The Improbable Differential Attack: Cryptanalysis of Reduced Round CLEFIA

Cihangir TEZCAN

École Polytechnique Fédérale de Lausanne, Switzerland

(This work was done at)
Institute of Applied Mathematics
Middle East Technical University, Ankara, Turkey

INDOCRYPT 2010
December 14, 2010, Hyderabad, India

Outline

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β

A (Very) Short Introduction to Differential Cryptanalysis

- Differential Cryptanalysis
  - Discovered by E. Biham and A. Shamir, early 1980s
  - Find a path (characteristic) so that when the input difference is α, output difference is β with high probability
- Truncated Differential Cryptanalysis
  - Discovered by L. Knudsen, 1994
  - Find a path (differential) so that when the input difference is α, output difference is β with high probability
  - Only parts of the differences α and β are specified
- Impossible Differential Cryptanalysis
  - Discovered by E. Biham, A. Biryukov, A. Shamir, 1998
  - Find a path (impossible differential) so that when the input difference is α, the output difference is never β
- And others (Higher-order Differential, Boomerang,...)

A (Very) Short Introduction to Differential Cryptanalysis

- Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

A (Very) Short Introduction to Differential Cryptanalysis

- Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$

A (Very) Short Introduction to Differential Cryptanalysis

- Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$
Impossible Differential	p	0	$p_0 = 0$

A (Very) Short Introduction to Differential Cryptanalysis

- Statistical attacks on block ciphers make use of a property of the cipher so that an incident (characteristic, differential,...) occurs with different probabilities depending on whether the correct key is used or not.

Attack Type	Probability of the incident for a wrong key	probability of the incident for the correct key	Note
Statistical Attacks (Differential, Truncated,...)	p	p_0	$p_0 > p$
Impossible Differential	p	0	$p_0 = 0$
Improbable Differential	p	p_0	$p_0 < p$

Improbable Differentials

- Assume that α and β differences are observed with probability p for a random key.

Improbable Differentials

- Assume that α and β differences are observed with probability p for a random key.
- Obtain a nontrivial differential so that a pair having α input difference have β' output difference with probability p' where β' is different than β.

Improbable Differentials

- Assume that α and β differences are observed with probability p for a random key.
- Obtain a nontrivial differential so that a pair having α input difference have β' output difference with probability p' where β' is different than β.
- Hence for the correct key, probability of observing these differences becomes $p_0 = p \cdot (1 - p')$.

Improbable Differentials

- Assume that α and β differences are observed with probability p for a random key.
- Obtain a nontrivial differential so that a pair having α input difference have β' output difference with probability p' where β' is different than β.
- Hence for the correct key, probability of observing these differences becomes $p_0 = p \cdot (1 - p')$.

Caution

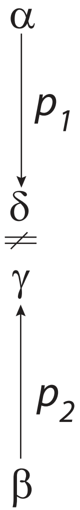
If there are nontrivial differentials from α to β, p_0 becomes bigger than $p \cdot (1 - p')$.

Two Techniques to Obtain Improbable Differentials

Two methods to obtain improbable differentials:

1. Use two differentials that miss in the middle with high probability (almost miss in the middle technique)
2. Expand impossible differentials to improbable diffrentials by adding a differential to the top and/or below the impossible differential (expansion technique)

Almost Miss-in-the-Middle Technique



$$p' = p_1 \cdot p_2$$

Improbable Differentials

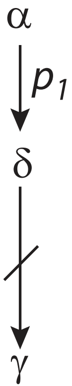
Two methods to obtain improbable differentials:

1. Use two differentials that miss in the middle with high probability (almost miss in the middle technique)
2. Expand impossible differentials to improbable diffrentials by adding a differential to the top and/or below the impossible differential (expansion technique)

Improbable Differentials from Impossible Differentials

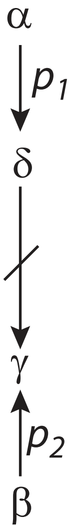
$p' = 1$

Improbable Differentials from Impossible Differentials



$p' = p_1$

Improbable Differentials from Impossible Differentials



$$p' = p_1 \cdot p_2$$

Pros and Cons of the Expansion Method

Pros:

- Longer differentials
- Attack on more rounds

Cons:

- Data complexity increases (because p_0 increases)
- Time complexity increases (since we use more data)
- Memory complexity increases (we need to keep counters for the guessed keys)

Pros and Cons of the Expansion Method

Pros:

- Longer differentials
- Attack on more rounds

Cons:

- Data complexity increases (because p_0 increases)
- Time complexity increases (since we use more data)
- Memory complexity increases (we need to keep counters for the guessed keys)

Data Complexity and Success Probability

Blondeau et al. proposed acurate estimates of the data complexity and success probability for many statistical attacks including differential and truncated differential attacks.

Making appropriate changes, these estimates can be used for improbable differential attacks, too.

Data Complexity and Success Probability

Blondeau et al. proposed acurate estimates of the data complexity and success probability for many statistical attacks including differential and truncated differential attacks.

Making appropriate changes, these estimates can be used for improbable differential attacks, too.

Previous attacks where $p_0 < p$

Early examples of improbable differential attack:

- J. Borst, L. Knudsen, V. Rijmen: "Two Attacks on Reduced IDEA"
- L. Knudsen, V. Rijmen: "On the Decorrelated Fast Cipher (DFC) and Its Theory"

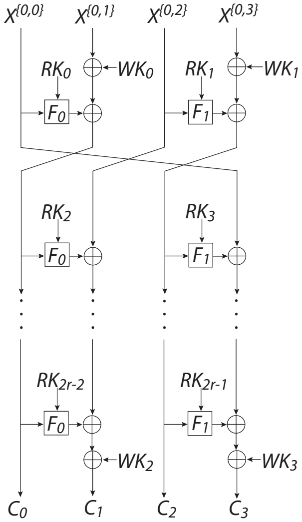
CLEFIA

- Developed by Sony in 2007
- *Clef* means *key* in French.
- Block length: 128 bits
- Key lengths: 128, 192, and 256 bits
- Number of rounds: 18, 22, or 26
- Previous best attacks: Impossible differential attacks on 12, 13, 14 rounds for 128, 196, 256-bit key lengths by Tsunoo et al.
- We converted these attacks to improbable differential attacks using the expansion technique
- Current best attacks: Improbable differential attacks on 13, 14, 15 rounds for 128, 196, 256-bit key lengths

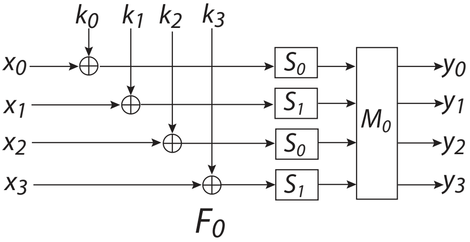
CLEFIA

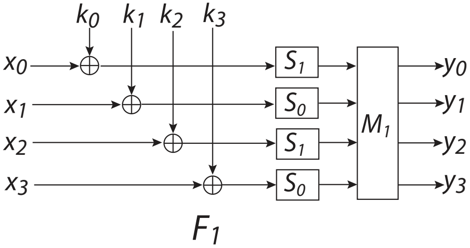
- Developed by Sony in 2007
- *Clef* means *key* in French.
- Block length: 128 bits
- Key lengths: 128, 192, and 256 bits
- Number of rounds: 18, 22, or 26
- Previous best attacks: Impossible differential attacks on 12, 13, 14 rounds for 128, 196, 256-bit key lengths by Tsunoo et al.
- We converted these attacks to improbable differential attacks using the expansion technique
- Current best attacks: Improbable differential attacks on 13, 14, 15 rounds for 128, 196, 256-bit key lengths

CLEFIA: Encryption Function



CLEFIA: F_0 and F_1 Functions





10-round Improbable Differential

We will use the following two 9-round impossible differentials that are introduced by Tsunoo et al.,

$$[0_{(32)}, 0_{(32)}, 0_{(32)}, [X, 0, 0, 0]_{(32)}] \nrightarrow_{9r} [0_{(32)}, 0_{(32)}, 0_{(32)}, [0, Y, 0, 0]_{(32)}]$$
$$[0_{(32)}, 0_{(32)}, 0_{(32)}, [0, 0, X, 0]_{(32)}] \nrightarrow_{9r} [0_{(32)}, 0_{(32)}, 0_{(32)}, [0, Y, 0, 0]_{(32)}]$$

where $X_{(8)}$ and $Y_{(8)}$ are non-zero differences.

10-round Improbable Differential

We obtain 10-round improbable differentials by adding the following one-round differentials to the top of these 9-round impossible differentials,

$$[[\psi,0,0,0]_{(32)},\zeta_{(32)},0_{(32)},0_{(32)}] \rightarrow_{1r} [0_{(32)},0_{(32)},0_{(32)},[\psi,0,0,0]_{(32)}]$$
$$[[0,0,\psi,0]_{(32)},\zeta'_{(32)},0_{(32)},0_{(32)}] \rightarrow_{1r} [0_{(32)},0_{(32)},0_{(32)},[0,0,\psi,0]_{(32)}]$$

which hold when the output difference of the F_0 function is ζ (resp. ζ') when the input difference is $[\psi,0,0,0]$ (resp. $[0,0,\psi,0]$).

13-round Improbable Differential Attack

We choose ψ and corresponding ζ and ζ' depending on the difference distribution table (DDT) of S_0 in order to increase the probability of the differential. In this way we get $p' \approx 2^{-5.87}$.

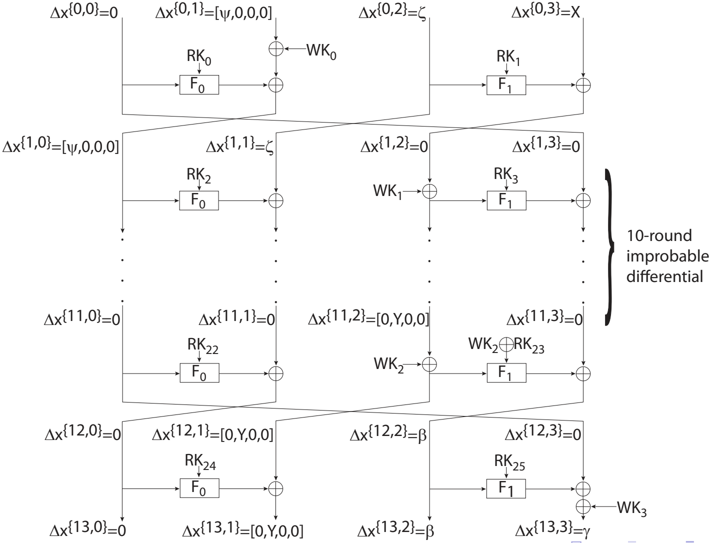
We put one additional round on the plaintext side and two additional rounds on the ciphertext side of the 10-round improbable differentials to attack first 13 rounds of CLEFIA that captures RK_1, $RK_{23,1} \oplus WK_{2,1}$, RK_{24}, and RK_{25}.

13-round Improbable Differential Attack

We choose ψ and corresponding ζ and ζ' depending on the difference distribution table (DDT) of S_0 in order to increase the probability of the differential. In this way we get $p' \approx 2^{-5.87}$.

We put one additional round on the plaintext side and two additional rounds on the ciphertext side of the 10-round improbable differentials to attack first 13 rounds of CLEFIA that captures RK_1, $RK_{23,1} \oplus WK_{2,1}$, RK_{24}, and RK_{25}.

13-round Improbable Differential Attack



13-round Improbable Differential Attack

Table: Comparison of Tsunoo et al.'s impossible attack with the expanded improbable attack

Rounds	Attack Type	Key Length	Data Complexity	Time Complexity	Memory (blocks)	Success Probability
12	Impossible	128	$2^{118.9}$	2^{119}	2^{73}	-
13	Improbable	128	$2^{126.83}$	$2^{126.83}$	$2^{101.32}$	%99

14 and 15-round Improbable Differential Attacks

By using the similar expansion technique, we can apply improbable differential attack on

- 14-round CLEFIA when the key length is 192 bits
- 15-round CLEFIA when the key length is 256 bits

Conclusion

We provided

1. a new cryptanalytic technique called *improbable differential attack* where a differential holds with less probability when tried with the correct key
2. two techniques to obtain improbable differentials
3. data complexity estimates for improbable differential attacks
4. state of art attacks on the block cipher CLEFIA

Conclusion

THANK YOU FOR YOUR ATTENTION