

Block Cipher Cryptanalysis - Part 1

Gerardo Pelosi

Department of Electronics, Information and Bioengineering (DEIB)
Politecnico di Milano

gerardo.pelosi - at - polimi.it

Overview

Lesson contents

- Basics of Block Cipher Cryptanalysis
- Algebraic Known Plaintext Attack of Block Ciphers w/o Sboxes
 - The *Trivial* cipher
 - Algebraic Cryptanalysis of *Trivial*
- Statistical Known Plaintext Attack: Linear Cryptanalysis
 - The *Simple* cipher
 - Linear Cryptanalysis of *Simple*

Block Cipher Cryptanalysis

Approaches

- Modern block cipher cryptanalysis aims at either recovering the key with an effort **smaller than bruteforce**
- *Known-ciphertext-only* cryptanalysis is a symptom of a deeply flawed cipher (Caesar, Vigenère, Playfair *et al.*)
- We will tackle techniques requiring either a *known plaintext* or a *related (chosen) plaintext* assumption
- Block cipher cryptanalyses are usually split into two families: **algebraic** and **statistical**

Block Cipher Cryptanalysis

Algebraic Analysis

A cipher can be seen as a *large* set of Boolean simultaneous equations involving key bits (variables), ptx and ctx bits (known terms).

Either one or both of the following findings should be obtained **efficiently** to have a successful cryptanalysis

- A **solution** (in closed form), for the simultaneous equations yields the key from one (or more) ptx/ctx pairs
- The discovery that **only a subset** of the key bits are actually involved in the simultaneous equations, while a portion of them self-cancel
 - Only the involved key bits are effectively used by the cipher in encryption

Block Cipher Cryptanalysis

Statistical Analysis

- A perfect cipher is able to produce a ctx **independent** from the ptx
- All the computationally secure ones produce a ctx where the probability that a bit is either one or zero is biased ($= \frac{1}{2} \pm \epsilon$) by the ptx value
- Thus, a relation r between ptx and ctx bits may hold with bias $\epsilon \neq 0$
 - E.g., “even numbers of 1s in the ptx \rightarrow even number of 1s in the ctx”
- **Goal:** find such relations between ptx and ctx, and exploit the statistical biases to extract a portion of the key

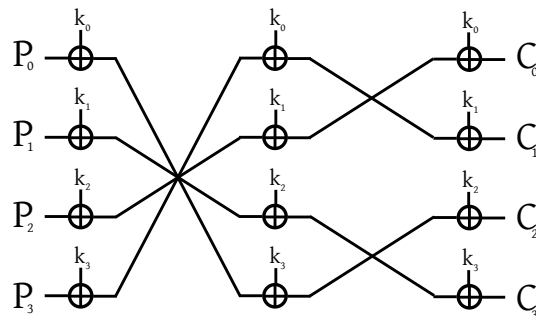
Block Cipher Cryptanalysis

Starting out

- From now on, *linear* will be referring to linearity w.r.t. the addition modulo 2, i.e., eXclusive-OR (xor)
- Recall that the multiplication mod 2 is the Boolean “and” operation and that $x^2 \text{ mod } 2 = x$ if you only care for solutions in $\{0, 1\}$
- First step: observe that any **linear** cipher is **trivial** to cryptanalyze
 - Obtaining the key with a *known plaintext attack* = solving a set of simultaneous linear equations
- First example: the *Trivial* cipher, only has *diffusion* and *key addition*

Block Cipher Cryptanalysis

the “Trivial” Cipher



- 4-bit block, 4-bit key
- Key schedule: a repetition of the key

Block Cipher Cryptanalysis

Cryptanalysis of “Trivial”: Algebraic Approach

- Rewrite the relations between ptx, ctx and key bits as equations with binary coefficients:
$$\begin{aligned} C_0 &= P_2 \oplus k_2 \oplus k_1 \oplus k_0 \\ C_1 &= P_3 \oplus k_3 \oplus k_0 \oplus k_1 \\ C_2 &= P_0 \oplus k_0 \oplus k_3 \oplus k_2 \\ C_3 &= P_1 \oplus k_1 \oplus k_2 \oplus k_3 \end{aligned} \quad \Rightarrow \quad \begin{aligned} P_2 \oplus C_0 &= k_2 \oplus k_1 \oplus k_0 \\ P_3 \oplus C_1 &= k_3 \oplus k_0 \oplus k_1 \\ P_0 \oplus C_2 &= k_0 \oplus k_3 \oplus k_2 \\ P_1 \oplus C_3 &= k_1 \oplus k_2 \oplus k_3 \end{aligned}$$
- This is a set of linear simultaneous eq.s, where the **ptxs and ctxs are known**: just solve it for k_0, k_1, k_2, k_3
- Any cipher made only with a linear *key addition* and a linear *diffusion* layer can be broken with the same technique

Block Cipher Cryptanalysis

Cryptanalysis of “Trivial”: Statistical Approach

- Since in *Trivial* $C_0 = P_2 \oplus k_2 \oplus k_1 \oplus k_0$:
 - If the relation $r : C_0 = P_2$ holds, then either:
 - ① $k_0 = k_2 = k_1 = 0$
 - ② $k_0 = k_1 = 1, k_2 = 0$
 - ③ $k_0 = k_2 = 1, k_1 = 0$
 - ④ $k_1 = k_2 = 1, k_0 = 0$
 - If the relation $r' : C_0 \neq P_2$ holds, then either:
 - ① $k_0 = k_2 = k_1 = 1$
 - ② $k_0 = k_1 = 0, k_2 = 1$
 - ③ $k_0 = k_2 = 0, k_1 = 1$
 - ④ $k_1 = k_2 = 0, k_0 = 1$
- In both cases, looking at the value of a ptx-ctx bit pair, out of $2^3 = 8$ possible values for k_0, k_1, k_2 only 4 possibilities are left
- This is equivalent to a key space reduction by a factor of 2, and can always be done since either r holds with $Pr(r) = 1$, or r' does.

Nonlinear Relations

Enter the S-Boxes

- Sound ciphers have **nonlinear** components (S-Boxes) preventing efficient closed form solution of simultaneous equations
 - Solving simultaneous equations with $\text{deg.} > 1$ in \mathbb{Z}_p is NP-Complete
- Without S-Boxes, the **linear** relations between ptx and ctx bits always hold (i.e., with probability =1)
- With S-Boxes, **linear** relations may still hold with a probability $\neq \frac{1}{2}$

Key Idea of Linear Cryptanalysis

- ① Exploit the relations holding with a bias (i.e., with probability $\frac{1}{2} \pm \epsilon$) to provide a **key-independent linear approximation** of a cipher portion
- ② (i) Use the approximation in place of all-but one rounds of the cipher, and then (ii) use it to recover the last round key

Linear Cryptanalysis

Approximation of a 4-to-4 S-box

- We need to check how well **linear** relations “fit” the S-Box
- How many linear eq.s between S-Box inputs and outputs can be written?
 - Linear equation \Rightarrow a polynomial with degree 1 (e.g.: $X_1 \oplus X_3 \oplus X_4$)
 - The equations can be written as $\bigoplus_i X_i = \bigoplus_j Y_j \oplus c, c \in \{0, 1\}$
 - Up to 8 variables involved in each relation (4 inputs, 4 outputs), two possible results $\Rightarrow 2^4 \cdot 2^4 \cdot 2 = 2^9$ possible relations
- If a given eq. with $c=0$ holds with probability $\frac{1}{2} + \epsilon$, then same eq. with $c=1$ would hold with probability $\frac{1}{2} - \epsilon$
- Since we are interested in the magnitude $|\epsilon|$ of ϵ , we will arbitrarily pick $c=0$

Linear Cryptanalysis

Bias computations for a 4-to-4 bit S-box

- A linear **input-output relation** for a 4-to-4 bit S-box is:

$$a_0 X_0 \oplus a_1 X_1 \oplus a_2 X_2 \oplus a_3 X_3 = b_0 Y_0 \oplus b_1 Y_1 \oplus b_2 Y_2 \oplus b_3 Y_3; \quad a_i, b_i \in \{0, 1\}$$
- For each choice of the binary coefficients a_i, b_i out of $(2^4)^2 = 256$ possible choices $\{(0000, 0000), \dots, (0010, 1001), \dots\}$, a different equation can be written. To assess how well each equation approximates the S-box, we compute their probabilities as follows.
 - Given one equation (e.g., $X_0 \oplus X_3 = Y_2$), let us initialize a counter $\text{ctr} \leftarrow 0$
 - For each of the 16 S-box inputs $(x_0, x_1, x_2, x_3) \in \{0000, 0001, \dots\}$
 - Compute the output values $(y_0, y_1, y_2, y_3) = \text{Sbox}(x_0, x_1, x_2, x_3)$
 - If the equation at hand holds, then increment ctr
 - Store the bias value $\epsilon = Pr - \frac{1}{2} = \frac{\text{ctr} - 8}{16}$ for the equation at hand as “ $\text{ctr} - \frac{\text{Sbox_size}}{2}$ ” (Sbox_size=16, to handle integers and not fractions)
- Obviously, the relation given by $\langle (a_0, a_1, a_2, a_3), (b_0, b_1, b_2, b_3) \rangle = \langle 0000, 0000 \rangle$ will always be true (sum of no input bits = sum of no output bits) i.e., $Pr(r)=1$ or bias $\epsilon = \frac{1}{2}$ (maximum) or *integer bias* = $\frac{\text{Sbox_size}}{2}$ (maximum)

S-Box Description

Small, yet troublesome

- We will tackle a 4×4-bit S-Box, corresponding to a $\{0, 1\}^4 \mapsto \{0, 1\}^4$ nonlinear map
- It is obtained considering the first S-Box of DES and setting to 00 the two leftmost input bits
- The complete description is provided below (input on the top row, $X_0 X_1 X_2 X_3$, in hexadecimal; output nibble, $Y_0 Y_1 Y_2 Y_3$, on the bottom one)

0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
E	4	D	1	2	F	B	8	3	A	6	C	5	9	0	7

Bias table for the S-box

$$a=(a_0 a_1 a_2 a_3) : \mathcal{X}(X) \quad b=(b_0 b_1 b_2 b_3) : \mathcal{Y}(Y)$$

$$a_0 X_0 \oplus a_1 X_1 \oplus a_2 X_2 \oplus a_3 X_3 = b_0 Y_0 \oplus b_1 Y_1 \oplus b_2 Y_2 \oplus b_3 Y_3; \quad a_i, b_i \in \{0, 1\}$$

$a : \mathcal{X}(X) \downarrow b : \mathcal{Y}(Y) \rightarrow$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0 : 0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1 : X_3	0	0	-2	-2	0	0	-2	6	2	2	0	0	2	2	0	0
2 : X_2	0	0	-2	-2	0	0	-2	-2	0	0	2	2	0	0	-6	2
3 : $X_2 \oplus X_3$	0	0	0	0	0	0	0	0	2	-6	-2	-2	2	2	-2	-2
4 : X_1	0	2	0	-2	-2	-4	-2	0	0	-2	0	2	2	-4	2	0
5 : $X_1 \oplus X_3$	0	-2	-2	0	-2	0	4	2	-2	0	-4	2	0	-2	-2	0
6 : $X_1 \oplus X_2$	0	2	-2	4	2	0	0	2	0	-2	2	4	-2	0	0	-2
7 : $X_1 \oplus X_2 \oplus X_3$	0	-2	0	2	2	-4	2	0	-2	0	2	0	4	2	0	2
8 : X_0	0	0	0	0	0	0	0	0	-2	2	2	-2	2	-2	-2	6
9 : $X_0 \oplus X_3$	0	0	-2	-2	0	0	-2	-2	-4	0	-2	2	0	4	2	-2
A : $X_0 \oplus X_2$	0	4	-2	2	-4	0	2	-2	2	2	0	0	2	2	0	0
B : $X_0 \oplus X_2 \oplus X_3$	0	4	0	-4	4	0	4	0	0	0	0	0	0	0	0	0
C : $X_0 \oplus X_1$	0	-2	4	-2	-2	0	2	0	2	0	2	4	0	2	0	-2
D : $X_0 \oplus X_1 \oplus X_3$	0	2	2	0	-2	4	0	2	-4	-2	2	0	2	0	0	2
E : $X_0 \oplus X_1 \oplus X_2$	0	2	2	0	-2	-4	0	2	-2	0	0	-2	-4	2	-2	0
F : $X_0 \oplus \dots \oplus X_3$	0	-2	-4	-2	-2	0	2	0	0	-2	4	-2	-2	0	2	0

Linear Cryptanalysis

How to read a bias table

- The previous bias table can be read as follows:
 - **Choose input bits** \rightarrow represent them as a vector $(a_0, a_1, a_2, a_3) \rightarrow$ read them as a 4-bit binary row index value
 - **Choose output bits** \rightarrow represent them as a vector $(b_0, b_1, b_2, b_3) \rightarrow$ read them as a 4-bit binary column index value
 - Look up the value v . If signs are not used, then a Color-Coding is adopted: red is positive, whereas blue is negative
 - The bias for the chosen relation is $\epsilon = \frac{v}{(\text{Sbox_size})}$
- Example:
 - Choose input bits $X_0, X_1, X_2, X_3 \rightarrow (0, 0, 0, 1) \rightarrow$ row 1
 - Choose output bits $X_0, Y_1, Y_2, Y_3 \rightarrow (0, 1, 1, 1) \rightarrow$ column 7
 - The value v is +6, thus the relation $r : X_3 = Y_1 \oplus Y_2 \oplus Y_3$ holds with probability $\Pr(r) = \frac{1}{2} + \frac{(+6)}{16} = \frac{1}{2} + \frac{3}{8} = \frac{7}{8}$
- The last input bit of the S-Box input is equal to the sum of the last three output bits ($r : X_3 = Y_1 \oplus Y_2 \oplus Y_3$) 7 times out of 8

Tackling a *Not so Trivial Cipher*

Recap

- Known: we have a set of *approximate linear relations* which can replace the S-box with a known probability
- **Known:** the *linear portion of the cipher* is described by linear relations
- **Goal-1:** Obtain a **key-independent** linear relation equivalent to all the rounds of the cipher save for the last one, holding with a given bias
- **Goal-2:** Use the approximation to derive a group of bits of the final round-key. The values guessed for a group of bits in input to the last round are employed together with the ctx bits to recover some bits of the last round key

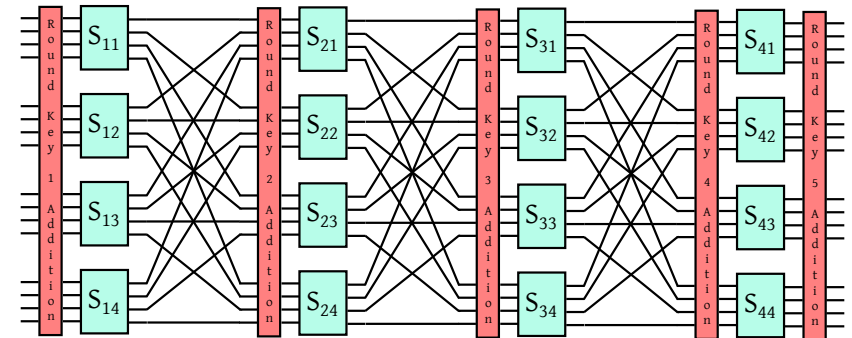
Target cipher

the *Simple* cipher

- 16-bit block, 4 rounds, 80-bit key
- No keyschedule, 16-bit used in each round
- SPN design: [AddRoundKey, SBox, Perm]×3, [AddRoundKey, SBox]×1, plus a final AddRoundKey
- The **round key addition** is performed via bitwise xor
- The **S-boxes** are all the same, and match the one we just analysed
- **Permutation**: i -th bit of j -th box goes into the j -th bit of i -th Sbox
- No permutation in the last round: trivial to eliminate as it acts bitwise; an extra round key addition is performed to secure the inputs to the last round s-boxes

Target cipher

the *Simple* cipher



Chaining Approximations

How to build a whole cipher approximation

- We now know how
 - to approximate a single S-box and
 - to write a linear relation for a diffusion stage
- To obtain a full cipher approximation we still need to:
 - 1 Find a way to compute the bias if we use more than one approximation (i.e., chain them to approximate more than a single S-Box)
 - 2 Cope with the effects of the intermediate key additions
- We will start with the statistical tool which allows us to combine two approximations: the Pile-up Lemma [1]

Linear Cryptanalysis

Pile-up Lemma [1] - Toolbox

- Consider two random variables Z_1, Z_2 over $\{0, 1\}$, with their respective distributions

$$\Pr(Z_1=z_1) = \begin{cases} p_1 & \text{if } z_1 = 0 \\ 1 - p_1 & \text{if } z_1 = 1 \end{cases} \quad \Pr(Z_2=z_2) = \begin{cases} p_2 & \text{if } z_2 = 0 \\ 1 - p_2 & \text{if } z_2 = 1 \end{cases}$$

- If we take Z_1 to be **independent** from Z_2 , we obtain:

$$\Pr(Z_1 = z_1, Z_2 = z_2) = \begin{cases} p_1 p_2 & z_1 = 0, z_2 = 0 \\ p_1(1 - p_2) & z_1 = 0, z_2 = 1 \\ (1 - p_1)p_2 & z_1 = 1, z_2 = 0 \\ (1 - p_1)(1 - p_2) & z_1 = 1, z_2 = 1 \end{cases}$$

- We can now derive $\Pr(Z_1 \oplus Z_2 = 0)$ as

$$\Pr(Z_1 = 0, Z_2 = 0) + \Pr(Z_1 = 1, Z_2 = 1) = p_1 p_2 + (1 - p_1)(1 - p_2)$$

Linear Cryptanalysis

Pile-up Lemma - Toolbox

- For the sake of clarity, explicit ϵ_1, ϵ_2 rewriting: $p_1 = \frac{1}{2} + \epsilon_1, p_2 = \frac{1}{2} + \epsilon_2$
- The biases ϵ_1, ϵ_2 , are in the range $-\frac{1}{2} \leq \epsilon_1, \epsilon_2 \leq \frac{1}{2}$ and highlight how much the probabilities deviate from an fair coin toss
- We can now obtain the following definition for $\Pr(Z_1 \oplus Z_2 = 0)$:

$$\Pr(Z_1 \oplus Z_2 = 0) = p_1 p_2 + (1 - p_1)(1 - p_2)$$

$$= \frac{1}{2} + 2\epsilon_1 \epsilon_2$$

- Let us denote the bias associated to the $r : Z_1 \oplus Z_2 = 0$ as $2\epsilon_1 \epsilon_2 = \epsilon_{1,2}$

Linear Cryptanalysis

Pile-up Lemma [1]

- Following the previous results, we can generalize to $n \geq 2$ **independent** random variables, by induction:

$$\Pr(Z_1 \oplus Z_2 \oplus \dots \oplus Z_n = 0) = \frac{1}{2} + 2^{n-1} \prod_{i=1}^n \epsilon_i$$

- Equivalently, $\frac{1}{2} + \epsilon_{1,\dots,n}$ assuming $\epsilon_{1,\dots,n} = 2^{n-1} \prod_{i=1}^n \epsilon_i$

Proof:

- Assume validity of the Lemma for $n-1$ variables:

$$\Pr(\bigoplus_{i=1}^{n-1} Z_i = 0) = \frac{1}{2} + \epsilon_{1,\dots,n-1} \text{ where } \epsilon_{1,\dots,n-1} = 2^{n-2} \prod_{i=1}^{n-1} \epsilon_i$$

- Define the binary variable $W = \bigoplus_{i=1}^{n-1} Z_i$. Then

$$\Pr(W \oplus Z_n = 0) = \dots = \frac{1}{2} + 2\epsilon_{1,\dots,n-1} \cdot \epsilon_n \Rightarrow \epsilon_{1,\dots,n} = 2^{n-1} \prod_{i=1}^n \epsilon_i$$

Pile-up Lemma and Independence

Example of issues when the random variables are not independent

Let Z_1, Z_2, Z_3 be independent binary random variable with biases $\epsilon_1 = \epsilon_2 = \epsilon_3 = \frac{1}{4}$. We can compute directly

$$Z_{12} = Z_1 \oplus Z_2 \quad \text{with bias} \quad \epsilon_{12} = 2\epsilon_1 \epsilon_2 = \frac{1}{8}$$

$$Z_{23} = Z_2 \oplus Z_3 \quad \text{with bias} \quad \epsilon_{23} = 2\epsilon_2 \epsilon_3 = \frac{1}{8}$$

$$Z_{13} = Z_1 \oplus Z_3 \quad \text{with bias} \quad \epsilon_{13} = 2\epsilon_1 \epsilon_3 = \frac{1}{8}$$

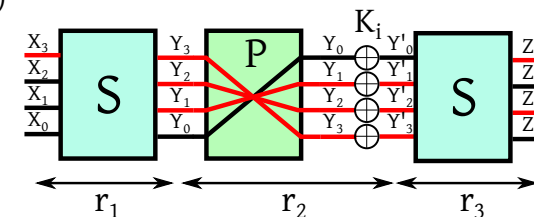
Note that the random variables Z_{12} and Z_{23} cannot be independent.

If they were independent, then by the Pile-up lemma the bias of $Z_{13} = Z_1 \oplus Z_3 = (Z_1 \oplus Z_2) \oplus (Z_2 \oplus Z_3) = Z_{12} \oplus Z_{23}$ would be equal to $2 \cdot \frac{1}{8} \cdot \frac{1}{8} = \frac{1}{32}$, which is not the case

Use of the Pile-up lemma for combining relations

Example

Now we assume relations among input and output values of a cipher round as equalities to 0, associating each of them to a random variable (X_i, Z_i) . The goal is to have a relation between X_i and Z_i without any other intermediate variable (in particular, without the ones associated with a round key bit)



$$r_1 : X_3 \oplus Y_1 \oplus Y_2 \oplus Y_3 = 0 \quad \epsilon_1 = +\frac{6}{16}$$

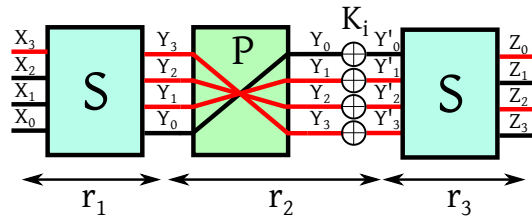
$$r_2 : (Y'_3 \oplus Y_3 \oplus K_3) \oplus (Y'_1 \oplus Y_1 \oplus K_1) \oplus (Y'_2 \oplus Y_2 \oplus K_2) = 0 \quad \epsilon_2 = +\frac{1}{2}$$

$$r_3 : Y'_1 \oplus Y'_2 \oplus Y'_3 \oplus Z_0 \oplus Z_2 = 0 \quad \epsilon_3 = -\frac{4}{16}$$

(r_2 is always true (i.e., $\epsilon = +\frac{1}{2}$) as permutation and key addition are linear)

Use of the Pile-up lemma for combining relations

Example



Combine r_2, r_3 into r_{23} adding relations member-wise and compute ϵ_{23}

$$r_{23} : Y_3 \oplus Y_2 \oplus Y_1 \oplus Z_0 \oplus Z_2 \oplus K_3 \oplus K_2 \oplus K_1 = 0 \quad \epsilon_{23} = 2\epsilon_2\epsilon_3 = \epsilon_3 = -\frac{4}{16}$$

$$r_1 : X_3 \oplus X_2 \oplus X_1 \oplus Y_1 = 0 \quad \epsilon_1 = +\frac{6}{16}$$

Combine r_{23} and r_1 (use pile-up lemma, assuming r_1, r_{23} as independent)

$r_{123} : X_3 \oplus Z_0 \oplus Z_2 = (K_3 \oplus K_2 \oplus K_1)$ we consider key bits as constants, which implies considering $r_{123} : X_3 \oplus Z_0 \oplus Z_2 = 0$, with $|\epsilon_{123}| = |2\epsilon_1\epsilon_{23}| = \frac{3}{16}$

Linear Cryptanalysis

Whole cipher approximation

- We are closing in on our target: obtain an approximation of a part of the cipher up to the **input of the last round s-boxes**
- We still need to do two things
 - ① Choose which biases to use for the S-Boxes and which S-Boxes to approximate
 - ② Deal with the four round-keys being added in between
- We will start choosing which biased relations to use and which S-Boxes to approximate
- The relations are chosen with two (possibly contrasting) goals:
 - ① Minimize the number of output bits so to minimize the number of active boxes (or the bias will thin down...)
 - ② Employ SBox linear approximations with the highest possible biases

Linear Cryptanalysis

Linear Path along the *Simple* cipher

- Notation:
 - $U_{i,j}$ represents the j -th input bit (counting from 1 to 16, bottom to top in our picture) to the i -th round **S-Boxes** (counting from 1 to 4)
 - $V_{i,j}$ represents the j -th output bit (counting from 1 to 16, bottom to top in our picture) to the i -th round **S-Boxes**
 - $K_{i,j}$ represents the j -th bit (counting from 1 to 16, bottom to top in our picture) of the i -th round key
- We start by considering the input to the first round S-boxes: $\forall j \in [1, 16] U_{1,j} = P_j \oplus K_{1,j}$ as the first AddRoundKey acts on all bits
- We now choose an eq. for S_{13} which possibly includes a minimum number of output variables:

$$r_1 : X_0 \oplus X_2 \oplus X_3 = Y_1 \quad \text{on S-Box } S_{13}$$

$$\text{from the bias table we take } 4, \epsilon_{r_1} = \frac{4}{16} = \frac{1}{4}, \Pr(r_1) = \frac{3}{4}$$

Linear Cryptanalysis

Linear Path along the *Simple* cipher

- Applying $r_1 : X_0 \oplus X_2 \oplus X_3 = Y_1$ on S-box S_{13} , allows us to state that

$$V_{1,6} = U_{1,5} \oplus U_{1,7} \oplus U_{1,8} = (P_5 \oplus K_{1,5}) \oplus (P_7 \oplus K_{1,7}) \oplus (P_8 \oplus K_{1,8})$$
 with probability $\Pr(r_1) = 3/4, \epsilon_{r_1} = \frac{1}{4}$ *One box down, three to go :-)*
- Since the $V_{1,6}$ bit goes through the second AddRoundKey,

$$U_{2,6} = V_{1,6} \oplus K_{2,6}$$
- Following the wires, we obtain that our next relation to be considered needs to involve only $U_{2,6}$ among the input bits
- We need to choose a high-bias relation involving X_1 (the second Sbox input – corresp. to $V_{1,6}$); let's take

$$r_2 : X_1 = Y_1 \oplus Y_3 \quad \text{with bias } \epsilon_{r_2} = -\frac{1}{4}$$

Linear Cryptanalysis

Linear Path along the *Simple* cipher

- Applying $r_2 : X_1 = Y_1 \oplus Y_3$ ($\epsilon_{r_2} = -\frac{1}{4}$) on SBox S_{23} , allows us to state that

$$V_{1,6} \oplus K_{2,6} = U_{2,6} = V_{2,6} \oplus V_{2,8}$$

with probability $\Pr = \frac{1}{2} + \epsilon_{r_2} = \frac{1}{4}$

- ...*It's time to merge the two relations!* Applying the Pile-up lemma, we substitute $V_{1,6}$ with $P_5 \oplus K_{1,5} \oplus (P_7 \oplus K_{1,7}) \oplus P_8 \oplus K_{1,8}$, obtaining

$$r_{12} : P_5 \oplus K_{1,5} \oplus (P_7 \oplus K_{1,7}) \oplus P_8 \oplus K_{1,8} \oplus K_{2,6} = V_{2,6} \oplus V_{2,8}$$

with a bias of $\epsilon_{r_{1,2}} = 2\epsilon_{r_1}\epsilon_{r_2} = \frac{1}{4}(-\frac{1}{4}) = -\frac{1}{8}$

- ...*Two boxes down:* we have a linear approximation in the plaintext (and key bits) up to after the second S-box layer holding with $\Pr(r_{12}) = \frac{1}{2} - \frac{1}{8} = \frac{3}{8}$

Linear Cryptanalysis

Linear Path along the *Simple* cipher

- As the previous relation involves S-box outputs ($V_{2,6}, V_{2,8}$) wired to two different boxes on the 3rd layer, we now need to combine two relations to approximate S_{31} and S_{33}

- Employing the same r_2 as before on both boxes we obtain that

$$V_{3,6} \oplus V_{3,8} = V_{2,6} \oplus K_{3,6} \quad V_{3,14} \oplus V_{3,16} = V_{2,8} \oplus K_{3,14}$$

both holding with probability $-\frac{1}{4}$

- Piling them up (i.e., xor-ing them) we obtain that

$$r_3 : V_{3,6} \oplus V_{3,8} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,8} \oplus K_{3,14} = 0$$

holding with a (piled-up) bias of $2(-\frac{1}{4})(-\frac{1}{4}) = \frac{1}{8}$

Linear Cryptanalysis

Linear Path along the *Simple* cipher

- Combining our approximation of the third layer of boxes

$$r_3 : V_{3,6} \oplus V_{3,8} \oplus V_{2,6} \oplus K_{3,6} \oplus V_{3,14} \oplus V_{3,16} \oplus V_{2,8} \oplus K_{3,14} = 0$$

($\Pr(r_3) = \frac{1}{2} + \frac{1}{8}$) with the previous one for the first two

$$r_{12} : V_{2,6} \oplus V_{2,8} = P_5 \oplus K_{1,5} \oplus (P_7 \oplus K_{1,7}) \oplus P_8 \oplus K_{1,8} \oplus K_{2,6}$$

($\Pr(r_{12}) = \frac{1}{2} - \frac{1}{8}$) gives us the following relation

$$r_{123} : V_{3,6} \oplus V_{3,8} \oplus V_{3,14} \oplus V_{3,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_k = 0$$

holding with bias $2(\frac{1}{8})(-\frac{1}{8}) = -\frac{1}{32}$, where Σ_k is

$$\Sigma_k = K_{3,14} \oplus K_{3,6} \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6}$$

Linear Cryptanalysis

Dropping the key bits

- Adding the fourth round key, and packing all the key bits in Σ_k we get

$$r_4 : U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 \oplus \Sigma_k = 0$$

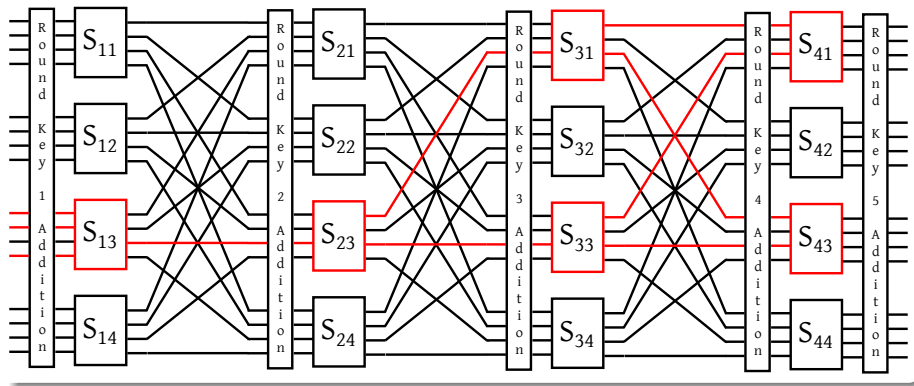
holding with a bias of $-\frac{1}{32}$, where $U_{4,i}$ are in input to the last s-box layer, and P_j are the ptx bits.

- We now consider the sum of the involved key bits as a single value Σ_k : this can only assume 0 or 1 as its value
- As the key is fixed, all the key bits have (at most) the net effect of flipping the sign of the relation bias which is thus $\pm\frac{1}{32}$**
- There we go :) We have a linear approximation, not dependent on the key bits, from the plaintext to the input of the fourth SBox layer!

$$U_{4,6} \oplus U_{4,8} \oplus U_{4,14} \oplus U_{4,16} \oplus P_5 \oplus P_7 \oplus P_8 = 0$$

Linear Cryptanalysis

Complete linear approximation path



Linear Cryptanalysis

Extracting the key bits for the last round

Consider a linear path along the first $r-1$ rounds of the cipher (holding with bias ϵ) which involves some ptx bits as well as some bits coming from the penultimate key-addition layer

- Call *partial subkeys* the key bits of the last round-key influenced by the output bits of our approximation
- Collect $N \geq \frac{1}{\epsilon^2}$ ptx/ctx pairs [1]
- ① Assume the partial subkey made of L bits. For each partial subkey value, $sk_i \in \{0, 1, \dots, 2^{L-1}\}$, count how many ptx/ctx pairs make the relation r hold, say N_{sk_i} , this number (Use the ctxs to feed the inverse of the S-Boxes activated on the last layer and compute $U_{4,j}$)
- ② Compute the biases $\frac{N_{sk_i}}{N} - \frac{1}{2}$ for each sk_i value
- ③ Select the partial subkey value with the highest bias

Later-rinse-repeat with other linear paths to get other partial subkeys

Linear Cryptanalysis

Summary

- ① Analyze the cipher Sboxes, computing the linear bias table
- ② Choose viable relations for an S-Box (i.e., the ones with highest bias which activates as few sboxes as possible)
- ③ Propagate the biases up to the input of the last s-box layer employing the Pile-up lemma
- ④ Collect $\geq \frac{1}{\epsilon^2}$ ptx/ctx pairs
- ⑤ Check for all the possible partial subkeys involved in the linear approximation which one best fits
- ⑥ Repeat for other *partial subkeys* until the subkey of the last round is completely derived. The entire analysis can be trivially repeated to compute also the subkeys in other rounds, re-using the same ptx/ctx pairs as before.

Further readings

Practice and real world examples

- A C implementation of the whole attack and a computer for the linear biases is available on the website
- A real world cipher known to be terribly vulnerable to linear cryptanalysis is FEAL [2]:
 - it's only 4 rounds, so you can try and crack it
- For the more determined: you can read [1] to explore the full DES linear cryptanalysis

Bibliography I



Mitsuru Matsui.

Linear cryptanalysis method for DES cipher.

In *Workshop on the theory and application of cryptographic techniques on Advances in cryptology*, EUROCRYPT '93, pages 386–397, 1994.



Mitsuru Matsui and Atsuhiro Yamagishi.

A New Method for Known Plaintext Attack of FEAL Cipher.

In Rainer A. Rueppel, editor, *Advances in Cryptology — EUROCRYPT' 92*, volume 658 of *Lecture Notes in Computer Science*, pages 81–91. Springer Berlin Heidelberg, 1993.