ECRYPT
http://www.ecrypt.eu.org

It's Not My Fault - On Fault Attacks on Symmetric Cryptography

Bart Preneel
COSIC, KU Leuven, Belgium
Bart.Preneel(at)esat.kuleuven.be
http://homes.esat.kuleuven.be/~preneel

FDTC – 9 September 2012

1

Symmetric crypto history 101

- pre-1915: manual encryption or simple devices

- 1915: rotor machines: (electro-)mechanical



- 1960: electronic encryption
- 1975: integrated hardware
- 1990: software

2

Cryptography: everywhere

everything is always connected everywhere

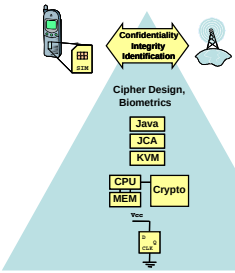





continuum between software and hardware
ASIC (microcode) – FPGA – fully programmable processor

3

Implementations in embedded systems



Protocol: Wireless authentication protocol design

Algorithm: Embedded fingerprint matching algorithms, crypto algorithms

Architecture: Co-design, HW/SW, SOC

Micro-Architecture: co-processor design

Circuit: Circuit techniques to combat side channel analysis attacks

Technology aware solutions?

Slide credit: Prof. Ingrid Verbauwhede

4

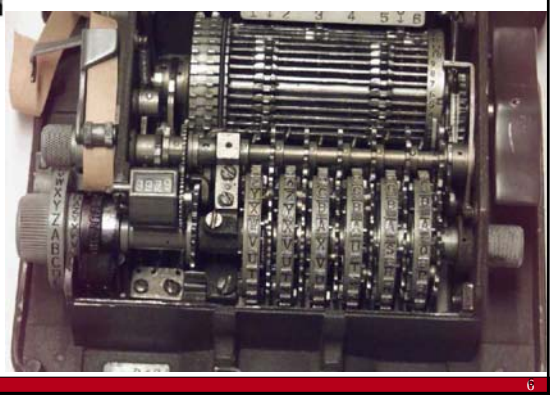
The sorcerer's apprentice guide to fault attacks

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 [24] caused faults in chips. Specifically, Uranium-235, Uranium-238 and Thorium-230 residues present in the packaging decay to Lead-206 while releasing particles. These particles create a charge in sensitive chip areas causing bits to flip.

[24] T. May and M.Woods. "A New Physical Mechanism for Soft Errors in Dynamic Memories", in the Proceedings of the *16th International Reliability Physics Symposium*, April, 1978.

5

Hagelin C38

6

Problem: what is this?

- Cryptogram [=14 January 1961 11.00 h]
- <AHQNE XVAZW IQFFR JENFV OUXBD
  LQWDB BXFRZ NJVYB QVGOZ KFYQV
  GEDBE HGMPS GAZJK RDJQC VJTEB
  XNZZH MEVGS ANLLB DQCGF PWCVR
  UOMWW LOGSO ZWVVV LDQNI YTZAA
  OIJDR UEAAV RWYXH PAWSV CHTYN
  HSUIY PKFPZ OSEAW SUZMY QDYEL
  FUVOA WLSSD ZVKPU ZSHKK PALWB
  SHXRR MLQOK AHQNE 11205 141100>

The answer

- Plaintext [=14 January 1961 11.00 h]
- DOFGD VISWA WVISW JOSEP HWXXW
  TERTI OWMIS SIONW BOMBO KOWVO
  IRWTE LEXWC EWSUJ ETWAM BABEL
  GEWXX WJULE SWXXW BISEC TWTRE
  SECVX XWRWV WMWPR INTEX WXXWP
  RIMOW RIENW ENVOY EWRUS URWWX
  XWPOU VEZWR EGLER WXXWS ECUND
  OWREP RENDR EWDUR GENCE WPLAN
  WBRAZ ZAWWC

The answer (in readable form)

- Plaintext [=14 January 1961 11.00 h]
- TRESECV. R V M PRINTEX. PRIMO
  RIEN ENVOYE RUSUR. POUVEZ
  REGLER. SECUNDO REPRENDRE
  DURGENCE PLAN BRAZZA VIS A
  VIS JOSEP H. TERTIO MISSION
  BOMBOKO VOIR TELEX CE SUJET
  AMBABELGE. JULES.

Resume urgently plan Brazzaville w.r.t. P. Lumumba

A strange cryptogram

- Cryptogram [=2 February 1961 22.00 h]
- <btwve ghqmg dviww zmdha xbvmx
  saftm nuqjs isvgn pjlcx infik
  jjibp bxyoh xmwpw amgbn iywgh
  lslnr btwve 11075 022200>

- <Note pour Smal. Votre message **printex** sans no du trois février 1961 indéchiffrable. Prière répéter>.

A strange cryptogram

- Plaintext [=2 February 1961 22.00 h]
- <btwve PRESE NCEWM ANKOV VSKYW
  AWEVI LLEWX XWBIS ECTWV OYAGE
  WPARA ITWTO UTWAW FAITW INUTI
  LEWVU >
- **encrypted session key should be: UEWVE (only 5,965,050 combinations)**
- **session key should be PFHCF rather than PHHCF**

Outline

- context and history
- symmetric crypto trends
  - maturity
  - lightweight crypto
  - physical attacks: side channel/fault
- fault attacks on AES
- challenges for research

Block ciphers

64-bit block

3-DES** (112-168)
IDEA (128)
MISTY1 (128)
GOST* (256)
KASUMI** (128-3G, 64-2G)
HIGHT** (128)
PRESENT (80-128)
TEA (128)
mCrypton (96-128)
KATAN64 (80)
KTANTAN64* (80)
KLEIN* (64-96-128)
DESXL (144)
LED (64-128)
PICCOLO (80-128)

96-bit block

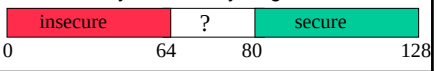
SEA (96)
PRINTcipher-96 (160)

128-bit block

AES (128-192-256)
CAMELLIA
RC6
SERPENT
CLEFIA

56 bits: < 1 hour with M$ 5
80 bits: 2 year with M$ 5
128 bits: 256 billion years with B$ 5

symmetric key lengths



13

Stream ciphers: the eSTREAM Portfolio

(http://www.ecrypt.eu.org/stream)

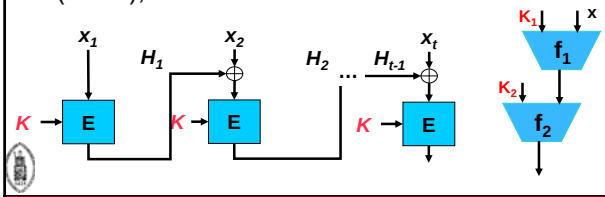
Software	Hardware
HC-128	~~F-FCSR-H v2~~
Rabbit	Grain v1
Salsa20/12	MICKEY v2
Sosemanuk	Trivium

Others: SNOW3G, MUGI

14

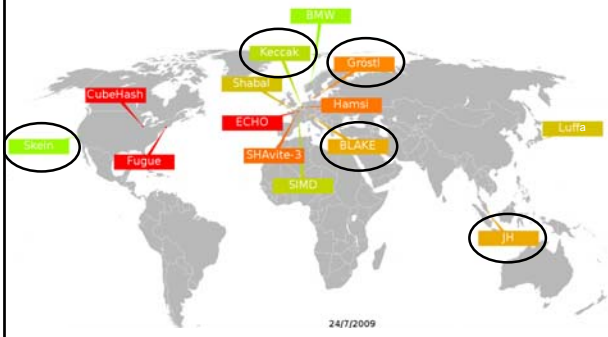
MAC algorithms

- block cipher based:
  - CBC-MAC (EMAC, CMAC) and PMAC
- hash function based: HMAC
- universal hash function based: GMAC (GCM), UMAC



15

Hash functions: SHA-3 finalists

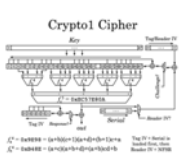


Slide credit: Christophe De Cannière

16

Status of symmetric cryptology: ☺

- many mature and well understood designs available
  - consequence: new attacks published that need 2^{123} chosen plaintexts, 2^{233} memory and time 2^{253}
- weak algorithms are (slowly) disappearing
  - Keeloq
  - Crypto-1
  - Hitag2
  - A5/1 and A5/2
  - E0
  - …



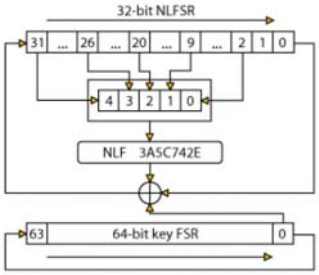
17

Trend: lightweight crypto

18

Keeloq [Smit+/-'85]
aka the M$10 cipher

- block length: 32
- key length: 64
- rounds: 528

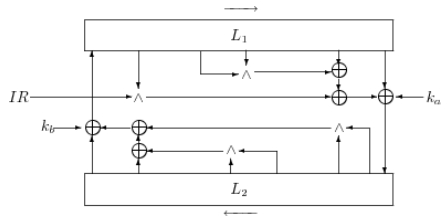


19

KATAN/KTANTAN
[De Cannière-Dunkelman-Knežević'09]
http://www.cs.technion.ac.il/~orrd/KATAN/

- block length: 32, 48, 64
- key length: 80
- rounds: 254

462-1054 gates



20

PRINTcipher
[Knudsen-Leander-Poschmann-Robshaw'10]

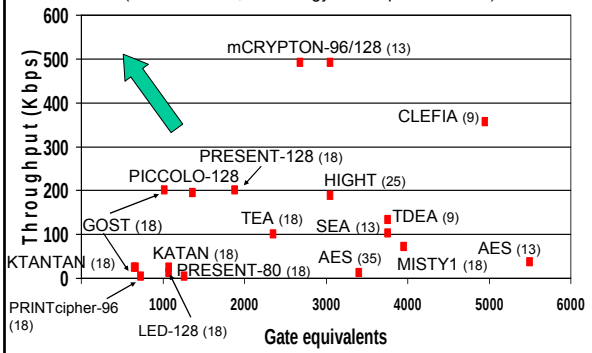
- IC printing technology (different for each print)
- hardwired key

- block length: 48, 96
- key length: 80, 160
- rounds: 48, 96
- 3-bit S-boxes
- key-dependent bit-permutations

402-967 gates

21

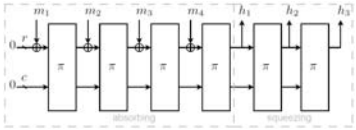
Low cost hw: throughput versus area
[Bogdanov+08,Sugawara+08]
(100 KHz clock, technology in multiples of 10 nm)



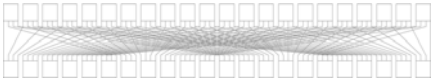
22

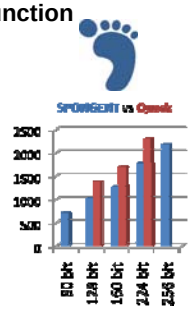
SPONGENT: Lightweight Hash Function

Narrow SPONGE construction



Unkeyed PRESENT-type permutation π: 4-bit S-box and bit diffusion

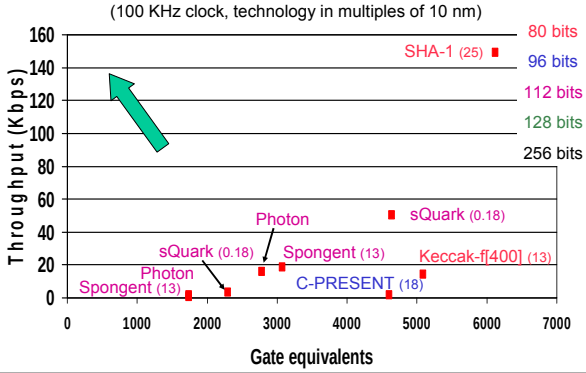




- smallest footprint
- low power
- conservative security

23

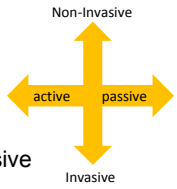
Low cost hw: throughput versus area
(100 KHz clock, technology in multiples of 10 nm)



24

Physical Attacks

- active versus passive
  - active: perturbate and conclude
  - passive: observe and infer
- invasive versus non-invasive
  - invasive: open package and contact chip
  - semi-invasive: open package, no contact
  - non-invasive: no modification
- side channel: passive and non-invasive
  - timing, power, electromagnetic
  - very difficult to detect
  - often inexpensive to set-up
  - often: need lots of measurements → automating
- circuit modification: active and invasive
  - expensive to detect invasion (chip might be without power)
  - very expensive equipment and expertise required



25

Fault attacks

very powerful attack models
- fix specific bits at 0/1
- dynamically fix specific bits at 0/1
- change 1/more specific bits
- change 1/more specific bytes
- changes state in a specific round
- change some value during the calculation

26

Fault attacks (2)

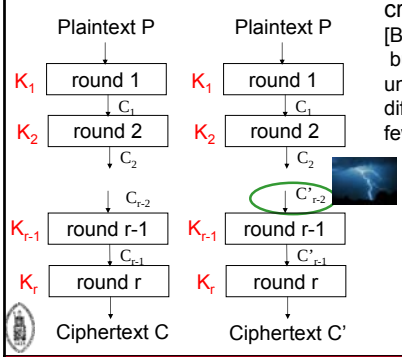
some attack models are so powerful that they allow for "trivial" attacks

exhaustive search over K_{right} : $2^{k/2}$
exhaustive search over K_{left} : $2^{k/2}$

27

Differential Fault Analysis (DFA)

[Biham-Shamir'97]



Differential cryptanalysis [Biham-Shamir'90] but with unknown input difference
fewer rounds (1-2-3-4)

28

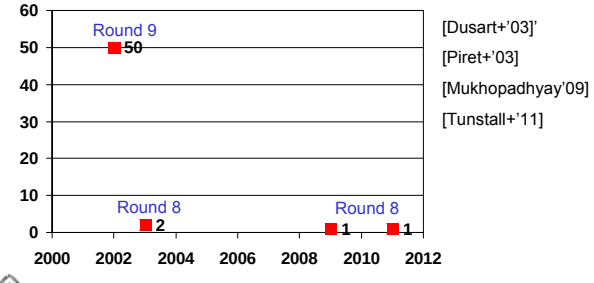
Outline

- context and history
- symmetric crypto trends
  - maturity
  - lightweight crypto
  - physical attacks: side channel/fault
- fault attacks on AES
- challenges for research

29

DFA on AES-218

faults for simple byte attacks



30

DFA on AES-128 [Derbez+11]

- start of round 7:
  - impossible differential attack: 45 faults and time/memory 2^{40}
  - meet-in-the-Middle attack: 5-10 faults and complexity 2^{40} - 2^{60}
  - extensions to AES-192 and AES-256 (start of round n-4) with comparable complexity
- conclusion:
  - protect 5 first and last rounds (all rounds of AES-128)
  - or all the rounds?
- [Piret-Quisquater'03] *"It is not clear whether ciphers with a more intrcate structure could be broken with so few ciphertext pairs"*

31

Challenges (1): industry

- effective countermeasures are expensive
  - masking (against side channel attacks) does not work
  - protecting only outer rounds of a block cipher will not help
- security by obscurity: is this scientific? (August Kerckhoffs)

- how are solutions certified?
  - which information about the certification is public?
  - how is information shared from hardware vendor to software/OS vendor to integrator and end consumer?
  - what about backdoors?

32

Challenges (2): academia

- impact
  - about 150 block ciphers + 50 stream ciphers + 100 hash functions
  - 300 ciphers x 7 attack models = 2100 papers
- attacking lightweight crypto

B. Gierlichs, L. Batina, C. Clavier, T. Eisenbarth, A. Gouget, H. Handschuh, T. Kasper, K. Lemke-Rust, S. Mangard, A. Moradi, and E. Oswald, "Susceptibility of eSTREAM Candidates towards Side Channel Analysis," In ECRYPT Workshop, SASC - The State of the Art of Stream Ciphers, C. De Cannière, and O. Dunkelman (eds.), 28 pages, 2008.

33

Challenges (2): academia

- leakage + tamper resilience: enormous blowup so not even close to practical

34

Challenges (3): collaboration

- industry: develop sharing methods
- academia: evaluate implementations with (multiple) countermeasures
- alternative: academia focuses on reverse engineering
- need transparency for evaluation

35

The end

Thank you for your attention

36