New Types of Cryptanalytic Attacks Using Related Keys

Eli Biham

Presented by: Nael Masalha

Outline

- Introduction
- LOKI89
- Related Keys
- Chosen Key Attack
- Chosen plaintext attack
- Summary

Introduction

- The author studies the influence of key scheduling algorithms on the strength of blockciphers.
- New types of attacks are described:
  - Chosen key chosen plaintext attack
  - Chosen key known plaintext attack
  - Chosen plaintext attack based on complementation property
- The new attacks are independent of the number of rounds of the attacked cryptosystem.
- Attacks are applicable to both variants of LOKI
- Attacks are not applicable to DES

LOKI89

- Feistel structure
- 64-bit plain/ciphertext and key length
- 16 rounds
- Similar to DES with replaced *F* function
- Replaced initial and final permutations
- Replaced key scheduling algorithm
- Key scheduling algorithm takes 64-bit key
- Defines its left half as K_1 and its right half as K_2
- Each other subkey $K_i = ROL12(K_j), j = i-2$
- Subkeys of odd rounds share the same bits
- Subkeys of even rounds share the same bits

Related keys

- Algorithms of extracting the subkeys of the various rounds are the same.
- Given a key we can shift all the subkeys one round backwards
- A new set of valid subkeys is received.
- Define new key from the new subkeys
- We call these keys *related keys*.

Chosen key attacks

- Two related keys with certain relationship are used and several plaintexts are encrypted under each of them.
- The attacker knows only the relationship between the keys but not the keys themselves.
- Two attacks:
  - Chosen plaintext attack with 2^{17} chosen plaintexts.
  - Know plaintext attack with 2^{33} know plaintexts.

Chosen key attacks

- Given the key $K = (K_L , K_R)$
- Fix two subkeys K_2 and K_3
- Define $K^* = (K_2 , K_3) = (K_R , ROL12(K_L))$
- If the data before the second round in an encryption under the key K equals the data before the first round in an encryption under the key K^*, then the data and the inputs of the F functions are the same in both executions shifted by one round.
- $P^* = (P_R, P_L \oplus K_L \oplus ROL12(K_L) \oplus F(P_R \oplus K_R \oplus K_L))$
- $C^* = (C_R \oplus K_L \oplus ROL12(K_L) \oplus F(C_L \oplus K_R \oplus K_L), C_L)$

Chosen key attacks

- Chosen key chosen plaintext attack based on this property chooses two groups, each one with size 2^{16}, plaintexts.
- $P_0,\ldots,P_{65535}$: whose right halves equal P_R and 32-bit left halves randomly chosen.
- $P^*_0,\ldots,P^*_{65535}$: whose left halves equal P_R and 32-bit right halves randomly chosen.

Chosen key attacks

- Two unknown related keys are used to encrypt these two groups.
- A key K is used to encrypt the first 2^{16} plaintexts.
- A key $K^*=(K_R,ROL12(K_L))$ is used to encrypt the other 2^{16} plaintexts.

Chosen key attacks

- In every pair of plaintexts P_i and P^*_j we are guaranteed that $P^*_{jL} = P_{iR}$.
- By the birthday paradox with a high probability there exists two plaintexts P_i and P^*_j such that

$$P_{jR}{}^* = P_{iL} \oplus K_L \oplus ROL12(K_L) \oplus F(P_{iR} \oplus K_R \oplus K_L)$$

- It is easy to identify this pair, if it exists, by checking whether $C^*_R = C_L$. This test has a probability of 2^{-32} to pass accidentally.

Chosen key attacks

- Such a pair reveals the value of

$$F(P_R \oplus K_R \oplus K_L) \oplus F(C_L \oplus K_R \oplus K_L) = {P_R}^* \oplus P_L \oplus {C_L}^* \oplus C_R$$

in which the only unknown value is $K_L \oplus K_R$

Chosen key attacks

- Chosen key know plaintext attack uses 2^{32} plaintexts P_i encrypted under an unknown key K, and 2^{32} known plaintexts P^*_j encrypted under related key $K^*=(K_R,ROL12(K_L))$.
- By the birthday paradox there is a high probability to have a pair in which the property holds.
- It is easy to identify this pair by the 2^{32} common bits of the plaintexts and 2^{32} common bits of the ciphertexts.

Chosen plaintext attacks

- A chosen plaintext attack reduces the complexity of exhaustive search using related keys.
- This attack is combined with the attacks based on complementation properties.
- In this attack the encryption is done using one key.

Chosen plaintext attacks

- LOKI89 key complementation property causes any key to have 15 equivalent keys which encrypt the plaintext to the same ciphertext.
- The 15 keys are the original key XORed with the 15 possible 64-bit hexadecimal numbers whose digits are identical.
- Known plaintext attack can be carried out with a complexity of 2^{60}.

Chosen plaintext attacks

- Another complementation property of LOKI89 is due the observation that XORing the key with an hexadecimal value $gggggggghhhhhhhh_x$ and XORing the plaintext by $iiiiiiiiiiiiiiii_x$ where $g \in \{0_x, \dots, F_x\}$, $\mathrm{h} \in \{0_x, \dots, F_x\}$ and $\mathrm{i} = \mathrm{g} \oplus h$ results in XORing the ciphertext by $iiiiiiiiiiiiiiii_x$
- For each key, there is one equivalent key whose four most bits are zero, and one complement key whose four most significant bits of its both halves are zero.
- This property reduces the complexity of a chosen plaintext attack by a further factor 16 to 2^{56}.

Chosen plaintext attacks

- Choose any plaintext P_0, and calculate the 15 plaintexts P_i, $\mathrm{i} \in \{0_x, \ldots, F_x\}$, by $P_i = P_0 \oplus iiiiiiiiiiiiiiii_x$.
- Given the 16 ciphertexts $\{C_i\}$, under an unknown key K, try all the 2^{56} keys K' in which eight bits are zero: the four most significant bits of both halves.
- Encrypt P_0 by each trial K'.
- If the result equals one of the values $C_i \oplus iiiiiiiiiiiiiiii_x$, the original key is likely to be either $K = K' \oplus 00000000iiiiiiii_x$ or any one of its 15 equivalent keys.

Chosen plaintext attacks

- The *next* operation takes 32-bit value, rotates it 12 bits to the left(ROL12) and XORs it with an 32-bit hexadecimal number whose all digits are equal, such that the four most significant bits of result are zero.
- Prepare a list of about 2^{27} half-keys$\{L_i\}$, with the properties:
  - Four most significant bits are zero
  - The list contains one value from any pair L_i and L_j for which $L_i = next(L_j)$
  - The list is minimal

Chosen plaintext attacks

Cycle Size	Number of Cycles	Number of elements in the Cycle
1	16	16
2	120	240
4	16,320	65,280
8	33,546,240	268,369,920

Chosen plaintext attacks

- Choose any plaintext P_0
- calculate the 15 plaintexts P_i, $\mathrm{i} \in \{0_x, \dots, F_x\}$, by $P_i = P_0 \oplus iiiiiiiiiiiiiiii_x$.
- For each P_i, choose 2^{32} $P_{i,k} = (P_{iR}, P_{iL} \oplus k)$
- Given the ciphertexts $\{C_i\}$, $\{C_{i,k}\}$, try all 2^{55} keys K' of the forms: $K' = (L_i, L_j)$ and $K' = (ROL12(L_i), ROR12(L_j))$
- Encrypt P_0 by each trial K' into C'.
- If the result equals one of the values $C_i \oplus iiiiiiiiiiiiiiii_x$, the original key is likely to be either $K = K' \oplus 00000000iiiiiii_x$ or any one of its 15 equivalent keys.
- If C'_L equals one of the values $C_{i,kR} \oplus iiiiiiii_x$, continue encryption of P_0 with 17th round, and if the result C'' equals $C_{i,k} \oplus iiiiiiiiiiiiiiii_x$, then the original key is likely K = $(K'_R, ROL12(K'_L))$

Chosen plaintext attacks

- The complexity of this attack is twice 2^{54}, i.e. 2^{55}.
- Optimized attack has complexity 1.5 times 2^{54}

Thank You