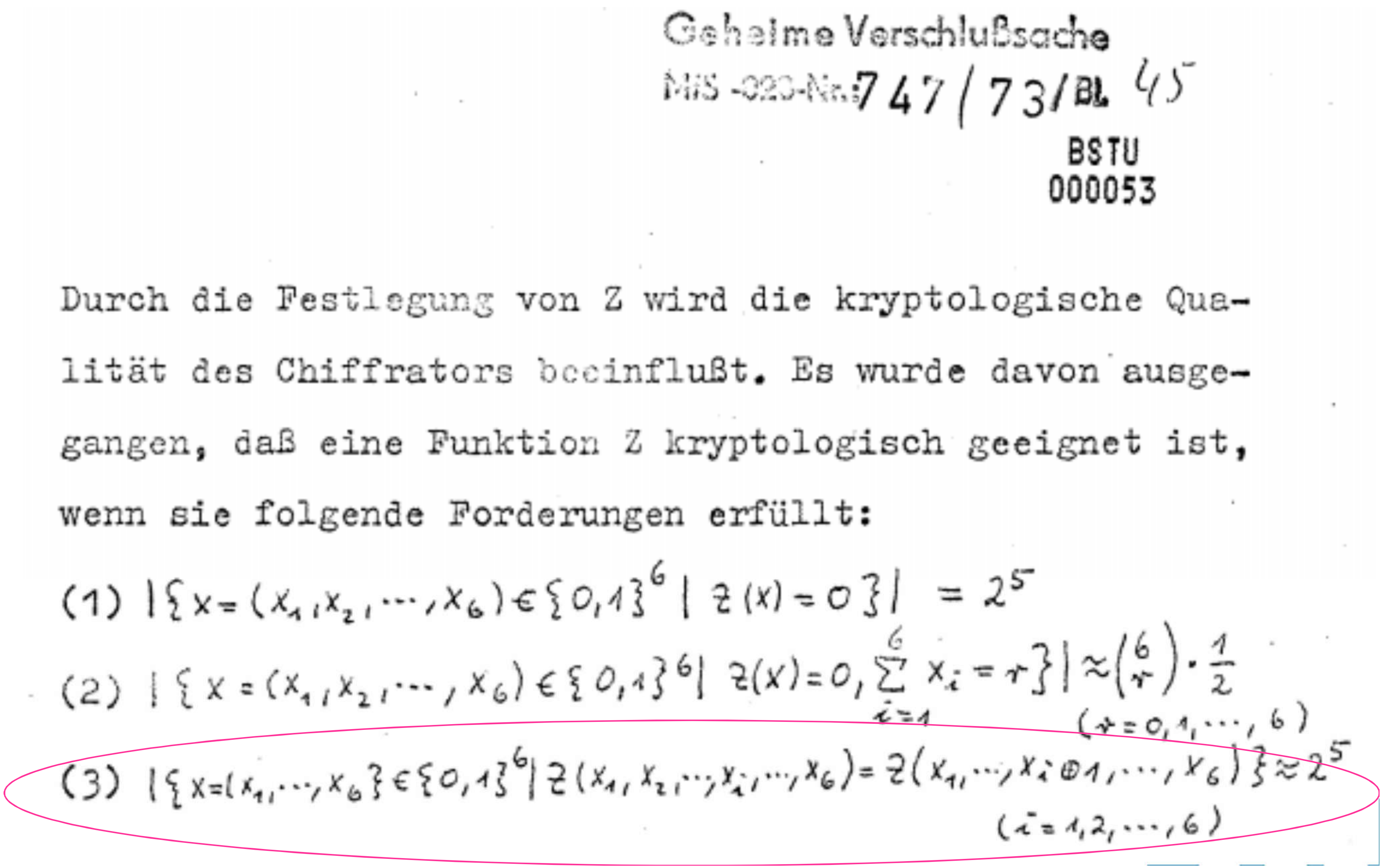
Coppersmith explains: "After discussions with NSA…

it was decided that disclosure of the design considerations would reveal the technique of DC,
a powerful technique […]
would weaken the competitive advantage
the U. S. enjoyed over other countries
in the field of cryptography.

“Official” History

- Differential Cryptanalysis :
  Biham-Shamir [1991]

DC was studied in Eastern Germany in 1973!



Geheime Verschlußsache
MfS -020-Nr.: 747/73/Bl. 45

BSTU
000053

Durch die Festlegung von Z wird die kryptologische Qualität des Chiffrators beeinflußt. Es wurde davon ausgegangen, daß eine Funktion Z kryptologisch geeignet ist, wenn sie folgende Forderungen erfüllt:

(1) $|\{x=(x_1,x_2,\cdots,x_6)\in\{0,1\}^6 \mid z(x)=0\}| = 2^5$

(2) $|\{x=(x_1,x_2,\cdots,x_6)\in\{0,1\}^6 \mid z(x)=0, \sum_{i=1}^{6} x_i = r\}| \approx \binom{6}{r}\cdot\frac{1}{2}$ $(r=0,1,\cdots,6)$

(3) $|\{x=(x_1,\cdots,x_6\}\in\{0,1\}^6 \mid z(x_1,x_2,\cdots,x_i,\cdots,x_6)=z(x_1,\cdots,x_i\oplus 1,\cdots,x_6)\}\approx 2^5$ $(i=1,2,\cdots,6)$

Fault Attacks on PCs [this paper]

Rule Nb. 1

Never believe what hackers claim.

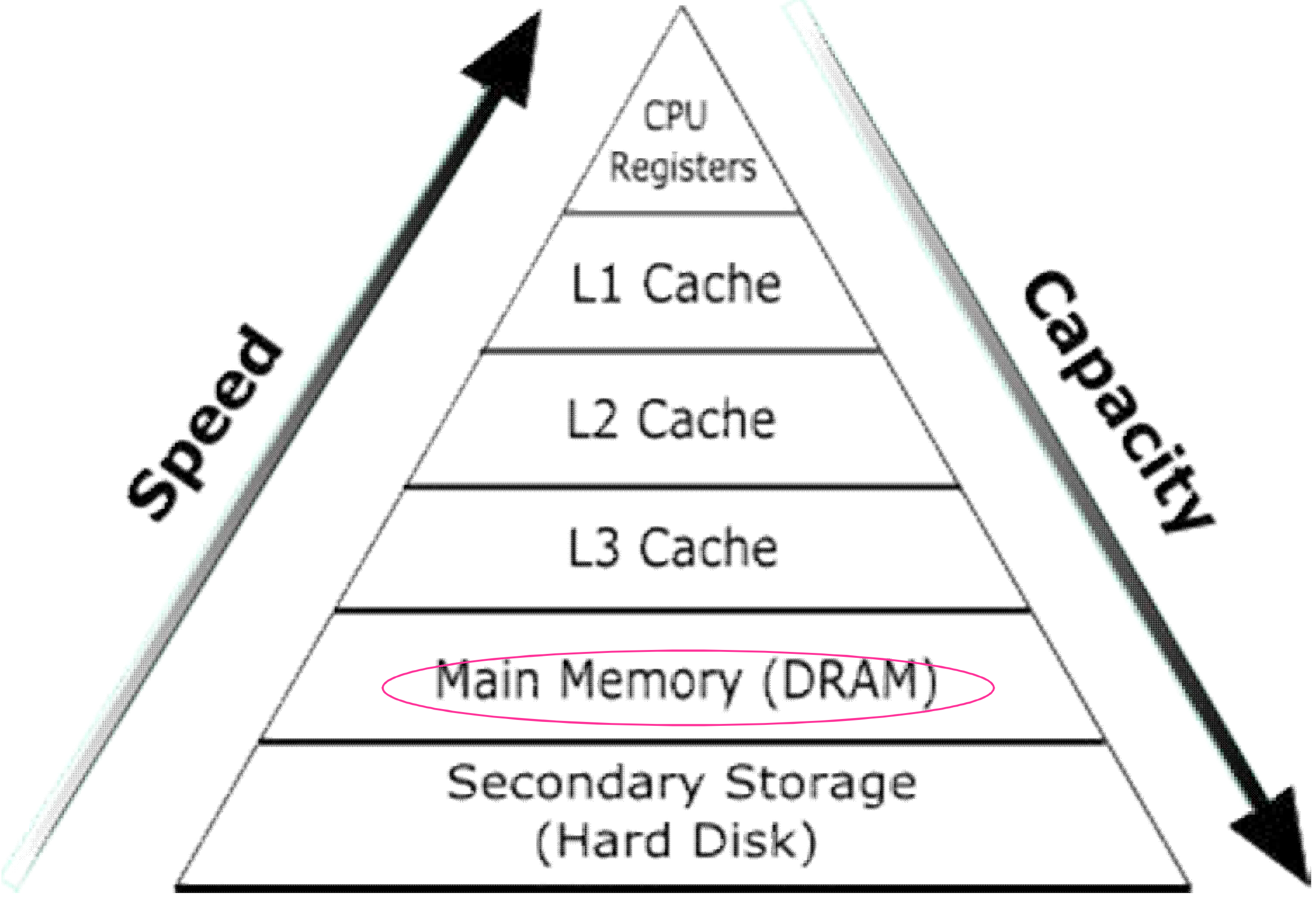
=> Most attacks described in current literature do NOT work as claimed or it is hard to make them work

=> Many other require root access. However.

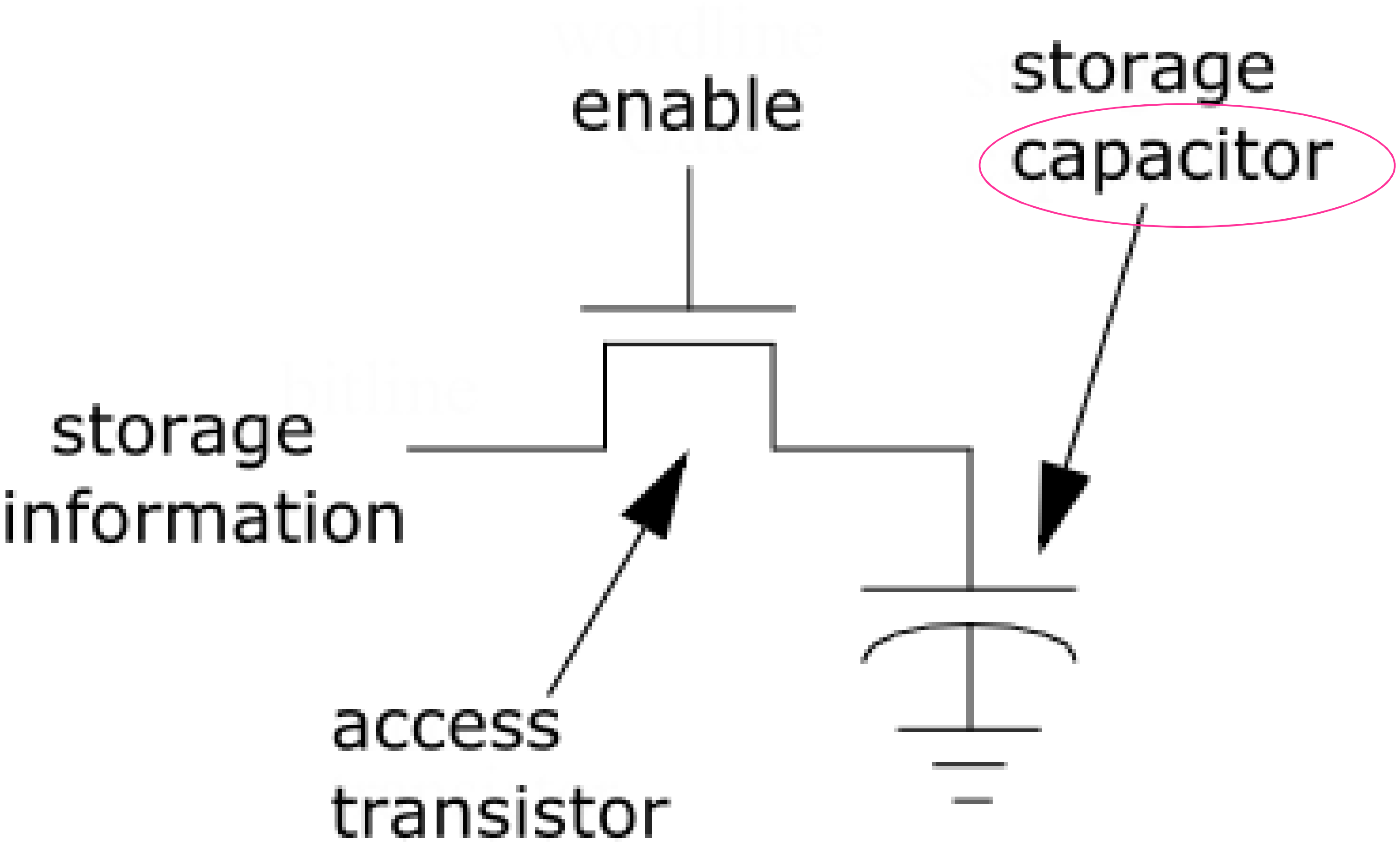
if attacker is root => lots of things he can do….

Our work: practical attacks without root privileges, also work in VM, and some of the highest speeds EVER achieved.

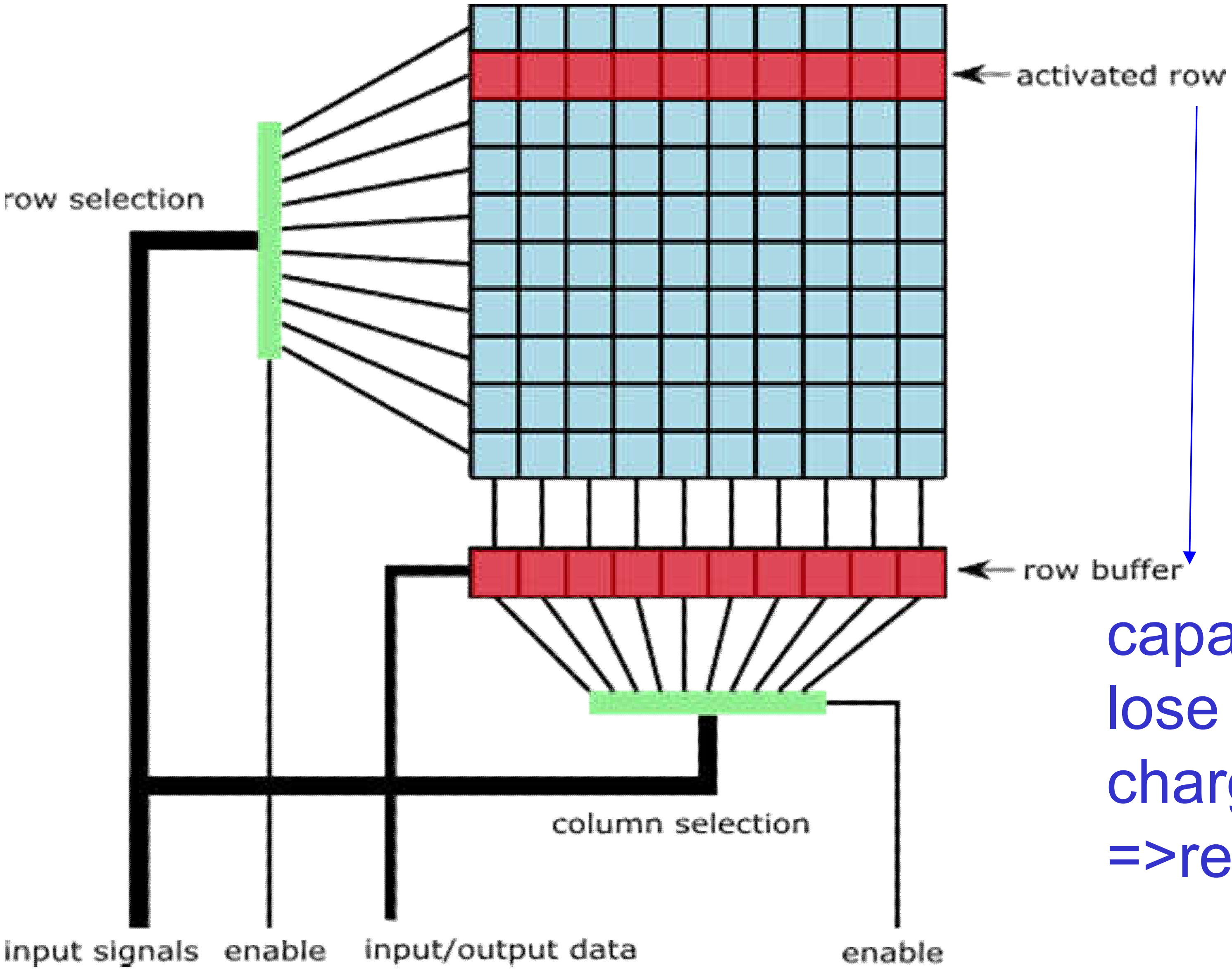
Our Goal: Introduce Faults in RAM



RAM cell

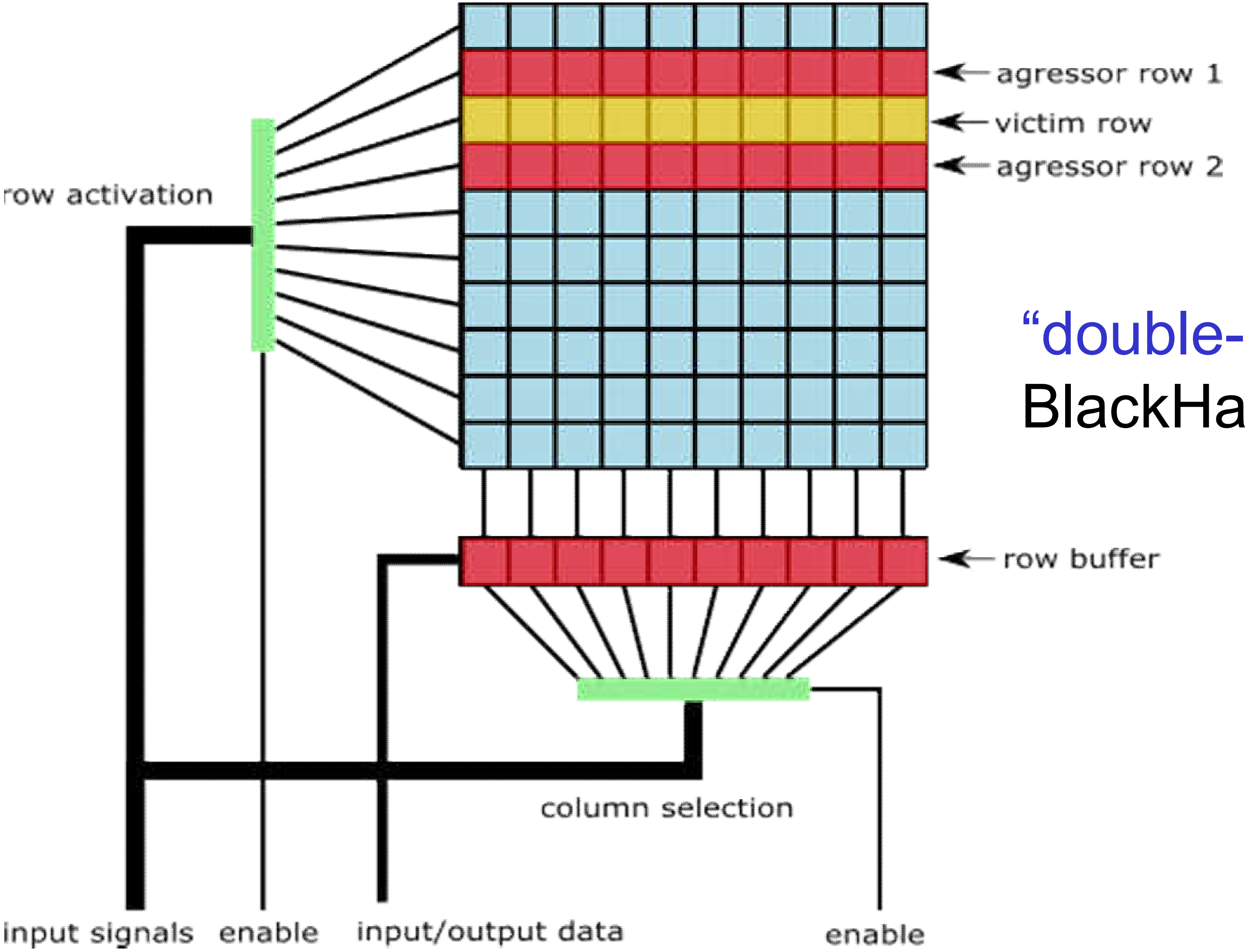

wordline
enable
storage
capacitor
bitline
storage
information
access
transistor

Arrays of Capacitors – normal R operation



capacitors lose their charge =>refresh

RowHammer Attack



"double-sided"
BlackHat'15

Difficulties

- How to bypass the cache???

=>otherwise the data is not read from RAM

- Avoid the row buffer of the target row

=>otherwise the data is not read from RAM either!

SBDR – goal to achieve

- Same Bank Different Rows

[Dullien Seaborn 2015]

⇒Considered a minimum requirement to launch a RowHammer attack…

⇒just this leads to quite poor attacks…

⇒like 5 bit flips in 10 minutes

⇒of course just ONE bit flipped could achieve sth spectacular

⇒recover a valuable Bitcoin private key worth M$...

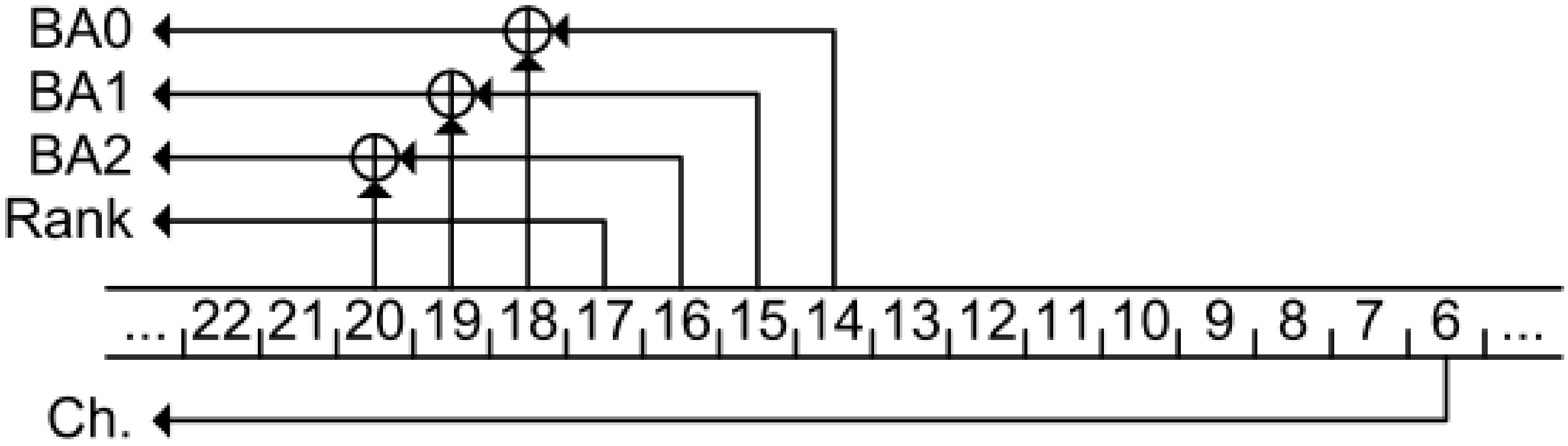
Cache Avoidance / Data Eviction

⇒Fill the cache with lots of data.

⇒CLFlush instruction, all attacks in our paper need/use it

- ⇒In user space on Intel processors
  - ⇒ARM in mobile phones are MORE secure!!!!

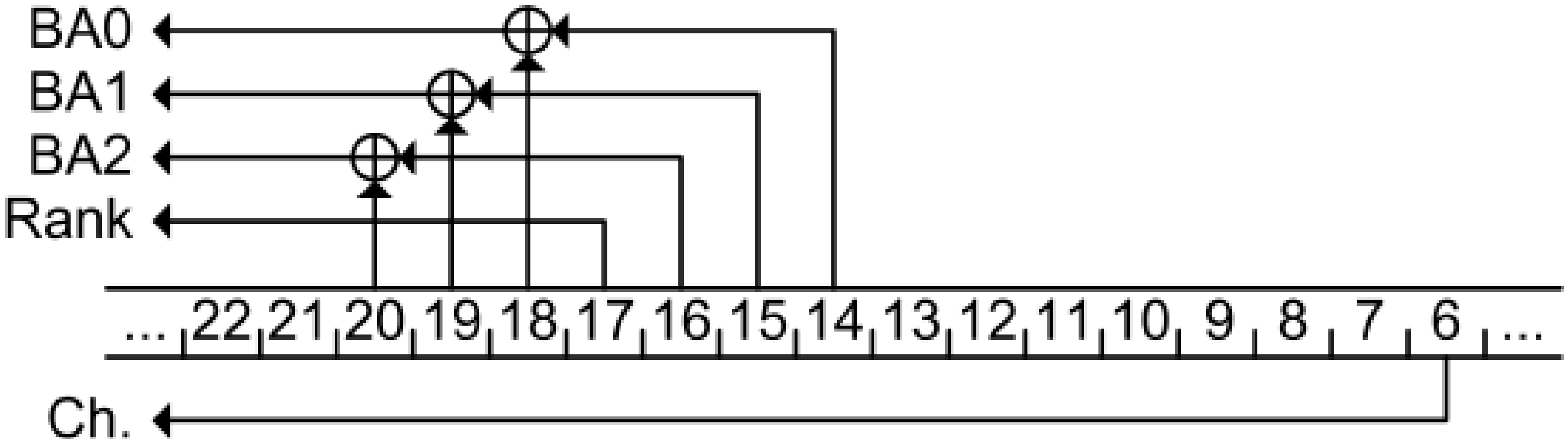
Obfuscation!



S&P’13 => security by obscurity!

- documented by AMD,
- secrecy by Intel…
- cf. new processors, DDR4, etc.

Beware!



Attacker CAN reverse engineer ±EASILY:
cf. our tcrh tool [and S+P'13 and Usenix 2007]

github.com/vp777/Rowhammer

another trick we use:

⇒increase page size

⇒the mapping is “more” transparent to the user…

⇒the offset is the same as the physical offset

github.com/vp777/Rowhammer

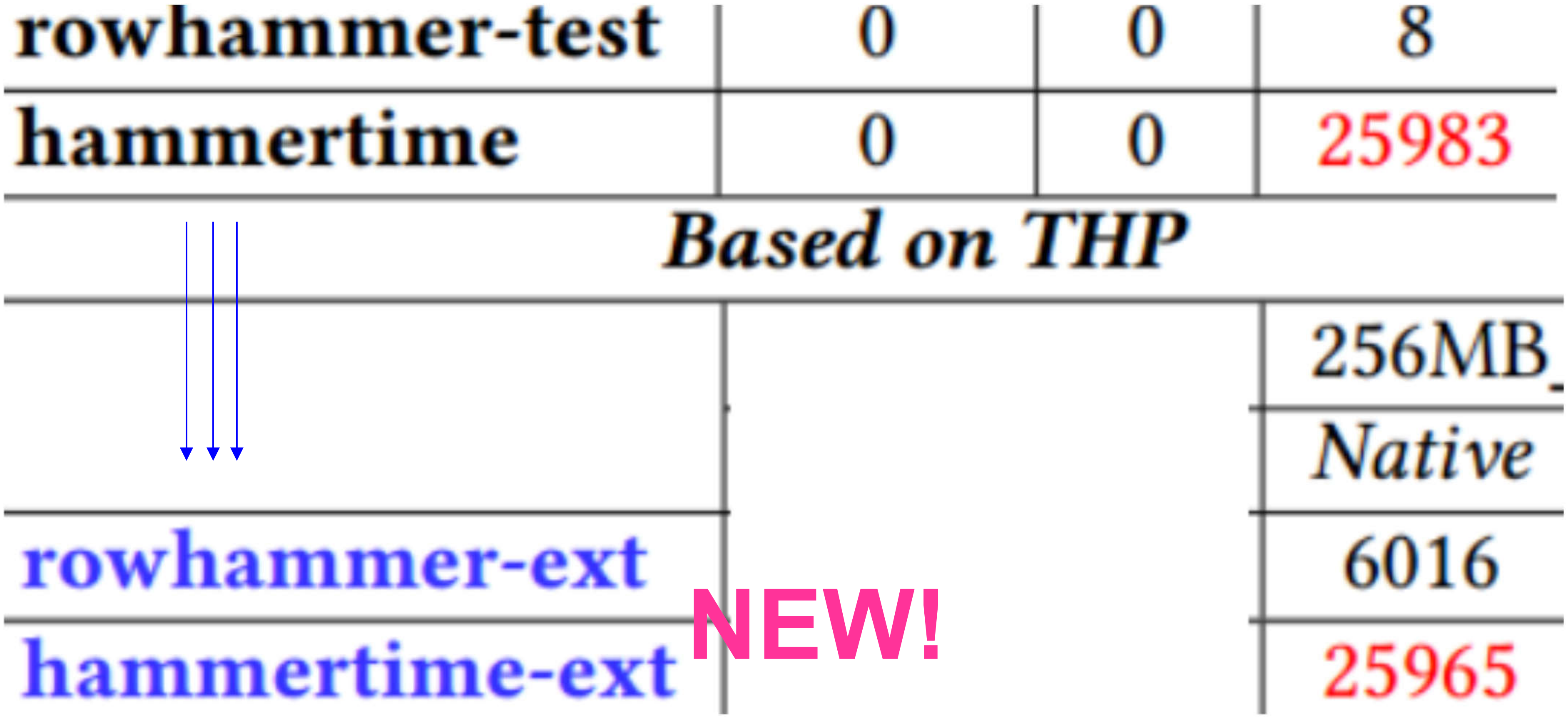
cf. our hprh tool

=>pages can be up to 1G on Intel!

=> we use the THP feature or Linux 4K=>2M

THP => incredible boost

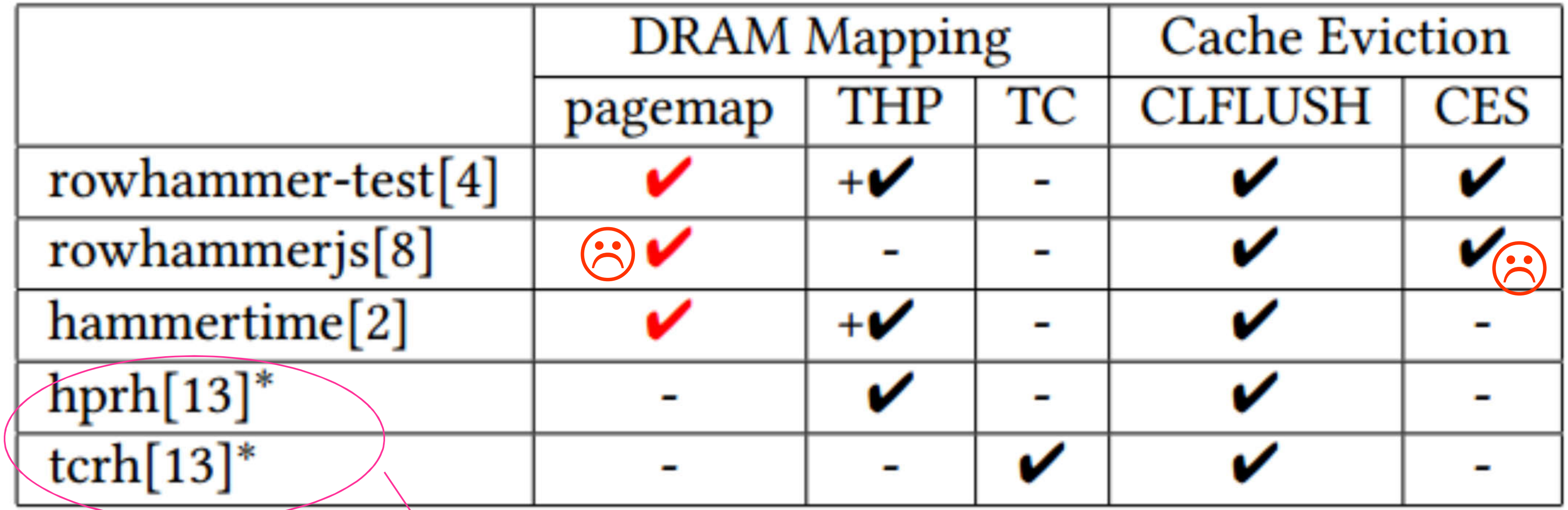
⇒We also provide patches to 2 third party rowhammer attack which add the THP ability!



rowhammer-test	0	0	8
hammertime	0	0	25983
Based on THP			
			256MB_ *Native*
rowhammer-ext			6016
hammertime-ext			25965

NEW!

Comparison of Attack Tools



	DRAM Mapping			Cache Eviction	
	pagemap	THP	TC	CLFLUSH	CES
rowhammer-test[4]	✔	+✔	-	✔	✔
rowhammerjs[8]	☹ ✔	-	-	✔	✔☹
hammertime[2]	✔	+✔	-	✔	-
hprh[13]*	-	✔	-	✔	-
tcrh[13]*	-	-	✔	✔	-

[4]=Dullien-Seaborn 2015

[8]=Gruss-Maurice 2016-17

[2]=Tatar, 2016

[13]=our two new software tools:

github.com/vp777/Rowhammer

new tools we developed

our hprh tool =

Huge Page RowHammer

our tcrh tool =

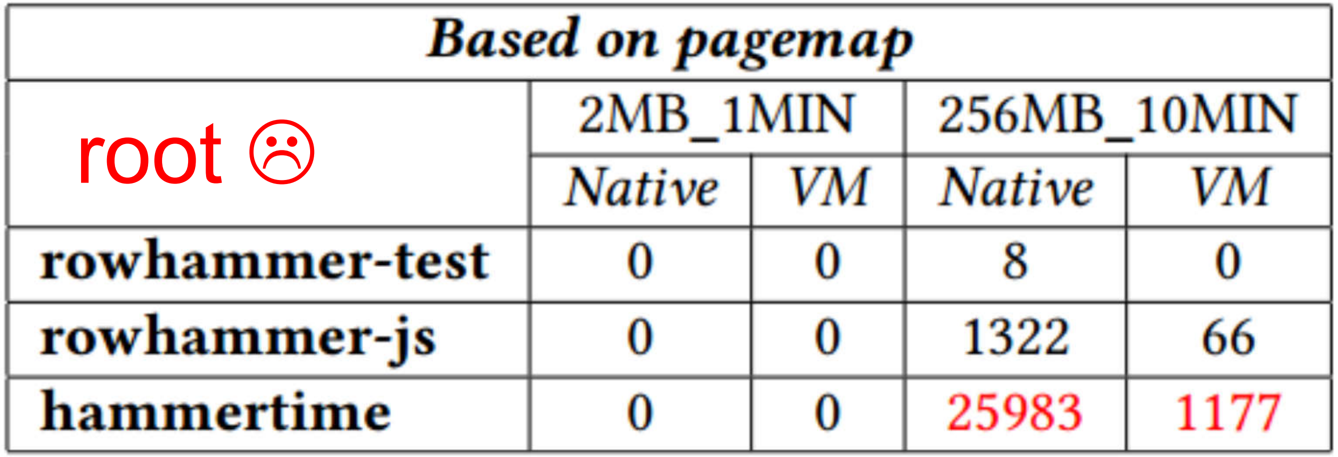
Timing Channel RowHammer

github.com/vp777/Rowhammer

Results:

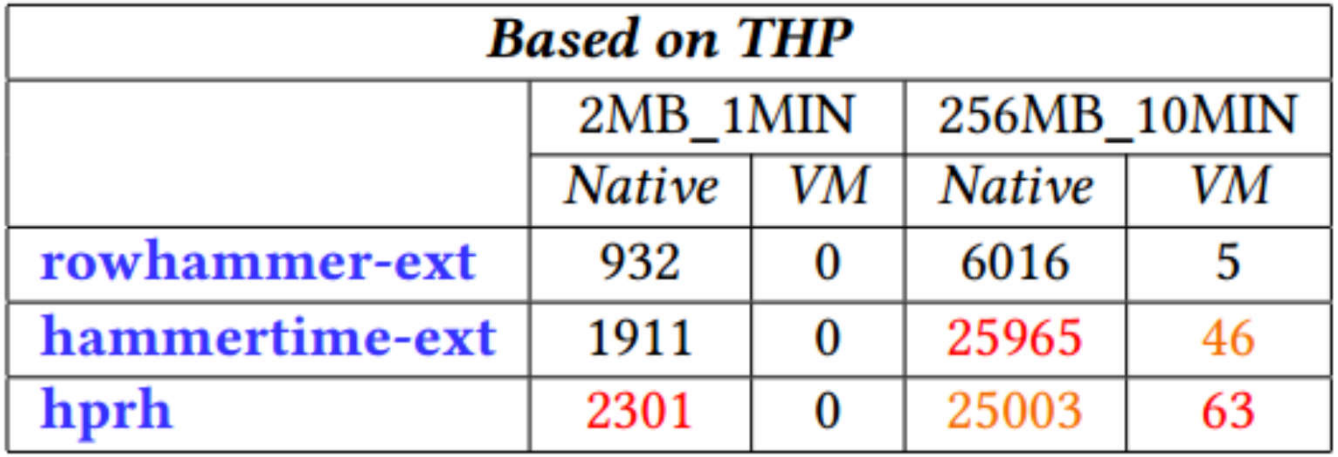
#Bits Flipped

/ 10 minutes



Based on pagemap				
root ☹	2MB_1MIN		256MB_10MIN	
	Native	*VM*	*Native*	*VM*
rowhammer-test	0	0	8	0
rowhammer-js	0	0	1322	66
hammertime	0	0	25983	1177

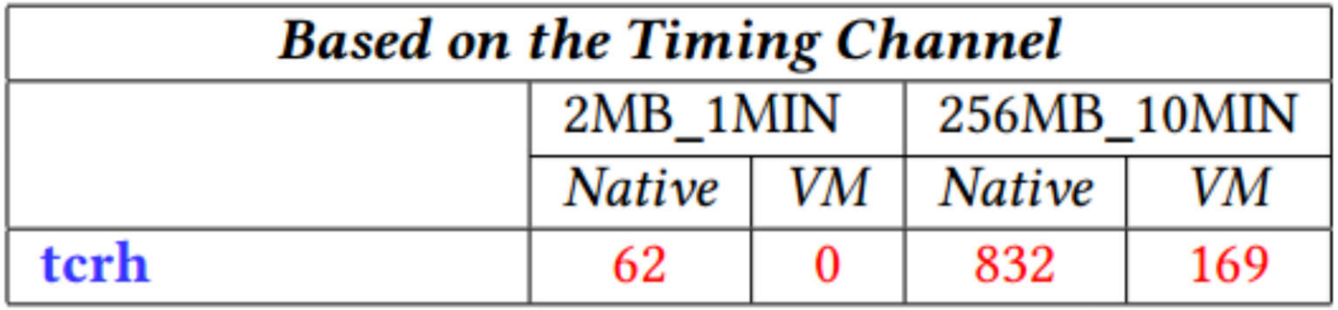
MODIFIED!



Based on THP				
	2MB_1MIN		256MB_10MIN	
	Native	*VM*	*Native*	*VM*
rowhammer-ext	932	0	6016	5
hammertime-ext	1911	0	25965	46
hprh	2301	0	25003	63

NEW!

=> github.com/vp777/Rowhammer



Based on the Timing Channel				
	2MB_1MIN		256MB_10MIN	
	Native	*VM*	*Native*	*VM*
tcrh	62	0	832	169