Une école de l'IMT

Attaques par injection de fautes

Laurent Sauvage

Presentation Outline

Introduction to Fault Injection Attack

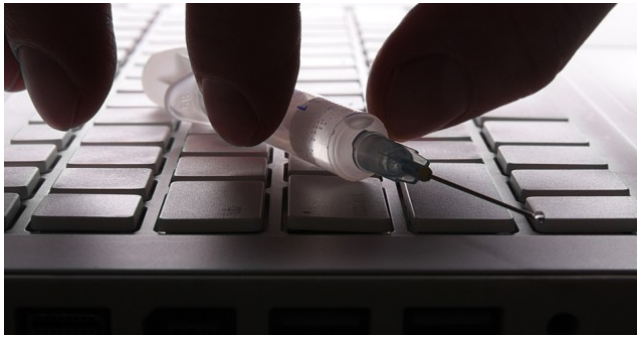
Countermeasures Against Fault Injection Attack

Fault Analysis on Data Encryption Standard (DES)

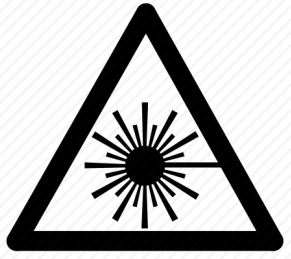
Presentation Outline

Cryptography is Everywhere, Mathematically Robust, but. . .

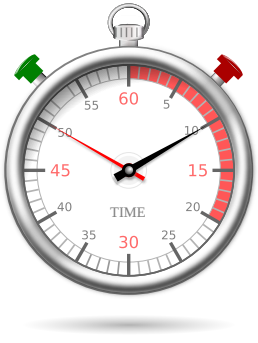
…Threatened by Attacks on Cyber-Physical Systems!

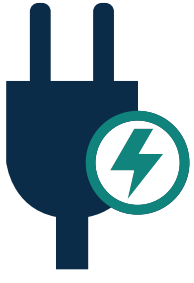


Code injection attack

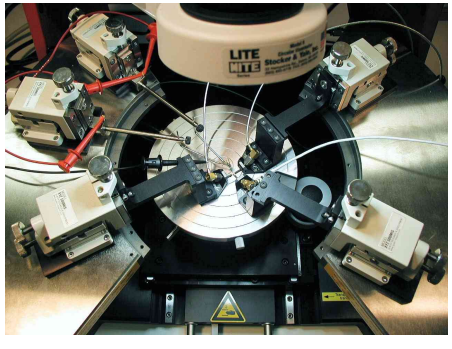


Fault injection attack





Side-channel attack

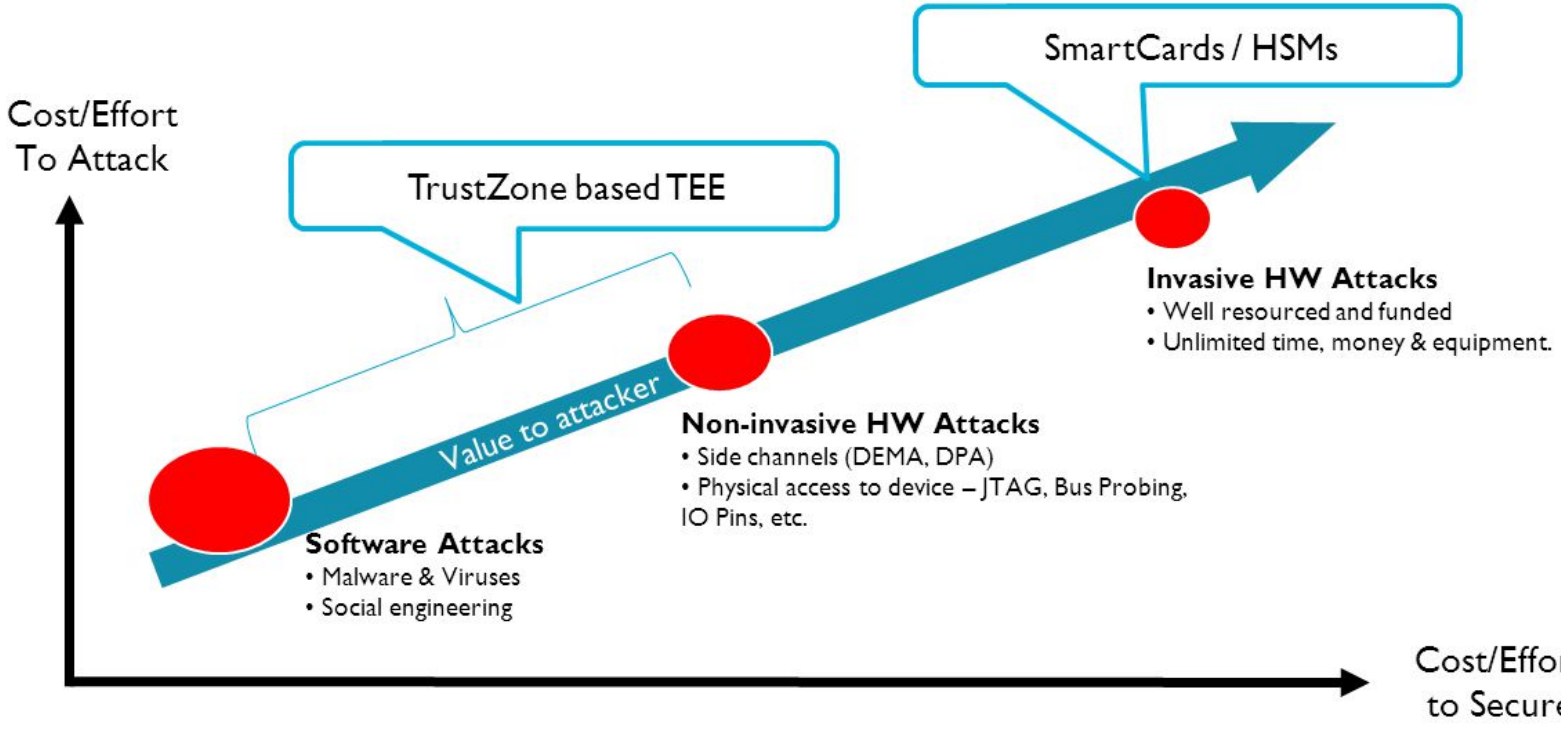


Physical attack

Local & Remote

ARM Technology Symposium 2013

Security Profiles



12

ARM

Hack of Sony Playstation 3 (2010)

Sony

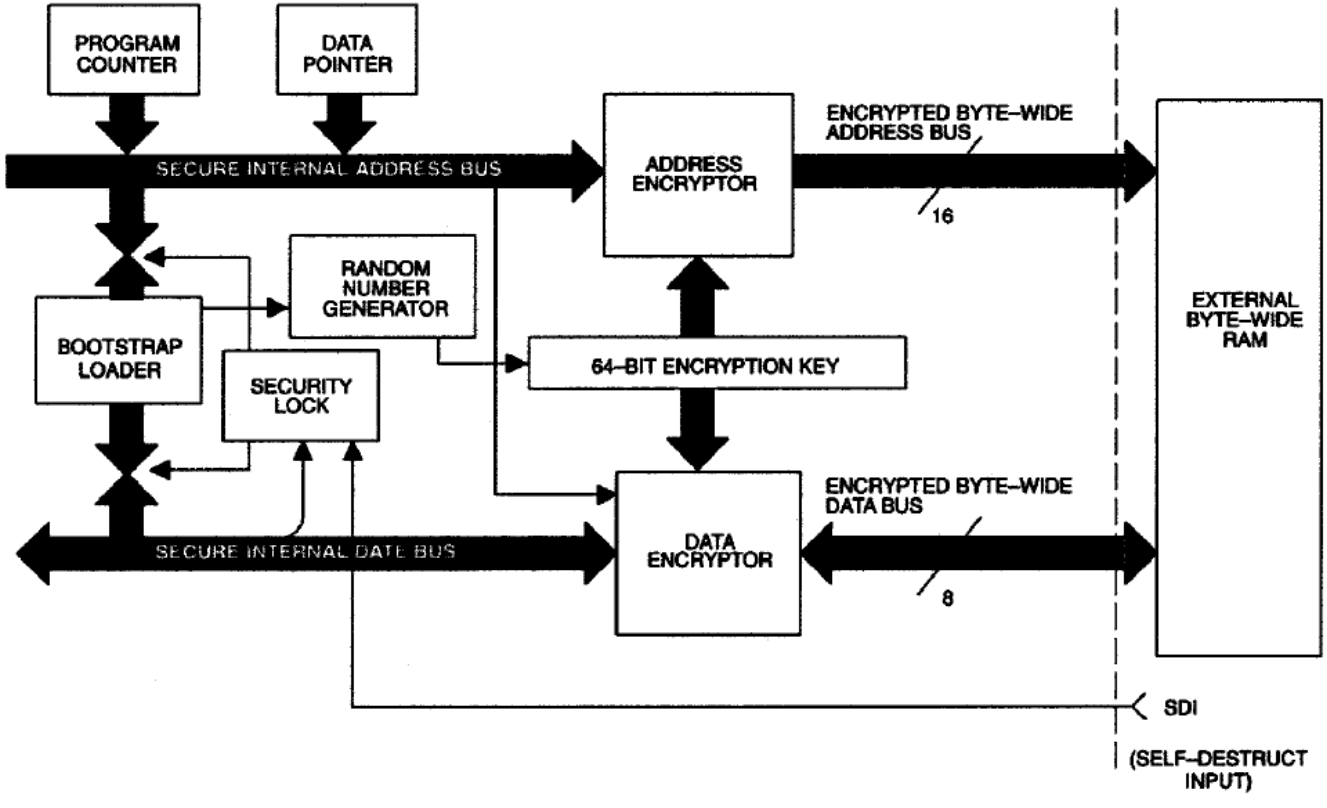
- High resources (human, funding)
- Expert in protecting game console (>20 years)

Hackers

- Have few resources
- Didn’t find vulnerability for 3 years
- Hack in 5 weeks: exploit assisted by fault injection attack
- Use low-cost (<$300) equipment

A Secure Microcontroller in 1996

Dallas Semiconductor DS5002FPM



- DES-like encryption of address/data of NV memory
- 64-bit key from on-chip TRNG (unknown by everyone)
- Top-layer coating against microprobing (FIPS 140-1)
- Erasure of secrets w/o V_{CC} (10-year lithium battery)

Breaking Microcontrollers in 1996

Ross J. Anderson and Markus G. Kuhn, Tamper Resistance – a Cautionary Note, In Proceedings of the Second USENIX Workshop ON Electronic Commerce, November 18-21 1996, Oakland, California. ISBN 1-880446-83-9, pp. 1–11

A typical subroutine found in security processors

```
1 b = answer_address
2 a = answer_length
3 if (a == 0) goto 8
4 transmit(*b)
5 b = b + 1
6 a = a - 1
7 goto 3
8 ...
```

- Write a first bytes at memory address @b to the serial port
- Lines 4–7 are executed a times (e.g., $a = 128$ for a RSA-1024 signature)

Breaking Microcontrollers in 1996

Ross J. Anderson and Markus G. Kuhn, Tamper Resistance – a Cautionary Note, In Proceedings of the Second USENIX Workshop ON Electronic Commerce, November 18-21 1996, Oakland, California. ISBN 1-880446-83-9, pp. 1–11

Fault injection attack (non-invasive)

```
1 b = answer_address
2 a = answer_length
3 if (a == 0) goto 8
4 transmit(*b)
5 b = b + 1
6 a = a - 1
7 goto 3
8 ...
```

"(...) a clock (...) or a power glitch (...) transforms either the conditional jump in line 3 or the loop variable decrement in line 6 (dumping) the remaining memory, which if we are lucky will include the keys we are looking for."

Works on any (**single**) check of passwords, access rights, protocol responses, etc.

Differential Fault Analyses Are Powerful!

Exploiting couples of right/wrong computations

Number of faulted ciphertexts (C') to disclose the key (best attacker)

Algorithm	**Key space**	**# C'**
RSA (CRT) [BDL97]	2^{1024}	1
RSA-1024 [BDH+97]		3083
DES [BS97]	2^{56}	11
AES-128 [PQ03]	2^{128}	2
AES-256 [TMA11]	2^{256}	2
ECDSA/P-192 [BBB+11]	2^{192}	36
Midori-128 [**?**]	2^{128}	2
R-LWE-based PQC [BBK16]	2^{512}	2304

What about other lighweight & PQC algorithms ?

Presentation Outline

Introduction to Fault Injection Attack

Countermeasures Against Fault Injection Attack

Fault Analysis on Data Encryption Standard (DES)

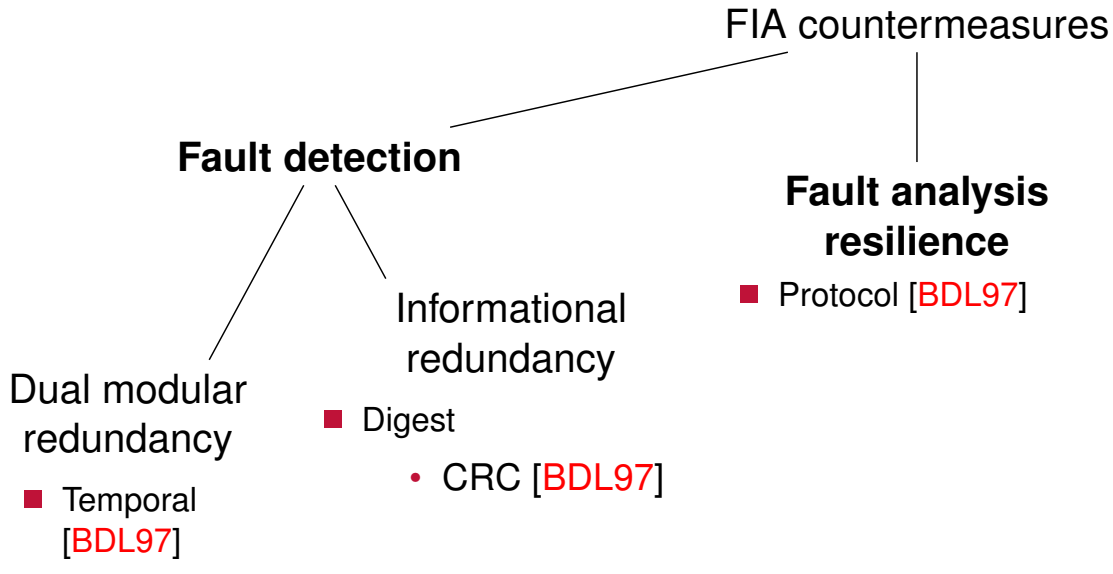
The Bellcore's...

Dan Boneh, Richard A. DeMillo, and Richard J. Lipton, On the importance of checking cryptographic protocols for faults (extended abstract),), Lecture Notes in Computer Science, vol. 1233, Springer, 1997, pp. 37–51

...Countermeasures

1. Check the output of computation using:
   - the same function (Dual modular redundancy)
   - or, the inverse function
2. Add error detection bits (e.g. CRC) to protect critical security parameters (p, q, etc.)
3. Random padding so that the signer never signs the same message (1st DFA requirement)

Protections Against FIA: a Classification



Bitflip on Secret Exponent

Differential Fault Analysis

Feng Bao, Robert H. Deng, Yongfei Han, Albert B. Jeng, A. Desai Narasimhalu, and Teow-Hin Ngair,

Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient

), Lecture Notes in Computer Science, vol. 1361, Springer, 1997, pp. 115–124

$$
\begin{aligned}
S &= m^d \pmod{n} \\
&= m_{t-1}^{d_{t-1}} \cdots m_i^{d_i} \cdots m_1^{d_1} m_0^{d_0} \pmod{n} \quad \text{with } m_i = m^{2^i} \pmod{n} \\
S' &= m_{t-1}^{d_{t-1}} \cdots m_i^{d_i'} \cdots m_1^{d_1} m_0^{d_0} \pmod{n} \quad \text{with } d_i' = 1 - d_i
\end{aligned}
$$

$$
\Rightarrow \frac{S'}{S} = \frac{m_i^{1-d_i}}{m_i^{d_i}} \pmod{n} = \begin{cases} m_i \pmod{n} & \text{if } d_i = 0, \\ \dfrac{1}{m_i} \pmod{n} & \text{if } d_i = 1. \end{cases}
$$

Bitflip on Secret Exponent

A Countermeasure: Infective Computation

Feng Bao, Robert H. Deng, Yongfei Han, Albert B. Jeng, A. Desai Narasimhalu, and Teow-Hin Ngair,

Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient

), Lecture Notes in Computer Science, vol. 1361, Springer, 1997, pp. 115–124

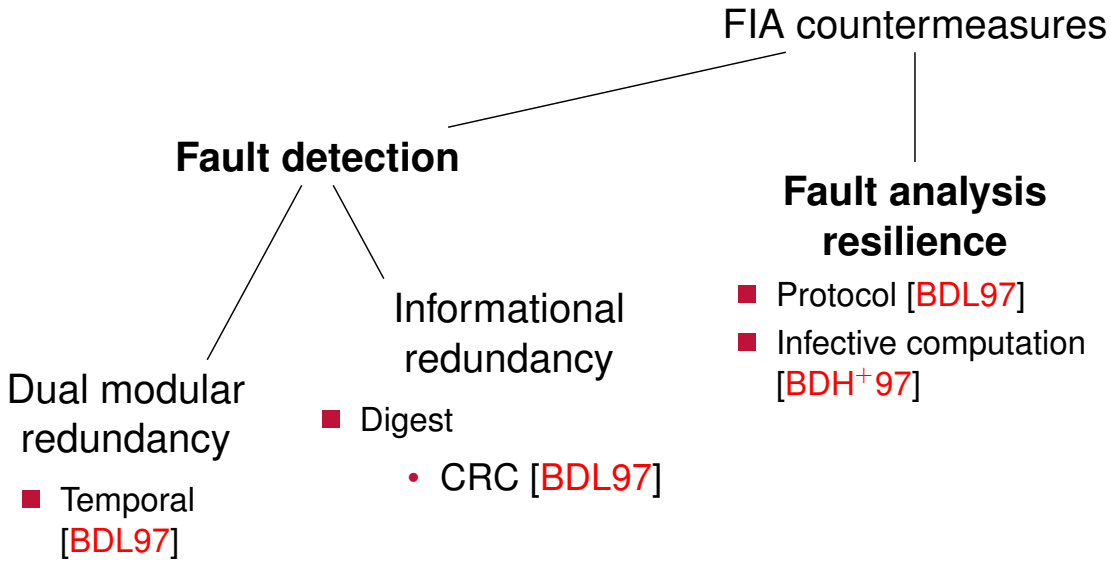
$$m^* \leftarrow mr \pmod{n} \qquad \text{with } r \text{ a random number}$$

$$S^* \leftarrow {m^*}^d \pmod{n}$$

$$S \leftarrow \frac{S^*}{r^d} \pmod{n}$$

$$\Rightarrow \frac{S'}{S} = \frac{m_i^{1-d_i} \dfrac{r_i^{1-d_i}}{r_i^{d_i}}}{m_i^{d_i}} \pmod{n} \begin{cases} m_i r_i \pmod{n} & \text{if } d_i = 0, \\ \dfrac{1}{m_i r_i} \pmod{n} & \text{if } d_i = 1. \end{cases}$$

Protections Against FIA: a Classification



Shamir's Trick (Ring Embedding)

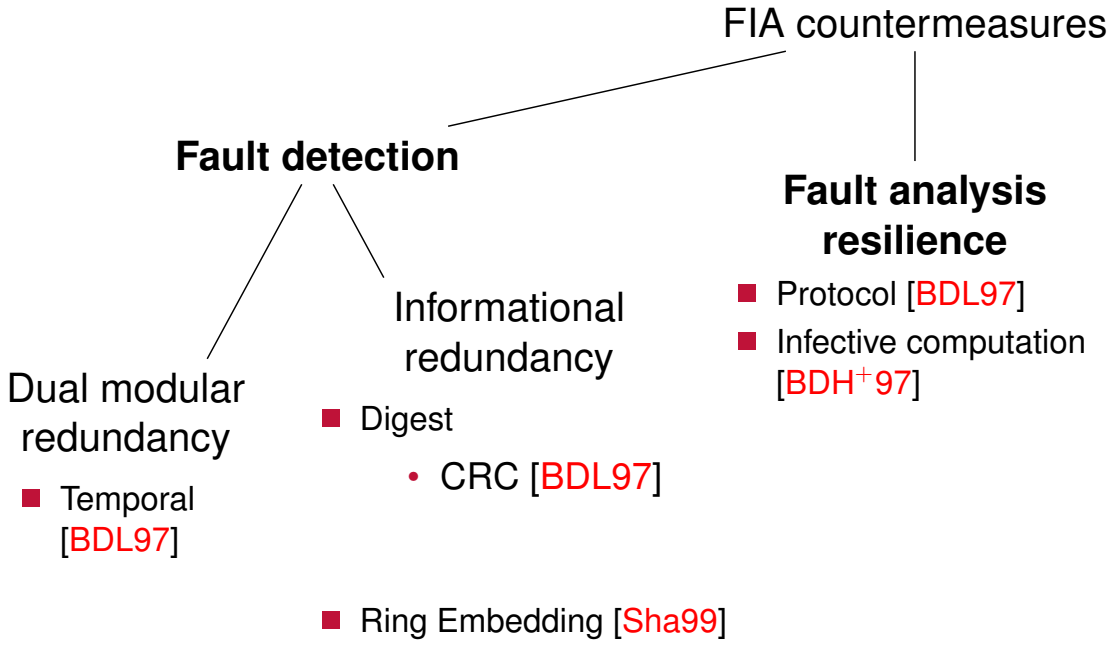
A. Shamir, Method and apparatus for protecting public key schemes from timing and fault attacks, November 23 1999, US Patent 5,991,415

Protecting the computation of $S = \mathrm{CRT}(S_p, S_q)$ with

$$\begin{cases} S_p = m^{d_p} \pmod{p}, \\ S_q = m^{d_q} \pmod{q}. \end{cases}$$

1. Select a k-bit random integer r (typically, $k = 32$)
2. Compute
$$\begin{cases} s_p^* = m^d \pmod{rp} \\ s_q^* = m^d \pmod{rq} \end{cases}$$
3. If $s_p^* \equiv s_q^* \pmod{r}$, return $S = \mathrm{CRT}(s_p^*, s_q^*)$

Protections Against FIA: a Classification



Low-cost Protections

Oliver Kömmerling and Markus G. Kuhn, Design principles for tamper-resistant smartcard processors,), USENIX Association, 1999

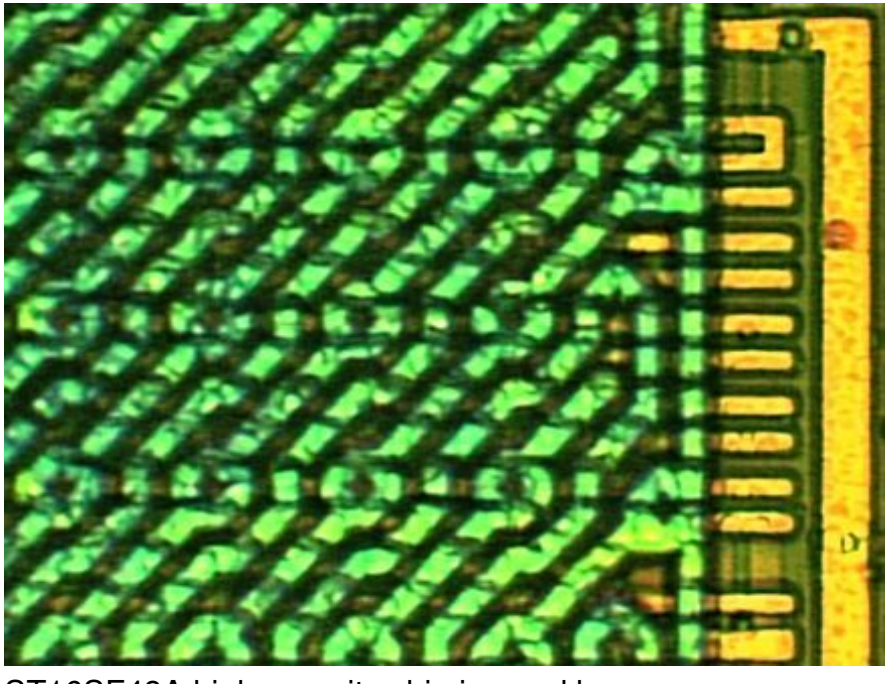
3.1 Randomized clock signal

- random insertion of dummy cycles + dummy activity
- jitter on clock cycle

3.2 Randomized multithreading

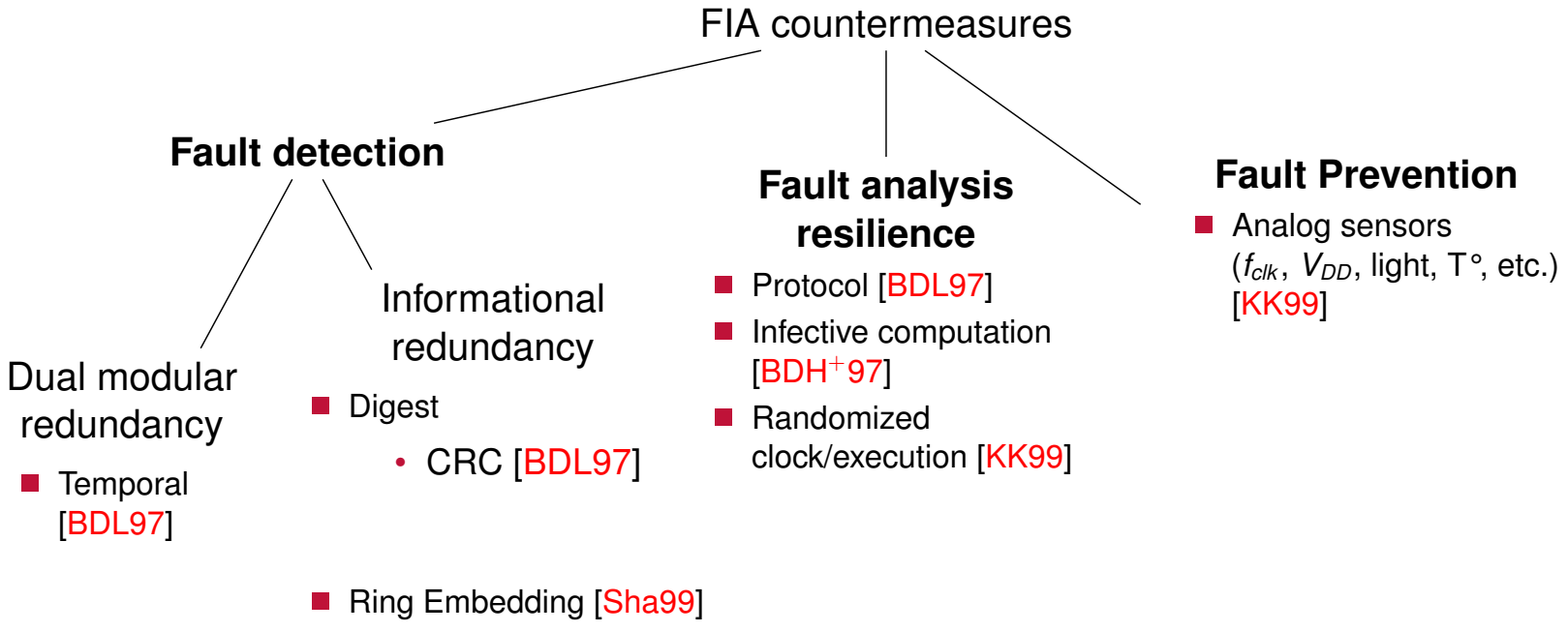
- Analog sensors (f_{clk}, V_{DD}, light, T°, etc.)

3.6 Top-layer Sensor Meshes



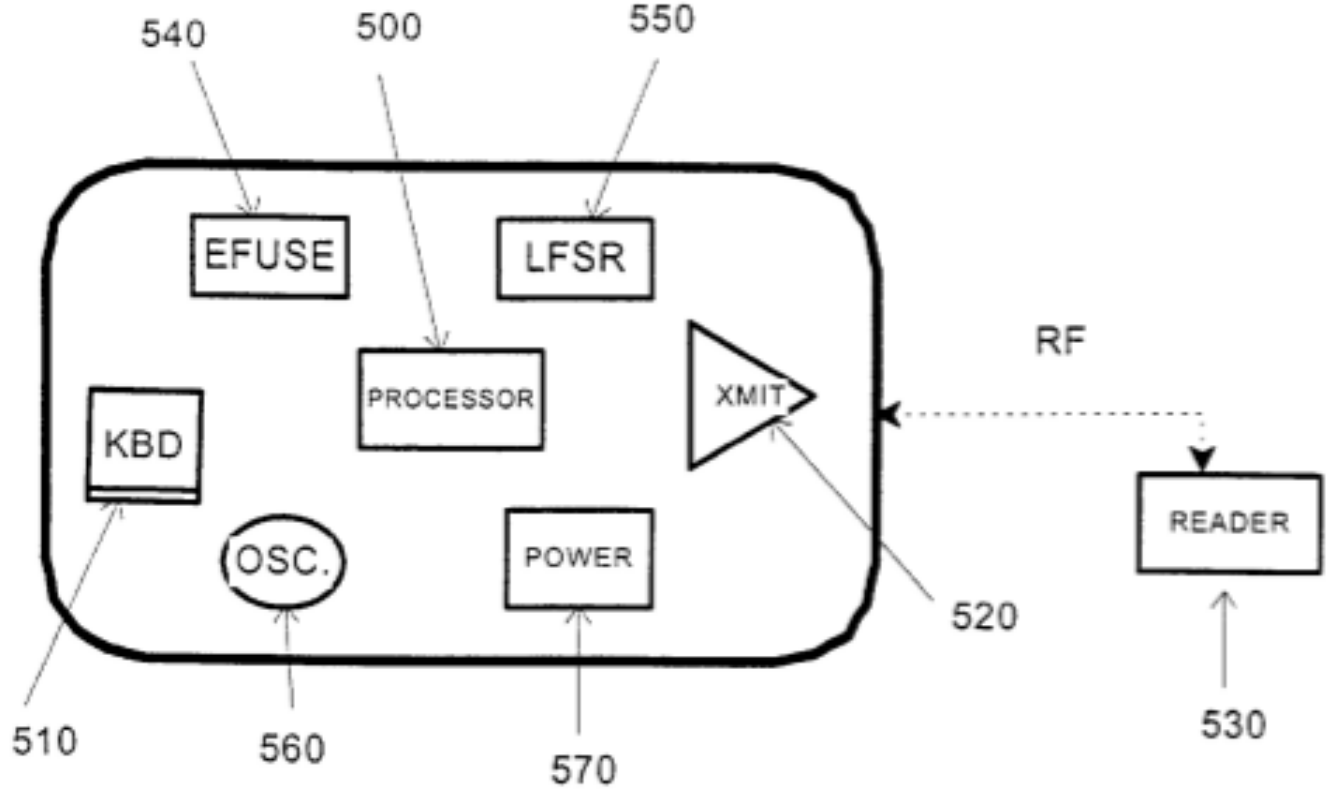
ST16SF48A high-security chip imaged by a confocal microscope

Protections Against FIA: a Classification



A Secure Credit Card in 2001

E.E. Kelley, F. Motika, P.V. Motika, and E.M. Motika, Secure credit card, November 4 2003, "US Patent 6,641,050"



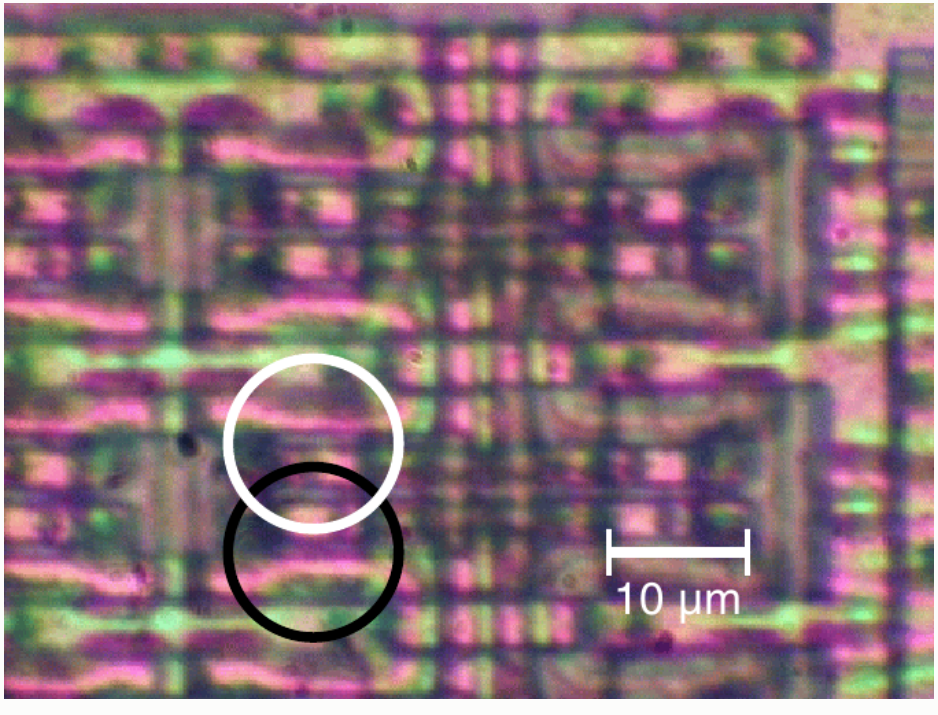
Clock (560) and power (570) generators: Welcome aboard!

Removing of attack paths!

The Dark Side of the Force

Sergei P. Skorobogatov and Ross J. Anderson, Optical Fault Induction Attacks, Cryptographic Hardware and Embedded Systems - CHES 2002, Lecture Notes in Computer Science, vol. 2523, Springer Berlin Heidelberg, 2003, pp. 2–12 (English)

Optical fault induction attack



Illumination of the white (or black) circle causes the SRAM cell (PIC 16F84, 1996, $\geq$350 nm) to change its state from ‘1’ to ‘0’ (or ‘0’ to ‘1’)

Low-cost Protections

Oliver Kömmerling and Markus G. Kuhn, Design principles for tamper-resistant smartcard processors,), USENIX Association, 1999

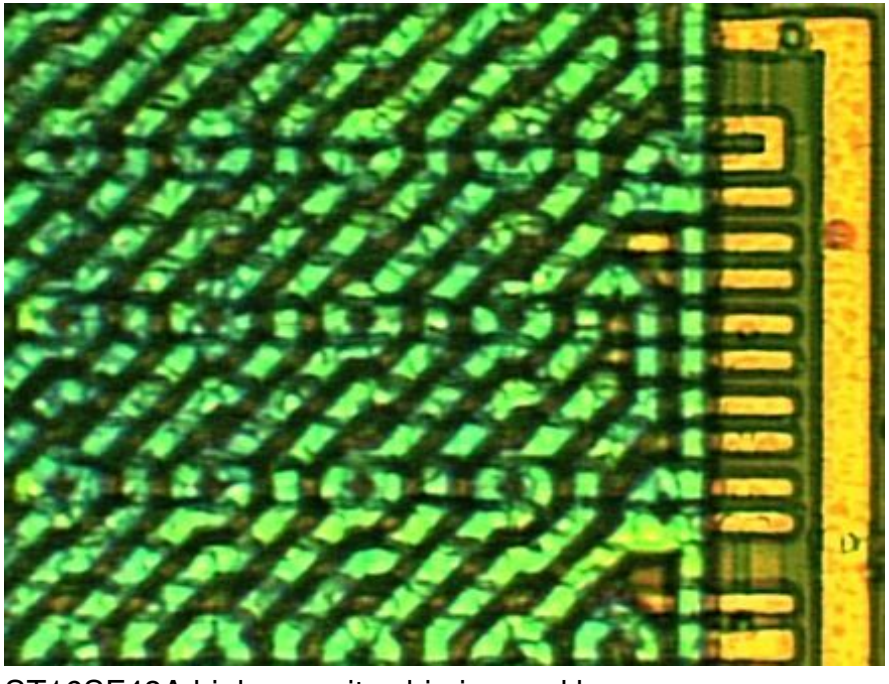
3.1 Randomized clock signal

- random insertion of dummy cycles + dummy activity
- jitter on clock cycle

3.2 Randomized multithreading

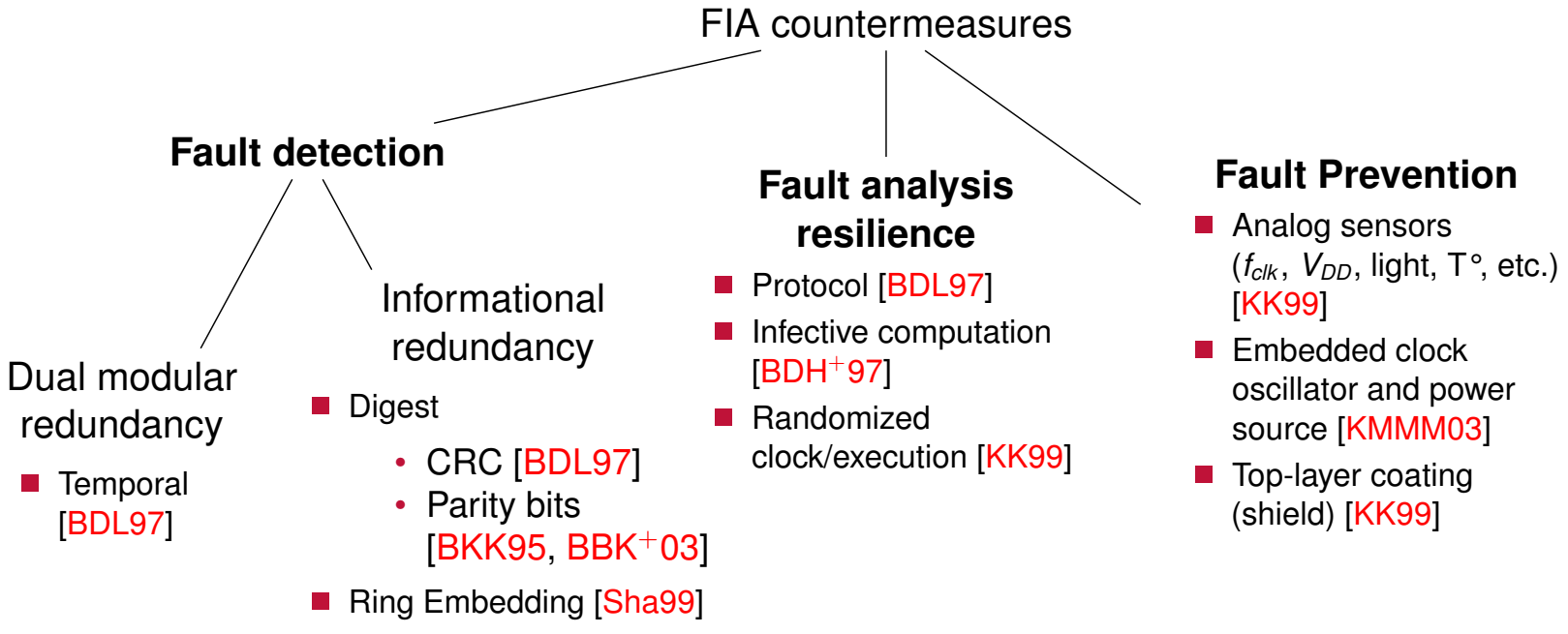
- Analog sensors (f_{clk}, V_{DD}, light, T°, etc.)

3.6 Top-layer Sensor Meshes



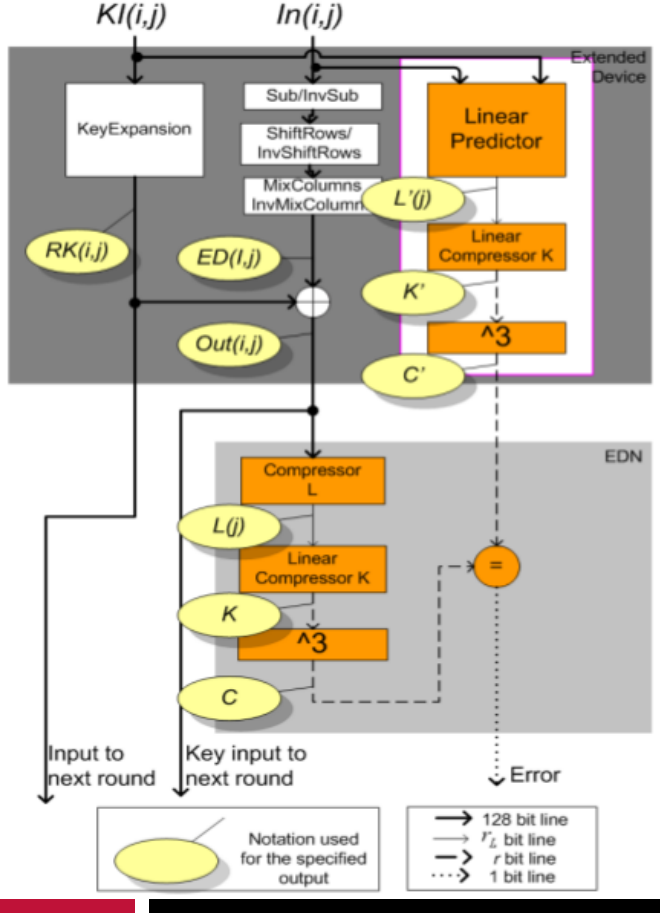
ST16SF48A high-security chip imaged by a confocal microscope

Protections Against FIA: a Classification



Robust Non-linear Codes

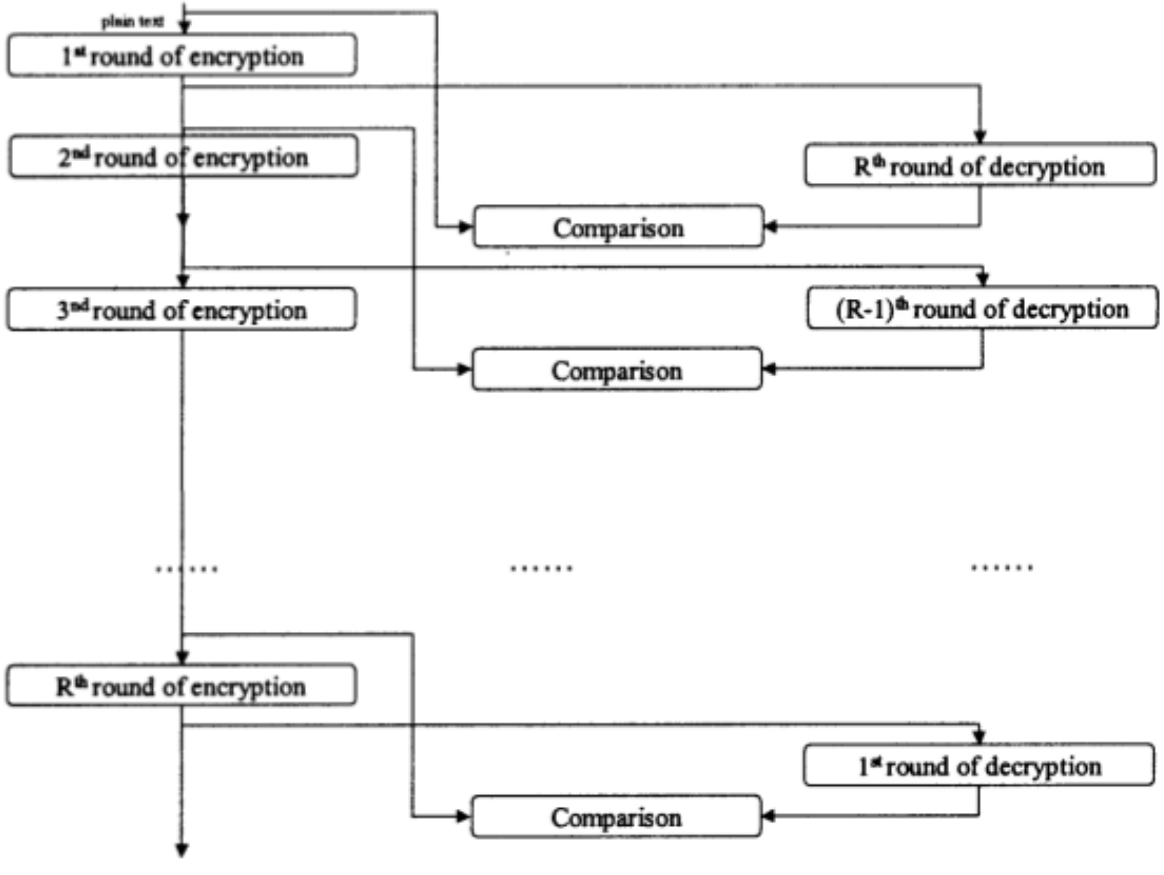
Mark G. Karpovsky, Konrad J. Kulikowski, and Alexander Taubin, Robust protection against fault-injection attacks on smart cards implementing the advanced encryption standard, 2004 International Conference on Dependable Systems and Networks (DSN 2004), 28 June - 1 July 2004, Florence, Italy, Proceedings, IEEE Computer Society, 2004, pp. 93–101



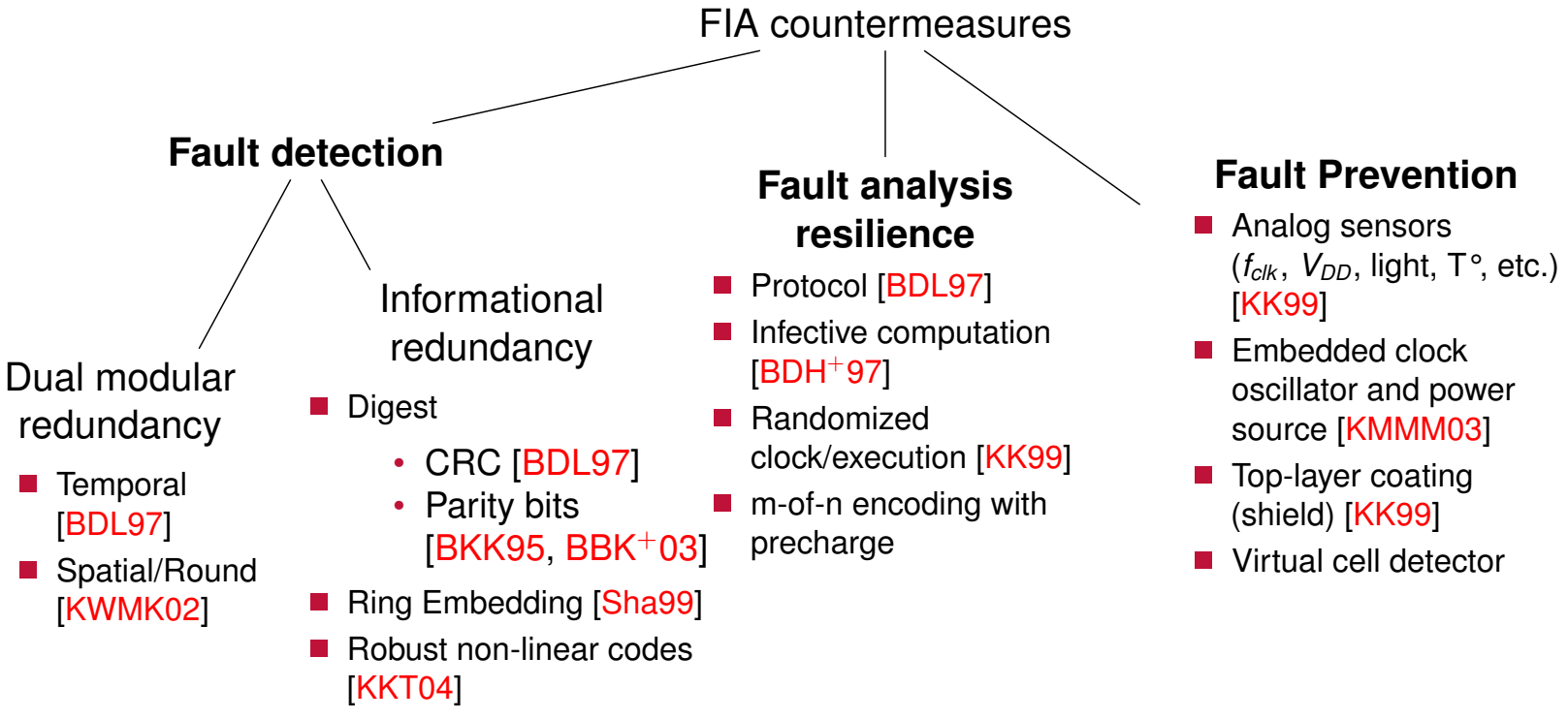
- Error coverage
  - linear: 2^{-r}
  - non-linear: 2^{-2r}
- Two cubic networks
- $r = 28 \rightarrow$ 77 % area overhead

Concurrent Error Detection at Round Level

Ramesh Karri, Kaijie Wu, Piyush Mishra, and Yongkook Kim, Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers, IEEE Trans. on CAD of Integrated Circuits and Systems **21** (2002), no. 12, 1509–1517

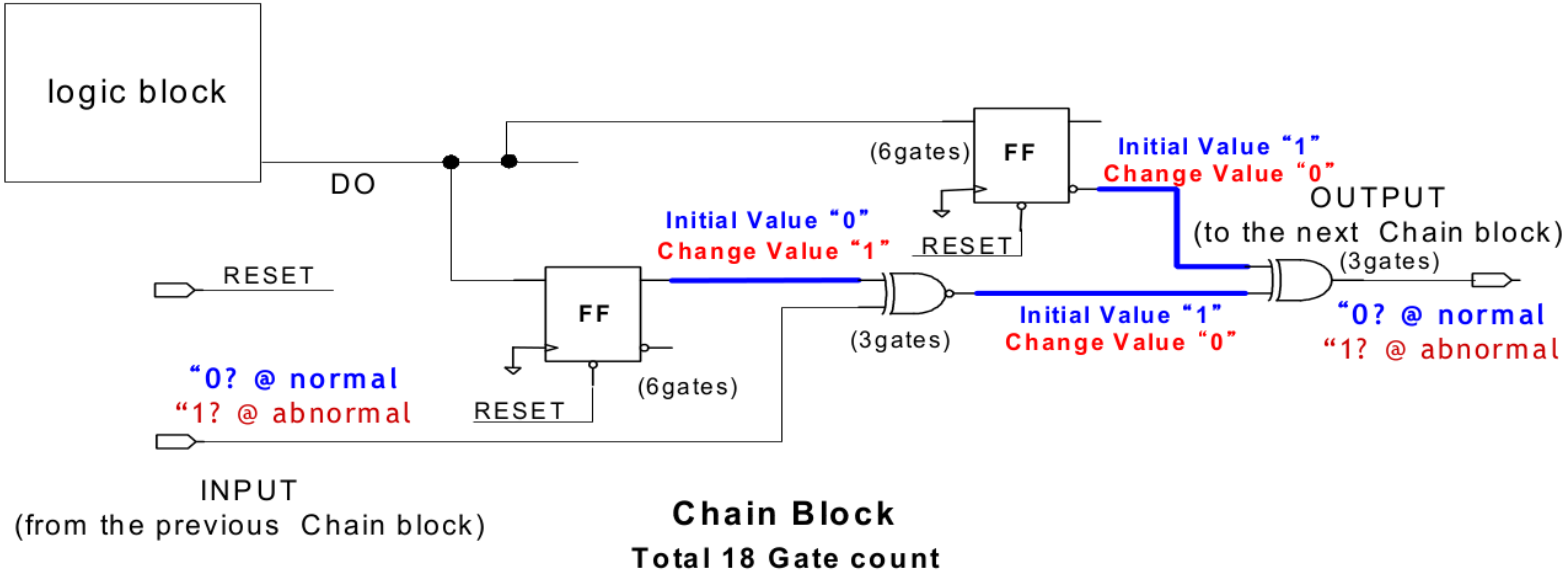


Protections Against FIA: a Classification



Virtual Cell detector

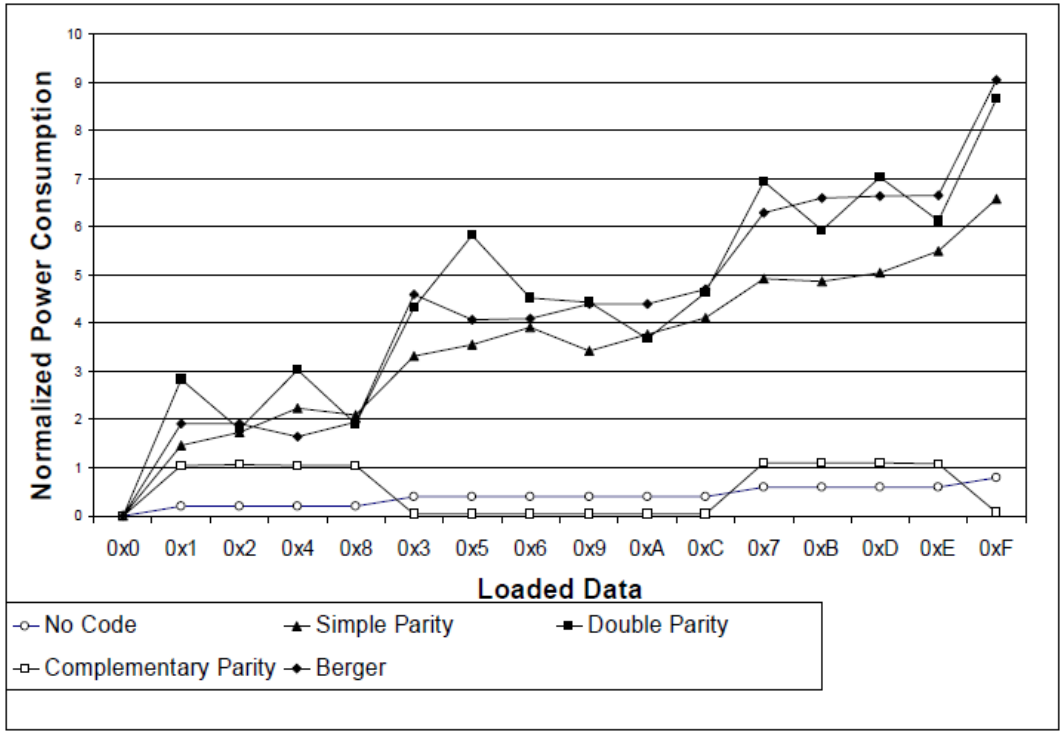
SAMSUNG DIGITall – FDTC 2007



- After reset, each cell output is ’0 or ’1
- Chain of dual-rail FF, with alarm propagation

Redundancy Makes SCA Easier

Vincent Maingot and Régis Leveugle, Error detection code efficiency for secure chips, 13th IEEE International Conference on Electronics, Circuits, and Systems, ICECS 2006, Nice, France, December 10-13, 2006, IEEE, 2006, pp. 561–564



"It is indeed useless to protect a circuit against only one type of attack since the hacker will use the easiest possible attack leading to the expected secret disclosure."

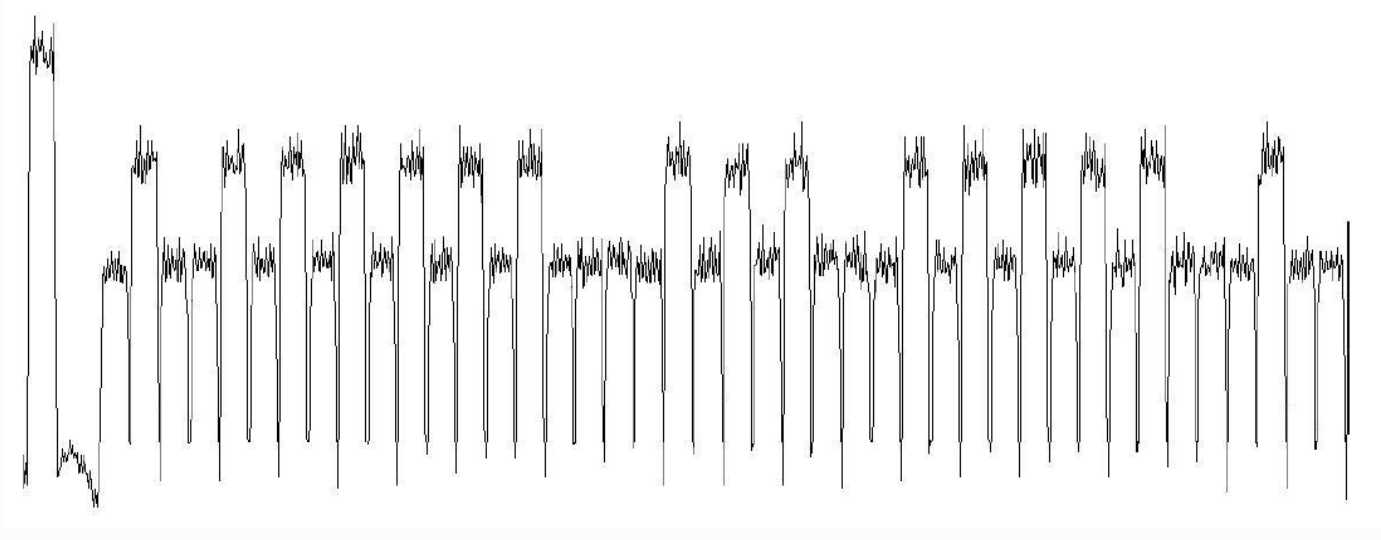
Redundancy vs PACA

Frédéric Amiel, Karine Villegas, Benoît Feix, and Louis Marcel,

Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel Analysis,

FDTC, IEEE Computer Society, 10 September 2007, Vienna, Austria, pp. 92–102

PACA on atomic S&M ($R_0 = R_0 \times R_k$) w/ redundancy

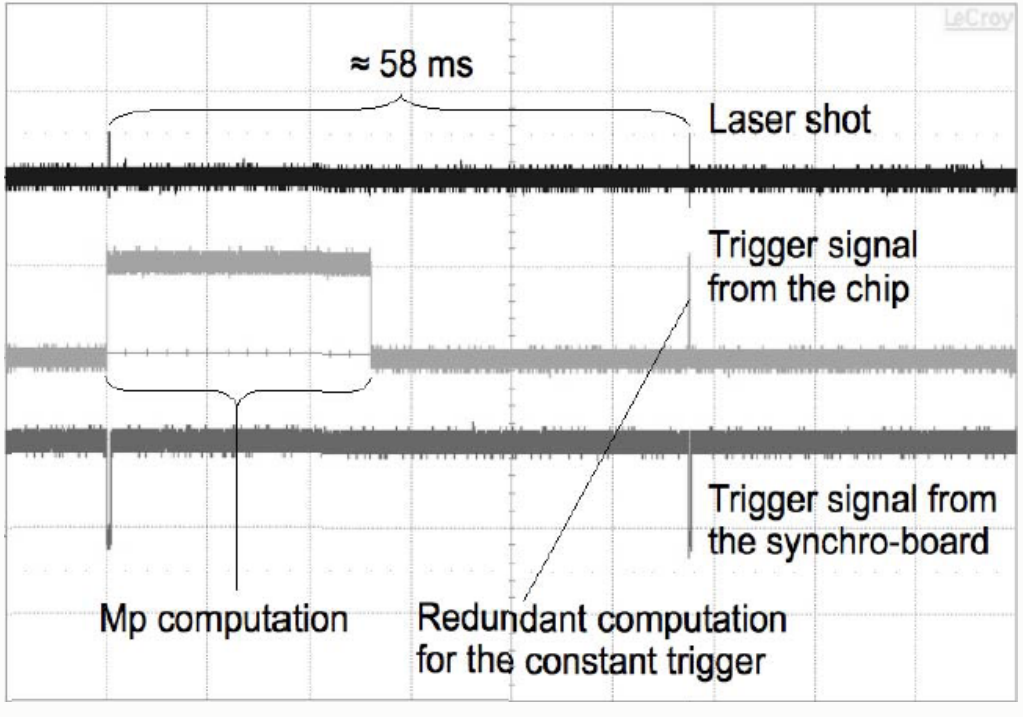


"The fault is detected at the end of the command. Unfortunately, this is too late, even if the result is not returned."

How Does Redundancy Resist HO-FIA ?

Elena Trichina and Roman Korkikyan, Multi fault laser attacks on protected CRT-RSA,), IEEE Computer Society, 2010, pp. 75–86

20-FIA on check and infective countermeasures

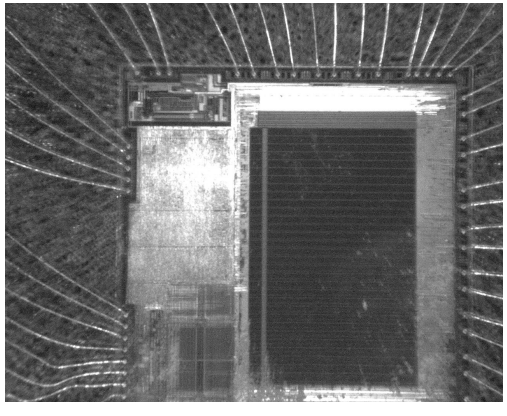


- 32-bit ARM Cortex M3
- Laser reload: 200 ms

Pros & Cons of Laser Fault Injection (1/2)

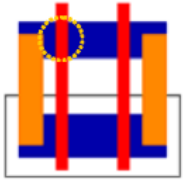
Michel Agoyan, Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, Anne-Lise Ribotta, and Assia Tria, How to flip a bit?, 16th IEEE International On-Line Testing Symposium (IOLTS) 2010), 5-7 July, 2010, Corfu, Greece, IEEE Computer Society, 2010, pp. 235–239

✔ Effect highly local. . .



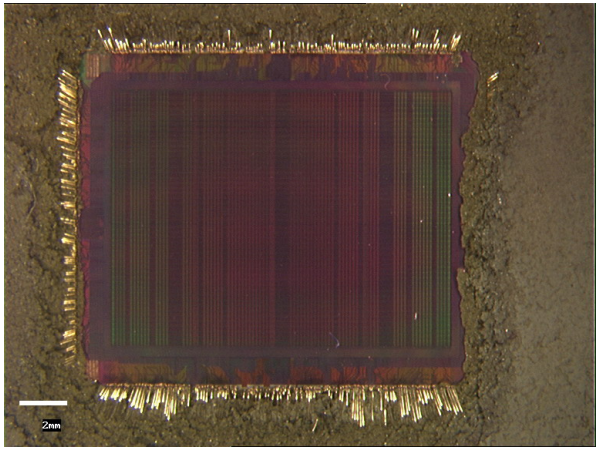
5 µm laser beam on ATmega128 chip

✖ . . .for all technology nodes ?

	Transistor	SRAM Cell
350nm		
130nm		
90nm		
65nm		

Pros & Cons of Laser Fault Injection (2/2)

- ✖ Sample preparation (depackaging, backside thinning, etc.) quite delicate



Stratix Altera FPGA

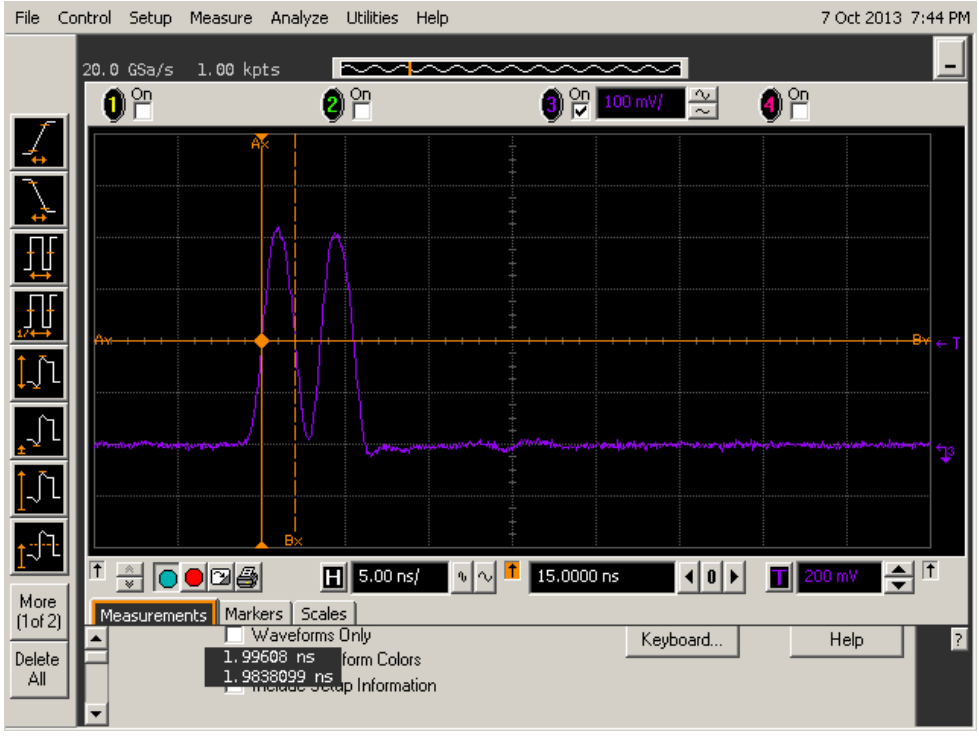
- ✖ High cost
- ✖ Hard to use against FPGA
  - no standing-out area (regular matrix)
  - permanent faults (modification of the FPGA configuration) [CLC+09]

Fault Injection Using Radiated EM Pulses

Assumed Benefits

- no sample preparation
- medium cost
- efficient on FPGA
- effect rather local

EM Multi-glitch Injection @ 250 MHz



How do the defense strategies resist HO-FIA ?

- Fault detection (bis)
- o Fault Prevention
- \+ Fault analysis resilience

Presentation Outline

Introduction to Fault Injection Attack

Countermeasures Against Fault Injection Attack

Fault Analysis on Data Encryption Standard (DES)

À vous de jouer !

Documents supports

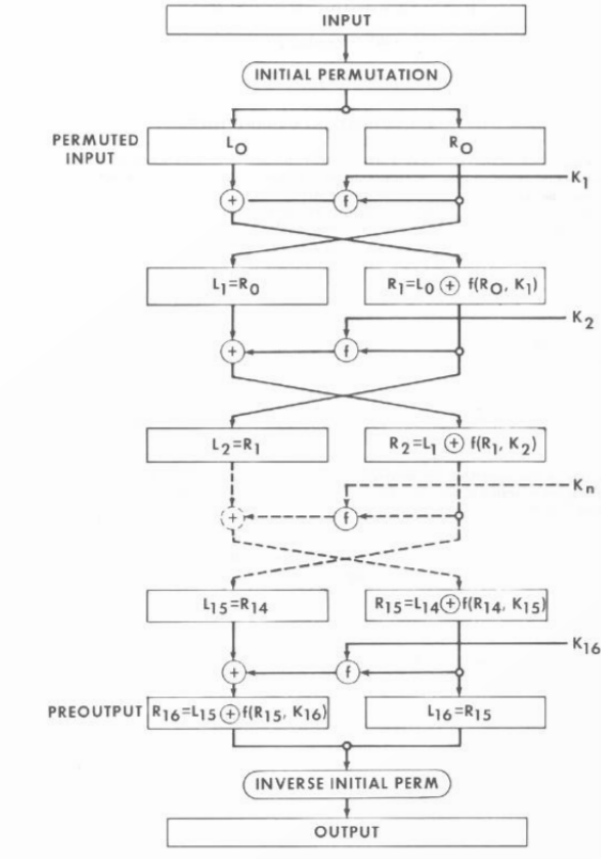
Contenu de l'archive `DFA_DES.zip` :

`fips46-3.pdf`	La publication du FIPS décrivant DES
`des_block.pyc`	Classe python DES
`des_block_demo.py`	Démo utilisation de `des_block`
`DFA_DES_challenges.pyc`	Les paramètres des challenges
`DFA_DES_elev.py`	Code minimal à compléter

Data Encryption Standard (DES) [Nat77]

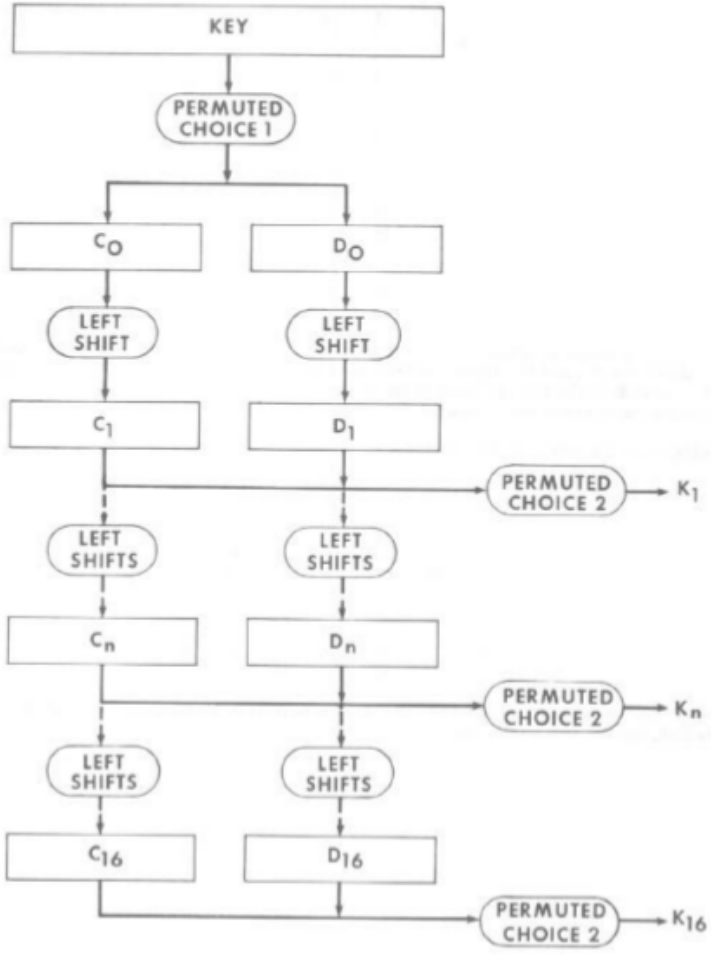
Iterative Feistel Scheme

$$C = \mathrm{IP}^{-1} \circ \left(\bigcirc_{r=1}^{16} \mathrm{F}_{k_r} \right) \circ \mathrm{IP}\,(P)$$



Data Encryption Standard (DES) [Nat77]

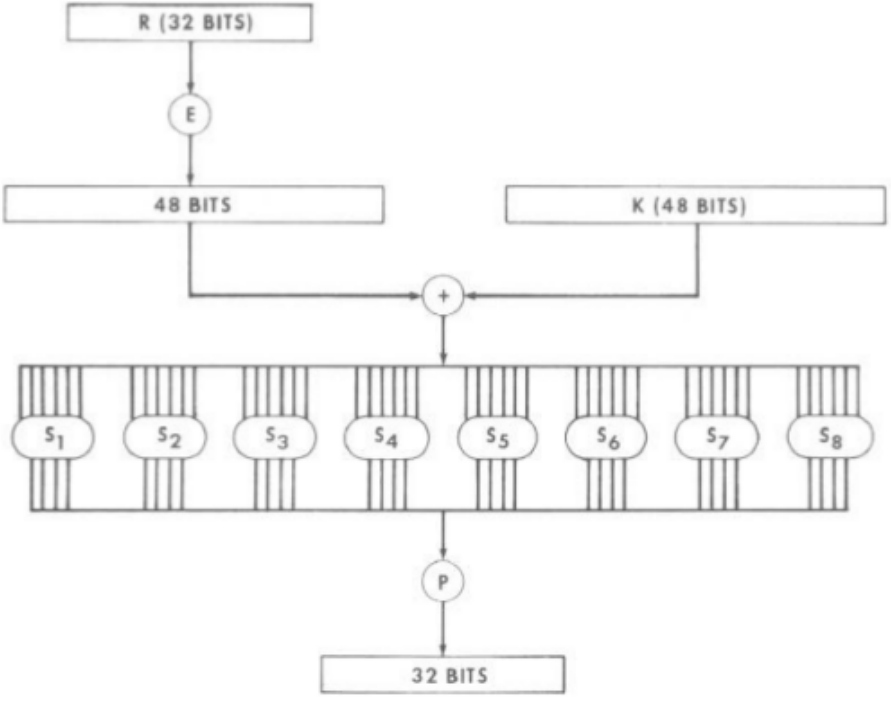
Key Scheduling



Data Encryption Standard (DES) [Nat77]

The Feistel function F

- Expansion (E) from 32 bits to 48 bits
- Key mixing
- Substitution (S_{1-8})
- Permutation (P)



À vous de jouer !

Simple Fault Analysis

Défi 1 : SFA sur chiffrement avorté

- Faute : une seule itération du calcul de la fonction de Feistel (puis IP^{-1})
- $P = \texttt{0x0000000000000000}$ et $C' = \texttt{0x0000000000000000}$

Q1 Donner les sous-clés candidates pour $K_{1,1}$.

Q2 En supposant que le nombre de sous-clés candidates est le même pour les autres $K_{1,i}$, donner le nombre de clés candidates pour K_1.

Q3 En déduire le nombre de bits restant à trouver.

À vous de jouer !

Simple Fault Analysis

Défi 2 : SFA sur chiffrement avorté

- La clé de chiffrement est la même que précédemment.
- La faute est également la même, mais l'attaquant :
  - envoie $P = \texttt{0xffffffffffffffff}$;
  - récupère $C' = \texttt{0xffffffffffffffff}$.

Q1 Exprimer l'équation générale en sortie d'une boîte S_i en fonction de R_r et L_r, avec :
- $i \in \{1, \ldots, 8\}$ le numéro de la boîte S ;
- $r \in \{1, \ldots, 16\}$ le numéro du tour.

Q2 En déduire l'équation en sortie de la boîte S_1.

Q3 Donner les nouvelles sous-clés candidates pour $K_{1,1}$.

Q4 À l'aide des résultats du défi précédent, en déduire $K_{1,1}$.

À vous de jouer !

Simple Fault Analysis

Défi 3 : SFA sur calcul des sous-clés avorté

- Faute : une seule itération du calcul des sous-clés (K_2 à K_{16} sont nulles)
- $P = \texttt{0x0000000000000000}$ et $C' = \texttt{0xffffffffffffffff}$

Q1 Donner les sous-clés candidates pour chaque boîte S.

À vous de jouer !

Differential Fault Analysis

TD : théorie de la DFA sur DES

- **Q1** Donner l'équation de R_{16} en fonction de R_{15} et L_{15}.
- **Q2** Même question lorsque l'entrée du 16^{e} tour est fautée ($R_{15} \rightarrow R'_{15}$, $L_{15} \rightarrow L'_{15}$ et $R_{16} \rightarrow R'_{16}$).
- **Q3** En déduire et donner l'équation différentielle de $\Delta R_{16} = R_{16} \oplus R'_{16}$.
- **Q4** Donner la liste des inconnues, expliquer pourquoi l'attaque n'est pas possible, et proposer une solution.
- **Q5** Donner la nouvelle équation simplifiée.

À vous de jouer !

Differential Fault Analysis

Défi 4 : DFA au 16e tour sur une boîte S

- $C = \texttt{0x2462db7fdc0060da}$ et $C' = \texttt{0x2467db7fdc00e0ca}$

Q1 Donner l'équation différentielle en sortie de boîte $S1$.

Q2 Chercher puis donner les candidates pour la sous-clé $K_{16,1}$.

À vous de jouer !

Differential Fault Analysis

Défi 5 : DFA au 16e tour sur une boîte S

- La clé de chiffrement et la boîte S fautée sont les mêmes que précédemment
- $C = \texttt{0x1ef932fcde59e25e}$ et $C' = \texttt{0x1efd32fcded9625a}$

Q1 Chercher puis donner la valeur de la sous-clé $K_{16,1}$.

À vous de jouer !

Differential Fault Analysis

Défi 6 : DFA entière

- Liste de 12 couples (C, C')
- Fautes injectées dans R_{16}

Q1 Réaliser une DFA pour extraire la valeur de K_{16}

Q2 En déduire et donner la valeur de la clé maître *KEY*

References I

[ADM+10] Michel Agoyan, Jean-Max Dutertre, Amir-Pasha Mirbaha, David Naccache, Anne-Lise Ribotta, and Assia Tria, How to flip a bit ?, 16th IEEE International On-Line Testing Symposium (IOLTS) 2010), 5-7 July, 2010, Corfu, Greece, IEEE Computer Society, 2010, pp. 235–239.

[AK96] Ross J. Anderson and Markus G. Kuhn, Tamper Resistance – a Cautionary Note, In Proceedings of the Second USENIX Workshop ON Electronic Commerce, November 18-21 1996, Oakland, California. ISBN 1-880446-83-9, pp. 1–11.

[AVFM07] Frédéric Amiel, Karine Villegas, Benoît Feix, and Louis Marcel, Passive and Active Combined Attacks: Combining Fault Attacks and Side Channel FDTC, IEEE Computer Society, 10 September 2007, Vienna, Austria, pp. 92–102.

[BBB+11] Alessandro Barenghi, Guido Marco Bertoni, Luca Breveglieri, Gerardo Pelosi, and Andrea Palomba, Fault attack to the elliptic curve digital signature algorithm wit multiple bit faults,), ACM, 2011, pp. 63–72.

References II

[BBK+03] Guido Bertoni, Luca Breveglieri, Israel Koren, Paolo Maistri, and Vincenzo Piuri,
Error Analysis and Detection Procedures for a Hardware Implementation of the Adv
IEEE Trans. Computers **52** (2003), no. 4, 492–505.

[BBK16] Nina Bindel, Johannes A. Buchmann, and Juliane Krämer, Lattice-based signature schemes and their sensitivity to fault attacks, 2016 Workshop on Fault Diagnosis and Tolerance in Cryptography, FDTC 2016, Santa Barbara, CA, USA, August 16, 2016, IEEE Computer Society, 2016, pp. 63–77.

[BDH+97] Feng Bao, Robert H. Deng, Yongfei Han, Albert B. Jeng, A. Desai Narasimhalu, and Teow-Hin Ngair,
Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence
), Lecture Notes in Computer Science, vol. 1361, Springer, 1997, pp. 115–124.

[BDL97] Dan Boneh, Richard A. DeMillo, and Richard J. Lipton, On the importance of checking cryptographic protocols for faults (extended abstract),), Lecture Notes in Computer Science, vol. 1233, Springer, 1997, pp. 37–51.

References III

[BKK95] Adrian S. Butter, Chang Y. Kao, and James P. Kuruts, Des encryption and decryption unit with error checking, July 11 1995, US Patent 5,432,848A.

[BS97] Eli Biham and Adi Shamir, Differential Fault Analysis of Secret Key Cryptosystems, CRYPTO, LNCS, vol. 1294, Springer, August 1997, Santa Barbara, California, USA. DOI: 10.1007/BFb0052259, pp. 513–525.

[CLC+09] G. Canivet, R. Leveugle, J. Clediere, F. Valette, and M. Renaudin, Characterization of Effective Laser Spots during Attacks in the Configuration of a V VLSI Test Symposium, 2009. VTS '09. 27th IEEE, 2009, pp. 327–332.

[KK99] Oliver Kömmerling and Markus G. Kuhn, Design principles for tamper-resistant smartcard processors,), USENIX Association, 1999.

[KKT04] Mark G. Karpovsky, Konrad J. Kulikowski, and Alexander Taubin, Robust protection against fault-injection attacks on smart cards implementing the advanced encryption standard, 2004 International Conference on Dependable Systems and Networks (DSN 2004), 28 June - 1 July 2004, Florence, Italy, Proceedings, IEEE Computer Society, 2004, pp. 93–101.

References IV

[KMMM03] E.E. Kelley, F. Motika, P.V. Motika, and E.M. Motika, Secure credit card, November 4 2003, "US Patent 6,641,050".

[KWMK02] Ramesh Karri, Kaijie Wu, Piyush Mishra, and Yongkook Kim, Concurrent error detection schemes for fault-based side-channel cryptanalysis of symmetric block ciphers, IEEE Trans. on CAD of Integrated Circuits and Systems **21** (2002), no. 12, 1509–1517.

[ML06] Vincent Maingot and Régis Leveugle, Error detection code efficiency for secure chips, 13th IEEE International Conference on Electronics, Circuits, and Systems, ICECS 2006, Nice, France, December 10-13, 2006, IEEE, 2006, pp. 561–564.

[Nat77] National Institute of Standards and Technology, FIPS PUB 46: Data encryption standard (des), Jan 1977.

[PQ03] Gilles Piret and Jean-Jacques Quisquater, A differential fault attack technique against SPN structures, with application to the AES and KHAZAD,), Lecture Notes in Computer Science, vol. 2779, Springer, 2003, pp. 77–88.

References V

[SA03] Sergei P. Skorobogatov and Ross J. Anderson, Optical Fault Induction Attacks, Cryptographic Hardware and Embedded Systems - CHES 2002, Lecture Notes in Computer Science, vol. 2523, Springer Berlin Heidelberg, 2003, pp. 2–12 (English).

[Sha99] A. Shamir, Method and apparatus for protecting public key schemes from timing and fault attacks, November 23 1999, US Patent 5,991,415.

[TK10] Elena Trichina and Roman Korkikyan, Multi fault laser attacks on protected CRT-RSA,), IEEE Computer Society, 2010, pp. 75–86.

[TMA11] Michael Tunstall, Debdeep Mukhopadhyay, and Subidh Ali, Differential fault analysis of the advanced encryption standard using a single fault,), Lecture Notes in Computer Science, vol. 6633, Springer, 2011, pp. 224–233.