Slide Attacks

FSE 1999

Alex Biryukov David Wagner

Nadav Greenberg

Lecturer: DR. Orr Dunkelman

First Things First…

- Biryukov and Wagner wrote the paper in 1999. I think it is noteworthy to assume that some of the ciphers that are still in use have been modified and improved. The paper itself offers up some possible cryptanalytic solutions.

Abstract

- There is a general belief that even a relatively weak cipher may become strong if its number of rounds is made large.
- Slide attack is a new generic known/chosen plaintext attack on product ciphers.
- In many cases the attack is independent of the number of rounds in the cipher.
- The paper illustrates the power of the slide attack tool by giving practical attacks on several ciphers (TREYFER, a variants of DES).

Introduction

- Fast block ciphers tend to use more and more rounds, as computer speed improves.
- Known cryptanalytic techniques are being rendered useless.
- Differential and Linear analysis (Statistic attacks which excel in pushing statistical irregularities and biases through many rounds of ciphers), are finally reaching a limit.
- This is due to the fact that each additional round requires an exponential effort.

Introduction

AES contest

- Speed was one of the main criteria. Few of the leading algorithms (and not the slow ones had high number of rounds)
- CAST[48], MARS [32], SERPENT[32], RC6[20]

- The "winner" – Rijndael [10,12,14]

Introduction

- This reflects the widespread belief that after a high number of rounds even “weak” ciphers become very strong. E.g. Double-DES [32] and triple-DES [48].
- Therefore, it is very important to create new tools which are independent of the number of rounds.

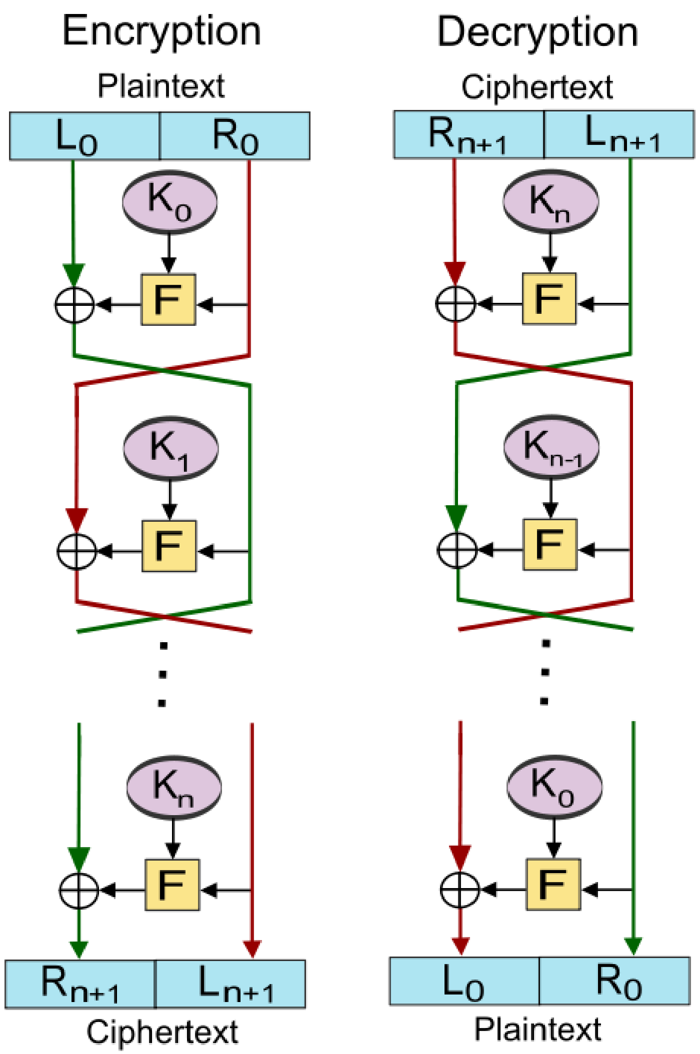
Introduction

History

- Grossman & Tuckerman (1978) showed how to break a weakened Feistel cipher[1] by a chosen plaintext attack independent of number of rounds.

[1] An 8 round Feistel cipher with 8 bits of key material per round used to swap between two s-boxes (S_0 & S_1) in a Lucifer-like manner.

Introduction - Feistel Cipher diagram



(http://upload.wikimedia.org/wikipedia/commons/thumb/f/fa/Feistel_cipher_diagram_en.svg/511px-Feistel_cipher_diagram_en.svg.png)

Introduction - Slide Attacks

- New Class of Generic Attack which together with new cryptanalytic tools are applicable to any iterative or recursive process over the finite domain.

- These attacks can start functioning when the iterative processes shows a certain measure of property independent repetition of cipher rounds.

- Are called '*self-related key attacks*' because they are essentially a **special case** of *'related key-attacks*'. Though these attacks require a known/chosen plaintext assumption and are more practical than most '*related key-attacks*'.

Introduction

Comparison

Slide attacks	Generic (Differential or Linear)
Range from exploiting key scheduling weaknesses to exploiting more general cipher structure properties (dependent on cipher design) **Prevention**: The easiest way to prevent this attack is to destroy the self-similarity of the iterative process. (*By using **iterative counters** or **fixed random constants**).* * More sophisticated versions are harder to analyze and defend against.	Concentrate mainly on propagation properties of the encryption engine. (Assuming a strong key-scheduling to produce independent subkeys). **Prevention**: Add more rounds to the iterative process.

Introduction

The process

- Usually arises when the key-schedule produces a periodic subkey sequence, when $F_i=F_j$ for all $i \equiv j \bmod p$.[2]
- Begins by analyzing several *homogenous ciphers* [3].
- *Simplest case: p=1 leads to all round subkeys being the same.*

[2] P represents the period.

[3] Block ciphers that decompose into r iterations of a single key-dependent permutation F_i.

Introduction

Complexity

- The complexity in n-bit block block-ciphers, is usually close to $O(2^{n/2})$ known-plaintexts.

- For **Feistel ciphers** where the round function F_j modifies only half of the block, there is also a chosen-plaintext variant which can often cut the complexity down to $O(2^{n/4})$.

- Schemes relying on key-dependent S-boxes are also vulnerable to slide attacks. Also in general autokey ciphers and data dependent transformations are potentially vulnerable to such attacks

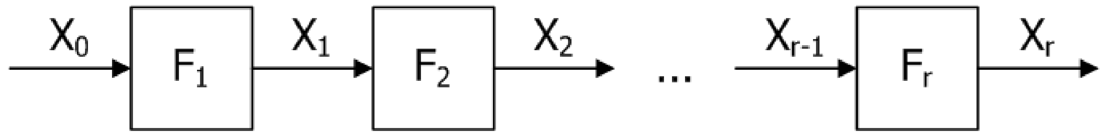
Introduction

Complexity (continues)

cipher	# Rounds	Key Bits	Data Complexity	Time Complexity
Blowfish Modified Variant without round subkeys	16	448	2^{27} Chosen-Plaintext	2^{27}
Treyfer	32	64	2^{32} Known-Plaintext	2^{44}
2K-DES	64	96	2^{33} Adaptive Chosen-plaintext	2^{33}
2K-DES	64	96	2^{32} Known-Plaintext	2^{50}
WAKE-ROFB	k	32n	2^{32} Chosen-resynchronization (IV)	2^{32}

A typical Slide Attack

- Typical Block Cipher:



- Process of encrypting the n-bit plaintext X_0 under a typical product cipher to obtain the ciphertext X_r.

- X_j – intermediate value of the block after j rounds of encryption.
- $X_j = F_j (x_j -1, k_j)$

A typical Slide Attack

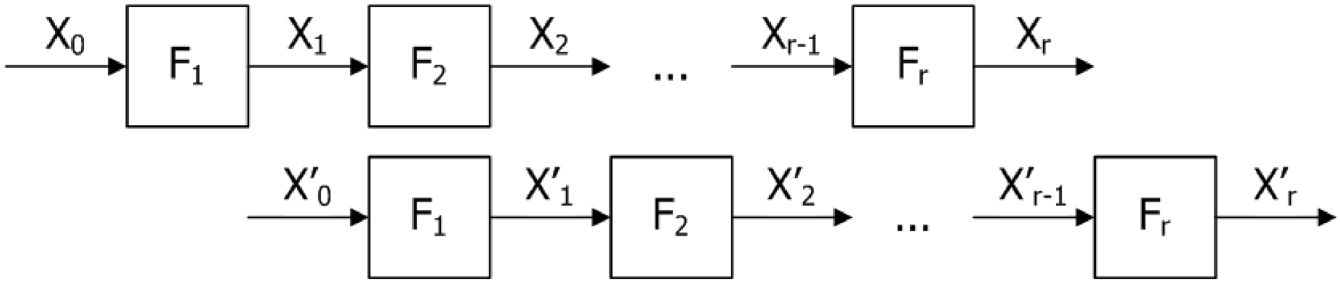
- The attack presented is ***independent of the number of rounds of the cipher.*** It views the cipher as a product of identical permutations $F(x,k)$ [4], where k is a fixed secret key.
- The only requirement on F is that it be very weak against known-plaintext attack with two plaintext-ciphertext pairs.
- F is a weak permutation if given the two equations $F(x_1,k)= y_1$ and $F(x_2,k)= y_2$ it is 'easy' [5] to extract the key k.

[4] F might include more than one round of the cipher.

[5] The amount of *easiness* may vary between different ciphers.

A typical Slide Attack

- The idea is to slide one copy of the encryption process, so that the two processes are one round out of phase.



A typical Slide Attack

Definitions

- We suppose that $F_j=F_{j+1}$ for all $j\geq 1$ [6], meaning that all round functions are the same.
- This leads us to - if $X_1=X'_0$, then $X_r=X'_{r-1}$ *(Proof by induction).*

- "**Slid Pair**" is a pair of known plaintexts and their corresponding ciphertexts (P,C) & (P',C'), where F(P)=P' and F(C)=C'.

[6] This assumption is required to make the Slide-Attack work.

A typical Slide Attack

The attack:

- We obtain $2^{n/2}$ known texts (P_i,C_i) and seek a Slid Pair.
- According to the Birthday Paradox, around one Slid Pair is expected to be found.
- Recognizing a Slid Pair - check whether it is possible that $F(P_i)=P_{i'}$ and $F(C_i)=C_{i'}$ both hold the same key.

- When the pair is found it is expected to be able to recover some bits of the cipher key[7] (The rest of the bits will be recovered in other methods such as *exhaustive search* or by obtaining a few more Slid Pairs).

[7] About n bits of key material when the key length is longer than n.

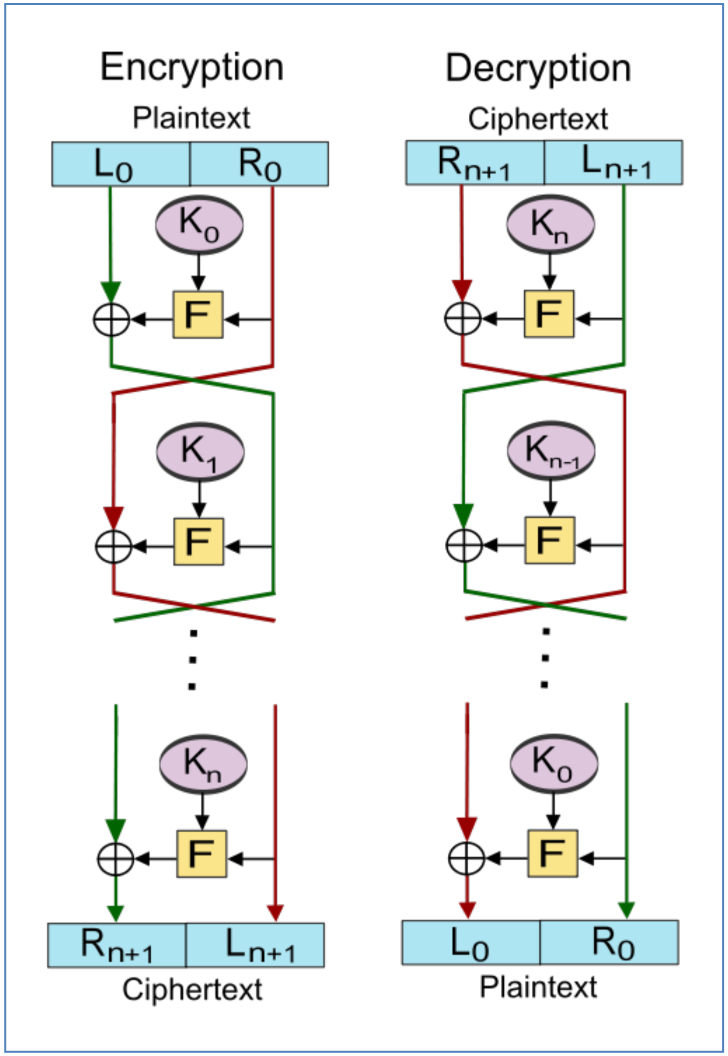
A typical Slide Attack

- When the round function is weak it is easy to find the match pair and recover the entire key.

- For n-bit block cipher with repeating round subkey, all it needs is about $O(2^{n/2})$ known plaintext to recover unknown key, while the native approach requires $O(2^n)$ work.

Feistel ciphers

- The round function of Feistel Cipher is: $F((l,r))=(r \oplus f(l),l)$
- Only half of the input is modified in each round.



(http://upload.wikimedia.org/wikipedia/commons/thumb/f/fa/Feistel_cipher_diagram_en.svg/511px-Feistel_cipher_diagram_en.svg.png)

Feistel ciphers

<u>The Known-Plaintext Attacks</u>:

- F(x)=x’ is recognized by comparing the *left* side of x with the *right* side of x’.
- This leave $2^{n/2}$ known texts and $2^{n/2}$ offline work.
- The offline work - seeks potential Slid Pairs using a lookup table with $2^{n/2}$ entries sorted based on the *left* halves of the plaintext.
- Expectations: To find a Slid Pair with *only* ***one*** false alarm *(which can be detected in the second phase)*.
- The Slid pair gives about n bits of information about the key. More pairs can be sought after if necessary (in case not all the key material was revealed).

Feistel ciphers

The Chosen-Plaintext Attacks:

- When chosen-plaintext queries are available, data complexity can be reduced to about $2^{n/4}$ texts by using carefully chosen structures.[8]

[8] E. Biham, *New Types of Cryotanalytic Attacks Using Related Keys*, J. of Cryptology, Vol.7, pp.229-246, 1994.

Feistel ciphers

The Chosen-Plaintext Attacks (continues):

- First we select an n/2-bit value for the left side input and build a pool of $2^{n/4}$ plaintexts. We do so by selecting $2^{n/4}$ random n/2-bit values for the right side input.
- Another pool of $2^{n/4}$ plaintexts is built by using the value from the left side input as the right side output and selecting $2^{n/4}$ random n/2-bit values for the left side output.
- This gives us $2^{n/2}$ plaintext pairs, with the probability of $2^{-n/2}$ and so it is expected to find a Slid Pair.

- When dealing with an unbalanced Feistel cipher (i.e. *Skipjack cipher*) the effect of a chosen plaintext attack can be greater.

Feistel ciphers

The Probable-Plaintext Attacks:

- The complexity of known plaintext slide attacks can be reduced when the plaintext contains some redundancy.

- The exact complexity of the probable-plaintext and ciphertext-only slide attacks can vary widely: some plaintext distributions increase the complexity of slide attacks, while others reduce the complexity substantially.

- The exact details of the attack will depend intimately on the distribution of the plaintexts.

An introductory Example 2K-DES

- Using DES (16 rounds with 56-bit key) build 2K-DES with 64 rounds and 2 keys (K_1 , K_2) of 48-bits (96-bit key altogether).
- K_1 used in *odd* rounds and K_2 in the *even* ones, and are used instead of DES subkeys.

- This cipher is immune to exhaustive search and probably the conventional differential and linear attacks will also fail due to its increased number of rounds.

2K-DES

Attacks on this cipher:

- For any known plaintext-ciphertext pair (P,C), “decrypt” the ciphertext C one round under all possible 2^{32} outputs from the last round *f* function[9].
- For each 2^{32} resulting texts C’ ,request the decryption P’ (that is one round over P, meaning $P' = F^{-1}(P, K_2)$).
- Since F preserves 32 bits of the input, almost all the wrong guesses of C’ can be removed.
- For all remaining (P’,C’), K_2 can be derived from the equations $F(P', K_2) = P$ and $F(C', K_2) = C$.

[9] DES is based on Horst Feistel's Lucifer cipher

2K-DES

- To find K_1 we can use exhaustive search or even better to repeat the attack by “sliding” to the other side using the known K_2 that was found.

- This attack uses one known plaintext (P,C) pair, 2^{33} adaptive chosen plaintexts and 2^{33} time.

Treyfer

Descripion:

- TREYFER[10] is a 64-bit block-cipher / MAC[11] with 64-bit key designed for smart-card applications.
- It has very compact design (only 29 byte of code) and 32 rounds.
- Algorithm:

```
for (r=0; r < NumOfRounds; r++)
{
    text[8] = text[0];

    for (i=0; i < 8; i++)
        text[i+1] = (text[i+1] + Sbox[(key[i] + text[i]) % 256]) <<< 1;
        /* Rotate 1 Left */

    text[0] = text[8];
}
```

[10] Designed by Gideon Yuval.

[11] Message Authentication Code.

Treyfer

The Attack:

- To make the cipher compact and fast, the designers simply used its 64-bit key “byte by byte” every time, making a 32 identical permutations.
- The native approach was to try all 2^{63} pairs to check if F(P,K)=P’ and F(C,K)=C’ suggest the same 64-bit key and since this check is $2/32=1/16=2^{-4}$, the overall complexity is 2^{59}.

Treyfer

- Better approach is with 2^{32} known plaintexts, 2^{44} time (offline) and 2^{32} memory.
- We guess the 2 subkeys k[0] and k[7] with $2^8 x 2^8 = 2^{16}$. For each guess we use the 2^{32} known plaintext. That leaves us with $2^{16} x 2^{32} x 2^{-4} = 2^{44}$.