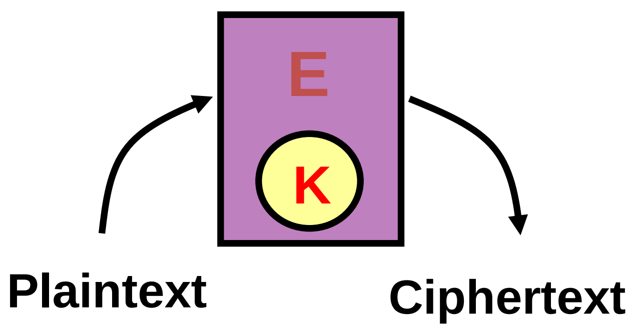
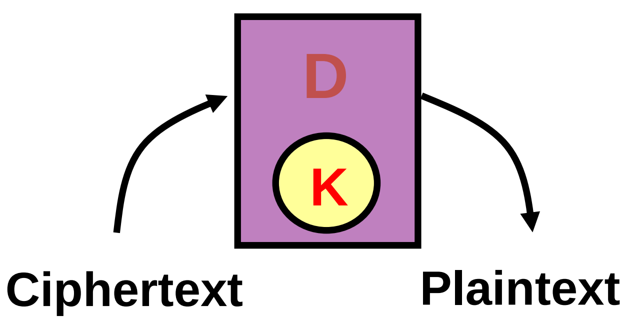
Week 7: Cryptanalysis

Block Cipher – Attack Scenarios

- Attacks on encryption schemes
  - Ciphertext only attack: only ciphertexts are given
  - Known plaintext attack: (plaintext, ciphertext) pairs are given
  - Chosen plaintext attack: (chosen plaintext, corresponding ciphertext) pairs
  - Adaptively chosen plaintext attack
  - Chosen ciphertext attack: (chosen ciphertext, corresponding plaintext) pairs
  - Adaptively chosen ciphertext attack



Encryption Oracle



Decryption Oracle

Cryptanalysis of Block Ciphers

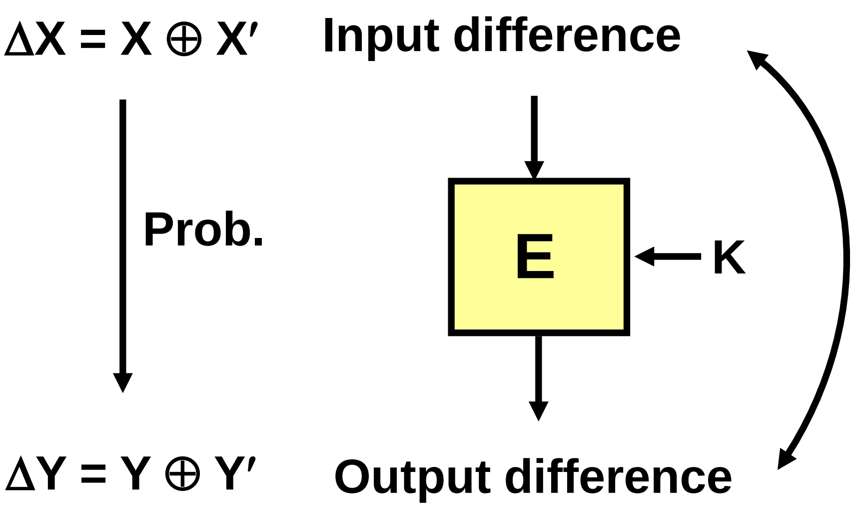
- **Statistical Cryptanalysis**
  - **Differential cryptanalysis (DC)**
  - **Linear Cryptanalysis (LC)**
  - **Various key schedule cryptanalysis**
- **Algebraic Cryptanalysis**
  - **Interpolation attacks, etc.**
- **Side Channel Cryptanalysis**
  - **timing attacks**
  - **differential fault analysis**
  - **differential power analysis, etc.**

Differential Cryptanalysis

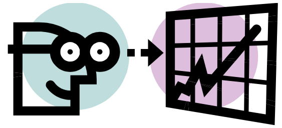
Cryptanalysis of Block Ciphers - DC


- **Differential Cryptanalysis**
  - ✓ **E. Biham and A. Shamir : Crypto90, Crypto92**
    - ✓ **Chosen plaintext attack, O(Breaking DES_{16} ~ 2^{47})**
  - ✓ **Look for correlations in Round function input and output (DES : 2^{47})**
    - **high-probability differentials, impossible differentials**
    - **truncated differentials, higher-order differentials**

* E.Biham, A. Shamir,"Differential Cryptanalysis of the Data Encryption Standard", Springer-Verlag, 1993



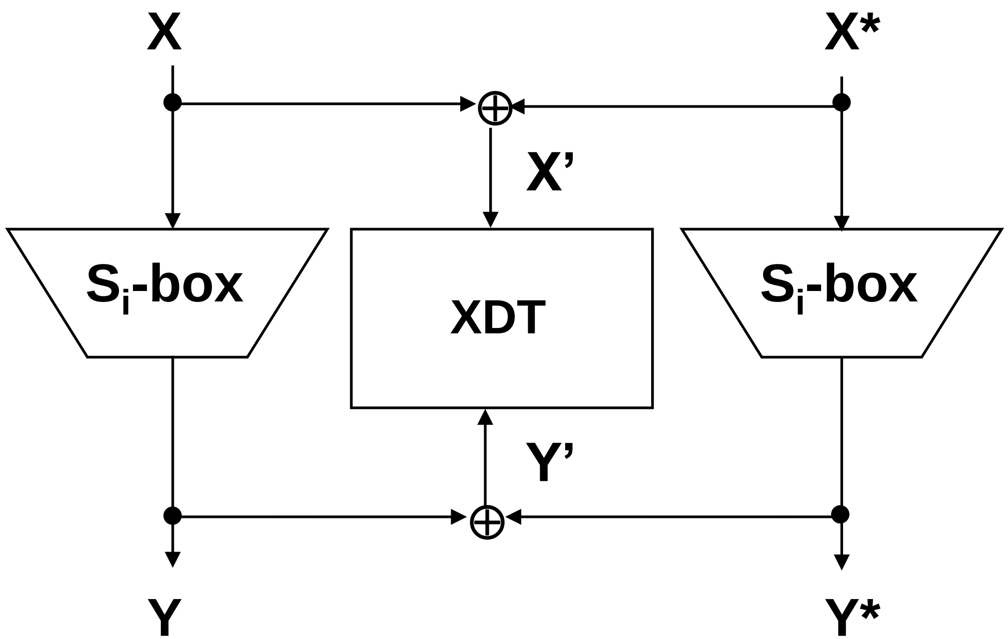
Statistically non-uniform probability distribution: higher prob. for some fixed pattern ΔX & ΔY



DC on DES

- {E,P,IP} : (Discard linear components(IP, FP)
- Properties of XOR ($X' = X \oplus X^*$)
  - $P(X))' = P(X) \oplus P(X^*) = P(X')$
  - XOR : $(X \oplus Y)' = (X \oplus Y) \oplus (X^* \oplus Y^*) = X' \oplus Y'$
  - Mixing key : $(X \oplus K)' = (X \oplus K) \oplus (X^* \oplus K) = X'$
  - Differences(=xor) are linear in linear operation and in particular the result is ***key independent***.

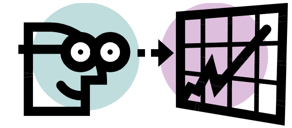
XOR Distribution Table



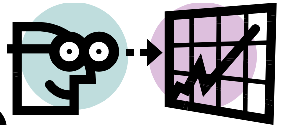
- X' = {0,1,…63}, Y'= {0,1,…15}
- For a given S-box, pre-compute the number of count of X' and Y' in a table

* % of entry in DES S-boxes : 75 ~ 80%

XOR Distribution Table of S4 box

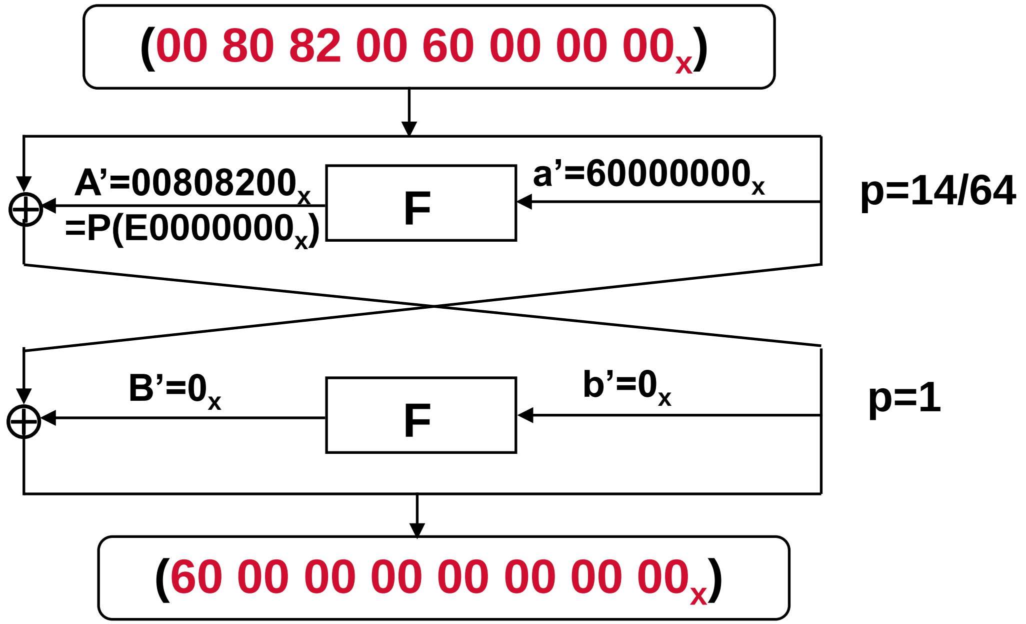


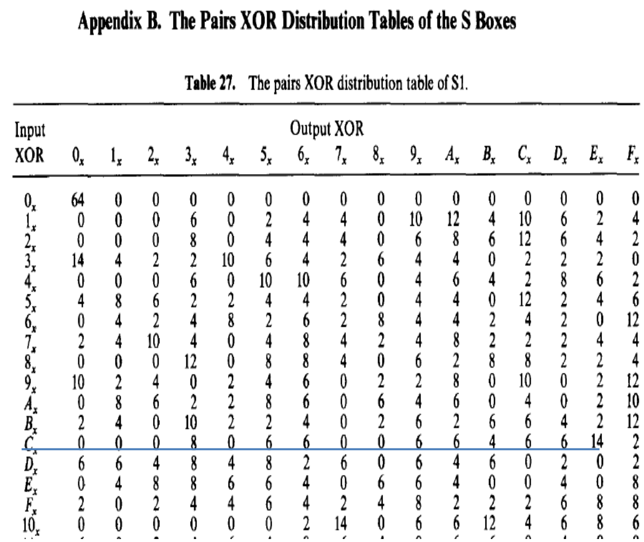
Input	Output XOR															
XOR	0x	1x	2x	3x	4x	5x	6x	7x	8x	9x	Ax	Bx	Cx	Dx	Ex	Fx
0x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1x	0	0	0	0	0	16	16	0	0	16	16	0	0	0	0	0
2x	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
3x	8	6	2	0	2	4	8	2	6	0	4	6	0	6	2	8
4x	0	0	0	8	0	0	12	4	0	12	0	4	8	4	4	8
5x	4	2	2	8	2	12	0	2	2	0	12	2	8	2	2	4
6x	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
7x	4	2	6	4	6	0	16	6	2	0	0	2	4	2	6	4
8x	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
9x	8	4	4	4	4	0	8	4	4	0	0	4	4	4	4	8
Ax	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
Bx	0	12	0	8	0	0	0	0	12	0	0	12	8	12	0	0
Cx	0	0	0	4	0	8	4	8	0	4	8	8	4	8	8	0
Dx	8	4	4	4	4	0	0	4	4	8	0	4	4	4	4	8
Ex	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
Fx	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
10x	0	0	0	0	0	8	12	4	0	12	8	4	0	4	4	8
11x	4	2	2	16	2	4	0	2	2	0	4	2	16	2	2	4
12x	0	0	0	8	0	4	4	8	0	4	4	8	8	8	8	0
13x	8	2	6	0	6	4	0	6	2	8	4	2	0	2	6	8
14x	0	8	8	0	8	0	8	0	8	8	0	0	0	0	0	16
15x	8	4	4	0	4	8	0	4	4	0	8	4	0	4	4	8
16x	0	8	8	4	8	8	0	0	8	0	8	0	4	0	0	8
17x	4	6	2	4	2	0	0	2	6	16	0	6	4	6	2	4
18x	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
19x	4	4	4	0	4	4	16	4	4	0	4	4	0	4	4	4
1Ax	0	6	6	4	6	0	4	6	6	4	0	6	4	6	6	0
1Bx	0	6	6	4	6	4	0	6	6	0	4	6	4	6	6	0
1Cx	0	8	8	8	8	4	0	0	8	0	4	0	8	0	0	8
1Dx	4	4	4	0	4	4	0	4	4	16	4	4	0	4	4	4
1Ex	0	6	6	0	6	4	4	6	6	4	4	6	0	6	6	0
1Fx	0	0	12	8	12	0	0	12	0	0	0	0	8	0	12	0



Differential Characteristic

- 2-round characteristic in S_1 box $(0C_x \text{ --> } E_x$ with 14/64)





Appendix B. The Pairs XOR Distribution Tables of the S Boxes

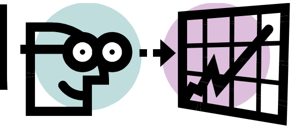
Table 27. The pairs XOR distribution table of S1.

Input XOR	Output XOR 0_x	1_x	2_x	3_x	4_x	5_x	6_x	7_x	8_x	9_x	A_x	B_x	C_x	D_x	E_x	F_x
0_x	64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1_x	0	0	0	6	0	2	4	4	0	10	12	4	10	6	2	4
2_x	0	0	0	8	0	4	4	4	0	6	8	6	12	6	4	2
3_x	14	4	2	2	10	6	4	2	6	4	4	0	2	2	2	0
4_x	0	0	0	6	0	10	10	6	0	4	6	4	2	8	6	2
5_x	4	8	6	2	2	4	4	2	0	4	4	0	12	2	4	6
6_x	0	4	2	4	8	2	6	2	8	4	4	2	4	2	0	12
7_x	2	4	10	4	0	4	8	4	2	4	8	2	2	2	4	4
8_x	0	0	0	12	0	8	8	4	0	6	2	8	8	2	2	4
9_x	10	2	4	0	2	4	6	0	2	2	8	0	10	0	2	12
A_x	0	8	6	2	2	8	6	0	6	4	6	0	4	0	2	10
B_x	2	4	0	10	2	2	4	0	2	6	2	6	6	4	2	12
C_x	0	0	0	8	0	6	6	0	0	6	6	4	6	6	14	2
D_x	6	6	4	8	4	8	2	6	0	6	4	6	0	2	0	2
E_x	0	4	8	8	6	6	4	0	6	6	4	0	0	4	0	8
F_x	2	0	2	4	4	6	4	2	4	8	2	2	2	6	8	8
10_x	0	0	0	0	0	0	2	14	0	6	6	12	4	6	8	6

60_x (0110_b) after EXP -> $0C_x$=001100_b to S1-box

➔1110_b (E_x) after P -> 00808200_x

Searching Way for round keys



(1) Choose suitable Plaintext (Pt) XOR.

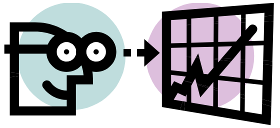
(2) Get 2 Pts for a chosen Pt and obtain the corresponding Ct by encryption

(3) From Pt XOR and pair of Ct, get the expected output XOR for the S-boxes of final round.

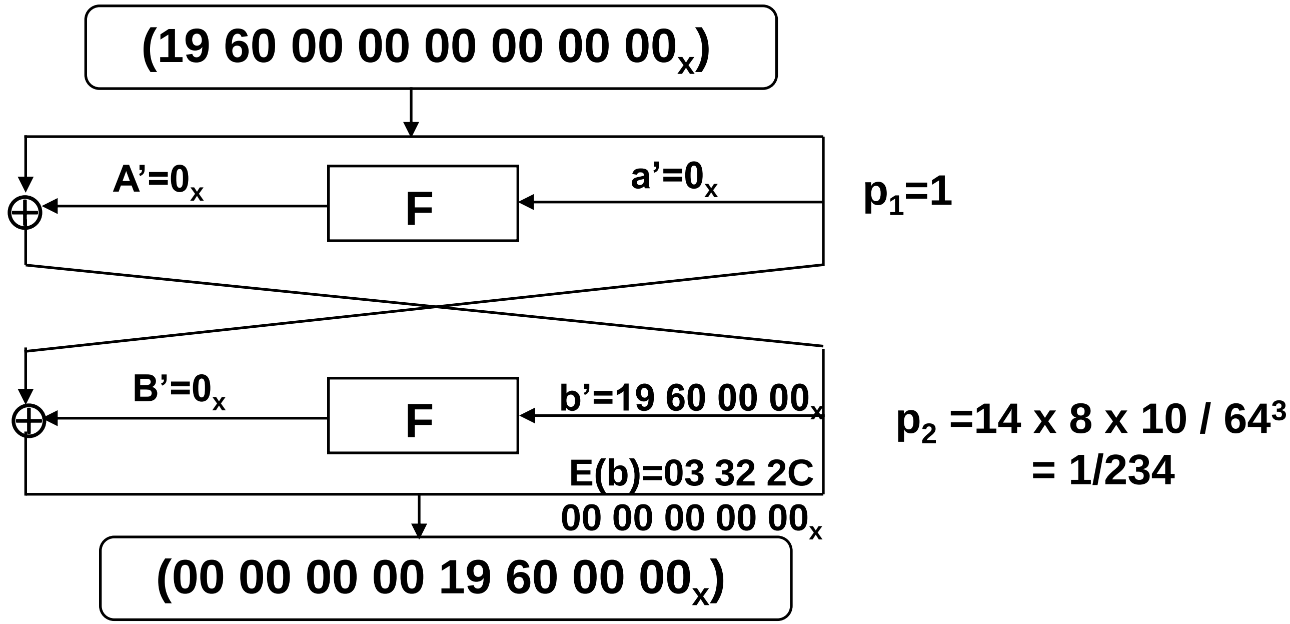
(4) Count the maximum potential key at the final round using the estimated key

(5) Right key is a subkey of having large number of pairs of expected output XOR

Iterative Characteristic



- Self-concatenating probability
- Best iterative char. of DES

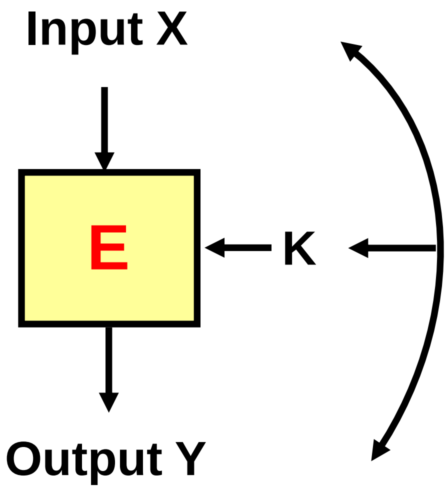


Linear Cryptanalysis

Cryptanalysis of Block Ciphers - LC

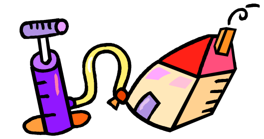
- ***Linear Cryptanalysis***
  - ✓ **Matsui : Eurocrypt93, Crypto94**
  - ✓ **Known Plaintext Attack, O(Breaking DES_{16}) ~ 2^{43}**
  - ✓ **Look for correlations between key and cipher input and output**
    - **linear approximation, non-linear approximation,**
    - **generalized I/O sums, partitioning cryptanalysis**

* M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Proc. of Eurocrypt'93,LNCS765, pp.386-397



Linear equation between some bits of X, Y and K may hold with higher prob. than others

Basic principle of LC



(Goal) : Find linear approximation

$$P[i_1,i_2,\ldots,i_a] \oplus C[j_1,j_2,\ldots,j_b]=K[k_1,k_2,\ldots,k_c]$$

with significant prob. p ($\neq$ ½)

where $A[i,j,\ldots,k]=A[i] \oplus A[j] \oplus \ldots \oplus A[k]$

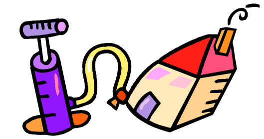
(Algorithm)MLE(Maximum Likelihood Estimation)

(Step 1) For given P and C, compute $X=P[i_1,i_2,\ldots,i_a] \oplus C[j_1,j_2,\ldots,j_b]$, let N = # of Pt given,

(Step 2) **if** $|X=0| > N/2$ **then** $K[k_1,k_2,\ldots,K_c]=0$ **else** 1.

if $|X=0| < N/2$ **then** $K[k_1,k_2,\ldots,k_c]=1$ **else** 0.

Linear Distribution Table(I)



- For a S-box S_a,(a=1,2,…,8) of DES

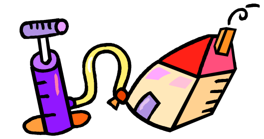
  $NS_a(\alpha,\beta)$= #{x | 0 ≤ x < 64, parity(x•α) = parity(S(x)•β)}

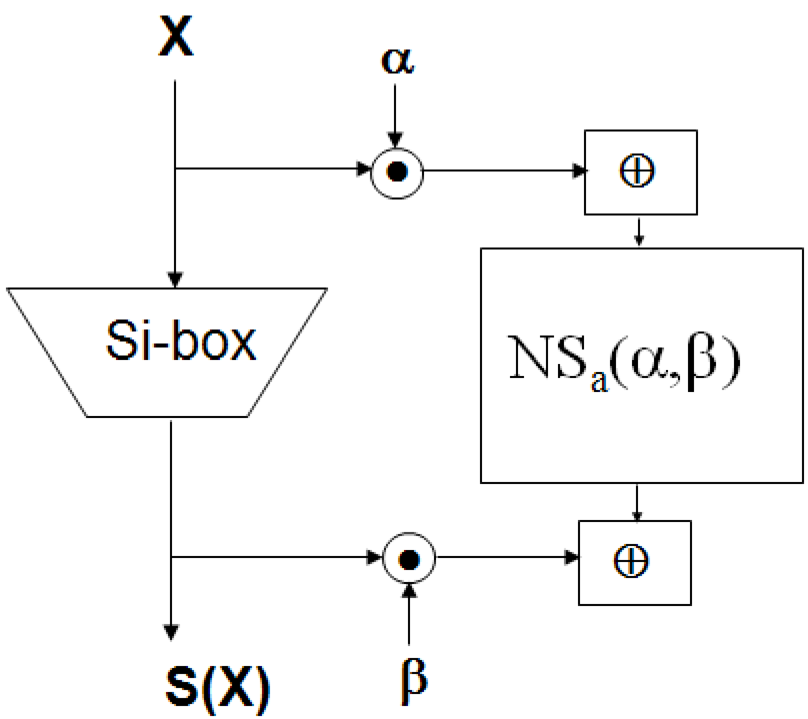
  1≤ α ≤ 63 , 1 ≤ β ≤15, • : dot product (bitwise AND)

- Ex) $NS_5(16,15)$ =12
  - ✓ The 5-th input bit at S5-box is equal to the linear sum of 4 output bits with probability 12/64.
  - ✓ X[15] ⊕ F(X,K)[7,18,24,29]=K[22] with 0.19
  - ✓ X[15] ⊕ F(X,K)[7,18,24,29]=K[22] ⊕ 1 with 1-0.19=0.81

(Note) least significant at the right and index 0 at the least significant bit (Little endian)

Linear Distribution Table(II)





- $NS_a(\alpha,\beta)$ has even values.
- If α =1,32(20_x), 33(21_x), $NS_a(\alpha, \beta)$=32
- $NS_a(\alpha, \beta)$ varies from 0 to 64

Linear Distribution Table(III) – part of S5 box

horizontal axes indicate α and β respectively, and each entry shows $NS_5(\alpha, \beta) - 32$. A complete table tells us that equation (4) is the most effective linear approximation in all S-boxes (i.e. $|NS_a(\alpha, \beta) - 32|$ is maximal); therefore, equation (5) is the best approximation of F-function.

The following Lemma is now trivial from the definition of S-boxes.

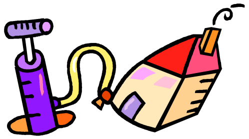
Lemma 1

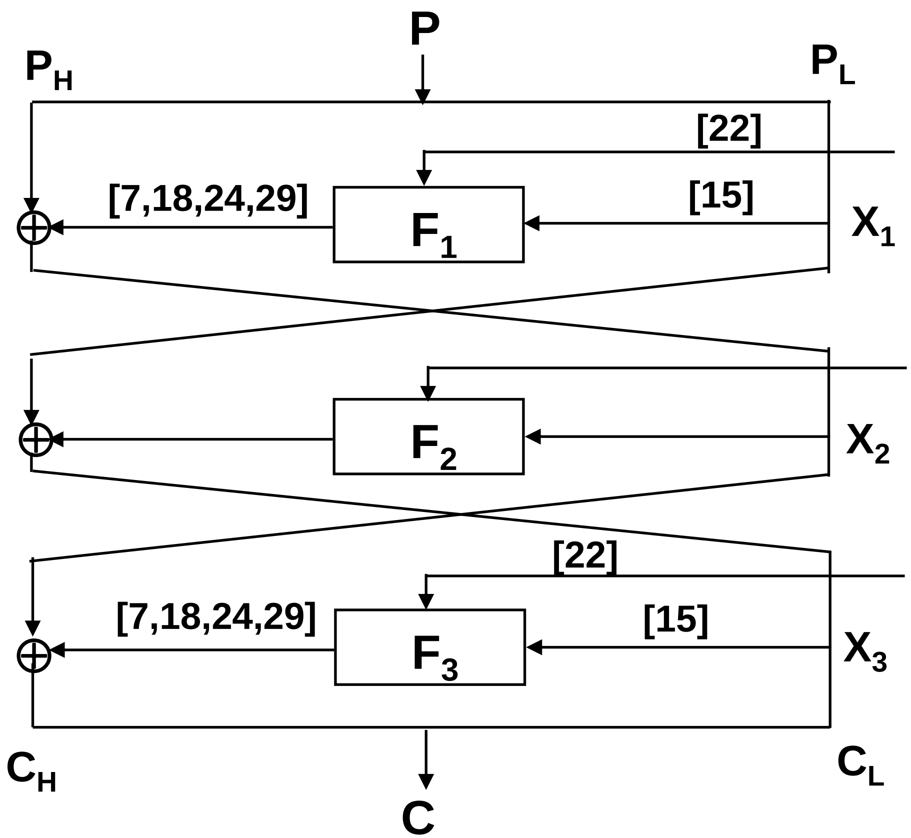
(1) *$NS_a(\alpha, \beta)$ is even.*

(2) *If $\alpha = 1, 32$ or 33, then $NS_a(\alpha, \beta) = 32$ for all S_a and β.*

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	4	−2	2	−2	2	−4	0	4	0	2	−2	2	−2	0	−4
3	0	−2	6	−2	−2	4	−4	0	0	−2	6	−2	−2	4	−4
4	2	−2	0	0	2	−2	0	0	2	2	4	−4	−2	−2	0
5	2	2	−4	0	10	−6	−4	0	2	−10	0	4	−2	2	4
6	−2	−4	−6	−2	−4	2	0	0	−2	0	−2	−6	−8	2	0
7	2	0	2	−2	8	6	0	−4	6	0	−6	−2	0	−6	−4
8	0	2	6	0	0	−2	−6	−2	2	4	−12	2	6	−4	4
9	−4	6	−2	0	−4	−6	−6	6	−2	0	−4	2	−6	−8	−4
10	4	0	0	−2	−6	2	2	2	2	−2	2	4	−4	−4	0
11	4	4	4	6	2	−2	−2	−2	−2	−2	2	0	−8	−4	0
12	2	0	−2	0	2	4	10	−2	4	−2	−8	−2	4	−6	−4
13	6	0	2	0	−2	4	−10	−2	0	−2	4	−2	8	−6	0
14	−2	−2	0	−2	4	0	2	−2	0	4	2	−4	6	−2	−4
15	−2	−2	8	6	4	0	2	2	4	8	−2	8	−6	2	0
16	2	−2	0	0	−2	−6	−8	0	−2	−2	−4	0	2	10	−20
17	2	−2	0	4	2	−2	−4	4	2	2	0	−8	−6	2	4
18	−2	0	−2	2	−4	−2	−8	4	6	4	6	−2	4	−6	0
19	−6	0	2	−2	4	2	0	4	−6	4	2	−6	4	−2	0
20	4	−4	0	0	0	0	0	−4	−4	4	4	0	4	−4	0
21	4	0	−4	−4	4	−8	−8	0	0	−4	4	8	4	0	4
22	0	6	6	2	−2	4	0	4	0	6	2	2	2	0	0
23	4	−6	−2	6	−2	−4	4	4	−4	−6	2	−2	2	0	4
24	6	0	2	4	−10	−4	2	2	0	−2	0	2	4	−2	−4
25	2	4	−6	0	−2	4	−2	6	8	6	4	10	0	2	−4
26	2	2	−8	−2	4	0	2	−2	0	4	2	0	−2	−2	0
27	2	6	−4	−6	0	0	2	6	8	0	−2	−4	−6	−2	0
28	0	−2	2	4	0	−6	2	−2	6	−4	0	2	−2	0	0
29	4	−2	6	−8	0	−2	2	10	−2	−8	−8	2	2	0	4
30	−4	−8	0	−2	−2	−2	2	−2	2	−2	6	4	4	4	0
31	−4	8	−8	2	−6	−6	−2	−2	2	−2	−2	−8	0	0	0

3-round DES by LC





$X_2[7,18,24,29] \oplus P_H[7,18,24,29] \oplus P_L[15] = K_1[22]$ ---------- (1)

$p_1 = 12/64$

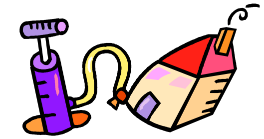
$X_2[7,18,24,29] \oplus C_H[7,18,24,29] \oplus C_L[15] = K_3[22]$ ---------- (2)

$p_3 = 12/64$

(1) $\oplus$ (2) => $X_2[7,18,24,29] \oplus C_H[7,18,24,29] \oplus C_L[15] \oplus X_2[7,18,24,29] \oplus P_H[7,18,24,29] \oplus P_L[15] = K_1[22] \oplus K_3[22]$ with prob. = $(p_1 * p_3) + (1 - p_1) * (1 - p_3)$

* ignore IP and FP like DC

Piling-up lemma in LC

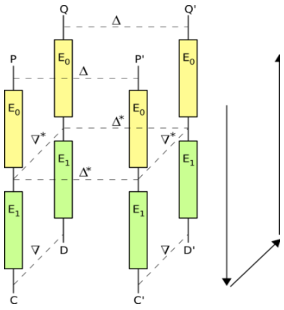


- If independent prob. value, X_i 's ($1 \leq i \leq n$) have prob p_i to value 0, $(1-p_i)$ to value 1,
  $p = \{ \Pr(X_1 \oplus X_2 \oplus \ldots \oplus X_n) = 0\}$
  $= 2^{n-1}\prod_{i=1}^{n}(p_i - 1/2) + 1/2.$

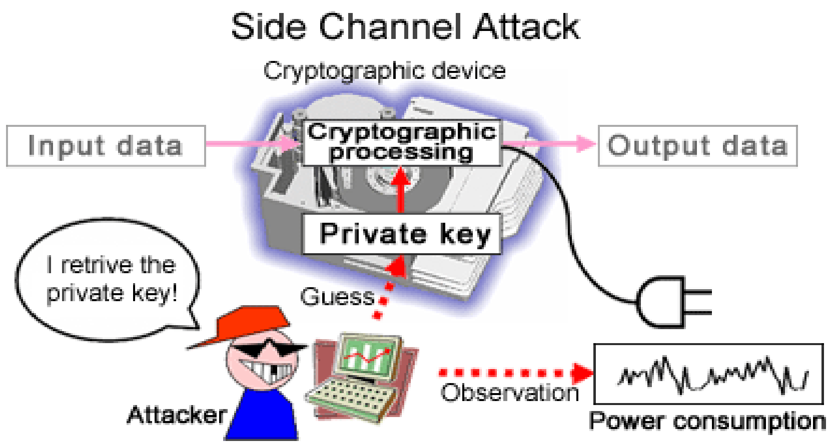
- # of known pt req'd for LC with success prob. 97.7% is $|p - 1/2|^{-2}$

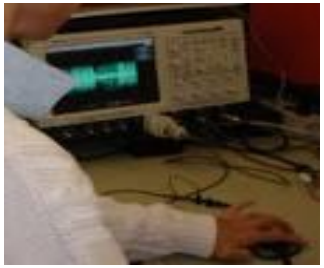
Variation of DC and LC

- Multiple LC : Kaliski & Robshaw [CR94]
- Differential-Linear Cryptanalysis : Langford & Hellman [CR94]
- Nonlinear Approximation in LC : Knudsen [EC96]
- Partitioning Cryptanalysis : Harpes & Massey [FSE97]
- Interpolation Attack : Jakobsen & Knudsen [FSE97]
- Differential Attack with Impossible Characteristics : Biham [EC99], etc.
- Related-key Attack : Kelsey, Schneier, Wagner [CR96]
- Boomerang Attack : Wagner[FSE99]
- Amplified Boomerang Attack : Kelsey, Kohno & Schneier[FSE00]



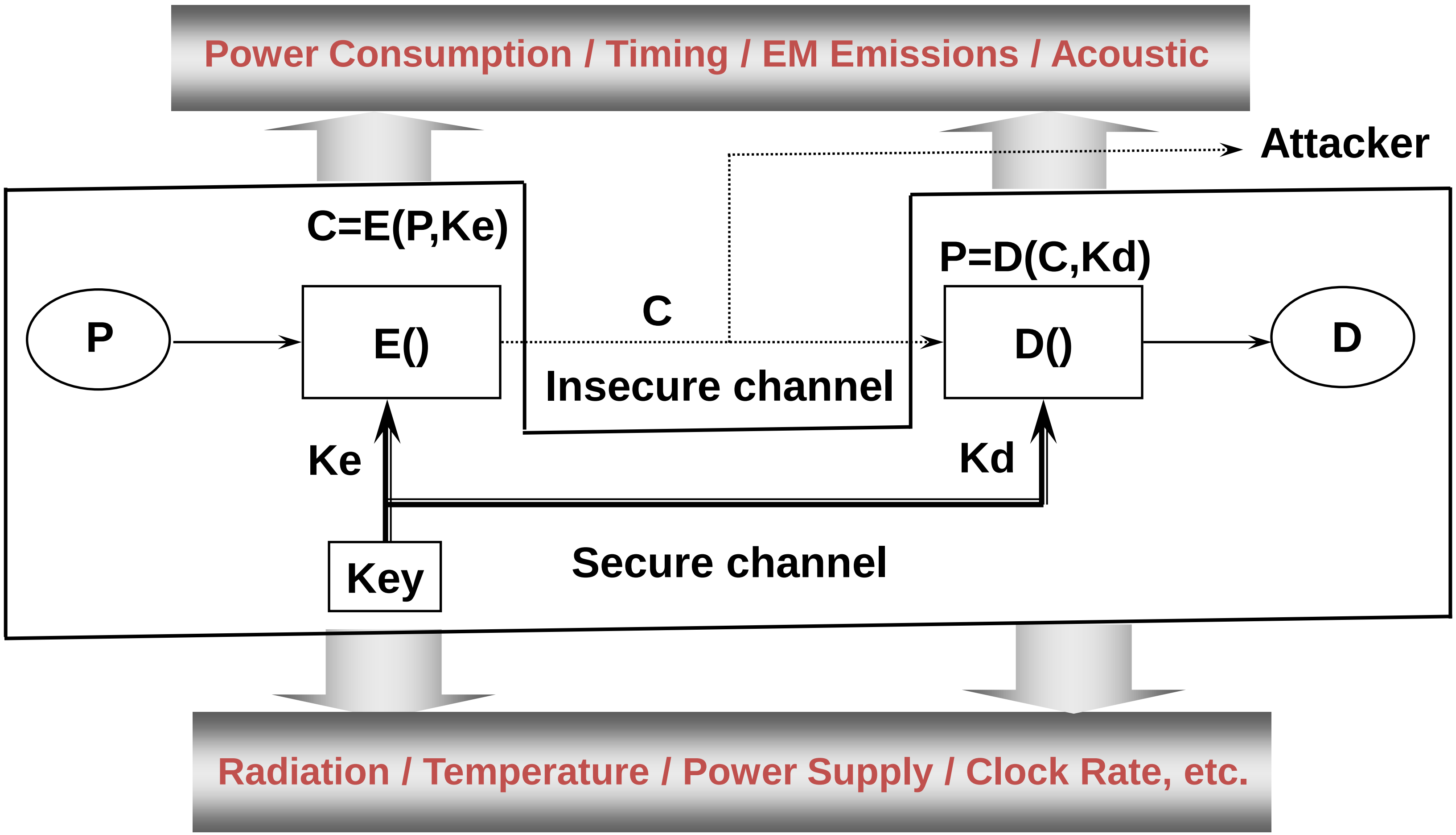
Side Channel Attack



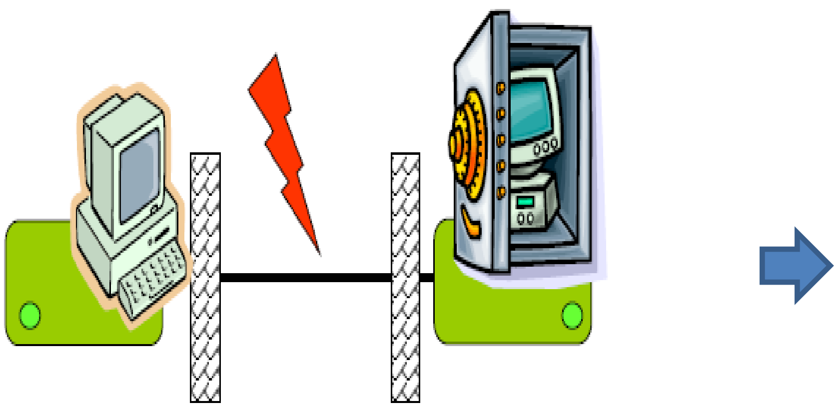


Side Channel

Traditional Cryptographic Model vs. Side Channel



Model of Attack
-Embedded security



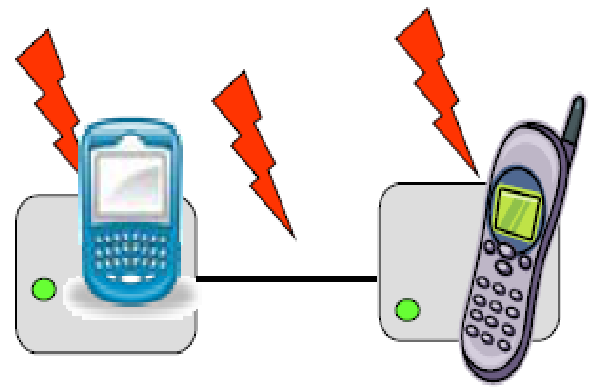
Old Model (simplified view):

-Attack on channel *between* communicating parties

-Encryption and cryptographic operations in *black* boxes

-Protection by strong mathematic algorithms and protocols

-Computationally secure



New Model (also simplified view):

-Attack channel *and* endpoints

-Encryption and cryptographic operations in *gray* boxes

-Protection by strong mathematic algorithms and protocols

-Protection by secure implementation

Need secure implementations not only algorithms

Concept: Origin

- Due to instruction which is executed
- Due to the date which is processed
- Due to some physical effects which are often not well understood, often called noise

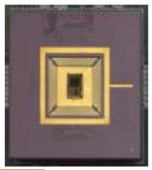
Classifications

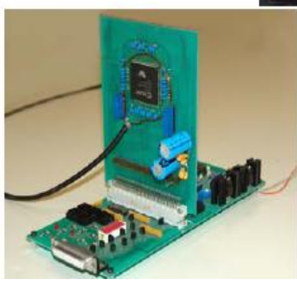
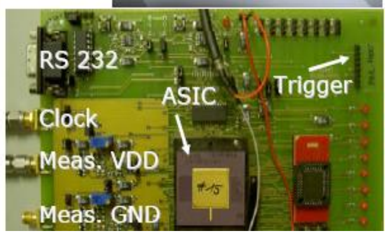
- Active vs. Passive
  - Active: Power glitches or laser pulses
  - Passive: EM-radiation
- Invasive vs. Non-invasive
  - Invasive: bus probing
  - Non-Invasive: Power measurements
- Side Channel: passive and non-invasive
  - Very difficult to detect
  - Often cheap to set-up
  - Mostly: need lots of measurements
- Analysis capability
  - "Simple" attacks: one measurements-visual inspection
  - "Differential" and "Higher" Multiple measurements-signal processing

Attacking Scenario

Devices under attack

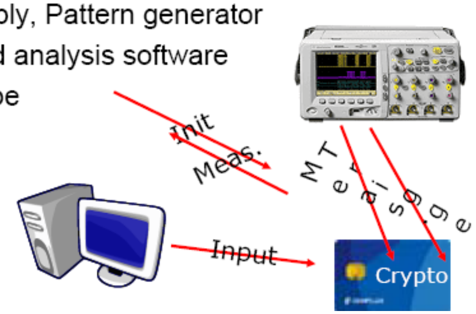
- SmartCard
- FPGA, ASIC
- Etc.



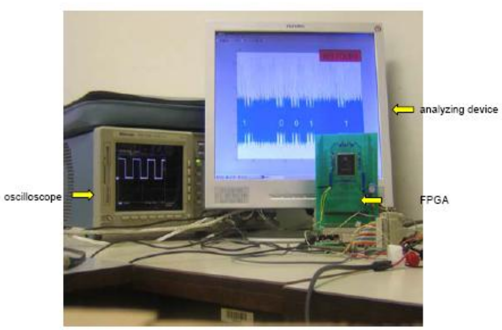



The lab – measurement setup

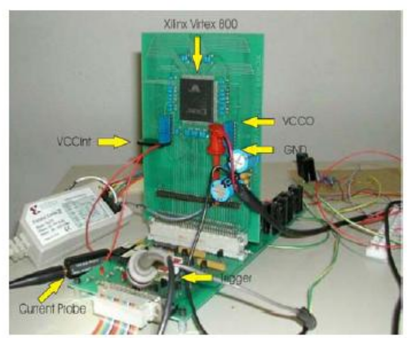
- Cryptographic device under attack
- Probe, measurement circuit
- Power supply, Pattern generator
- Control and analysis software
- Oscilloscope
- PC



Power Analysis: Measurement setup (1)

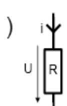


Power Analysis: Measurement setup (2)



Probe / Measurement circuit

- An oscilloscope can only measure voltage
  - Current flow needs to be transformed into a proportional voltage signal
- Simple resistor in series (Ohm's law: U = R x I)
  - Measure voltage drop over the resistor
- Current probe (Current flow -> electric field)



- Dedicated measurement circuit in the design

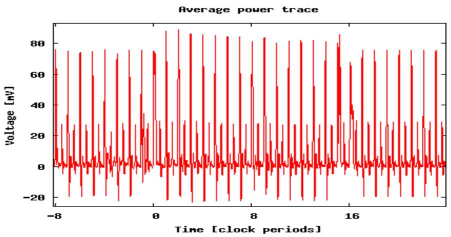
Timing Analysis

- *Paul C. Kocher*, "*Timing Attacks on Implementations of Diffie—Hellman, RSA, DSS, and Other Systems",* Advances in Cryptology - CRYPTO '96, Springer-Verlag, 1996 , LNCS , *Vol. 1109* , pp. 104-113.

- **Cryptosystems can take different amounts of time to process different inputs.**
  - Performance optimizations in software
  - Branching/conditional statements
  - Caching in RAM
  - Variable length instructions (multiply, divide)

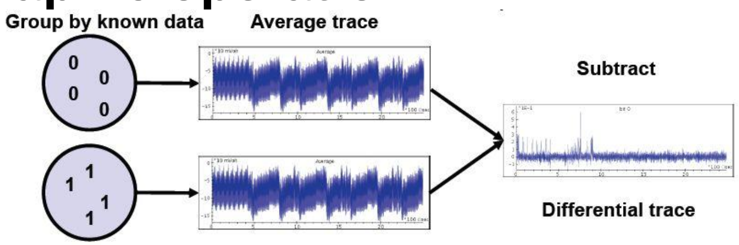
- **Countermeasures**
  - Make all operations run in same amount of time
    - Set all operations by the slowest one
  - Add random delays
  - Blind signature technique

Power Analysi



- Paul C. Kocher and Joshua Jaffe and Benjamin Jun "*Differential Power Analysis",* Advances in Cryptology -CRYPTO '99, Springer-Verlag, 1999 , LNCS , *Vol.1666* , pp.388-397

- **The power consumed by a cryptographic device was analyzed during the processing of the cryptographic operation**
  - Simple Power Analysis
  - Differential Power Analysis

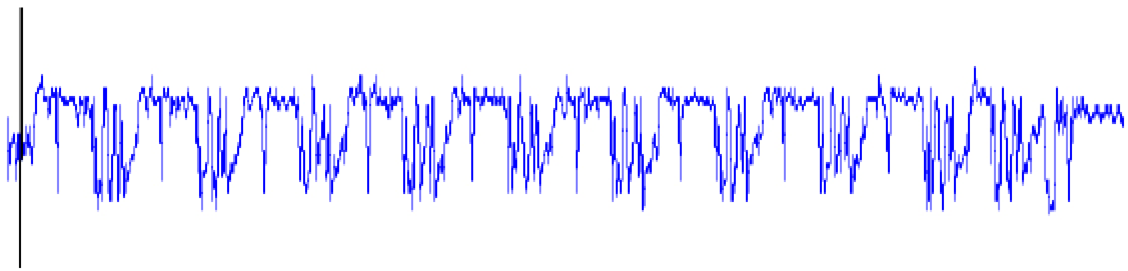


- **Countermeasures**
  - Don't use secret values in conditionals/loops
  - Ensure little variation in power consumption between instructions
  - Reducing power variations (shielding, balancing)
  - Randomness (power, execution, timing) + counters on card
  - Algorithm redesign (non-linear key update, blinding)
  - Hardware redesign (decouple power supply, gate level design)

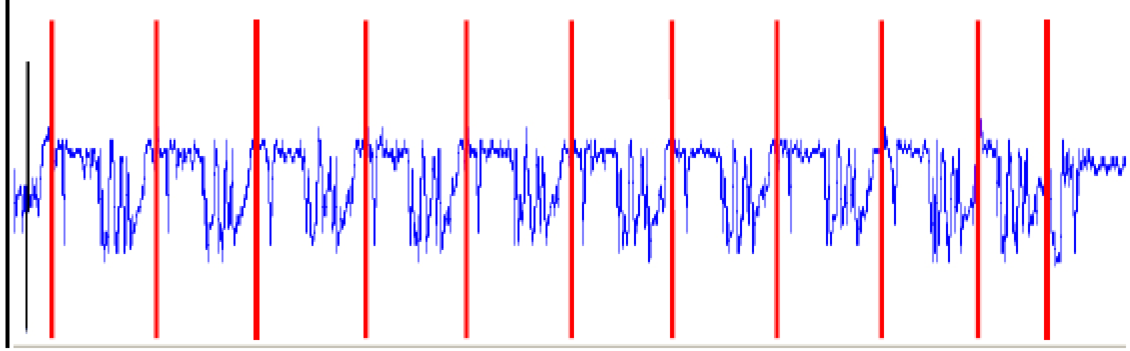
Understand DPA http://www.cryptography.com/

SPA on AES : # of Round?

- What is the keylength of this AES implementation?



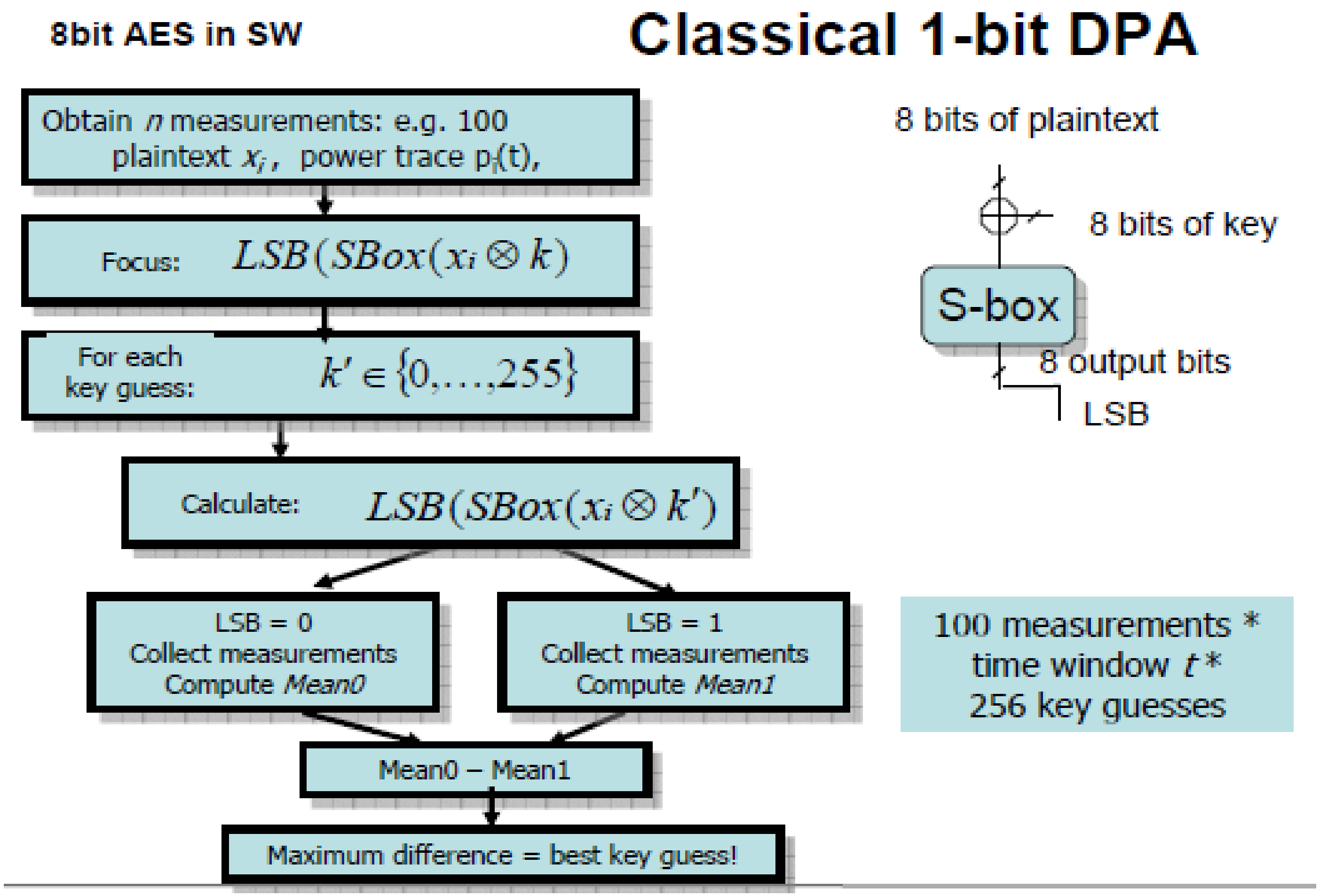
- 10 rounds => AES-128



How DPA works?

- Obtain sufficient number (*n*) of measurements
  - In general: uniform, random inputs; fixed, unknown key k
- Choose an appropriate intermediate result
  - Preferably only a few bits involved (e.g. for AES the bytes are processed separately until the first MixCol operation)
  - Preferably high diffusion within these bits
  - Preferably after a non-linear transformation (e.g. Sbox)
- For each key hypothesis k':
  - based on known plain-/ciphertext and key hypothesis k', predict the intermediate result for each measurement
  - Apply a statistical test to reject/verify the key hypothesis
    - Here: difference of means

Algorithm to find 1-bit



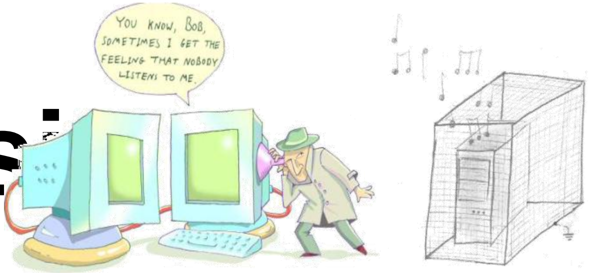
EM Emissions

- D. Agrawal and B. Archambeault and J. R. Rao and P. Rohatgi
  "*The EM Side-Channel(s)"*, Cryptographic Hardware and Embedded Systems - CHES 2002, Springer-Verlag, 2003 , LNCS *, Vol. 2523* , pp.29-45

- EM side channels include a higher variety of information and can be additionally applied from a certain distance.
  (e.g, GPS jamming by N. Korea in 2011)

- **Countermeasures**
  - Redesign circuits
  - Shielding
  - EM noise

Acoustic Analysis



- *Keyboard Acoustic Emanations,* Dmitri Asonov and Rakesh Agrawal, IBM Almaden Research Center, 2004.
- Acoustic cryptanalysis - On noisy people and noisy machines by Adi Shamir and Eran Tromer