An Invitation to Improbable Differential Cryptanalysis

Cihangir TEZCAN

Department of Cryptography
Institute of Applied Mathematics
Middle East Technical University

June 1, 2010

1.1. Introduction

- 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.

1.1. Introduction

- 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	$p_0 > p$

1.1. Introduction

- 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	-

1.1. Introduction

- 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	-
Improbable Differential	p	p_0	$p_0 < p$

1.2. Improbable Differentials

- Obtain a differential so that a pair having α input difference **does not** have β output difference with probability p'.

1.2. Improbable Differentials

- Obtain a differential so that a pair having α input difference **does not** have β output difference with probability p'.
- Assume that α and β differences are observed with probability p for a wrong key.

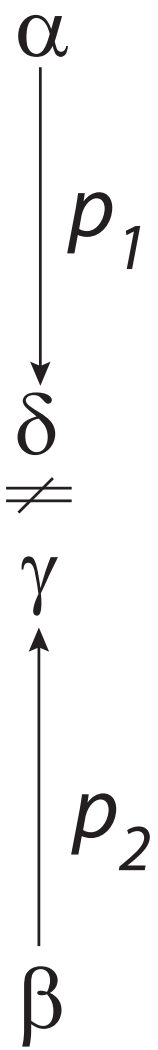
1.2. Improbable Differentials

- Obtain a differential so that a pair having α input difference **does not** have β output difference with probability p'.
- Assume that α and β differences are observed with probability p for a wrong key.
- Hence for the correct key, probability of observing these differences becomes $p_0 = p \cdot (1 - p')$.

1.2. Improbable Differentials

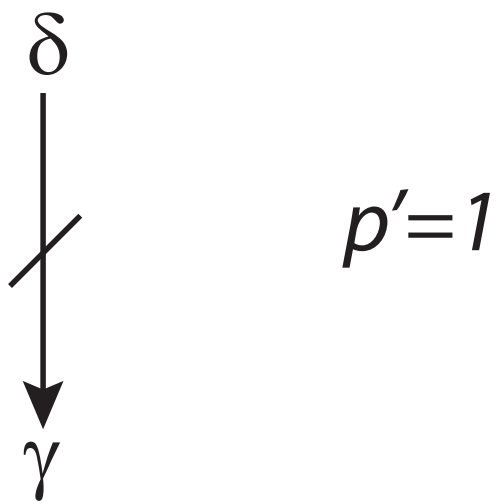
- Obtain a differential so that a pair having α input difference **does not** have β output difference with probability p'.
- Assume that α and β differences are observed with probability p for a wrong key.
- Hence for the correct key, probability of observing these differences becomes $p_0 = p \cdot (1 - p')$.

1.3. Almost Miss-in-the-Middle Technique

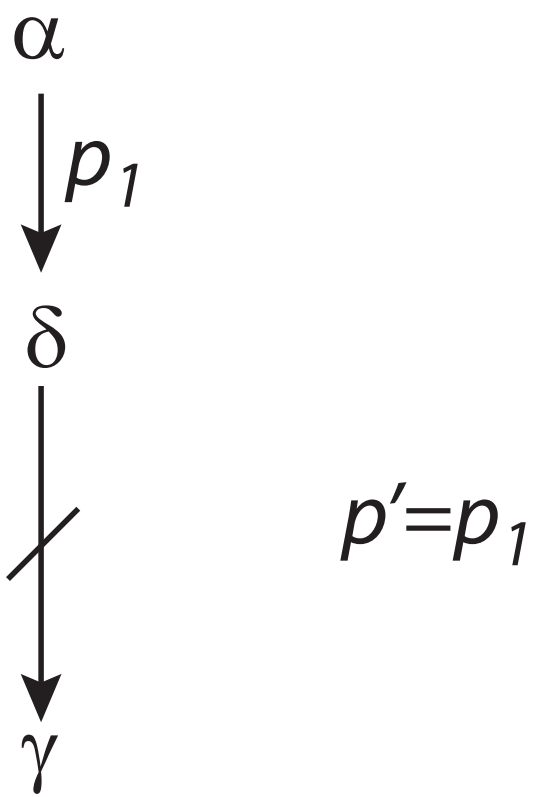


$$p' = p_1 \cdot p_2$$

1.4. Improbable Differentials from Impossible Differentials



1.4. Improbable Differentials from Impossible Differentials



1.4. Improbable Differentials from Impossible Differentials

$$p' = p_1 \cdot p_2$$

1.5. Conclusion

Dear Sir/Madam,

You are cordially invited to apply improbable differential attack to your favorite block cipher or hash function.

Sincerely yours,
Cihangir Tezcan