Few Other Cryptanalytic Techniques

Debdeep Mukhopadhyay

Assistant Professor
Department of Computer Science and Engineering
Indian Institute of Technology Kharagpur
INDIA -721302

Objectives

- **Boomerang Attack**
- **Square Attack**

Some Common Cryptanalysis Techniques

1. Linear Cryptanalysis
2. Differential Cryptanalysis
3. Differential-Linear Cryptanalysis
4. Impossible Differential Attack
5. Truncated Differential Attack
6. Higher Order Differential Attack
7. Probabilistic Higher Order Differential Attack
8. Integral Attack

Some Common Cryptanalysis Techniques

9. Boomerang Attack
10. Rectangle Attack
11. Slide Attack
12. Interpolation Attack
13. Square Attack
14. Fault Attacks/ Side Channel Attacks
15. Correlation (Statistical) Attack
16. Algebraic Attack (XL/XLS)

Recap about Differential Cryptanalysis

- We have seen in our discussion on Differential Cryptanalysis:
  - eliminating high probability differentials guarantees security.
  - if p is the upper bound on the probability of any differential for the cipher, at least 1/p texts are needed to break the cipher.
  - so to increase the security, reduce p.

The folk theorem is wrong…

- Impossible Differential Attacks: A differential with sufficiently low probability can be used for an attack.
- Boomerang attacks: Even if no differentials for the whole cipher does not have either high or low probability, may still be vulnerable to differential style attacks.

Boomerang Attack Basics

- **The attack considers four plaintexts, P, P', Q and Q'.**
- **The attacker also notes four ciphertexts, C, C', D and D'.**
- **Quartet: (P, P', Q, Q')**
- **4 queries:**
  - **2 encryption: P, P'**
  - **2 decryption: D, D'**

Boomerang Attack Basics

$E = E_1 \circ E_0$

E_0 : first half of the cipher.

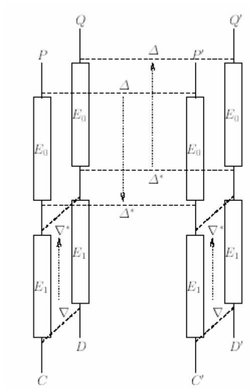
E_1 : second half of the cipher.

Differential Characteristics for the half ciphers:

$E_0 : \ \Delta \rightarrow \Delta^*$

$E_1^{-1} : \ \nabla \rightarrow \nabla^*$

Boomerang Attack Basics



$$E_0(Q) \oplus E_0(Q') = E_0(P) \oplus E_0(P') \oplus E_0(P) \oplus E_0(Q) \oplus E_0(P') \oplus E_0(Q')$$
$$= E_0(P) \oplus E_0(P') \oplus E_1^{-1}(C) \oplus E_1^{-1}(D) \oplus E_1^{-1}(C') \oplus E_1^{-1}(D')$$
$$= \Delta^* \oplus \nabla^* \oplus \nabla^* = \Delta^*.$$

Note that this characteristic is the same as that of the inverse of E_0.

Thus, the difference in the plaintexts Q and Q' is the same as that in P and P'.
Hence, the name is "Boomerang".

Example: COCONUT98

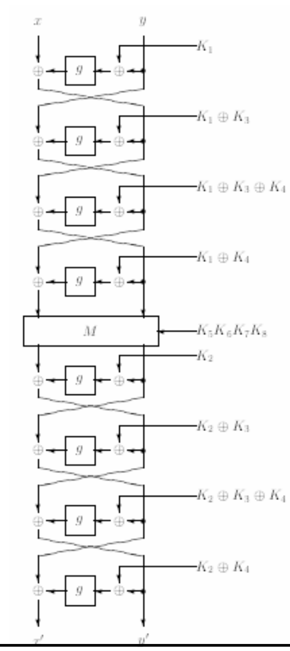
- **Designed to protect against DC.**
  - **full cipher provides no good differential characteristics.**
- **Uses a 256 bit key, $K=(k_1,k_2,\ldots,k_8)$**

i	1	2	3	4
k_i	k_1	k_1^k_3	k_1^k_3^k_4	k_1^k_4

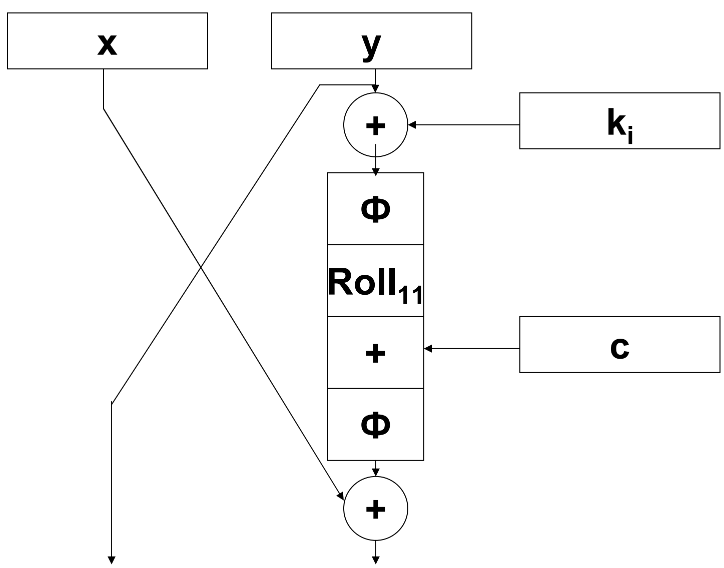
i	5	6	7	8
k_i	k_2	k_2^k_3	k_2^k_3^k_4	k_2^k_4

Coconut98 parameters

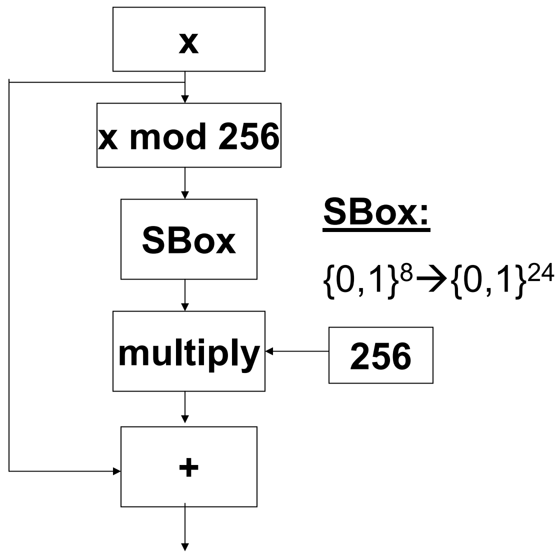
- **64 bit block cipher**
- **3 parts**
- **An M layer between 4 Feistel rounds**



Feistel Rounds of COCONUT98



The Phi Function



The M layer

$$M(xy) = (xy \oplus K_5K_6) \times K_7K_8 \bmod GF(2^{64})$$

Here, $p(x) = x^{64} + x^{11} + x^2 + x + 1$

Design is based on decorrelation theory.

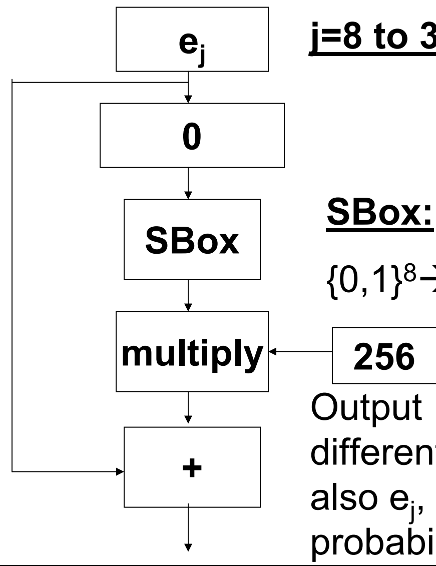
If K_7K_8 are unknown then the probability of a non-zero input differential to produce an output differential is $1/(2^{64}-1)$.

But for a fixed key, the output differential does not depend on the input value but depends only on the input differential.

Differential Analysis of the Phi Function

Consider an input differential

$=e_j$, which is a 32 bit differential with the j^{th} bit flipped.



j=8 to 31

SBox:

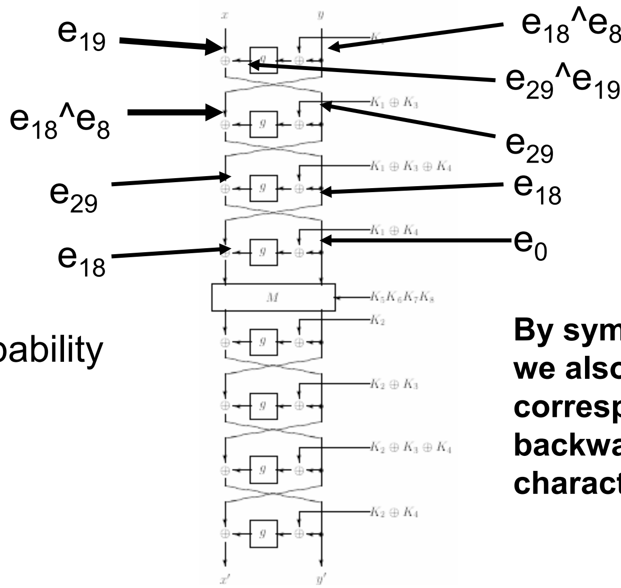
$\{0,1\}^8 \rightarrow \{0,1\}^{24}$

Output differential is also e_j, with a probability ≈½

Differential taking into account ROL_{11}

- **ROL_{11} is a circular shift by 11 bits.**
- **If the entire Feistel function is considered, there are 3 additions.**
  - **$(x+a \bmod 2^{32})+b \bmod 2^{32}$ is equivalent to $x+c \bmod 2^{32}$, where $c=a+b$**
- **Thus the output differential is e_{j+11}. The subscripts are taken modulo 32.**
- **Similarly, $e_j \wedge e_k \rightarrow e_{j+11} \wedge e_{k+11}$ with probability ≈1/4**

Good characteristics for 4 rounds



Probability

≈2^{-4}

By symmetry, we also get corresponding backward characteristics

Obtaining full round characteristics

- **Need to find some way to take advantage of these half round characteristics.**
- **The M layer creates problem for standard DC.**
- **Boomerang attack helps us to control the effect of the M layer.**
- **Key idea! M is affine. So, for a fixed key, there is an excellent characteristics with probability 1:**

$$\nabla^* \rightarrow M^{-1}(\nabla^*)$$

Success Probability

Define the complete cipher, E=$\varphi_1 \circ M \circ \varphi_0$

Here, $E_0 = \varphi_0, E_1 = \varphi_1 \circ M$

It does not matter that $M^{-1}(\nabla^*)$ is unknown to attacker. What is important is it depends only on the key and not on the values of the ciphertexts.

Define, $p_{\Delta^*} = \Pr[\Delta \xrightarrow{\varphi_0} \Delta^*],\ q_{\nabla^*} = \Pr[\nabla \xrightarrow{\varphi_1^{-1}} \nabla^*]$

Success Probability $\approx \sum_{\Delta^*} p_{\Delta^*}^2 \sum_{\nabla^*} q_{\nabla^*}^2$

Fact: If, $\Delta = \nabla = (e_{10}, e_{31})$ provides $p \approx 1/1900$.

The actual attack

- **Criteria of success: Q^Q'=(?,e_{31})**
  - **improves the probability to 1/950.**
- **Thus with about 950.4=3800 chosen plaintext/ciphertext queries, should give 1 useful quartet.**
- **Thus with 16 x 3800 queries, 16 useful quartets are expected.**

Finding k_1

- Take this quartet to find k_1.
  - guess k_1.
  - we have the fact that if (P,P',Q,Q') is a useful quartet then after round of encryption the XOR difference must be (e_{31},0) for both P,P' pair and Q,Q' pair
  - for ½ of the wrong keys this holds.
  - Each useful quartet gives 1 bit of information from P,P' pair and 1 bit information from Q,Q' pair.
  - Thus 16 useful quartets should give the entire key k_1

Obtaining other keys

- Similarly, we obtain

  k_1, k_1^k_3, k_1^k_3^k_4, k_1^k_4,

  k_2,k_2^k_3,k_2^k_3^k_4,k_2^k_4

  This helps to obtain the entire 128 bits of the key.

Complexity of the attack is around 2^{16}.

Square attacks on 4 round AES

- **Let Λ be an <u>active set of 256 states</u>, that are all different in some of the state bytes and are all equal in the other state bytes.**

$$\forall x,y \in \begin{cases} x_{i,j} \neq y_{i,j} & \text{if (i,j) active} \\ & x_{i,j} = y_{i,j} \end{cases}$$

Since the bytes of a Λ set are either constant or takes all possible values,

$$\oplus_{x \in \Lambda} x_{i,j} = 0, \forall i, j$$

Invariance of the active set

- **Consider a Λ set in which only one byte is active.**
- **Lets observe the propagation of the active set through 3 AES rounds.**
- **SubBytes, AddRound keys does not alter the property of active set.**
- **ShiftRow transposes the active byte position.**
- **The column in which there is one active byte, because of the linear transformations with invertible coeffients, there is one column with 4 active bytes.**

2^{nd} Round

- **2^{nd} round AddRoundkey and SubBytes does not alter the property of 4 active bytes.**
- **In the 2^{nd} round, shift row transposes one active byte to each column.**
- **MixColumn converts each column to have 4 active bytes.**

3^{rd} Round

- **3^{rd} round AddRoundkey and SubBytes does not alter the property of 4 active bytes per column.**
- **ShiftRow merely transposes.**

3^{rd} Round

If the input be denoted by a and the outputs by b:

$$\therefore \oplus b_{i,j} = \oplus MixColumn(a_{i,j})$$
$$= \bigoplus(02.a_{i,j} \oplus 03.a_{i+1,j} \oplus a_{i+2,j} \oplus a_{i+3,j})$$
$$= (02 \oplus a_{i,j}) \oplus (03 \oplus a_{i+1,j}) \oplus a_{i+2,j} \oplus a_{i+3,j}$$
$$= 0$$

The Attack

- **Hence all bytes at the input of the last (4^{th}) round add upto 0.**
- **Last round does not have MixColumn.**
- **So we can guess the last round key, and xor to check for the above property.**
- **Probability of success for wrong keys 1/256.**
- **Thus, with 2^8 plaintext queries the key is obtained.**

Points to ponder!

- **Can you rewrite the square attack to work for 5 rounds?**
- **Can it work for 6 rounds?**
- **Will the same attack work for AES-192 and AES-256?**

Further Reading

- **S. Vaudenay, “Provable Security for Block Ciphers”**
- **D. Wagner, “The Boomerang Attack”, FSE 99**
- **J. Daemen, V. Rijmen, The Design of Rijndael, Springer**
- **J. Daemen, L. Knudsen, V. Rijmen, “The block cipher SQUARE”**

Next Days Topic

- **Overview on S-Box Design Principles**