

A Methodology for Differential-Linear Cryptanalysis and Its Applications

Jiqiang Lu

Presenter: Jian Guo

Institute for Infocomm Research,
Agency for Science, Technology and Research,
1 Fusionopolis Way, Singapore 138632

FSE 2012

Outline

- 1 Preliminaries
- 2 Differential-Linear Cryptanalysis: Previous and Our Methodologies
- 3 Application to 13 Rounds of the DES Block Cipher
- 4 Application to 10 Rounds of the CTC2 Block Cipher
- 5 Application to 12 Rounds of the Serpent Block Cipher
- 6 Conclusions

1.1 A Cryptanalytic Attack

- Is an algorithm that **distinguishes a cryptosystem from a random function**.
- Usually measured using the following three metrics:
 - * **Data** complexity
 - * **Memory (storage)** complexity
 - * **Time (computational)** complexity
- Commonly regarded as effective if it is **faster** (i.e., it has lower time complexity) **than exhaustive key search**.
 - * An exhaustive key search would take 2^n encryption operations for an n -bit block cipher.

1.2 Differential Cryptanalysis

- Takes advantage of how a specific difference in a pair of plaintexts can affect a difference in the pair of ciphertexts.
- A differential is the combination of the input difference and the output difference.
- The probability of the differential (α, β) for an n -bit block cipher \mathbb{E} , written $\Delta\alpha \rightarrow \Delta\beta$, is

$$\Pr_{\mathbb{E}}(\Delta\alpha \rightarrow \Delta\beta) = \Pr_{P \in \{0,1\}^n}(\mathbb{E}(P) \oplus \mathbb{E}(P \oplus \alpha) = \beta).$$

- For a random function, the expected probability of any differential is 2^{-n} .

If $\Pr_{\mathbb{E}}(\Delta\alpha \rightarrow \Delta\beta)$ is larger than 2^{-n} , we can use the differential to distinguish \mathbb{E} from a random function.

1.3 Linear Cryptanalysis

- Exploits correlations between a particular linear function of the plaintexts and a second linear function of the ciphertexts.
- A linear approximation is the combination of the two linear functions.
- The probability of the linear approximation (α, β) for an n -bit block cipher \mathbb{E} , written $\Gamma\alpha \rightarrow \Gamma\beta$, is defined to be

$$\Pr_{\mathbb{E}}(\Gamma\alpha \rightarrow \Gamma\beta) = \Pr_{P \in \{0,1\}^n}(P \odot \alpha = \mathbb{E}(P) \odot \beta).$$

- For a random function, the expected probability of any linear approximation is $\frac{1}{2}$.

If the bias $\epsilon = |\Pr_{\mathbb{E}}(\Gamma\alpha \rightarrow \Gamma\beta) - \frac{1}{2}|$ is sufficiently large, we can use the linear approximation to distinguish \mathbb{E} from a random function.

1.4 A General Assumption in Practice

- It is **usually hard to get the accurate probability** of a differential (or linear approximation).
- A multi-round differential (or linear approximation) is usually constructed by concatenating a few one-round differentials (respectively, linear approximations).
- The probability of the multi-round differential (or linear approximation) is regarded as the product (respectively, the piling-up function) of the probabilities of the one-round differentials (respectively, linear approximations) under the following **Assumption (1)**:

Assumption (1)

The involved round functions behave independently.

2.1 Langford and Hellman's Methodology

- Introduced in 1994.
- A differential-linear distinguisher:
 - * Treat a block cipher \mathbb{E} as a cascade of two sub-ciphers $\mathbb{E} = \mathbb{E}_1 \circ \mathbb{E}_0$.
 - * Use a linear approximation $\Gamma\gamma \rightarrow \Gamma\delta$ with bias ϵ for \mathbb{E}_1 .
 - * Use a differential $\Delta\alpha \rightarrow \Delta\beta$ with **probability 1** for \mathbb{E}_0 , which has a **zero output difference in the bits concerned by $\Gamma\gamma$** .
- Concerned event: $\delta \odot \mathbb{E}(P) = \delta \odot \mathbb{E}(P \oplus \alpha)$, where P is a randomly chosen plaintext block.
- Probability: $\frac{1}{2} + 2\epsilon^2$ under Assumption (1) and the following **Assumption (2)**:

Assumption (2)

The two inputs for \mathbb{E}_1 , i.e., $\mathbb{E}_0(P)$ and $\mathbb{E}_0(P \oplus \alpha)$, behave as independent inputs with respect to the linear approximation.

If the bias $2\epsilon^2$ is sufficiently large, we can use the differential-linear distinguisher to distinguish \mathbb{E} from a random function.

2.2 Biham, Dunkelman and Keller's Methodology

- Introduced in 2002.
 - * A reviewer mentioned that the same methodology appeared in 1995 in Langford's PhD thesis (which seems to be not publicly accessible).
- A differential-linear distinguisher:
 - * Treat \mathbb{E} as a cascade of two sub-ciphers $\mathbb{E} = \mathbb{E}_1 \circ \mathbb{E}_0$.
 - * Use a linear approximation $\Gamma\gamma \rightarrow \Gamma\delta$ with bias ϵ for \mathbb{E}_1 .
 - * Use a differential $\Delta\alpha \rightarrow \Delta\beta$ with **probability p** for \mathbb{E}_0 , with $\beta \odot \gamma = 0$.
- Concerned event: $\delta \odot \mathbb{E}(P) = \delta \odot \mathbb{E}(P \oplus \alpha)$.
- Probability: $\frac{1}{2} + 2p\epsilon^2$ under Assumptions (1), (2) and the following **Assumption (3)**:

Assumption (3)

The output parities $\delta \odot \mathbb{E}(P)$ and $\delta \odot \mathbb{E}(P \oplus \alpha)$ have a uniform and independent distribution in $\{0, 1\}$ for the cases $\mathbb{E}_0(P) \oplus \mathbb{E}_0(P \oplus \alpha) \neq \beta$.

If the bias $2p\epsilon^2$ is sufficiently large, we can use the differential-linear distinguisher to distinguish \mathbb{E} from a random function.

2.3 Our Methodology

Works under only Assumptions (1) and (2).

- Treat an n -bit block cipher \mathbb{E} as a cascade of two sub-ciphers $\mathbb{E} = \mathbb{E}_1 \circ \mathbb{E}_0$.
- Use a linear approximation $\Gamma\gamma \rightarrow \Gamma\delta$ with bias ϵ for \mathbb{E}_1 .
- Given an input difference α for \mathbb{E}_0 , compute

$$\hat{p} = \sum_{\beta \in \{0,1\}^n, \gamma \odot \beta = 0} \Pr_{\mathbb{E}_0}(\Delta\alpha \rightarrow \Delta\beta).$$

Theorem (1)

$\Pr_{P \in \{0,1\}^n}(\mathbb{E}(P) \odot \delta = \mathbb{E}(P \oplus \alpha) \odot \delta) = \frac{1}{2} + 2(2\hat{p} - 1)\epsilon^2$ under Assumptions (1) and (2).

2.4 Implications

Our methodology:

- **More reasonable** than Biham et al.'s methodology.
 - * Requires one less assumption than Biham et al.'s methodology.
- **More general** than Biham et al.'s methodology.
 - * Holds when Biham et al.'s as well as Langford and Hellman's methodology holds.
 - * Holds in some situations where Biham et al.'s methodology does not hold.
- Can lead to some **better differential-linear cryptanalytic results** than Biham et al.'s and Langford and Hellman's methodologies.

3.1 The DES Block Cipher

- Based on the Lucifer block cipher designed by IBM.
- Published by NBS (NIST) in 1977.
- Well known to both academia and industry.
- A 64-bit block cipher with a user key of 56 bits.
- Has a Feistel structure, and a total of 16 rounds.
- Currently still being widely used in reality.

3.2 A 11-Round Differential-Linear Distinguisher

- \mathbb{E}_0 : Rounds 1–5
- \mathbb{E}_1 : Rounds 6–11
- $\Gamma\gamma \rightarrow \Gamma\delta$: $0x0000000001040080 \rightarrow 0x2104008000008000$ with bias $\epsilon = 2^{-8.04}$.
- $\alpha = 0x4000000000000000$.
- $\hat{p} = 0.500993547648294625$.

By Theorem (1), the distinguisher has a bias $2(2\hat{p} - 1)\epsilon^2 \approx 2^{-24.05}$.

3.3 Attack Outline

Attack the first thirteen rounds from Rounds 1 to 13.

- Use the 11-round distinguisher from Rounds 2 to 12.
- Obtain the ciphertexts for $2^{52.1}$ chosen plaintexts.
- Guess the required 10 subkey bits $(K_{1,1}, K_{13,1})$.
 1. Check the number of plaintext pairs meeting the criteria.
 2. Compute its deviation from $2^{50.1}$.
- For the guess of $(K_{1,1}, K_{13,1})$ with the largest deviation, exhaustively search for the remaining 46 key bits.

3.4 Attack Performance

- Requires $2^{52.1}$ chosen plaintexts and a memory of $2^{56.1}$ bytes.
- Has a time complexity of $2^{54.2}$ 13-round DES encryptions.
- Breaks **5 more rounds** than the previous differential-linear attack using Langford and Hellman's methodology.
 - * In 1994, Langford and Hellman applied their methodology to obtain a 6-round differential-linear distinguisher, and finally broke 8-round DES.
- Breaks **4 more rounds** than the previous differential-linear attack using Biham et al.'s methodology.
 - * In 2002, Biham et al. applied their methodology to obtain a 7-round differential-linear distinguisher, and finally broke 9-round DES.

4.1 The CTC2 Block Cipher

- Designed to show the strength of algebraic cryptanalysis on block ciphers by Courtois — the proposer of algebraic cryptanalysis.
- Presented in 2007.
- Has a variable block size, a variable length key, and a variable number of rounds.
- Has an substitution-permutation structure.

We consider the version that has a 255-bit block size and a 255-bit key.

4.2 A 8.5-Round Differential-Linear Distinguisher

- \mathbb{E}_0 : Rounds 1 – 3
- \mathbb{E}_1 : Rounds 4 to immediately before the permutation operation of Round 9.
- $\Gamma\gamma \rightarrow \Gamma\delta$: $e_{5,33,49,54,101,112,131,138,155,168,188,193,217,247,251} \rightarrow e_{32,151}$ with bias $\epsilon = 2^{-33}$.
- $\alpha = e_0$.
- $\hat{p} = 0.5625$.

By Theorem (1), the distinguisher has a bias $2(2\hat{p} - 1)\epsilon^2 = 2^{-68}$.

4.3 Attack Outline

Attack the first ten rounds from Rounds 1 to 10.

- Use the 8.5-round distinguisher from Rounds 2 to immediately before the permutation operation of Round 10.
- Obtain the ciphertexts for 2^{142} chosen plaintexts.
- Guess the required 48 bits of the subkey K_0 .
 1. Check the number of plaintext pairs meeting the criteria.
 2. Compute its deviation from 2^{140} .
- For the subkey guess with the largest deviation, exhaustively search for the remaining 207 key bits.

4.4 Attack Performance

- Requires 2^{142} chosen plaintexts and a memory of $2^{54.2}$ bytes.
- Has a time complexity of 2^{207} 10-round CTC2 encryptions.
- Breaks **4 more rounds** than Courtois' algebraic attack.
- Breaks **2 more rounds** than the previous differential-linear attack using Biham et al.'s methodology.
 - * In 2009, Dunkelman and Keller applied Biham et al.'s methodology to obtain a 7-round differential-linear distinguisher, and finally broke 8-round CTC2.
 - * Much worse, we find the previous attack can **not** break that many rounds, because of a flaw.

5.1 The Serpent Block Cipher

- Designed by Anderson, Biham and Knudsen in a rather conservative way.
- Published in 1998.
- One of the five AES finalists, second to the Rijndael cipher that became the AES.
- A 128-bit block cipher with a user key of 256 bits.
 - * Shorter keys can be used by appending a one and as many zeros as required.
- Has an substitution-permutation structure, and a total of 32 rounds.
- Included in the GNU project for possible use in real-world cryptographic applications.

5.2 A 9-Round Differential-Linear Distinguisher

- \mathbb{E}_0 : Rounds 2 to 4
- \mathbb{E}_1 : Rounds 5 to 10.
- $\Gamma\gamma \rightarrow \Gamma\delta$: $0x00400000000000000000000000000002 \rightarrow 0x000B0000B000030000B0200E00000010$ with bias $\epsilon = 2^{-27}$.
- $\alpha = 0x000000A0000000000000000000000000$.
- $\hat{p} = 0.4944110107421875$.

By Theorem (1), the distinguisher has a bias $2(2\hat{p} - 1)\epsilon^2 \approx 2^{-59.41}$.

5.3 Attack Outline

Attack the first twelve rounds from Rounds 0 to 11.

- Use the 9-round distinguisher from Rounds 2 to 10.
- Obtain the ciphertexts for $2^{124.5}$ chosen plaintexts.
- Guess the required 152 subkey bits used in Rounds 0, 1 and 11.
 1. Check the number of plaintext pairs meeting the criteria.
 2. Compute its deviation from $2^{123.5}$.
- For the 2^{104} subkey guesses with the relatively larger deviations, exhaustively search for the remaining 132 key bits.

5.4 Attack Performance

- Requires $2^{124.5}$ chosen plaintexts and a memory of $2^{129.5}$ bytes.
- Has a time complexity of $2^{244.9}$ 12-round Serpent encryptions.
- Breaks **the same number of rounds** as the previous differential-linear attack using Biham et al.'s methodology.
 - * In 2008, Dunkelman, Indesteege and Keller applied Biham et al.'s methodology to obtain a 9-round differential-linear distinguisher, and finally broke 12-round Serpent, following Biham et al.'s attack on 11-round Serpent.
 - * Anyway, our new result is **more reasonable**, as it works under only two assumptions.

6. Conclusions

Have given a new methodology for differential-linear cryptanalysis under only the original two assumptions.

- The new methodology is more general and reasonable than Biham et al.'s methodology.
- The new methodology can lead to some better differential-linear cryptanalytic results than Biham et al.'s and Langford and Hellman's methodologies.
- The presented attacks are theoretical, but provide a comprehensive understanding of the security of the block ciphers.
- Block cipher designers should pay attention to this new methodology when designing ciphers.

1. Preliminaries
2. Differential-Linear Cryptanalysis: Previous and Our Methodologies
3. Application to 13 Rounds of the DES Block Cipher
4. Application to 10 Rounds of the CTC2 Block Cipher
5. Application to 12 Rounds of the Serpent Block Cipher
6. Conclusions

Summary of our and previous main results

Cipher	Attack Technique	Rounds	Data	Time	Year/Author(s)
CTC2 (255-bit version)	Algebraic	6	4CP	2^{253} Enc.	2007/Courtois
	Differential	7^\dagger	2^{15} CP	2^{15} Enc.	2009/Dunkelman, Keller
	Differential-linear	8^\dagger	2^{37} CP	2^{37} Enc.	2009/Dunkelman, Keller
		10	2^{142} CP	2^{207} Enc.	2012/Lu
DES	Differential	full	$2^{47.2}$ CP	2^{37} Enc.	1992/Biham, Shamir
	Linear	full	2^{43} KP	2^{47} Enc.	1993/Matsui
	Davis's attack	full	2^{50} KP	2^{50} Enc.	1997/Biham, Biryukov
	Differential-linear	8	768CP	2^{40} Enc.	1994/Langford, Hellman
		9	$2^{15.75}$ CP	2^{38} Enc.	2002/Biham, Dunkelman, Keller
		10	$2^{29.66}$ CP	2^{44} Enc.	2012/Lu
13		$2^{52.1}$ CP	$2^{54.2}$ Enc.	2012/Lu	
Serpent	Differential	8	2^{84} CP	$2^{206.7}$ Enc.	2001/Biham, Dunkelman, Keller
	Amplified boomerang	9	2^{110} CP	2^{252} Enc.	2001/Kelsey, Kohno, Schneier
	Boomerang	10	$2^{126.3}$ ACPC	2^{165} Enc.	2002/Biham, Dunkelman, Keller
	Rectangle	10	$2^{126.3}$ CP	2^{165} Enc.	2002/Biham, Dunkelman, Keller
	Linear	11	2^{118} KP	2^{178} Enc.	2007/Collard, Standaert, Quisquater
	Differential-linear	12	$2^{123.5}$ CP	$2^{249.4}$ Enc.	2008/Dunkelman, Indesteege, Keller
		$2^{124.5}$ CP	$2^{244.9}$ Enc.	2012/Lu	

CP: Chosen Plaintexts, KP: Known Plaintexts, ACPC: Adaptively Chosen Plaintexts and Ciphertexts, Enc.: Encryptions, †: There is a flaw.

Thank you!

Questions or Comments are welcome, please contact Jiqiang Lu via
lvjiqiang@hotmail.com